ICLE | RESTRICTIVE COVENANTS AND TRADE SECRETS IN GEORGIA

PROGRAM MATERIALS

JANUARY 10, 2019

Thursday, January 10, 2019 **ICLE: State Bar Series**

RESTRICTIVE COVENANTS AND TRADE SECRETS IN GEORGIA

6 CLE Hours, Including
2 Ethics Hours | 4 Trial Practice Hours

Sponsored By: **Institute of Continuing Legal Education**

The Institute of Continuing Legal Education's publications are intended to provide current and accurate information on designated subject matter. They are offered as an aid to practicing attorneys to help them maintain professional competence with the understanding that the publisher is not rendering legal, accounting, or other professional advice. Attorneys should not rely solely on ICLE publications. Attorneys should research original and current sources of authority and take any other measures that are necessary and appropriate to ensure that they are in compliance with the pertinent rules of professional conduct for their jurisdiction.

ICLE gratefully acknowledges the efforts of the faculty in the preparation of this publication and the presentation of information on their designated subjects at the seminar. The opinions expressed by the faculty in their papers and presentations are their own and do not necessarily reflect the opinions of the Institute of Continuing Legal Education, its officers, or employees. The faculty is not engaged in rendering legal or other professional advice and this publication is not a substitute for the advice of an attorney. This publication was created to serve the continuing legal education needs of practicing attorneys.

ICLE does not encourage non-attorneys to use or purchase this publication in lieu of hiring a competent attorney or other professional. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

Although the publisher and faculty have made every effort to ensure that the information in this book was correct at press time, the publisher and faculty do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

The Institute of Continuing Legal Education of the State Bar of Georgia is dedicated to promoting a well organized, properly planned, and adequately supported program of continuing legal education by which members of the legal profession are afforded a means of enhancing their skills and keeping abreast of developments in the law, and engaging in the study and research of the law, so as to fulfill their responsibilities to the legal profession, the courts and the public.

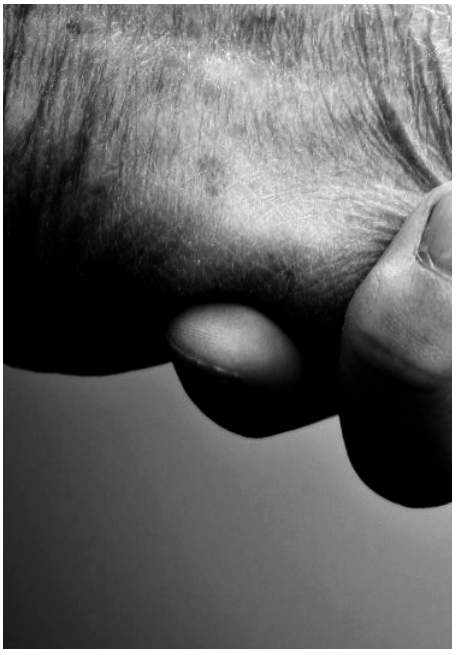
Printed By:

State Bar of Georgia

INSTITUTE OF CONTINUING LEGAL EDUCATION

SOLACE
Support of Lawyers, All Concern Encouraged

HOW CAN WE HELP YOU?



Who are we?

SOLACE is a program of the State Bar of Georgia designed to assist those in the legal community who have experienced some significant, potentially life-changing event in their lives. SOLACE is voluntary, simple and straightforward. SOLACE does not solicit monetary contributions but accepts assistance or donations in kind.

How does SOLACE work?

If you or someone in the legal community is in need of help, simply email SOLACE@gabar.org. Those emails are then reviewed by the SOLACE Committee. If the need fits within the parameters of the program, an email with the pertinent information is sent to members of the State Bar.

What needs are addressed?

Needs addressed by the SOLACE program can range from unique medical conditions requiring specialized referrals to a fire loss requiring help with clothing, food or housing. Some other examples of assistance include gift cards, food, meals, a rare blood type donation, assistance with transportation in a medical crisis or building a wheelchair ramp at a residence.

Contact SOLACE@gabar.org for help.

The purpose of the SOLACE program is to allow the legal community to provide help in meaningful and compassionate ways to judges, lawyers, court personnel, paralegals, legal secretaries and their families who experience loss of life or other catastrophic illness, sickness or injury.

TESTIMONIALS

In each of the Georgia SOLACE requests made to date, Bar members have graciously stepped up and used their resources to help find solutions for those in need.

A solo practitioner's quadriplegic wife needed rehabilitation, and members of the Bar helped navigate discussions with their insurance company to obtain the rehabilitation she required.

A Louisiana lawyer was in need of a CPAP machine, but didn't have insurance or the means to purchase one. Multiple members offered to help.

A Bar member was dealing with a serious illness and in the midst of brain surgery, her mortgage company scheduled a foreclosure on her home. Several members of the Bar were able to negotiate with the mortgage company and avoided the pending foreclosure.

Working with the South Carolina Bar, a former paralegal's son was flown from Cyprus to Atlanta (and then to South Carolina) for cancer treatment. Members of the Georgia and South Carolina bars worked together to get Gabriel and his family home from their long-term mission work.

Contact SOLACE@gabar.org for help.

TABLE OF CONTENTS

AGENDA

Presiding:
Benjamin I. Fink, Program Chair; Berman Fink Van Horn PC, Atlanta, GA

THURSDAY, JANUARY 10, 2019

7:30 **REGISTRATION AND CONTINENTAL BREAKFAST**
(All attendees must check in upon arrival. A jacket or sweater is recommended.)

8:10 **WELCOME AND PROGRAM OVERVIEW**
Benjamin I. Fink

8:15 **RESTRICTIVE COVENANTS IN EMPLOYMENT AND OTHER AGREEMENTS**
Benjamin I. Fink

9:15 **TRADE SECRETS, CONFIDENTIAL INFORMATION AND COMPUTER FRAUD AND ABUSE**
Neal F. Weinrich, Berman Fink Van Horn PC, Atlanta, GA

10:15 **BREAK**

10:25 **CHOICE OF LAW, VENUE AND OTHER PROCEDURAL ISSUES IN RESTRICTIVE COVENANT LITIGATION**
John G. Perry, Womble Bond Dickinson (US) LLP, Atlanta, GA

11:25 **LITIGATION AND ADR STRATEGIES IN RESTRICTIVE COVENANT DISPUTES**
Gary S. Freed, Freed Howard LLC, Atlanta, GA
F. Beaumont "Beau" Howard, Freed Howard LLC, Atlanta, GA

12:25 **LUNCH**

12:55 **FORENSIC INVESTIGATIONS AND E-DISCOVERY IN RESTRICTIVE COVENANT LITIGATION**
Gregory L. Fordham**,** Fordham Forensics, Inc., Alpharetta, GA

1:55 **BREAK**

2:10 **MEDIATION/SETTLEMENT OF THE RESTRICTIVE COVENANT CASE . . .AN INTERACTIVE PANEL DISCUSSION**
Terrence Lee Croft, JAMS/Croft ADR, Atlanta, GA
Charles A. Hawkins, II, The Hawkins Firm LLC, Atlanta, GA
David N. Schaeffer, Miles Mediation, Atlanta, GA

3:10 **ADJOURN**

State Bar of Georgia
INSTITUTE OF CONTINUING LEGAL EDUCATION

STATE BAR SERIES

Restrictive Covenants In Employment And Other Agreements

Presented By:

Benjamin I. Fink

Non-Competition and Non-Solicitation Covenants in Employment Agreements and the Sale of a Business

Benjamin I. Fink, Esq.
Neal F. Weinrich, Esq.
Berman Fink Van Horn P.C.
www.bfvlaw.com
www.georgia-noncompete.com
January 10, 2019

I. Introduction

Restrictive covenants in employment agreements are an important tool in protecting the customers, clients, and competitive information of client businesses from being taken by an officer, agent, or employee who leaves the client's employment.

Absent an agreement containing restrictive covenants, the legal restrictions on an employee's ability to take business and information after leaving the client's employment are minimal. Subject to rights the employer may have under the Georgia Trade Secrets Act, the Georgia Computer Systems Protection Act, common law tort claims, and federal statutes prohibiting unauthorized authorized access to computer systems, a former employee owes no duty to the employer to refrain from competing or soliciting customers of the employer.

Similarly, restrictive covenants that are ancillary to the sale of a business can be a critical tool in protecting the value of the acquired business. A purchaser is not likely to acquire a business if it knows that the seller will be able to compete against the business, as this would diminish the value of the acquired business.

Likewise, restrictive covenants ancillary to professional partnership agreements, which are subjected to a lesser scrutiny than those covenants ancillary to employment agreements, can protect the owners of a professional partnership, association or corporation from having their co-owners freely compete against the business without any restriction.

Historically, Georgia courts were among the strictest in the country when it came to enforcement of restrictive covenants in employment agreements. In 1977, Justice Jordan of the Supreme Court of Georgia famously commented that "[t]en Philadelphia lawyers could not draft an employer-employee restrictive covenant agreement that would pass muster under the recent rulings of this court." Fuller v. Kolb, 238 Ga. 602, 605, 234 S.E.2d 517, 518 (1977) (Jordan, J., dissenting). That all changed with the recent passage of the restrictive covenant act (the "Act").

Although restrictive covenants require careful thought and analysis, enforceable covenants can be written if the drafter knows and understands the legal issues impacting such agreements.

A. The Act

1. The Legislative History Underlying the Act

In 2007, Representative Kevin Levitas introduced proposed legislation that would drastically change the law concerning restrictive covenants in Georgia. H.B. 667, 149th Leg., Reg. Sess. (Ga. 2007); H.B. 527, 149th Leg., Reg. Sess. (Ga. 2007). The legislation was not voted on during the 2007 or 2008 legislative sessions. However, in 2008, the House of Representatives appointed a Study Committee to analyze issues related to restrictive covenants in Georgia and to consider and recommend any action or legislation for the 2009 session that the Committee believed appropriate or necessary. H.R. 1879, 149th Leg., Reg. Sess. (Ga. 2008). The Georgia Senate appointed a similar Study Committee. The House Committee issued a report expressing a need for change to Georgia's law on restrictive covenants and offering proposed legislation to effectuate its findings and recommendations. Consistent with the Report, Representative Levitas introduced legislation during the 2009 session which would amend Chapter of 8 of Title 13. H.B. 173, 150th Leg, Reg. Sess. (Ga. 2009). This legislation was overwhelmingly passed by the Georgia House of Representatives and Senate. The bill was signed by the Governor on April 29, 2009.

Given that Georgia's hostility to restrictive covenants is based in its Constitution, before the law became effective, an amendment to the Georgia Constitution had to be approved. Absent such an amendment, the legislation would likely be declared unconstitutional, similar to the Restrictive Covenant Act of 1990.[1] A resolution proposing an amendment to the Constitution was introduced during the 2009 legislative session. H.R. 178, 150th Leg., Reg. Sess. (Ga. 2009). This resolution was not voted on during the 2009 session; however, it was voted on and passed in the 2010 session.

As a result, on November 2, 2010, Georgia voters were asked to answer the following question: "Shall the Constitution of Georgia be amended so as to make Georgia more economically competitive by authorizing legislation to uphold reasonable competitive agreements?" H.R. 178, 150th Leg., 2d Sess. (Ga. 2010). An overwhelming majority of Georgia voters answered this question in the affirmative. As such, the proposed amendment passed.[2]

---

[1] This statute was declared unconstitutional by the Georgia Supreme Court. Jackson & Coker, Inc. v. Hart, 261 Ga. 371, 405 S.E.2d 253 (1991). The case law prior to the statute remains good law as to agreements signed before the effective date of the new Act. Vortex Protective Serv., Inc. v. Dempsey, 218 Ga. App. 763, 463 S.E.2d 67 (1995).

[2] Some commentators have argued that the ballot language was written by supporters to ensure a "yes" vote. These critics have argued that the ballot language was unconstitutionally

2. The Issues with the Effective Date of the Act

Following the passage of the amendment, the question of *when* Georgia's restrictive covenants law changed was still somewhat unclear. According to the statute itself, H.B. 173 was intended to go into effect on the day following the ratification of the amendment. See H.B. 173, 150th Leg., Reg. Sess. (Ga. 2009), at § 4. However, under article X, section 1, paragraph VI of the Georgia Constitution, an amendment to the Constitution becomes effective on the first day of January following its ratification, unless the amendment or the resolution proposing the amendment provides otherwise. Neither the amendment nor H.R. 178 stated that the amendment would go into effect immediately. Therefore, the amendment to the Constitution did not go into effect until January 1, 2011. As such, during the approximately two-month period when the legislation had gone into effect but the amendment had not yet gone into effect, H.B. 173 was arguably unconstitutional as the Constitution had not yet been amended. This "gap" was apparently unintended by the legislature. Moreover, the problem with the timing of the effective date called into question the constitutional foundation of the statute.

As a result, H.B. 30 was introduced in the 2011 session of the Georgia House of Representatives to address the timing issue and to attempt to cure any problems with the constitutionality of the statute based on the timing issues. This bill was intended to essentially reenact H.B. 173 and cure the timing issue of when the law when into effect: "During the 2010 legislative session the General Assembly enacted HR 178 (Ga. L. 2010, p. 1260), the constitutional amendment necessary for the statutory language of HB 173 (Act No. 64, Ga. L. 2009, p. 231), and the voters ratified the constitutional amendment on November 2, 2010. It has been suggested by certain parties that because of the effective date provisions of HB 173 (Act No. 64, Ga. L. 2009, p. 231), there may be some question about the validity of that legislation. It is the intention of this Act to remove any such uncertainty by substantially reenacting the substantive provisions of HB 173 (Act No. 64, Ga. L. 2009, p. 231), but the enactment of this Act should not be taken as evidence of a legislative determination that HB 173 (Act No. 64, Ga. L. 2009, p. 231) was in fact invalid." See H.B. 30, 151st Leg., Reg. Sess., (Ga. 2011), at § 1.

---

vague, deceptive, or misleading. Although Georgia courts historically have been reluctant to closely scrutinize ballot referendum language, an argument can be made that existing precedent does not apply because the effect of the passage of the referendum is that the Georgia General Assembly gains powers it did not previously have (i.e., the ability to legislate in the area of restraints of trade). There are currently no reported decisions addressing a challenge to the validity of the new law based on the argument that the ballot referendum language was unconstitutionally vague, but this issue should be considered when evaluating the enforceability of covenants governed by the new law.

H.B. 30 was passed by both chambers of the General Assembly and was signed by the Governor. The bill went into effect on May 11, 2011. See generally, Becham v. Synthes (U.S.A.), No. 5:11-CV-73 (MTT), 2011 WL 4102816, at *4 (M.D. Ga. Sept. 14, 2011) ("In sum, the 2009 law become effective November 3, 2010, but without the necessary constitutional foundation in place. The constitutional amendment changing Georgia's public policy became effective January 1, 2011. The legislation curing any constitutional defect became effective May 11, 2011.").

The passage of H.B. 30 still left open the question of what applied to restrictive covenants entered into between January 1, 2011 and May 11, 2011. According to an unpublished opinion from the Eleventh Circuit Court of Appeals, agreements entered into *after the amendment took effect but before the passage of H.B. 30* must be analyzed under Georgia's old case law. Becham v. Synthes (U.S.A), 482 Fed. Appx. 387, 392 (11th Cir. 2012). In Becham, the Eleventh Circuit held that while H.B. 173 was effective on November 3, 2010, it was unconstitutional the "moment it went into effect," as the constitutional amendment was not yet effective. Id. The Eleventh Circuit further opined that the constitutional amendment, which went into effect on January 1, 2011, did not revive H.B. 173, because the General Assembly did not substantially reenact that law after January 1, 2011. Id. Rather, H.B. 30 was enacted and went into effect on May 11, 2011. Id. The Eleventh Circuit thus indicated that Georgia's old law applies to all agreements entered into before May 11, 2011, after which date Georgia's public policy changed with the enactment of H.B. 30. Id. at 392-93. ("[W]e conclude that Georgia's public policy did not change until May 2011 . . . ."). Neither the Georgia Court of Appeals nor the Georgia Supreme Court has addressed this issue yet.

3. The Changes in Georgia's Restrictive Covenants Law by Virtue of the Act

The new law substantially changes Georgia law on restrictive covenants. One notable change is that Georgia courts are now able to modify unreasonable restraints. As set forth below, under longstanding Georgia case law pre-dating the statute, if a restriction in a covenant was found by a court to be overbroad, the court could not modify the covenant to make the restriction reasonable. Rather, the covenant was unenforceable in its entirety. For example, if the geographic territory in which an employee was restricted from working included areas where the employee did not work for or represent the employer, the covenant could not be modified by a court to restrict the employee from working in only those areas in which the employer may reasonably restrict the employee from working. Instead, the entire covenant would be declared unenforceable. Furthermore, if one covenant against competition in an employment agreement was found to be overbroad and unenforceable, the other covenants against competition in the agreement were rendered

unenforceable. The new legislation changes these rules by permitting the courts to modify overbroad restrictions based on their determination of what is reasonable.

4. The Act Does Not Apply to Contracts Pre-dating its Effective Date

Importantly, by its terms, the new law does not apply to contracts entered into before it became effective. See H.B. 30, 151st Leg., Reg. Sess. (Ga. 2011), at § 5; see also H.B. 173, 150th Leg., Reg. Sess. (Ga. 2009), at § 4. In decisions since the constitutional amendment went into effect, courts have applied Georgia's pre-existing case law to contracts entered into before it became effective. See Gordon Document Prods., Inc. v. Serv. Techs., Inc., 308 Ga. App. 445, 448 n.5, 708 S.E.2d 48, 57 n.5 (2011) (applying old law to 2003 and 2007 agreements); Cox v. Altus Healthcare & Hospice, Inc., 308 Ga. App. 28, 30, 706 S.E.2d 660, 664 (2011) (applying old law to 2009 agreement); see also Clark v. Johnson Truck Bodies, LLC, No. CV411-132, 2012 WL 1014827, at *6 (S.D. Ga. Mar. 23, 2012) (applying old law to 2008 agreement and entering summary judgment for Plaintiff *sua sponte* because the unenforceable provisions could not be "blue-penciled"); Becham v. Synthes (U.S.A.), No. 5:11-CV-73 (MTT), 2011 WL 4102816, at *4 (M.D. Ga. Sept. 14, 2011) (applying old law to covenants agreed to on December 1, 2010, reasoning that the covenants were agreed to after H.B. 173 went into effect but before the necessary constitutional amendment went into effect on January 1, 2011); Boone v. Corestaff Support Servs., Inc., 805 F. Supp. 2d 1362, 1369 (N.D. Ga. 2011) (applying old law to 2008 agreement).

5. Georgia Appellate Opinions Interpreting the Act

The only published Georgia appellate court opinion interpreting the Act is *Carpetcare Multiservices, LLC v. Carle*, -- Ga. App. --, 819 S.E.2d 894 (Ga. App. Oct. 3, 2018). In *Carpetcare*, an employer sued a former independent contractor for violating his non-compete. The independent contractor moved to dismiss on the grounds that the non-compete was unenforceable. The non-compete stated that for one year after the end of employment, the contractor would not provide any service to any customer with whom he had contact during the term of his employment. In other words, the non-compete was a client-based restriction that prohibited him from servicing the customers with whom he dealt.

The employee argued this non-compete was unenforceable because it did not contain a geographic limitation. The trial court agreed. A divided Court of Appeals affirmed the trial court's ruling.

The majority's conclusion was based primarily on the wording of O.C.G.A. § 13-8-53(a). This section of the new non-compete law states that "enforcement of contracts that restrict competition during the term of a

restrictive covenant, so long as such restrictions are reasonable in time, geographic area, and scope of prohibited activities, shall be permitted." The majority interpreted this provision to mean that a *non-compete* must have a reasonable geographic limitation. The majority also pointed to other parts of the non-compete statute that address the types of territorial limitations that may be used in a non-compete. O.C.G.A. § 13-8-53(c)(2); O.C.G.A. § 13-8-56(2). The majority also noted that whereas the statute requires a *non-compete* have a territory, O.C.G.A. § 13-8-53(b) expressly provides that a *customer non-solicit* need not contain a geographic limitation. As the parties did not dispute that that the covenant at issue was a non-compete rather than a customer non-solicit, the majority concluded that the absence of a territory was fatal to the non-compete.

In trying to save its non-compete, Carpetcare argued that the statutory requirement of a geographic limitation need not be interpreted literally. Rather, Carpetcare argued that narrowly limiting the scope of the covenant to only the customers that the contractor dealt with meets the *reasonableness* requirements of the statute and therefore should satisfy the geography requirement. The majority concluded that such an interpretation would ignore the plain and ordinary language of the statutory text, which requires that a non-compete have a geographic limitation.

Judge Ray dissented. He concluded that the statute does not specifically require a geographic restriction. Rather, he wrote that it only requires any geographic restriction be reasonable. Here, despite the non-compete not having a geographic restriction, the covenant only restricted the contractor from engaging in post-termination competitive activities with those customers with whom he had dealt. In Judge Ray's view, this was a reasonable restriction and "the lack of a geographic area restriction is of no consequence." Judge Ray noted that Carpetcare's non-compete allowed the independent contractor to work in his line of business in any territory as long as he was not working for customers he dealt with. In his view, the former employer could have drafted the non-compete significantly more broadly such and the majority's holding was therefore "not a reasonable outcome."

Given the divided court, this decision has limited precedential value. However, it does shed light on how certain judges on the Court of Appeals interpret aspects of the new non-compete statute. And, practitioners who draft non-competes should be aware non-competes that limit prohibiting competitive services to former customers could be subject to attack without a reasonable territory. The fact that two of the three justices construed the statute narrowly is not surprising given that the statute is in derogation of the common law.

Notably the Court of Appeals did not address whether the non-compete could have been saved through "blue penciling", as the trial court's ruling on this issue was not part of the appeal. Carpetcare is seeking certiorari from the Georgia Supreme Court; its petition remains pending as of the completion of these materials.

6. Federal District Court Decisions Interpreting the Act

While Georgia appellate opinions applying the new law are sparse, There are a number of unpublished federal district court opinions applying the Act. These cases provide practitioners some guidance on how judges may deal with various issues arising under the new law. See Interra Int'l, LLC v. Al Khafaji, No. 1:16-CV-1523-MHC, 2017 WL 4866266 (N.D. Ga. Mar. 21, 2017) (finding non-solicitation covenant compliant with new law, but striking over broad tolling provision); Novelis Corp. v. Smith, No. 1:16-CV-1557-ODE, 2017 WL 1745635 (N.D. Ga. Mar. 10, 2017) (entering preliminary injunction enforcing two-year non-compete against former plant manager); CSM Bakery Sols., LLC v. Debus, No. 1:16-CV-03732-TCB, 2017 WL 2903354, at *7 (N.D. Ga. Jan. 25, 2017) (dissolving injunction enforcing non-compete and non-solicit against former sales representative of a bakery manufacturer based on finding that sales representative was not the type of employee under the statute against whom a non-compete is permissible); LifeBrite Labs., LLC v. Cooksey, No. 1:15-CV-4309-TWT, 2016 WL 7840217 (N.D. Ga. Dec. 9, 2016) (finding non-compete without a territory is invalid and holding that the Act does not authorize the Court to insert a territory); Cellaris Franchise, Inc. v. Duarte, No. 2:15-cv-00101-WCO, 2015 WL 6517487 (N.D. Ga. Oct. 21, 2015) (entering injunction enforcing restrictive covenants in franchise agreement); ID Tech., LLC v. Hamilton, No. 1:14-CV-00594-TWT, 2014 WL 12703272 (N.D. Ga. Mar. 24, 2014) (denying motion for TRO to enforce non-compete where employee only worked for company for two months and non-compete did not contain a territory); Pedowitz Grp., LLC v. Ogden, No. 1:13-CV-00839-RLV, 2013 WL 11319834 (N.D. Ga. Nov. 29, 2013) (denying preliminary injunctive relief where the plaintiff failed to demonstrate that North America was a reasonable geographic limitation); NCR Corp. v. Manno, No. 3:12-CV-121-TCB, 2012 WL 12888663 (N.D. Ga. Oct. 26, 2012) (entering a preliminary injunction which included a territorial restriction based on a list of competing organizations and a territory defined as the area where the former employer does business); PointeNorth Ins. Grp. v. Zander, No. 1:11-CV-3262-RWS, 2011 WL 4601028 (N.D. Ga. Sept. 30, 2011) (blue penciling over broad customer non-solicitation covenant in May 11, 2011 employment agreement to apply only to customers that the former employee contacted or assisted with insurance).

7. Conclusion

As there is limited case law interpreting the Act and given that Georgia's pre-existing case law remains relevant since the new law does not apply retroactively, these materials discuss both Georgia's pre-existing case law and the new statute.

Of course, drafters preparing restrictive covenants under the Act are advised to carefully review the new legislation as they prepare such covenants. Given that cases applying the new law are sparse, an article containing a hypothetical problem discussing some of the issues a practitioner may confront when litigating agreements containing restrictive covenants which are governed by the Act is attached to these materials. A copy of the Act is also attached. All of the common law cases cited below are still relevant to analyzing covenants entered into prior to the effective date of the new statute.

B. Types of Covenants

Under the common law pre-dating the Act, there was a "fundamental distinction" between covenants not to compete and not to solicit and they were analyzed differently. See Habif, Arogeti & Wynne, P.C. v. Baggett, 231 Ga. App. 289, 295, 498 S.E.2d 346, 353 (1998).

1. Non-competition

This type of covenant prohibits the employee from performing competitive activities in a certain geographic area for a limited time after termination of employment and is designed primarily to protect the employer's "investment of time and money in developing the employee's skills." Habif, Arogeti & Wynne, P.C. v. Baggett, 231 Ga. App. 289, 295, 498 S.E.2d 346, 353 (1998).

2. Non-solicitation

a. Customers - This type of covenant restricts the employee from soliciting business from the employer's customers or prospective customers after termination of employment and is designed primarily to protect the employer's investment of time and money in developing customer relationships. Historically, this type of covenant only required a territorial restriction if the forbidden clients included the clients with whom the employee did not have a relationship prior to his departure. Habif, Arogeti & Wynne, P.C. v. Baggett, 231 Ga. App. 289, 295, 498 S.E.2d 346, 353 (1998).

b. Personnel - This type of covenant restricts the employee from recruiting employees of the employer after termination of employment.

C. Background

Until January of 2011, the Georgia Constitution stated that all contracts that had the effect of or were intended to defeat or lessen competition or encourage a monopoly were illegal and void. Ga. Const. art. III, § 6, para. V.

O.C.G.A. section 13-8-2 provides that contracts deemed contrary to public policy will not be enforced. According to the statute, contracts in general restraint of trade are an example of such unenforceable contracts.

Historically, Georgia courts considered restrictive covenants in employment contracts to be in partial restraint of trade and have only enforced them if the restraints were not unreasonable, were founded on valuable consideration, were reasonably necessary to protect the interest of the employer, and did not unduly prejudice the public interest. Rakestraw v. Lanier, 104 Ga. 188, 30 S.E. 735, 738 (1898).

The public policy relating to restrictive covenants was stated in Rakestraw where the court wrote: "[C]ontracts in unreasonable restraint of trade are contrary to public policy and void, because they tend to injure the parties making them; diminish their means of procuring livelihoods and a competency for their families; tempt improvident persons, for the sake of present gain, to deprive themselves of the power to make future acquisitions, and to expose them to imposition and oppression; tend to deprive the public of services of [citizens] in the employments and capacities in which they may be most useful to the community as well as themselves; discourage industry and enterprise, and diminish the products of ingenuity and skill; prevent competition, and enhance prices, and expose the public to all the evils of monopoly." Rakestraw v. Lanier, 104 Ga. 188, 30 S.E. 735, 738 (1898).

Georgia courts historically used a three pronged test "as a helpful tool" to determine the reasonableness of covenants ancillary to employment contracts. The covenants must be reasonably limited in terms of (1) the time in which they bind the employee, (2) the scope of conduct prohibited, and (3) geographical territory in which they bind the employee. Watson v. Waffle House, Inc., 253 Ga. 671, 672-73, 324 S.E.2d 175, 178 (1985); Howard Schultz & Assocs., Inc. v. Broniec, 239 Ga. 181, 183, 236 S.E.2d 265, 267 (1977).

Under the common law that existed prior to the passage of the Act, whether the restraint imposed by a restrictive covenant was reasonable was a question of law for determination by the court, which considered the nature and extent of the trade or business, the situation of the parties, and all other circumstances. See Allied Informatics, Inc. v. Yeruva, 251 Ga. App. 404, 406, 554 S.E.2d 550, 553 (2001); Osta v. Moran, 208 Ga. 544, 546, 430 S.E.2d 837, 839 (1993). In answering this question of law, the courts looked first at the restrictive covenants on their face. See, e.g., Ken's Stereo-Video Junction, Inc. v. Plotner, 253 Ga. App. 811, 813-14, 560 S.E.2d 708, 710 (2002) (affirming trial court's decision not to hold an evidentiary hearing, as "one was not required," where "restriction imposed . . . could not be saved by additional facts and [wa]s in fact void on its face" (quoting Koger Props. v. Adams-Cates Co., 247 Ga. 68, 69, 274 S.E.2d 329, 331 (1981))); AGA, LLC v. Rubin, 243 Ga. App. 772, 774, 533 S.E.2d 804, 806 (2000) ("Usually, whether a covenant is reasonable can appropriately be answered based upon the wording of the covenant."). But see Nat'l Teen-Ager Co. v. Scarborough, 254 Ga. 467, 469, 330 S.E.2d 711, 713 (1985) ("[T]he question whether a given covenant falls into the prohibited 'in any capacity' category generally is not determinable solely from the face of the contract.").

II. The Employment Agreement

A. Limitations on Restrictions of Competition and Solicitation

1. Requirement of Reasonableness

Even under the new legislation, post-termination non-competes must still be reasonable in time, geographic area, and scope of prohibited areas. O.C.G.A. § 13-8-53(a). The new law provides guidance and presumptions for crafting reasonable restrictions. O.C.G.A. § 13-8-53(c); O.C.G.A. § 13-8-56; O.C.G.A. § 13-8-57. Employers should still take heed to have their covenants be concise, precise and carefully tailored to their businesses' interests.

Under the old law, overly broad and prohibitive covenants were vulnerable to attack. Employers who tried to restrict former employees without good cause were disappointed when their covenants were struck down.

Under the old law, courts will balance the interests to be protected and the effects on both parties to the contract to determine if the covenants are "reasonable." Orkin Exterminating Co. v. Pelfrey, 237 Ga. 284, 285, 227 S.E.2d 251, 252 (1976); Rash v. Toccoa Clinic Med. Assocs., 253 Ga. 322, 323, 320 S.E.2d 170, 171 (1984).

In determining whether a covenant is reasonably limited with regard to these factors, the courts must balance the interest the employer seeks to protect against the impact the covenant will have on the employee, factoring in the effect of the covenant on the public's interest in promoting competition and the freedom of individuals to contract. Beckman v. Cox Broad. Corp., 250 Ga. 127, 130, 296 S.E.2d 566, 568 (1982); Windsor-Douglas Assocs., Inc. v. Patterson, 179 Ga. App. 674, 674, 347 S.E.2d 362, 363 (1986).

Under the old law, whether a restrictive covenant is "reasonable" is a question of law to be determined by the court based upon the language of the covenant Osta v. Moran, 208 Ga. 544, 546, 430 S.E.2d 837, 839 (1993); Rollins Protective Servs. Co., 249 Ga. 138, 287 S.E.2d 546 (1982); Koger Props. v. Adams-Cates Co., 247 Ga. 68, 69, 274 S.E.2d 329, 331 (1981).

Under Georgia case law applicable to restrictive covenants not drafted under the new legislation, an overbroad restrictive covenant could be found unenforceable on its face without the need for factual inquiry. See e.g., Ken's Stereo-Video Junction, Inc. v. Plotner, 253 Ga. App. 811, 813-14, 560 S.E.2d 708, 710 (2002) (affirming trial court's decision not to hold an evidentiary hearing, as "one was not required," where "restriction imposed . . . could not be saved by additional facts and [wa]s in fact void on its face" (quoting Koger Props. v. Adams-Cates Co., 247 Ga. 68, 69, 274 S.E.2d 329, 329 (1981))); New Atlanta Ear, Nose & Throat Assocs., P.C. v. Pratt, 253 Ga. App. 681, 685, 560 S.E.2d 268, 271 (2002) (finding enforceability of restrictive covenant "is a question of law for the court based upon the wording of the covenant[s]" at issue); Sanford v. RDA Consultants, Ltd., 244 Ga. App. 308, 310, 535 S.E.2d, 321, 323 (2000) ("[N]oncompetition covenant as written was unenforceable under Georgia law."); AGA, LLC v. Rubin, 243 Ga. App. 772, 774, 533 S.E.2d 804, 806 (2000) ("Usually, whether a covenant is reasonable can appropriately be answered based upon the wording of the covenant. However, [o]ccasionally facts might be necessary to show that a questionable restriction, though not void on its face, is, in fact, reasonable. . . . However, the indefinite restriction imposed in this case could not be saved by additional facts and is in fact void on its face.'" (alterations in original) (quoting Koger Props. v. Adams-Cates Co., 247 Ga. 68, 69, 274 S.E.2d 329, 329 (1981))); see also Rakestraw v. Lanier, 104 Ga. 188, 30 S.E. 735, 741 (1898). ("We are to construe [the covenant] as it is written, and, so construing it, we hold it to be void and of no binding force and effect."); Equifax Servs., Inc. v. Examination Mgmt. Servs., Inc., 216 Ga. App. 35, 40, 453 S.E.2d 488, 493 (1995) ("[W]e cannot ignore the fact that the covenant . . . is overbroad [and] unenforceable as written . . . .").

"In determining reasonableness, consideration must be given to the employee's right to earn a living, and the employee's ability to determine with certainty the area within which his post-employment actions are restricted. At the same time, the employer has a protectible interest in the customer relationships its former employee established and/or nurtured while employed by the employer, and is entitled to protect itself from the risk that a former employee might appropriate customers by taking unfair advantage of the contacts developed while working for the employer." W.R. Grace & Co. v. Mouyal, 262 Ga. 464, 466, 422 S.E.2d 529, 532 (1992) (citations omitted).

a. Scope of Conduct Restricted

(1) New law

Unger the new law, a restrictive covenant must provide only fair notice of the maximum scope of the activities, products or services restricted by the covenant, even if the description is generalized or could possibly be stated more narrowly to exclude extraneous matters. O.C.G.A. § 13-8-53(c)(1). In post-employment restrictive covenants, any good faith estimate of the activities, products, and services applicable at the time of termination suffices, even if the estimate includes extraneous activities, products, and services. Id. Post-employment covenants are to be construed narrowly as covering only the portions of the estimate related to activities actually conducted or products and services actually offered within a reasonable period of time prior to termination. Id.

Activities, products, or services that compete with those of an employer include activities, products, or services that are the same as or similar to those of the employer. Id. Activities, products, or services are sufficiently described if there is a reference to them which is qualified by the phrase "of the type conducted, authorized, offered, or provided within two years prior to termination" or similar language containing the same or a lesser time period. O.C.G.A. § 13-8-53(c)(2).

Under the new law, courts are to presume that the scope of restricted competition is measured by the business of the employer or other person or entity who proposes the covenant. O.C.G.A. § 13-8-56(3). Enforcing parties do

not need to prove that the entire scope of the covenant was violated, and failure to do so should not cause the court to refuse enforcement of violated provisions of the covenant. Id.

(2) Old law

Under the old law, the covenant must explain with particularity the nature of the business in which the employee is prohibited from engaging. Howard Schultz & Assocs., Inc. v. Broniec, 239 Ga. 181, 184, 236 S.E.2d 265, 268 (1977).

The business activities the employee is forbidden from participating in must be expressed with particularity and must relate to that which the employee did for the employer during employment. See Avion Sys., Inc. v. Thompson, 293 Ga. App. 60, 64, 666 S.E.2d 464, 468 (2008) (covenant which did not specify the restricted activities but instead prohibited employee from dealing with a client "for any pecuniary gain" was unenforceable); Whimsical Expressions, Inc. v. Brown, 275 Ga. App. 420, 423, 620 S.E.2d 635, 637-38 (2005) (where noncompete clause "attempted to preclude [painter] not only from performing painting services for prior clients , but also from acting as a salesperson . . ., it was overly broad," especially where employer "did not employ 'sales persons'"); Howard Schultz & Assocs., Inc. v. Broniec, 239 Ga. 181, 185, 236 S.E.2d 265, 268 (1977) (covenant prohibiting contractor "from engaging 'in any capacity whatsoever, in any business, activity, auditing practice, or in any other related activities, in competition with the principal or associate's business' found unenforceable); Allied Informatics, Inc. v. Yeruva, 251 Ga. App. 404, 554 S.E.2d 550 (2001); Fleury v. AFAB, Inc., 205 Ga. App. 642, 423 S.E.2d 49 (1992); see also Wright v. Power Indus. Consultants, Inc., 234 Ga. App. 833, 834, 508 S.E.2d 191, 193 (1998) (covenant prohibiting employees from acting as shareholders, partners or principals found over broad and unenforceable because this was prohibition on activities beyond those employees performed for former employer); Harville v. Gunter, 230 Ga. App. 198, 200, 495 S.E.2d 862, 864 (1998) (covenant prohibiting mere employee from being officer, director, shareholder or employee unenforceable because very different from employee's work for employer).

Prohibiting the former employee from engaging in any activity in which the employer might later decide to engage is also unreasonable and unenforceable. Watkins v. Avnet, Inc., 122 Ga. App. 474, 477, 177 S.E.2d 582, 584 (1970).

The scope of the activities prohibited probably need not be limited to the identical activities in which the employee engaged for the former employer. Edwards v. Howe Richardson Scale Co., 237 Ga. 818, 229 S.E.2d 651 (1976) (covenant prohibiting purchases and sales upheld even though mechanic did not buy or sell for former employer); Wesley-Jessen, Inc. v. Armento, 519 F. Supp. 1352 (N.D. Ga. 1981) (covenant prohibiting supervision of salesmen for competitor not unreasonable even though salesman had not supervised salesmen for employer); see also Palmer & Cay of Ga., Inc. v. Lockton Cos., 284 Ga. App. 196, 200, 643 S.E.2d 746, 749 (2007) (upholding two-year non-solicitation covenant prohibiting employees from selling products or services offered by the company during their employment and noting that such products need not be identical to the ones sold during their employment at the company but can be those that are "competitive or potentially competitive"). Cf. Puritan/Churchill Chem. Co. v. Eubank, 245 Ga. 334, 265 S.E.2d 16 (1980) (covenant prohibiting salesman from owning, managing, controlling, operating or participating in same business over broad); Browning v. Orr, 242 Ga. 380, 249 S.E.2d 65 (1978) (covenant prohibiting salesperson from participating in manufacture or distribution of competitive or similar products unenforceable). However, the restriction must be "rationally related" to the activities performed by the former employee. Wesley-Jessen, Inc. v. Armento, 519 F. Supp. 1352, 1358 (N.D. Ga. 1981).

Under the old law, it had been held that prohibiting a former employee from "aiding or abetting" others in engaging in conduct from which the employer may restrict the former employee may be unreasonably indefinite and over broad, and, therefore unenforceable if it, in effect, prohibits the former employee from acting as a supervisor or in some other capacity in which he could not directly, unduly influence customers of his former employer because of any special trust or confidence he may have developed with the customers through his prior employment. Am. Gen. Life & Accident Ins. Co. v. Fisher,

208 Ga. App. 282, 284, 430 S.E.2d 166, 168 (1993).

A covenant governed by the old law which specifies the type of activities it intends to restrict (e.g., managing, selling, repairing, etc.) will more likely be upheld; though the courts may look to other provisions in the agreement to define the scope of the conduct prohibited. See, e.g., Moore v. Preferred Research, Inc., 191 Ga. App. 26, 26-27, 381 S.E.2d 72, 73 (1989) (to determine what activities are restricted, the court must look to other provisions of the agreement which define the business activities licensed under the agreement); see also Riddle v. Geo-Hydro Eng'rs, Inc., 254 Ga. App. 119, 120-21, 561 S.E.2d 456, 458 (2002) (covenant not to solicit that "prohibit[ed] [Riddle] from contacting [certain] clients to sell them unrelated products . . . clearly [goes] beyond what is necessary to protect [Geo-Hydro's] business interests" and was thus "overbroad and unenforceable" (second, fourth, and fifth alterations in original)).

Under the law pre-dating the Act, courts considered the phrases "or otherwise" or "in any capacity" following a list of proscribed activities to be indefinite and have struck covenants containing such phrases down as unreasonable. Fleury v. AFAB, Inc., 205 Ga. App. 642, 643 423 S.E.2d 49, 49 (1992); Arnall Ins. Agency, Inc. v. Arnall, 196 Ga. App. 414, 396 S.E.2d 257 (1990); see also Nat'l Settlement Assocs. v. Creel, 256 Ga. 329, 349 S.E.2d 177 (1986); Ponders, Inc. v. Norman, 246 Ga. 647, 272 S.E.2d 345 (1980); Hudgins & Co. v. Cole, 247 Ga. 182, 183, 274 S.E.2d 462, 463 (1981); Howard Schultz & Assocs., Inc. v. Broniec, 239 Ga. 181, 236 S.E.2d 265 (1977); Federated Mut. Ins. Co. v. Whitaker, 232 Ga. 811, 209 S.E.2d 161 (1974); Firearms Training Sys. v. Sharp, 213 Ga. App. 566, 567, 445 S.E.2d 538, 540 (1994); Fantastic Sams Salons Corp. v. Maxie Enters., Inc., No. 3:11-CV-22 (CDL), 2012 WL 210889 (M.D. Ga. Jan. 24, 2012). But see Hulcher Servs., Inc. v. R.J. Corman R.R. Co., L.L.C., 247 Ga. App. 486, 492, 543 S.E.2d 461, 467 (2001) ("Where a noncompete covenant, *for someone other than a licensed professional*, is so broad that such former employee is prohibited from working for a competitor of the former employer in any capacity, such covenant is unreasonable." (emphasis added)).

Language that prohibits an employee from "engaging" in a competitive business has been consistently struck down

as over broad. See Uni-Worth Enters., Inc. v. Wilson, 244 Ga. 636, 639-40, 261 S.E.2d 572 (1979); Orkin Exterminating Co. v. Walker, 251 Ga. 536, 539, 307 S.E.2d 914, 917 (1983). See also Impreglon v. Newco Enters., Inc., 508 F. Supp. 2d 1222, 1237 (N.D. Ga. 2007) (covenant restricting former President from serving as Chief Executive or Operating Officer of any entity "which is engaged in the same business, or essentially the same business" as former employer lacks sufficient particularity).

Under the old law, the nature of the business interest the employer sought to protect needed to be clearly explained. Watkins v. Avnet, Inc., 122 Ga. App. 474, 177 S.E.2d 582 (1970).

Affiliates or other distinct corporate entities for whom the employee did not work could not be included in the scope of the covenant, unless they could be specifically identified and a specific justification for doing so could be articulated. See BellSouth Corp. v. Forsee, 265 Ga. App. 589, 594-96, 595 S.E.2d 99, 104-106, (2004) (affirming trial court's determination that covenant's territory was overbroad where it included "affiliated companies" of employer and employee could not ascertain what those companies were when agreement was executed); see also Szomjassy v. OHM Corp., 132 F. Supp. 2d 1041, 1049 (N.D. Ga. 2001) (covenant that included employer and another company, as well as "their affiliates and subsidiaries" was overbroad and went "too far"). But see Fox v. Avis Rent-A-Car Sys., Inc., 223 Ga. 571, 573, 156 S.E.2d 910, 912 (1967) (considering two covenants, Supreme Court upheld one covenant that, although expanded to include subsidiaries and affiliates, was limited in scope to those services performed by employee for his employer and found other non-competition covenant prohibiting competition with the company or "any subsidiary" to be "fatally defective and void because it [was] indefinite, and for this reason unreasonable, in the description of the prohibited business")

When considering the case of an employee in an executive position, the decision of Saxton v. Coastal Dialysis & Med. Clinic, Inc., 220 Ga. App. 805, 470 S.E.2d 252 (1996) should be considered. In that case, the Court of Appeals agreed that where the shareholders of a corporation entrusted all aspects of their business to the

former employee as the chief executive officer, the employer's "unusually broad and iron-clad restrictions" may be reasonable. Id. at 808-09, 255; see also Malice v. Coloplast Corp., 278 Ga. App. 395, 629 S.E.2d 95 (2006) (arbitrator's award finding that covenant is enforceable is not in manifest disregard of the law where arbitrator applied lesser scrutiny to covenant in employment agreement because executive had substantial bargaining power).

b. Duration of the Restraint

(1) New law

In enforcing restrictive covenants against former employees under the new law, a court is to presume that restraints that endure for two years or less are reasonable. O.C.G.A. § 13-8-57(b). See Cellairis Franchise, Inc. v. Duarte, No. 2:15-CV-00101-WCO, 2015 U.S. Dist. LEXIS 147890 (N.D. Ga. Oct. 21, 2015) (entering a preliminary injunction enforcing a franchise agreement's two-year non-compete against the agreement's personal guarantor, who had also been a franchise employee). The restraint is measured from the date the business relationship is terminated. O.C.G.A. § 13-8-57(b). Courts are also to presume that a restraint more than two years in duration is unreasonable. Id.

In enforcing restrictive covenants against a current or former distributor, dealer, franchisee, lessee of real or personal property, or licensee of a trademark, trade dress, or service mark, a court is to presume that restraints that endure for three years or less are reasonable, as measured from the date the business relationship was terminated. O.C.G.A. § 13-8-57(c). Courts are to presume that a restraint more than three years in duration is unreasonable. Id.

In enforcing restrictive covenants against owners or sellers of specific assets, shares, or ownership interests, courts are to presume as reasonable any restraint "the longer of five years or less in duration or equal to the period of time during which payments are being made to the owner or seller as a result of the sale . . . as measured from the date of termination of disposition of the owner or seller's interest." O.C.G.A. § 13-8-57(d).

Courts are also to presume as unreasonable a restraint more than the longer of five years in duration or the period of time during which payments are being made to the owner or seller as a result of the sale. O.C.G.A. § 13-8-57(d). This rule is arguably more restrictive than the old law which permitted a restrictive covenant ancillary to the sale of a business to remain in effect as long as the buyer operated the business. See Martinez v. DaVita, Inc., 266 Ga. App. 723, 728, 598 S.E.2d 334, 338 (2004).

(2) Old law

Under the old law, no time restriction was held unreasonable *per se*. Johnson v. Lee, 243 Ga. 864, 257 S.E.2d 273 (1979); see also Coleman v. Retina Consultants, P.C., 286 Ga. 317, 687 S.E.2d 457 (2009) (non-compete clause which contains no limitation on its duration is invalid).

Although one and two year durations were typical, a five-year limitation was also upheld. Smith v. HBT, Inc., 213 Ga. App. 560, 445 S.E.2d 315 (1994).

Under the old law, limitations in time needed to bear some relation to the amount of time needed by the former employer to re-establish and solidify its relationships with its customers. See Orkin Exterminating Co. v. Walker, 251 Ga. 536, 307 S.E.2d 914 (1983).

See also Kuehn v. Selton & Assocs., Inc., 242 Ga. App. 662, 530 S.E.2d 787 (2000) (covenant restricting real estate agent from doing business with tenants who were clients of former employer as long as clients remained in leased building or project was unreasonable and unenforceable, where language of covenant was unclear as to duration of restriction, and restriction thus had potential to be effective for decades).

Caution: See also Part H., infra, regarding tolling provisions.

c. Geographic Limitations

(1) New law

Under the statute, a restrictive covenant must only provide fair notice of the maximum geographic area covered by the restraint, even if the description is generalized or could possibly be stated more narrowly to exclude extraneous areas. O.C.G.A. § 13-8-53(c)(1). In post-employment restrictive covenants, a good faith estimate of the restricted geographic area applicable at termination satisfies this requirement, even if it includes extraneous geographic areas. Id. Post-employment covenants are to be construed to cover only the areas of the estimate that are actually involved within a reasonable period of time prior to termination. Id. The phrase "the territory where the employee is working at the time of termination" or similar language is a sufficient description of the restricted territory if the party bound by the restraint can reasonably determine the restraint's maximum reasonable scope at termination of the relationship. O.C.G.A. § 13-8-53(c)(2).

Furthermore, a geographic territory that includes the areas in which the employer does business at any time during the parties' relationship, even if not known at the time of entry into the restrictive covenant, is to be presumed reasonable provided that the total distance is reasonable and/or the agreement contains a list of particular competitors as prohibited employers for a limited period of time after the term of employment or business or contractual relationship. O.C.G.A. § 13-8-56(2). See NCR Corporation v. Manno, No. 3:12-CV-121-TCB, 2012 U.S. Dist. LEXIS 196750 (N.D. Ga. Oct. 26, 2012) (entering a preliminary injunction which included a territorial restriction based on a list of competing organizations and a territory defined as the area where the former employer does business). But see Pedowitz Group, LLC v. Ogden, No. 1:13-CV-00839-RLV, 2013 U.S. Dist. LEXIS 190499 (N.D. Ga. Nov. 29, 2013) (denying preliminary injunctive relief where the plaintiff failed to demonstrate that North America was a reasonable geographic limitation). In the Internet age, where business can be conducted with anyone in just about any location, a restricted territory that encompasses the area where the employer does business could in some contexts have the effect of imposing a worldwide restriction. However, courts may be unlikely to enforce a covenant that has such a broad territorial effect given that the total distance encompassed by

the covenant must be reasonable. See O.C.G.A. § 13-8-56(2)(A).

Under the analysis applied by the majority in *Carpetcare Multiservices, LLC v. Carle*, -- Ga. App. --, 819 S.E.2d 894 (Ga. App. Oct. 3, 2018), a restriction prohibiting an employee from servicing customers of his or her former employer must contain a reasonable territory.

A court should not refuse to enforce a covenant because the enforcing party did not prove that the covenant was violated with regard to the entire geographic area. O.C.G.A. § 13-8-56(3).

(2) Old law

(a) Non-Competition Covenants

Under the common law pre-dating the Act, a territorial limitation was a necessary element of a covenant against competition.

There were no unreasonable territorial restrictions *per se*. Johnson, 243 Ga. 864, 257 S.E.2d 273.

A territorial limitation was necessary to give the employee notice of what constituted a violation of the restrictive covenant and was required to specify with particularity the geographic area in which the employee was restricted. Wiley v. Royal Cup, Inc., 258 Ga. 357, 370 S.E.2d 744 (1988) (discussing and applying requirement of reasonable territorial restriction in non-competition covenants to non-solicitation covenant which applies to all customers of the employer during the two years prior to the employee's termination).

The reasonableness of the territory depended, not so much on the geographic size of the territory, as on the reasonableness of the territorial restriction in view of the facts and circumstances surrounding the case. Rollins Protective Servs. Co., 249 Ga. 138, 287 S.E.2d 546 (1982); see also Smith v. HBT, Inc., 213 Ga. App. 560, 445 S.E.2d 315 (1994) (large geographic area upheld).

Under the old law, there was a vital difference between the territory in which the employer does business and the territory in which the employee does business. Historically, a non-compete covenant could only apply in the geographic areas in which the employee worked for or represented the employer. Wiley v. Royal Cup, Inc., 258 Ga. 357, 370 S.E.2d 744 (1988).

Georgia courts would accept as *prima facie* valid a covenant related to the territory where the employee was employed as a legitimate protection of the employer's investment in customer relations and good will. Reardigan v. Shaw Indus., Inc., 238 Ga. App. 142, 144, 518 S.E.2d 144, 147 (1999). However, Georgia courts have consistently struck down non-compete covenants that apply wherever the employer was doing business only. See, e.g., Specialized Alarm Servs., Inc. v. Kauska, 189 Ga. App. 863, 377 S.E.2d 703 (1989); see also Beacon Sec. Tech. v. Beasley, 286 Ga. App. 11, 648 S.E.2d 440 (2007) (where employer failed to present evidence that employee performed each of the prohibited activities in each of the eight prohibited counties, covenant went further than necessary to protect employer's interests); Dent Wizard Int'l Corp. v. Brown, 272 Ga. App. 553, 556, 612 S.E.2d 873, 876 (2005) (where evidence showed that employee only worked in two to three of the four counties in a stated territory, "the restriction will be considered overly broad on its face unless the record contains evidence demonstrating a strong justification for such a restriction"); Nat'l Settlement Assocs. v. Creel, 256 Ga. 329, 331, 349 S.E.2d 177, 180 (1986) (covenant will be upheld if employee worked in a "substantial portion" of the territory); McAlpin v. Coweta Fayette Surgical Assocs., P.C., 217 Ga. App. 669, 458 S.E.2d 499 (1995) (restriction in employment agreement of physician defined by territory in which professional corporation had patients was enforceable).

A covenant could not bind an employee in geographic areas where the former employer had no business interest. A covenant which applies wherever the employer "generally does business" would not be enforced unless the employer can demonstrate that this territorial definition protects a "legitimate business interest" of the employer. W.R. Grace & Co. v. Mouyal, 262 Ga. 464, 422 S.E.2d 529 (1992); Am. Software USA, Inc. v. Moore, 264 Ga. 480, 448 S.E.2d 206 (1994); Peachtree Fayette Women's Specialists, LLC v. Turner, 305 Ga. App. 60, 699 S.E.2d 69 (2010) (rejecting

argument that stream of referrals which owner of medical practice receives from location at which former employee is prohibited from working justifies restricting employee from working in a location in which she did not treat any patients during her employment).

Territorial restrictions that encompass the entire United States or the world were consistently struck down as over broad and unenforceable. See Paramount Tax & Accounting, LLC v. H & R Block E. Enters., Inc., 299 Ga. App. 596, 683 S.E.2d 141 (2009) (language in noncompetition covenant failed to limit prohibited conduct to a specific geographic area and would prevent employee from accepting employment anywhere in the United States); Firearms Training Sys. v. Sharp, 213 Ga. App. 566, 567-68, 445 S.E.2d 538, 539-40 (1994) (worldwide restriction held unenforceable); Am. Software USA, Inc. v. Moore, 264 Ga. 480, 448 S.E.2d 206 (1994) (restriction encompassing the United States found unenforceable); Budget Rent-a-Car Corp. v. Fein, 342 F.2d 509 (5th Cir. 1965) (restriction encompassing Western Hemisphere unenforceable); see also Owens v. RMA Sales, Inc., 183 Ga. App. 340, 341, 358 S.E.2d 897, 899 (1987) (worldwide restriction is "not limited in territorial effect" and is unenforceable and illegal).

Territorial restrictions have also been struck down as over broad and unlawful where the restrictions (1) apply to any office of the employer, (2) are not limited to the employee's territory immediately prior to his leaving, and (3) the scope of the restriction cannot be determined until the employee's termination. See Orkin Exterminating Co. v. Walker, 251 Ga. 536, 538, 307 S.E.2d 914, 916-17 (1983) (territorial restriction not limited to employee's territory prior to leaving found unenforceable); Koger Props. v. Adams-Cates Co., 247 Ga. 68, 69, 274 S.E.2d 329, 331 (1981) (covenant not to compete which cannot be determined until date of employee's termination is too indefinite to be enforced); Crowe v. Manpower Temp. Servs., 256 Ga. 239, 240, 347 S.E.2d 560, 561 (1960) (territorial restriction that applied to any office of the employer declared unenforceable); AGA, LLC v. Rubin, 243 Ga. App. 772, 774, 533 S.E.2d 804, 806 (2000) (non-competition clause in physician's employment contract found overbroad and unenforceable because territory was undefinable until physician's employment ended, as covenant precluded him from rendering services in any hospital at which he regularly performed services for employer during term of agreement); Ceramic Metal

Coatings Corp. v. Hizer, 242 Ga. App. 391, 393, 529 S.E.2d 160, 163 (2000) (language referring to "any territory added during the course of the agreement" over broad as employee cannot determine with any certainty at the time he signed the agreement the extent of the prohibition); ALW Mktg. Corp. v. McKinney, 205 Ga. App. 184, 187-88, 421 S.E.2d 565, 567-68 (1992) (territorial restriction held too indefinite where not ascertainable at time agreement entered); Becham v. Synthes (U.S.A), 482 Fed. Appx. 387, 392 (11th Cir. 2012) ("First, the noncompete covenant fails because it contains 'a territorial limitation not determinable until the time of the employee's termination.'"). But see Habif, Arogeti & Wynne, P.C. v. Baggett, 231 Ga. App. 289, 293, 498 S.E.2d 346, 352 (1998) ("Even under strict scrutiny, restricting competition in seven contiguous counties in which the employee *had worked at some point* is reasonable, particularly where he *had worked in a substantial portion* of the seven-county area during the two years before his departure." (emphasis added)).

Additionally, in New Atlanta Ear, Nose & Throat Assocs., Inc. v. Pratt, 253 Ga. App. 681, 560 S.E.2d 268 (2002), the Court of Appeals stated that when particular office locations are specified, they must be done so with particularity and include street addresses. This requirement prohibits territorial restrictions from "shifting" and "expanding." In Pratt, the Court of Appeals held that a "listing of the prohibited locations ha[d] a fatal flaw: the addresses and the number of offices in each location are not identified, thus allowing (during the course of the agreement) the 16-mile circles of prohibited territory within each listed location to shift as offices move and to expand in number as offices are added." Id. at 686, 272 ("These very circumstances occurred, as the . . . office moved twice during the course of the agreement, approximately one-half mile each time.").

Georgia courts applying the common law have found that a geographic restriction that cannot be determined until the employee is terminated is also unreasonable. Rollins Protective Servs. Co., 249 Ga. 138, 287 S.E.2d 546 (1982); Durham v. Stand-by Labor of Ga., 230 Ga. 558, 198 S.E.2d 145 (1973); see also Pratt, 253 Ga. App. 681, 560 S.E.2d 268 (covenant allowing employer to shift and expand proscribed territory during term of agreement unenforceable); Ceramic & Metal Coatings Corp., 242 Ga. App. 391, 529 S.E.2d 160 (2000) (covenant found unenforceable because employee could not determine the territory with any certainty at the

time he signed the agreement; agreement referred to "any territory added during the course of the Agreement"); Jarrett v. Hamilton, 179 Ga. App. 422, 346 S.E.2d 875 (1986); Ferrellgas Partners, Inc. v. Barrow, No. 4-03-CV-107 (WDO), 2006 WL 372602 (M.D. Ga. Feb. 16, 2006) (prohibition restricting former employee from doing business with or soliciting the business of any customer within seventy miles of any customer served by employer held unreasonable where former employer and company that merged into it were the second and seventh largest propane gas companies in the country, respectively, and customer base was constantly changing and expanding); Szomjassy v. OHM Corp., 132 F. Supp. 2d 1041, 1049 (N.D. Ga. 2001) (covenant contemplating territories added after employment ended overbroad). But see O.C.G.A. § 13-8-53(c)(2) (overturning these cases as to covenants scrutinized under the new legislation).

Notes:

(a) Covenant not to compete covering entire state is not *per se* prohibited. Barry v. Stanco Commc'ns. Prods., 243 Ga. 68, 252 S.E.2d 491 (1979).

(b) "Metro Atlanta, Georgia area" is not a sufficiently definite area on which to base a covenant against competition. See Hamrick v. Kelley, 260 Ga. 307, 392 S.E.2d 518 (1990) (even in sale of business context); see also Tucker v. Ebsco Indus., Inc., No. 1:06-CV-1376-GET, 2007 WL 397065, at *3 (N.D. Ga. Feb. 1, 2007) (where agreement restricting employee from competing in "library territory" does not adequately define term, territorial restriction is too vague to be enforceable). But see Reardigan v. Shaw Indus., Inc., 238 Ga. App. 142, 145, 518 S.E.2d 144, 147 (1999) (Atlanta Metropolitan Statistical Area as defined by the United States Office of Management and Budget is sufficiently definite territorial description).

(c) Covenant prohibiting competition within a fifty mile radius of any city in which the former employee did business is unreasonable. Crowe v. Manpower Temp. Servs., 256 Ga. 239, 240, 347 S.E.2d 560, 561 (1960).

(d) Where a city (as opposed to a metropolitan area) is

> designated as the center of the radius, the covenant will be enforced. The use of the word "radius" presupposes a circle, the center of which is the city identified. Keeley v. Cardiovascular Surgical Assocs., P.C., 236 Ga. App. 26, 29-30, 510 S.E.2d 880, 884-85 (1999).

In Darugar v. Hodges, 221 Ga. App. 227, 229, 471 S.E.2d 33, 36 (1996), the Court of Appeals held that a "restriction against doing business with any of an employer's potential customers located in a specific geographical area, without regard to whether the employee ever made contact with those prospects, is over broad and unreasonable." (citing Vortex Protective Serv., Inc. v. Dempsey, 218 Ga. App. 763, 463 S.E.2d 67 (1995)).

However, in Chaichimansour v. Pets are People Too, No. 2, Inc., 226 Ga. App. 69, 485 S.E.2d 248 (1997), the Court of Appeals expressly disapproved of the holdings in Darugar and Vortex to the extent they suggest that prohibitions on competition with respect to customers or potential customers beyond those with whom the employee dealt during his employment will always be unreasonable, even if in a specified and reasonable geographic area. In that case, the Court upheld a non-compete which contained a narrow, specific territorial restriction which was closely tied to where the employee actually worked for the employer even though it prohibited her from providing veterinary services to anyone within the territory without regard to whether she had contact with them when she was working for the employer. Id. at 71-72, 250.

Although later decisions confirm the disfavor upon which Darugar and Vortex are viewed, these conflicting decisions illustrate the risks associated with drafting a non-compete covenant which existed under the old law. Chaichimansour v. Pets are People Too, No. 2, Inc., 226 Ga. App. 69, 72-74, 485 S.E.2d 248, 251-52 (1997) (McMurray, J., dissenting) (arguing that the continuing viability of cases permitting covenants which prohibit post-employment solicitation of any customer of the employer located in a specific geographic area should be questioned).

"Vortex Protective Svc. v. Dempsey and Darugar v. Hodges confused [the distinctions between covenants not to compete and covenants not to solicit] and analyzed covenants not to compete under the criteria applicable to covenants not to

solicit. The cases focused on the failure of the noncompete covenants to apply only to clients with whom the employee had had contact, and on the inability of the employee to accept business from unsolicited clients. Such an analysis applies to covenants not to solicit, not to covenants not to compete. Chaichimansour v. Pets Are People Too, No. 2 subsequently overruled Darugar and Vortex, holding that a noncompete covenant could validly preclude 'competition with respect to clients with whom the employee had not had contact while working for the employer.' Chaichimansour held valid a covenant not to compete precluding the employee from working as a veterinarian in a limited territory, even though such necessarily prevented the employee from accepting unsolicited business." Habif, Arogeti& Wynne, P.C. v. Baggett, 231 Ga. App. 289, 296, 498 S.E.2d 346, 353 (1998) (footnotes omitted).

(b) Non-Solicitation Covenants

A non-solicitation clause in an employment contract that prohibits the solicitation of the employer's clients that the employee actually contacted for a business purpose while serving the employer can be enforceable notwithstanding the absence of an explicit geographical limitation. W.R. Grace & Co. v. Mouyal, 262 Ga. 464, 422 S.E.2d 529 (1992); Am. Software USA, Inc. v. Moore, 264 Ga. 480, 448 S.E.2d 206 (1994); see also Murphree v. Yancey Bros. Co., 311 Ga. App. 744, 716 S.E.2d 824 (2011) (affirming injunction enforcing non-solicitation covenant); Exceptional Mktg. Grp., Inc. v. Jones, 749 F. Supp. 2d 1352 (N.D. Ga. 2010) (finding that nonsolicitation covenant is valid and denying defendant's motion to dismiss).

Under the old law, a non-solicitation covenant could not prohibit an employee from soliciting any client of the employer unless the covenant has an express, reasonable territorial limitation. Hulcher Servs., Inc. v. R.J. Corman R.R. Co., L.L.C., 247 Ga. App. 486, 543 S.E.2d 461 (2001); Vortex Protective Serv., Inc. v. Dempsey, 218 Ga. App. 763, 463 S.E.2d 67 (1995).

A non-solicitation covenant which prohibits employees from performing services for any and all former customers/clients regardless of whether the former employees performed services for or had business relationships with those customers/clients is unreasonable and under the old law, likely unenforceable. Dougherty, McKinnon & Luby, P.C. v.

Greenwald, Denzik & Davis, P.C., 213 Ga. App. 891, 447 S.E.2d 94 (1994); Windsor-Douglas Assocs., Inc. v. Patterson, 179 Ga. App. 674, 347 S.E.2d 362 (1986); see also Crump Ins. Servs. v. All Risks, Ltd., 315 Ga. App. 490, 727 S.E.2d 131 (2012) (holding that restrictive covenants are unenforceable under the old law when they are not limited geographically, prohibit former employees from accepting certain customers for two years regardless of whether the employee had directly worked with the customers before, and toll the two-year time period during any breach); Global Link Logistics, Inc. v. Briles, 296 Ga. App. 175, 674 S.E.2d 52 (2009) (non-solicitation covenant restricting employee from soliciting any of former employer's customers or employees is unenforceable); Morgan Stanley DW, Inc. v. Frisby, 163 F. Supp. 2d 1371 (N.D. Ga. 2001) (finding non-solicit over broad because it prohibited employees from contacting not only clients that they serviced, but anyone whose names became known to them during their employment). But see Palmer & Cay of Ga., Inc. v. Lockton Cos., 280 Ga. 479, 629 S.E.2d 800 (2006) (non-solicitation covenant not rendered unenforceable by failure to include restriction on period of time during which employee served customers).

A non-solicitation covenant also had to be limited to those services provided by the employee for the employer with respect to the covered customers/clients. See Riddle v. Geo-Hydro Eng'rs, Inc., 254 Ga. App. 119, 561 S.E.2d 456 (2002) (finding nonsolicit that covered solicitation for any reason to be unenforceable). But see Palmer & Cay of Ga., Inc. v. Lockton Cos., 284 Ga. App. 196, 200, 643 S.E.2d 746, 749 (2007) (employees prohibited from selling, to current customers which the employees served during their employment, identical products or services, or products that are "competitive or potentially competitive," to those offered by the company during their employment).

A non-solicitation covenant which restricts the employee from contacting customers with whom the employee had contact and also restricts the employee from contacting customers about whom the employee had confidential and/or proprietary information without regard to whether the employee had contact with those customers was unenforceable. Trujillo v. Great S. Equip. Sales, LLC, 289 Ga. App. 474, 657 S.E.2d 581 (2008) (rejecting argument that non-solicitation covenant simply restated confidentiality clause and finding that provision impermissibly broadened class of customers employee could not solicit).

The Act maintains and codifies some of these common law rules for non-solicitation covenants. See O.C.G.A. § 13-8-53(b) ("Any reference to a prohibition against 'soliciting or attempting to solicit business from customers' or similar language shall be adequate for such purpose and narrowly construed to apply only to: (1) such of the employer's customers, including actively sought prospective customers, with whom the employee had material contact; and (2) products and services that are competitive with those provided by the employer's business."); see also PointeNorth Ins. Grp. v. Zander, No. 1:11-CV-3262-RWS, 2011 WL 4601028 (N.D. Ga. Sept. 30, 2011) (blue penciling over broad customer non-solicitation covenant in May 11, 2011 employment agreement to apply only to customers that the former employee contacted or assisted with insurance). However, the Act also rejects some of these rules. For example, the Act effectively overrules Trujillo by allowing a non-solicitation covenant to apply to a customer about whom the employee obtained confidential information. See O.C.G.A. § 13-8-51(10) (broadened definition of "Material Contact").

2. Legitimate Business Interest

Notwithstanding the fact that the specific restraints imposed on the employee had to be tailored to the business interests the employer was seeking to protect, the employer also had to, as a threshold matter, have some legitimate business interest in imposing any restrictions on its former employee. Thus, under the old law, where a professional corporation had ceased to be in existence by operation of law, the corporation had no legitimate business interest in enforcing former employee's covenant not to compete. See Broome v. Ginsberg, 159 Ga. App. 202, 283 S.E.2d 1 (1980); see also O.C.G.A. § 13-8-55 (under new legislation, an employer seeking to enforce a restrictive covenant must plead and prove the existence of one or more legitimate business interests justifying the covenant).

3. Current and Prospective Customers

Non-solicitation covenants applying to "prospective" customers or clients have been upheld as reasonable under the old law. Covington v. D.L. Pimper Grp., Inc., 248 Ga. App. 265, 269, 546 S.E.2d 37, 41 (2001) (citing W.R. Grace & Co. v. Mouyal, 262 Ga. 464, 422 S.E.2d 529 (1992)). The new law also expressly permits employers to restrict solicitation of prospective customers.

O.C.G.A. § 13-8-53(b).

Under the old law, mere "cold calls" or sales calls in which no business relationship was developed may or may not be considered "contact" within the meaning of a non-solicitation covenant. See, e.g., Paul Robinson, Inc. v. Haege, 218 Ga. App. 578, 579, 462 S.E.2d 396, 398 (1995) (upholding one year covenant barring salesperson from contacting customers upon whom the salesperson had called within salesperson's territory for purpose of selling products competitive with employer and rejecting employee's argument that the same was over broad as it related to calls which did not lead to a customer relationship).

4. "Contact" Between Employee and Customer

Under the old law, "contact" has been broadly defined as "interaction between employee and the customer/client/account which takes place in an effort to further the business relationship." W.R. Grace & Co. v. Mouyal, 262 Ga. 464, 467, n.3, 422 S.E.2d 529, 533, n.3 (1992) (also noting that protectable employer's legitimate interest was "in keeping the employee from taking advantage of the goodwill generated during his employment with the employer to lure employer customers away"); see Augusta Eye Center, P.C. v. Duplessie, 234 Ga. App. 226, 226, 506 S.E.2d 242, 244 (1998) (agreement defined "material contact" as existing between employee and patients or potential patients "if interaction took place between them in an effort to further a business relationship").

In Wolff v. Protégé Sys., Inc., 234 Ga. App. 251, 506 S.E.2d 429 (1998), the Court of Appeals held that a covenant restricting the solicitation of customers with whom the employee "became acquainted" was overbroad without a territorial restriction. Similarly, in Dougherty, McKinnon & Luby, P.C. v. Greenwald, Denzik & Davis, P.C., 213 Ga. App. 891, 447 S.E.2d 94 (1994), the Court of Appeals explained the legitimate reasons for which an employer is permitted to restrain an employee from utilizing its contacts with clients. The Court of Appeals held that "[b]ecause of the nature of the professional-client relationship, [employees] would have gained some degree of trust, confidence, and rapport with clients for whom [they] performed services . . . [and] former employees have no unfair competitive advantage regarding customers with whom they did not work and had no business relationship while employed . . . ." Id. at 894, 96; see also Capricorn Sys., Inc. v. Pednekar, 248 Ga. App. 424, 427, 546 S.E.2d 554, 557 (2001) (nonsolicitation provision was overbroad where it was not limited to those relationships developed during employee's employment).

The new law includes a definition of "material contact" that is significantly broader than the definition of contact under the old law. O.C.G.A. § 13-8-51(10).

5. Acceptance of Unsolicited Business

A covenant not to compete by definition may preclude the employee from accepting related business (whether solicited or not) from any clients (whether previously contacted by him or not) if the employee is officed in, or is to perform the restricted activities in, the forbidden territory. Habif, Arogeti& Wynne, P.C. v. Baggett, 231 Ga. App. 289, 295, 498 S.E.2d 346, 353 (1998).

Under the old common law, absent a non-competition covenant, the employer could not prohibit a former employee from merely accepting business from the former employer's customers without any prior solicitation by the former employee. The case law held that nonsolicitation covenants can only restrict affirmative action by former employees. Singer v. Habif, Arogeti & Wynne, P.C., 250 Ga. 376, 297 S.E.2d 473 (1982); Burson v. Milton Hall Surgical Assocs., LLC, 343 Ga. App. 159, 164, 806 S.E.2d 239, 244 (Ga. App. 2017) (invaliding non-solicitation covenant which prohibited "communicating" with patients because the provision could cover unsolicited communications); Vulcan Steel Structures, Inc. v. McCarty, 329 Ga. App. 220, 764 S.E.2d 458 (2014) (same); Fine v. Commc'n Trends, Inc., 305 Ga. App. 298, 699 S.E.2d 623 (2010); Hilb, Rogal, & Hamilton Co. of Atlanta, Inc. v. Holley, 284 Ga. App. 591, 596, 644 S.E.2d 862, 866 (2007) (restrictive covenant precluding employee from "accepting an entreaty" from known or prospective customers is overly broad and unenforceable); Waldeck v. Curtis 1000, Inc., 261 Ga. App. 590, 592, 583 S.E.2d 266, 269 (2003) ("In recent years, the law has become quite clear: solicitation requires some type of affirmative action; therefore, a non-solicitation provision may not contain a bar on the acceptance of business from unsolicited clients."); Pregler v. C&Z, Inc., 259 Ga. App. 149, 575 S.E.2d 915 (2003); Akron Pest Control, Inc. v. Radar Exterminating Co., Inc., 216 Ga. App. 495, 455 S.E.2d 601 (1995) (attempting to define solicitation); Dougherty, McKinnon & Luby, P.C. v. Greenwald, Denzik & Davis, P.C., 213 Ga. App. 891, 447 S.E.2d 94 (1994); Fisher, 208 Ga. App. 282, 430 S.E.2d 166 (1993). But see Am. Gen. Life & Accident Ins. Co. v. Fisher, 208 Ga. App. 282, 284, 430 S.E.2d 166, 169 (1993) (Beasly, J. concurring) (submitting that covenant against acceptance, as well as solicitation, should be considered reasonable and upheld); Merrill Lynch, Pierce, Fenner & Smith, Inc. v. de Liniere, 572 F. Supp 246,

248 (N.D. Ga. 1983) (the force of Singer and its dicta is unclear because of the vote among the justices; the opinion represents a view of only three of the seven justices); Covington v. D.L. Pimper Grp., Inc., 248 Ga. App. 265, 546 S.E.2d 37 (2001) (upholding non-solicitation provision which prohibited "communication with" clients of former employer and distinguishing Singer v. Habif, Arogeti & Wynne, P.C. as inapposite).

The Act does not seem to have changed this rule. Thus, the cases on this issue which pre-date the Act appear to remain good law and employers may not prohibit their former employees from accepting unsolicited business. That said, if an employer included a prohibition on the acceptance of unsolicited business in a non-solicitation covenant, presumably a court could blue pencil out this portion of the prohibition if it found it to be overbroad.

6. Competitive Products or Services

Under the old law, an agreement needed to provide some description of products or services which are the subject of the covenant; the covenant could not merely state that all products or services provided by the employer are restricted unless the employee was involved in providing all such products or services. See also Palmer & Cay of Ga., Inc. v. Lockton Cos., 284 Ga. App. 196, 643 S.E.2d 746 (2007) (employees prohibited from selling to current customers which the employees served during their employment, identical products or services, as well as products that are "competitive or potentially competitive", to those offered by the company during their employment). But see O.C.G.A. § 13-8-53(c)(2) ("Activities, products or services shall be considered sufficiently described if a reference to the activities, products, or services is provided and qualified by the phrase 'of the type conducted, authorized, offered or provided within two years prior termination' or similar language containing the same or a lesser time period.").

7. Writing Requirement

A post-termination covenant prohibiting competition must be in writing. Pope v. Kem Mfg. Corp., 249 Ga. 868, 295 S.E.2d 290 (1982); see also Holsapple v. Smith, 267 Ga. App. 17, 20-21, 599 S.E.2d 28, 32 (2004) (covenant found to be ancillary to sale of business as opposed to employment because only written agreement was asset purchase agreement and employment agreement was never reduced to writing).

8. Look Back Requirement

In Palmer & Cay of Ga., Inc. v. Lockton Cos., 280 Ga. 479, 629 S.E.2d 800 (2006), the Supreme Court significantly changed Georgia law when it held that a non-solicitation covenant which did not contain a look back provision was enforceable. The scope of the covenants at issue included customers whom the employees had served during their respective terms of employment without any further limitation. Id. at 479, 629 S.E.2d at 802. The three employees had served terms of five, ten, and eleven years. Id. at 485, 629 S.E.2d at 805. Thus, under the covenants the employees were precluded from soliciting any customer whom they had served during the entire periods of their employment. Id. at 484, 629 S.E.2d at 804. The Supreme Court noted that "the critical factor is whether the former employee ever served the customer, not the length of time since he or she may have done so." Id. at 480, 629 S.E.2d at 802.

In perhaps an important subtlety in what is a very pro-employer decision, the Supreme Court did note that the covenants' terms applied to "customers," not "former customers." Id. at 482, 629 S.E.2d at 803. Considering that the covenants did not apply to the solicitation of "former customers," this result is perhaps more easily reconcilable with what are typically understood as legitimate "protectible employer interests." Id. Thus, the Court's holding does not stand for the proposition that a covenant precluding solicitation of former customers is enforceable. Based on the terms of the agreements in this case and the Court's construction of those terms, only "current" customers were included.

That being said, this decision was, to some degree, a departure from the pro-employee climate of Georgia's old restrictive covenant law. See id. (Hines, J., dissenting) ("The business climate in this state is ill served by, in essence, penalizing the long-term service of an employee."); Gill v. Poe & Brown of Ga., Inc., 241 Ga. App. 580, 524 S.E.2d 328 (1999) (striking covenant which applied to customers on a list created over four years before employee was terminated). In Gill, the Court noted that the fact that the employer may have already lost the business of some of the customers at the time of the employee's termination illustrates the problems created by a covenant that forbids an employee from soliciting a stagnant group of customers, since the employer has no legitimate business interest in preventing solicitation of former customers who may have severed their relationship with the employer years before the employee's termination. Id.; see also Wachovia Ins. Servs., Inc. v. Fallon, 299 Ga. App. 440, 443-44, 682 S.E.2d 657, 661 (2009)

(comparing Gill and Palmer & Cay and affirming trial court's finding that non-solicitation covenant was overly broad because it can be read to preclude employee from soliciting customers who had already severed their relationship with the employer); Orkin Exterminating Co. v. Walker, 251 Ga. 536, 538, 307 S.E.2d 914, 916-17 (1983) (covenant that does not appropriately limit the time frame to determine the customers to which the covenant applies is unenforceable); Smith Adcock & Co. v. Rosenbohm, 238 Ga. App. 281, 284-85, 518 S.E.2d 708 (1999) (finding covenant to be unenforceable because it applied to all "former company clients"); Variable Annuity Life Ins. Co. v. Joiner, 454 F. Supp. 2d 1297, 1303 (S.D. Ga. 2006) (nonsolicitation covenant ancillary to employment contract which restricts employee from soliciting any customers who were within the employees' territory and assigned to them at any time during the one-year period preceding their termination for one year after the termination of their employment is reasonable).

Thus, for non-solicitation covenants governed by the old law, Palmer & Cay leaves some uncertainty as to whether a look-back requirement still exists for determining whether there is a "current" relationship between a customer and employee.

B. Payment of Royalty in Event of Violation of Covenant

In the event the contract requires the employee to pay a royalty to the employer for the privilege of competing or soliciting customer or clients, it will be treated like a covenant not to compete. In Smith Adcock & Co. v. Rosenbohm, 238 Ga. App. 281, 518 S.E.2d 708 (1999), the Court found that a provision requiring an employee of an accounting firm who terminated his association with the firm to pay a royalty on gross fees collected from clients to whom he continued to render public accounting services would be treated like a covenant not to compete as it had the effect of lessening competition.

C. Forfeiture of Post-termination Compensation

In A.L. Williams & Assocs. v. Faircloth, 259 Ga. 767, 768, 386 S.E.2d 151, 153 (1989), the Georgia Supreme Court held that "[i]t would be paradoxical to strike down a covenant as invalid, and at the same time uphold a forfeiture that is conditioned upon a violation of that very covenant. Hence, a forfeiture provision that is conditioned expressly upon an invalid covenant must be invalid *in se*." However, in that case, the contract both proscribed competition and prescribed forfeiture. Id., at fn. 1. Thus, the Court explained, a provision of a contract which imposes as a condition to the recovery of benefits under a deferred compensation plan that the employee refrain from engaging in competitive employment is not violative of public policy as being in restraint of trade (and therefore not

subject to the same requirements as a restrictive covenant) if the provision does not also proscribe competitive activity. Id., fn. 1. Accord Sheppard v. Columbus Packaging Co., 146 Ga. App. 202, 245 S.E.2d 887 (1978) (citing Collins v. Storer Broad. Co., 217 Ga. 41, 120 S.E.2d 764 (1961) and Brown Stove Works v. Kimsey, 119 Ga. App. 453, 167 S.E.2d 693 (1969)); see also Stannard v. Allegis Grp., Inc., No. 1:08-cv-3357-TCB, 2009 WL 1309751 (N.D. Ga. April 27, 2009).

Therefore, if an agreement does not purport to obligate an employee to refrain from competing, but rather obligates the employer to pay a specified amount of money to the employee in the event the employee chooses not to engage in such competition, such agreement will not be equated with a restrictive covenant executed in connection with an employment contract purporting to prohibit the employee from competing with the employer following the termination of the employment relationship. See Dronzek v. Vaughn, 191 Ga. App. 468, 382 S.E.2d 188 (1989). In other words, if the restriction in the contract does not preclude the employee from engaging in competitive activity, but simply provides for the loss of the rights or privileges if he does, it is not in restraint of trade. See Nat'l Consultants, Inc. v. Burt, 186 Ga. App. 27, 366 S.E.2d 344 (1988); see also Hopkins v. Garner & Glover Co., 233 Ga. App. 264, 270, 504 S.E.2d 78, 83 (1998) ("[W]ritten contract could have expressly provided for loss of rights and privileges by forfeiture for engaging in competitive employment . . . .").

However, a contract providing for forfeiture of deferred compensation if the employee engages in "any other employment" is over broad and unenforceable. See Nat'l Consultants, Inc. v. Burt, 186 Ga. App. 27, 33, 366 S.E.2d 344, 350 (1988). Nat'l Consultants involved forfeiture provisions in the contracts of two insurance agents. Under their contracts, they were entitled to receive renewal commissions for as many years following termination of their employment as they had been with the company. They later executed addenda that specified the period of time for which each would receive renewal commissions. These addenda further provided that they would receive the renewal commissions as long as they did "not take any other employment." The Court of Appeals found that the conditional forfeiture of benefits provided for in the addenda was significantly broader than the provision upheld in Sheppard because it was not limited to *competitive* employment. Because this provision was an "ultrabroad" forfeiture provision that raised serious public policy implications, the Court of Appeals struck it down.

In Albany Bone & Joint Clinic, P.C. v. Hajek, 272 Ga. App. 464, 468, 612 S.E.2d 509, 513 (2005), a provision in the bylaws of a medical practice required departing member of the practice to accept a reduced price for his interest if he engaged in competition with the practice following his departure. The Court of Appeals held this provision was not a restraint of

trade where "one who leaves to work for a competitor is not singled out for disparate treatment," and the provision applied for departures for any reason, including death, disability, or retirement. The Court noted that the provision did not allow the practice to prohibit any business activities by the departing physician after employment and the practice could not sue the departing physician for any competitive business activity. The provision at issue did not purport to limit where the departing physician could practice medicine or with whom, what information he must keep confidential, or whom he may or may not recruit to work with him. It also did not purport to prevent him from soliciting his former patients. It did not restrain his legal ability to compete in any way and it did not "prejudice the interests of the public in a free and competitive market." Rather, it governed how the physician and the other shareholders were to be compensated for their shares in the event they cease active participation in the professional corporation. See also Physician Specialists in Anesthesia, P.C. v. MacNeill, 246 Ga. App. 398, 539 S.E.2d 216 (2000) (distinguishing liquidated damages provision operative upon breach from forfeiture of deferred compensation); Milhollin v. Salomon Smith Barney, Inc., 272 Ga. App. 267, 612 S.E.2d 72 (2005) (where employee lost salary under employer's benefit plan by leaving it was not improper forfeiture or covenant against competition because plan did not restrict employee from working elsewhere and continued employment was instead a condition precedent to receipt of benefits).

While these cases were decided under the old law, they remain relevant as drafters must decide whether to have a deferred compensation plan or forfeiture provision comply with the new statute, or whether they can disregard the requirements of the new statute because the applicable plan or forfeiture provision is not a restrictive covenant.

D. Employees' Agreements with Prior Employers

Employers considering hiring an employee should inquire whether the potential employee is subject to any restrictive covenants of a previous employer. The employer may be held liable for tortious interference with contractual relations if it induces or encourages former employees to breach valid post-employment restrictions. Carroll Anesthesia Assocs., Inc. v. Anesthcare, Inc., 234 Ga. App. 646, 507 S.E.2d 829 (1998).

If a potential employee says he does not have a non-compete, the employer should have the employee acknowledge the same in an offer letter or employment agreement, and also confirm that he has no confidential information or trade secrets of a former employer in his personal possession and will not bring any such information to his new employer.

E. Restrictive Covenants that Apply During the Term of an Agreement

Georgia law was not always clear as to whether duty-of-loyalty provisions which applied during the term of employment were subject to the same standards as post-termination restrictive covenants. However, in Atlanta Bread Co. Int'l v. Lupton-Smith, 287 Ga. 587, 679 S.E.2d 722 (2009), the Georgia Supreme Court, analyzing covenants in a franchise agreement governed by the old law, confirmed that restrictive covenants which apply during the term of an agreement are subject to the same reasonableness standards as post-termination restrictive covenants. See also Early v. MiMedx Grp., Inc., 330 Ga. App. 652, 768 S.E.2d 823 (2015), cert. denied (May 11, 2015) (invalidating provision requiring consultant to devote her full working time during the period of her consultancy); Matthew Focht Enters., Inc. v. Lepore, No. 1:12-cv-04479-WSD, 2013 WL 4806938 (N.D. Ga. Sept. 9, 2013) (finding that covenants which apply during the term of an independent contractor agreement were invalid).

Under Georgia's new restrictive covenants law, covenants which restrict competition during the term of the relationship are permitted as long as such restrictions are reasonable in time, geographic area, and scope of prohibited activities. O.C.G.A. § 13-8-53(a); see also O.C.G.A. § 13-8-56(4) ("Any restriction that operates during the term of an employment relationship, agency relationship, independent contractor relationship, partnership, franchise, distributorship, license, ownership of a stake in a business entity, or other ongoing business relationship shall not be considered unreasonable because it lacks any specific limitation upon scope of activity, duration, or geographic area so long as it promotes or protects the purpose or subject matter of the agreement or relationship or deters any potential conflict of interest"). While employers may only restrict competition after the term of an employment relationship by employees who meet certain criteria specified in the statute, it appears employers may restrict competition during the term of an employment relationship by *all* employees. O.C.G.A. § 13-8-53(a).

F. Liquidated Damages

Liquidated damages provisions are enforceable as part of an agreement with restrictive covenants subject to the general law relating to such contractual provisions. Habif, Arogeti & Wynne, P.C. v. Baggett, 231 Ga. App. 289, 498 S.E.2d 346 (1998).; Dominy v. Nat'l Emergency Servs., Inc., 215 Ga. App. 537, 451 S.E.2d 472 (1994); see also Physician Specialists in Anesthesia, P.C. v. MacNeill, 246 Ga. App. 398, 539 S.E.2d 216 (2000).

Liquidated damages are not favored when they act as a penalty, because they can be abused to coerce compliance with abusive or void non-competition provisions. Capricorn Sys., Inc. v. Pednekar, 248 Ga. App.

424, 546 S.E.2d 554 (2001).

G. Severability

Historically, Georgia courts have refused to "blue pencil" an over broad covenant ancillary to an employment agreement.

As discussed above, under Georgia's new restrictive covenants law, courts may judicially modify overly broad restrictive covenants. O.C.G.A. § 13-8-54. There are not yet any reported decisions from the Georgia appellate courts specifically addressing whether the definitions of "modify" and "modification" in the new law allow judges to rewrite covenants or merely blue-pencil them. O.C.G.A. § 13-8-51(11)-(12). In the first published decision in which a judge used the new "blue pencil," Judge Richard Story of the Northern District of Georgia modified a non-solicitation covenant to render it enforceable. PointeNorth Ins. Grp. v. Zander, No. 1:11-CV-3262-RWS, 2011 WL 4601028 (N.D. Ga. Sept. 30, 2011). In a more recent decision, Judge Thomas Thrash held that the term "modify" in O.C.G.A. section 13-8-53(d) does not grant courts the power to write in or rewrite terms to an otherwise unenforceable restrictive covenant. LifeBrite Labs., LLC v. Cooksey, No. 1:15-CV-4309-TWT, 2016 WL 7840217 (N.D. Ga. Dec. 9, 2016). Rather, according to Judge Thrash, trial courts may strike unreasonable restrictions and may narrow over-broad territorial restrictions, but they may not completely reform and rewrite contracts by supplying new and material terms. Id.

Under the case law applicable to covenants entered into prior to the new legislation's effective date, if any portion of a covenant fails, the entire covenant must fail. Am. Gen. Life & Accident Ins. Co. v. Fisher, 208 Ga. App. 282, 430 S.E.2d 166 (1993). Regardless of whether they are individually or collectively categorized as non-solicit or non-compete covenants, if one is unenforceable, then they are all unenforceable. Advance Tech. Consultants, Inc. v. RoadTrac, LLC, 250 Ga. App. 317, 551 S.E.2d 735 (2001) **(**overruling Wright v. Power Indus. Consultants, Inc., 234 Ga. App. 833, 834, 508 S.E.2d 191, 193 (1998) and Wolff v. Protégé Sys., Inc., 234 Ga. App. 251, 506 S.E.2d 429 (1998)); see also Jenkins Brick Co. v. Bremer, 321 F.3d 1366, 1369, n.2 (11th Cir. 2003) ("When Georgia courts find a provision offensive, the entire non-compete agreement is void."); Dent Wizard Int'l Corp., 272 Ga. App. 553, 556, 612 S.E.2d 873, 877 (2005) ("Georgia does not follow the 'blue pencil' doctrine of severability in construing employment contracts. Therefore, because one restrictive covenant in Brown's agreement is unenforceable, they are all unenforceable."); Johnstone v. Tom's Amusement Co., 228 Ga. App. 296, 300, 491 S.E.2d 394, 399 (1998) ("Blue-penciling not being available, the invalid nonsolicit provision necessarily invalidates the noncompete provision, and the noncompete provision is unenforceable on this ground alone."); Ward v. Process Control Corp., 247 Ga. 583, 584, 277 S.E.2d 671,

672 (1981) (if any covenant not to compete within a given employment contract is unreasonable in time, territory, or prohibited business activity, then all covenants not to compete within same contract are unenforceable; both the covenant not to solicit and the covenant not to compete are covenants not to compete for purposes of applying this rule). Compare Physician Specialists in Anesthesia, P.C. v. MacNeill, 246 Ga. App. 398, 539 S.E.2d 216 (2000) (holding that in middle scrutiny case an unenforceable non-compete did not void a non-solicit in the same agreement), with Donovan v. Hobbs Grp., LLC, 181 Fed. Appx. 782, 783 (11th Cir. 2006) (even assuming "sale of business" scrutiny applies, blue pencil cannot rewrite the covenants and insert clauses and provide sufficient limitations to render restrictions reasonable).

With the presence of a severability clause, however, confidentiality and nonrecruitment covenants within the same agreement as an unenforceable non-compete or non-solicitation covenant may be severable and enforceable on their own. See, e.g., Mathis v. Orkin Exterminating Co., 254 Ga. App. 335, 336, 562 S.E.2d 213, 214 (2002) (courts "analyze anti-piracy clauses in employment agreements separately from nonsolicit and noncompete clauses"); Sunstates Refrigerated Servs., Inc. v. Griffin, 215 Ga. App. 61, 449 S.E.2d 858 (1994); U3S Corp. of Am. v. Parker, 202 Ga. App. 374, 414 S.E.2d 513 (1991) (non-solicitation covenant could be enforced separately from unenforceable non-disclosure covenant); Kem Mfg. Corp. v. Sant, 182 Ga. App. 135, 355 S.E.2d 437 (1987); Johnstone v. Tom's Amusement Co., 228 Ga. App. 296, 491 S.E.2d 394 (1998).

With the addition of a severability clause, an unenforceable liquidated damages provision will be severed from the remainder of the agreement and should not invalidate otherwise enforceable restrictive covenants. Capricorn Sys., Inc. v. Pednekar, 248 Ga. App. 424, 546 S.E.2d 554 (2001); see also Vegesina v. Allied Informatics, Inc., 257 Ga. App. 693, 695, 572 S.E.2d 51, 53 (2002) (finding intent that contract be severable, in the absence of a severability clause, where "employment agreement contained multiple promises for [employee] to do or refrain from doing several things that were distinct and separate from the unenforceable liquidated damages provisions of the contract").

The invalidity of a restrictive covenant in an employment contract may not render an arbitration clause of a contract unenforceable under the Federal Arbitration Act where the arbitration agreement itself is not infirm. In other words, if an arbitration clause is valid and the dispute invokes the Federal Arbitration Act, the court should enforce it, even if the underlying contract might be declared invalid. See Hydrick v. Mgmt. Recruiters Int'l, Inc., 738 F. Supp. 1434, 1436 (N.D. Ga. 1990). But see Global Link Logistics, Inc. v. Briles, 296 Ga. App. 175, 674 S.E.2d 52 (2009) (where arbitration provision in employment agreement provides that either party may seek interim relief in court prior to the arbitrators having been

selected, trial court did not err in declaring restrictive covenants invalid).

However, depending on the language of the employment agreement and the parties' conduct, the trial court may determine whether the covenants are enforceable and thus, whether the covenants are subject to arbitration. In BellSouth Corp. v. Forsee, 265 Ga. App. 589, 596, 595 S.E.2d 99, 106 (2004), the Georgia Court of Appeals affirmed the trial court's entry of a "definitive ruling as to [a covenant's] unenforceability" by virtue of an interlocutory injunction and the trial court's corresponding determination that the invalid covenant should be severed from the agreement and arbitration provision, such that the trial court, not the arbitrator, determined whether the covenants were enforceable. But see Nitro-Lift Technologies, L.L.C. v. Howard, -- U.S. --, 133 S. Ct. 500 (2012).

H. Tolling

Absent an express provision to the contrary, the duration of a covenant is not tolled during the course of litigation. Coffee Sys. of Atlanta v. Fox, 227 Ga. 602, 182 S.E.2d 109 (1971); Hogan Mgmts. Servs., P.C. v. Martino, 242 Ga. App. 791, 530 S.E.2d 508 (2000).

A provision tolling the running of the time period of the covenant during the pendency of litigation, including all appeals, is enforceable. Paul Robinson, Inc. v. Haege, 218 Ga. App. 578, 578, 462 S.E.2d 396, 397 (1995) (enforceable tolling provision that read: "[I]n the event the enforceability of any of the terms of the Agreement shall be challenged in Court and [employee] is not enjoined from breaching any of the protective covenants, then if a court of competent jurisdiction finds that the challenged protective covenant is enforceable, the time periods ... shall be deemed tolled upon the filing of the lawsuit challenging the enforceability of this Agreement until the dispute is finally unsolved *[sic]* and all periods of appeal have expired." (second alteration in original)); see also Wesley-Jessen, Inc. v. Armento, 519 F. Supp. 1352, 1358 (N.D. Ga. 1981); Coffee Sys. of Atlanta v. Fox, 227 Ga. 602, 182 S.E.2d 109 (1971).

Under the old law, tolling of the period of the restraint while the former employee is in violation of the covenant is invalid in that it potentially extends the duration of the covenant without limit. ALW Mktg. Corp. v. McKinney, 205 Ga. App. 184, 421 S.E.2d 565 (1992); ALW Mktg. Corp. v. Hill, 205 Ga. App. 194, 422 S.E.2d 9 (1992); see also Gandolfo's Deli Boys, LLC v. Holman, 490 F. Supp. 2d 1353, 1359 (N.D. Ga. 2007) (tolling provision unenforceable for want of a definite time limitation); Gynecologic Oncology, P.C. v. Weiser, 212 Ga. App. 858, 443 S.E.2d 526 (1994) (unenforceable tolling provision not severable from the remainder of the covenant rendering covenant unenforceable in its entirety).

The Act does not change this rule. However, under the new law, presumably an unenforceable tolling provision is severable and could be blue-penciled.

I. Consideration

The prospect of employment or continued employment is adequate consideration for restrictive covenants. Thomas v. Coastal Indus. Servs., 214 Ga. 832, 108 S.E.2d 328 (1959); Baker v. Nat'l Credit Ass'n, 211 Ga. 635, 88 S.E.2d 19 (1955); Griffin v. Vandergriff, 205 Ga. 288, 53 S.E.2d 345 (1949). But see Glisson v. Global Sec. Servs., LLC, 287 Ga. App. 640, 653 S.E.2d 85 (2007) (agreement containing restrictive covenants executed while employee was under two-year employment contract was not supported by consideration).

The Act does not appear to change this rule.

J. Employer's Forfeiture of Enforcement of Covenant by Prior Breach of Agreement

An employer's breach of a termination provision in an employment contract could preclude the employer from enforcing a covenant not to compete in the agreement if the agreement does not contain severability language. See Marcre Sales Corp. v. Jetter, 223 Ga. App. 70, 476 S.E.2d 840 (1996) (citing ESAB Distrib. S.E. v. Flamex Indus., 243 Ga. 355, 254 S.E.2d 328 (1979)); Wake Broadcasters v. Crawford, 215 Ga. 862, 114 S.E.2d 26 (1960).

K. Employer's Recovery of Consideration Paid in Exchange for Unenforceable Restrictive Covenants

An employer cannot recover consideration paid to an employee in exchange for an unenforceable restrictive covenant through equitable remedies. Hilb, Rogal & Hamilton Co. of Atlanta v. Holley, 295 Ga. App. 54, 55, 670 S.E.2d 874, 876 (2008)

(trial court properly directed a verdict as to employer's unjust enrichment claim seeking recovery of consideration paid in exchange for unenforceable covenant which restricted employee from "accepting an entreaty" from any known or prospective customers).

L. Requirement of Notice of Termination by Employee

A contractual duty to provide a specified termination notice to the employer under a contract has been found to not constitute a restrictive covenant and to not constitute a covenant that falls along with void restrictive covenants in contract. The failure to comply with a contractual provision requiring a specified prior notice of termination may give rise to a claim for damages. Capricorn Sys., Inc. v. Pednekar, 248 Ga. App. 424, 427, 546 S.E.2d 554, 558 (2001).

M. Choice of Law and Choice of Forum Issues

1. Choice of Law

In 2003, the Georgia Supreme Court, in answering a certified question from the United States Court of Appeals for the Eleventh Circuit, reaffirmed that the law of the jurisdiction chosen by the parties to govern their contractual rights will not be applied by Georgia courts where application of the chosen law contravenes the policy of, or will be prejudicial to the interests of, the State of Georgia. See Convergys Corp. v. Keener, 276 Ga. 808, 809, 582 S.E.2d 84, 85 (2003) (rejecting "materially greater interest" test set forth in Restatement (Second) of Conflicts, § 187(2) and finding that Bryan v. Hall Chem., 993 F.2d 831 (11th Cir. 1993), and Nordson Corp. v. Plasschaert, 674 F.2d 1371 (11th Cir. 1982), were "erroneous"). Therefore, the chosen law of another state in an employment agreement will not be applied by a Georgia court to uphold the restrictive covenants if they violate Georgia law. See Nasco, Inc. v. Gimbert, 239 Ga. 675, 238 S.E.2d 368 (1977) (ignoring choice of law provision specifying the application of Tennessee law and applying Georgia law); Hostetler v. Answerthink, Inc., 267 Ga. App. 325, 328-29, 599 S.E.2d 271, 274-75 (2004); Hulcher Servs., Inc. v. R.J. Corman R.R. Co., L.L.C., 247 Ga. App. 486, 543 S.E.2d 461 (2001); Wolff v. Protégé Sys., Inc., 234 Ga. App. 251, 506 S.E.2d 429 (1998); Enron Capital & Trade Res. v. Pokalsky, 227 Ga. App. 727, 730, 490 S.E.2d 136, 139 (1997); see also Manuel v. Convergys Corp., 430 F.3d 1132, 1137 (11th Cir. 2005) (applying Georgia's choice of law rules as set forth in Keener); Keener v. Convergys Corp., 342 F.3d 1264 (11th Cir. 2003); Dothan Aviation Corp. v. Miller, 620 F.2d 504 (5th Cir. 1980); Mktg. & Research Counselors, Inc. v. Booth, 601 F. Supp. 615 (N.D. Ga. 1985).

While under the new law and constitutional amendment Georgia's current public policy favors enforcement of restrictive covenants, it appears courts will still apply Georgia's old public policy to determine the enforceability of choice of law provisions in employment agreements entered into prior to the effective date of the new law. LaPolla Indus., Inc. v. Hess, 325 Ga. App. 256, 265-66, 750 S.E.2d 467, 475-76 (2013) (disregarding Texas

choice of law provision in agreement signed before the effective date of the new law); Carson v. Obor Holding Co., 318 Ga. App. 645, 653-54, 734 S.E.2d 477, 484-85 (2012) (disregarding Florida choice of law provision in agreement signed before the effective date of the new law); see also Boone v. Corestaff Support Servs., Inc., 805 F. Supp. 2d 1362, 1369 (N.D. Ga. 2011) (finding that court should ignore Delaware choice of law provision in 2008 agreement and should apply Georgia law); Becham v. Synthes (U.S.A.), No. 5:11-CV-73 (MTT), 2011 WL 4102816, at *6 (M.D. Ga. Sept. 14, 2011) (disregarding Pennsylvania choice of law provision in employment agreement entered into in 2000 where Pennsylvania law contravenes Georgia's old public policy); see also Becham v. Synthes (U.S.A), 482 Fed. Appx. 387 (11th Cir. 2012); Hix v. Aon Risk Servs. S., Inc., No. 1:11-CV-3141-RWS, 2011 WL 5870059, at *3 (N.D. Ga. Nov. 22, 2011) ("[I]t is well settled that courts in Georgia apply Georgia law to determine the validity of restrictive covenants in a contract, even if the contract has a choice-of-law provision requiring application of foreign law."). But see Viking Group, Inc. v. Pickvet, Nos. 1:17-cv-103, 1:17-cv-116, 2017 U.S. Dist. LEXIS 67207 (W.D. Mich. May 3, 2017) (disagreeing with Boone and concluding that Sixth Circuit precedent requires applying Georgia's current public policy in analyzing whether to enforce a Michigan choice of law provision).

2. Choice of Forum

Historically, the Georgia courts viewed choice of forum provisions differently. They enforced choice of forum or exclusive jurisdiction provisions, absent case-specific evidence that enforcement of the foreign forum selection clause violates the public policy of Georgia. See Iero v. Mohawk Finishing Prods., Inc., 243 Ga. App. 670, 534 S.E.2d 136 (2000) (in declaratory judgment action on non-competition and non-disclosure covenants, contractual clause selecting New York court as exclusive forum for any dispute arising out of agreement is enforceable, since there was no manifest disparity in bargaining position, no fraud or overreaching in procurement of contract, and enforcement does not violate public policy); Rode v. St. Jude Med., S.C., Inc., No. 1:06-cv-02448-WSD, 2006 WL 3762065 (N.D. Ga. Dec. 20, 2006) (choice of forum provision upheld where there were no contentions of fraud, duress, or misrepresentation during contract formation; no intervening or unexpected occurrences that frustrated the purpose of the contract; and no proof that a Minnesota court will apply Minnesota law, rather than Georgia law). See also Hasty v. St. Jude Med. S.C. Inc., No. 7:06-cv-102(HL), 2007 WL 1428733 (M.D. Ga. May 11, 2007) (upholding choice of forum provision).

However, in 2011, in Bunker Hill Int'l, Ltd. v. Nationsbuilder Ins. Servs., 309 Ga. App. 503, 710 S.E.2d 662 (2011), the Georgia Court of Appeals found that an Illinois forum selection provision was void where the plaintiff demonstrated that the non-compete covenant violated Georgia

policy and the Illinois courts would likely enforce the covenant. Cases applying Bunker Hill have produced different outcomes. Compare Crump Ins. Servs. v. All Risks, Ltd., 315 Ga. App. 490, 492-93, 727 S.E.2d 131, 134 (2012) (enforcing a forum selection clause designating Maryland as the forum because, while the restrictive covenants would violate Georgia public policy, there was no showing that a Maryland court would enforce the covenants, since "Maryland's law on restrictive covenants was similar to Georgia's law") with LaPolla Indus., Inc. v. Hess, 325 Ga. App. 256, 265-66, 750 S.E.2d 467, 475-76 (2013) (following Bunker Hill and voiding Texas forum selection clause) and Carson v. Obor Holding Co., LLC, 318 Ga. App. 645, 734 S.E.2d 477 (2012) (following Bunker Hill and voiding Florida forum selection clause). See also Protz v. Bock & Clark Corp., No. 1:13-cv-1281-JEC, 2013 WL 1898142, at *4 (N.D. Ga. May 7, 2013) (applying federal law to enforceability of forum selection clause and not discussing Bunker Hill).

N. Covenants Ancillary to Sale of Business

1. The Scrutiny Applicable to Covenants Ancillary to the Sale of a Business

Georgia courts have historically distinguished between covenants ancillary to employment and covenants ancillary to the sale of a business. An employment agreement is treated similarly to a contract of adhesion based on the inequality of bargaining power between the parties to the contract. White v. Fletcher/Mayo/ Assocs., Inc., 251 Ga. 203, 303 S.E.2d 746 (1983). This consideration is typically not present in an arm's length sale of business transaction.

Courts treated restrictive covenants ancillary to the sale of a business different because "[s]pecial considerations often arise in the sale of a business." Hudgins v. Amerimax Fabricated Prods., 250 Ga. App. 283, 285, 551 S.E.2d 393, 396 (2001). There are certain factors that determine if restrictive covenants are ancillary to the sale of business: (1) an equality of bargaining power; and (2) when "the buyer pays and the seller receives a part of the total purchase price as consideration for th[e] covenant." Id. at 286, 396; see also Hicks v. Doors By Mike, Inc., 260 Ga. App. 407, 579 S.E.2d 833 (2003); Russell Daniel Irrigation Co., Ltd. v. Coram, 237 Ga. App. 758, 759, 516 S.E.2d 804, 805-06 (1999) ("'If it appears that his bargaining capacity was not significantly greater than that of a mere employee, then the covenant should be treated like a covenant ancillary to an employment contract . . . .'" (alteration in original) (quoting White v. Fletcher/Mayo/ Assocs., 251 Ga. 203, 208, 303 S.E.2d 746 (1983))). For instance, unlike covenants ancillary to employment agreements, restrictive covenants ancillary to the sale of a business are not required to be in writing, see Klein v. Williams, 212 Ga. App. 39, 441 S.E.2d 270 (1994), may be unlimited in time, provided the purchaser remains in business, see

Martinez v. Davita, Inc., 266 Ga. App. 723, 728, 598 S.E.2d 334, 338 (2004), and may restrict a former owner from competing in the territory served by the employer, not just in the area served by the former owner, see Mohr v. Bank of New York Mellon Corp., 393 Fed. Appx. 639, 645, (11th Cir. 2010) (reversing denial of preliminary injunction and remanding with instructions to enjoin former owners from competing against or soliciting the customers of former employer); see also Mohr v. Bank of New York Mellon Corp., 371 Fed. Appx. 10 (11th Cir. 2010).

Though restrictive covenants ancillary to the sale of a business have been subjected to less scrutiny than covenants ancillary to employment contracts, this lesser scrutiny does not mean that courts will liberally construe the *scope* of such covenants. Ferrellgas Partners, Inc. v. Barrow, No. 4-03-CV-107 (WDO), 2006 WL 372602 (M.D. Ga. Feb. 16, 2006) (former employee whose covenant prohibited him from "engaging in" propane business does not breach covenant by selling real estate to daughter operating competing business).

Unlike the common law rule applicable to covenants ancillary to employment, covenants ancillary to the sale of a business can be "blue penciled" to render an overbroad covenant reasonable. See Martinez v. Davita, Inc., 266 Ga. App. 723, 728, 598 S.E.2d 334, 338 (2004) (without expressly rejecting "any location" territory, noting that the trial court could "blue pencil" it if it were unenforceable). However, a trial court may not under the guise of the "blue pencil" method reform a covenant not to compete in a contract ancillary to the sale of a business which is otherwise unenforceable by reason of vagueness. Waste Mgmt. of Metro Atlanta, Inc. v. Appalachian Waste Sys., LLC, 286 Ga. App. 476, 480, 649 S.E.2d 578, 582 (2007)("[T]rial court correctly concluded that it could not add a term missing in the contract, even under the liberal treatment afforded covenants ancillary to the sale of a business."); see also Clower v. Orthalliance, Inc., 337 F. Supp. 2d 1322, 1334 (N.D. Ga. 2004) ("A court may 'blue-pencil' the covenant to make an offending covenant term reasonable, although it cannot actually reform a covenant that is void for vagueness.").

Even under the old law, once a trial court determines that a restrictive covenant ancillary to the sale of a business is overbroad, the trial court could "blue pencil" the covenant. This process was governed by the Georgia Supreme Court's decision in Jenkins v. Jenkins Irrigation, Inc., 244 Ga. 95, 259 S.E.2d 47 (1979). In an effort to "deter [covenant writers] from staking out more territory than is reasonable (e.g., America) in anticipation that the court will pare the territory to what which is reasonable," the Supreme Court affirmatively held that the applicable rules governing what is an acceptable territory were different if a trial court was required to "blue pencil" a restrictive covenant. Id. at 100, 259 S.E.2d at

51. In such an instance, the "blue penciled" territory must be more limited than if the parties had contractually agreed upon a reasonable territory themselves. The Supreme Court in Jenkins instructed that:

> [W]hen it becomes necessary for a superior court to use the blue pencil to prescribe the territory, the proscribed area usually should not be as extensive as the parties could have validly negotiated themselves, and it should be only such area as is shown by the buyer by clear and convincing evidence to be essential (as opposed to reasonably necessary) for the protection of his interests. Moreover, the superior court should disregard isolated transactions in the periphery in determining the area served by the seller, may disregard areas into which the buyer intended to expand, and may make such other territorial provisions as the court in its discretion finds appropriate for the protection of the parties and the public.

Id. at 101, 51-52 (emphasis added); see also Hamrick v. Kelley, 260 Ga. 307, 307-08, 392 S.E.2d 518, 518-19 (1990); Waste Mgmt. of Metro Atlanta, Inc. v. Appalachian Waste Sys., LLC, 286 Ga. App. 476, 480, 649 S.E.2d 578, 582 (2007).

Under the old law, if the buyer is unable to demonstrate the essential territory by clear and convincing evidence, it appears that the trial court is not required to "blue pencil" the covenant. Hudgins v. Amerimax Fabricated Prods., 250 Ga. App. 283, 287, 551 S.E.2d 393, 397 (2001) (remanding matter to "trial court . . . to determine whether the otherwise enforceable restrictions should apply to a smaller geographic area" (emphasis added)).

The Act applies to restrictive covenants in agreements between and among sellers and purchasers of a business, as defined by the statute. See O.C.G.A. § 13-8-52(a)(6); see also id. § 13-8-57(d) (providing that a five-year non-competition covenant against a seller of all or a material part of the assets of a business is presumed reasonable in duration).

2. Covenants Ancillary to Employment which are Executed in Conjunction with a Sale of a Business

Often, covenants ancillary to employment are executed in conjunction with a sale of a business. The question then becomes in which manner the court will consider the agreement.

In White v. Fletcher/Mayo/ Assocs., 251 Ga. 203, 208, 303 S.E.2d 746 (1983), for example, the court held that the covenant at issue was merely ancillary to employment where the bargaining capacity of a former vice-president of the merged company was not significantly greater than that of a mere employee, as indicated by the fact that the vice-president received

the same for his shares of the company as other shareholders and where the vice-president had no control of the overall management of the company.

The employment agreement and the purchase/sale agreement must be contemporaneous for the court to construe the covenant as ancillary to the sale. Am. Control Sys., Inc. v. Boyce, 303 Ga. App. 664, 694 S.E.2d 141 (2010) (reversing grant of summary judgment in favor of former shareholder where his bargaining capacity in negotiating the stock purchase agreement entered into at the same time as his employment agreement which contained the restrictive covenants at issue was significantly greater than that of a mere employee; therefore, restrictive covenants were ancillary to the sale of a business and subject to much less scrutiny than those ancillary to an employment contract). But see Lyle v. Memar, 259 Ga. 209, 378 S.E.2d 465 (1989) (more than a year between the sale and the execution of the employment agreement held to be not contemporaneous); Holsapple v. Smith, 267 Ga. App. 17, 20, 599 S.E.2d 28, 32 (2004) (trial court's treatment of two agreements as being executed simultaneously was erroneous where there were various drafts of letters of intent before written agreement was executed six days later); Siech v. Hobbs Grp., LLC, 198 Fed. Appx. 840 (11th Cir. 2006) (covenant was ancillary to employment rather than ancillary to the sale of a business where it was made by the buyer in connection with the sale of a business, rather than by the seller in conjunction with the acquisition of an interest in a business); Accurate Printers, Inc. v. Stark, 295 Ga. App. 172, 671 S.E.2d 228 (2008) (where owner of company was the party to an employment contract with seller of business, rather than the company, company did not have standing to enforce restrictive covenant).

The purchase/sale agreement and the employment agreement must also be between the same parties for a court to construe the agreements together and treat the covenants as ancillary to the sale of a business. See Lyle v. Memar, 259 Ga. 209, 378 S.E.2d 465 (1989) (sale of company between individuals and employment agreement between seller's president and the corporation; therefore, employment agreement not ancillary to the purchase and sale); see also Gale Indus., Inc. v. O'Hearn, 257 Ga. App. 220, 222, 570 S.E.2d 661, 663 (2002) (even though employment agreement executed same day as asset purchase agreement, the two agreements "cannot be construed together as part of the same transaction. The agreements do not involve the same parties or the same subject matter.").

However, if the purchase/sale agreement and the employment agreement each have their own set of restrictive covenants, they will each be considered as separate agreements. See Hix v. Aon Risk Servs. S., Inc., No. 1:11-CV-3141-RWS, 2011 WL 5870059, at *9 (N.D. Ga. Nov. 22, 2011) (finding that because the restrictive covenants in an employment

agreement were "wholly separate" from those in the purchase agreement, the restrictive covenants should be considered independently and strict scrutiny should apply to the restrictive covenants in the employment agreement).

Factors which will be considered by courts in determining whether the covenant is ancillary to the sale of the business include the following: (i) whether the original company was reliant upon the employee's skills; (ii) whether the employee was represented by an attorney in the transaction; (iii) whether the employment agreement was executed contemporaneously with other documents related to the sale of the business or whether the various documents reference each other; (iv) whether the employee was aware of the consequences of the sale of the stock; (v) whether the employee initiated the negotiations for the sale of the business or whether there was any pressure or duress; (vi) whether the employee profited from the sale; and (vii) whether the employee received relief from any personal liability for the debts of the pre-merger company. Drumheller v. Drumheller Bag & Supply, Inc., 204 Ga. App. 623, 420 S.E.2d 331 (1992); Annis v. Tomberlinn & Shelnutt Assocs., Inc., 195 Ga. App. 27, 392 S.E.2d 717 (1990) (court found covenant ancillary to sale of business where employee retained ownership interest in merged company and the covenant was stated in both the employment agreement and the purchase agreement). However, the Eleventh Circuit has, on at least one occasion, looked solely at the subject matter of the dispute to determine the applicable level of scrutiny. See MacGinnitie v. Hobbs Grp., LLC, 420 F.3d 1234, 1241 (11th Cir. 2005) ("Georgia law is clear, however, that even when an employment dispute is part of the sale of a business, if the dispute itself pertains to a contract of employment then the contract must be interpreted under the law governing such contracts."); see also Palmer & Cay, Inc. v. Marsh & McClennan Cos., 404 F.3d 1297, 1305 (11th Cir. 2005) (noting when an agreement for the sale of a business is also involved, "the Georgia Supreme Court has noted in dicta that a non-competition period that starts with the termination of employment 'is customary in cases of noncompetitive covenants ancillary to an employment contract'").

Additionally, the trial court should look at the manner in which the various agreements were memorialized. In Holsapple v. Smith, 267 Ga. App. 17, 20-21, 599 S.E.2d 28, 32 (2004), there were two non-contemporaneous agreements: an oral employment agreement and a written asset purchase agreement. The Court of Appeals held that the covenants against competition had to be a part of the asset purchase agreement because covenants ancillary to employment have to be in writing.

A second line of cases holds that an employment contract is not ancillary to the sale of a business unless the employee is "the heart and soul of the business" such that the business "would come to a halt without him." Arnall Ins. Agency, Inc. v. Arnall, 196 Ga. App. 414, 396 S.E.2d 257 (1990);

see also Stultz v. Safety & Compliance Mgmt., Inc., 285 Ga. App. 799, 804, 648 S.E.2d 129, 133 (2007) (in strict scrutiny context, covenant fails for indefiniteness where plaintiff failed to allege or present evidence that employee was the heart and soul of its alcohol and drug testing business). In Arnall, the general partner and manager of an insurance agency sold his interest in the company and, on the same day, executed an employment contract with restrictive covenants. The court held that the covenants were not ancillary to sale of the business and would be strictly construed because (i) the employee did not retain any interest in the merged company; (ii) the employee was hired as an agent and was not "the heart and soul" of the business; and (iii) the employment agreement and the purchase agreement had separate covenants and each document stood on its own. Arnall Ins. Agency, Inc. v. Arnall, 196 Ga. App. 414, 396 S.E.2d 257 (1990); see also Ceramic Metal Coatings Corp. v. Hizer, 242 Ga. App. 391, 394, 529 S.E.2d 160, 163 (2000) (employment agreement subject to strict scrutiny even though employee bought stock in closely held corporation during his employment because he did not own any stock when he signed agreement); Russell Daniel Irrigation Co., Ltd. v. Coram, 237 Ga. App. 758, 516 S.E.2d 804 (1999) (subjecting two restrictive covenants between same parties to different treatment even though they were found in agreements executed as part of same transaction; although partner became part owner of business as a result of transaction, covenants in employment agreement would be subjected to strict scrutiny as partner/employee had bargaining power of only a mere employee).

See also Attaway v. Republic Servs. of Ga., LLP, 253 Ga. App. 846, 558 S.E.2d 846 (covenants in employment agreement did not supersede covenants in sales agreement); Hudgins v. Amerimax Fabricated Prods., 250 Ga. App. 283, 285, 551 S.E.2d 393, 396 (2001) (covenant not to compete not ancillary to employment when minority shareholder/employee's employment terminated when company sold); Ceramic Metal Coatings Corp. v. Hizer, 242 Ga. App. 391, 394, 529 S.E.2d 160, 163 (2000) (though employee bought stock in closely held corporation, he did not own any stock when he signed the agreement; therefore, agreement would not be considered like ones involving partnerships or the sale of a business).

O. Covenants Ancillary to Other Agreements

Aside from restrictive covenants ancillary to employment contracts, there are several other types of covenants in restraint of trade which have been recognized by Georgia courts, including covenants ancillary to leases, franchise agreements, distributorship agreements, and independent contractor agreements.

These types of covenants have generally been treated by the Georgia courts like covenants ancillary to employment agreements. Fab'rik Boutique, Inc.

v. Shops Around Lenox, Inc., 329 Ga. App. 21, 763 S.E.2d 492 (2014) (covenant in lease agreement entered into prior to May 2011; applying strict scrutiny but enforcing covenant based on application of general rules of contract construction); Matthew Focht Enters., Inc. v. Lepore, No. 1:12-cv-04479-WSD, 2013 WL 4806938 (N.D. Ga. Sept. 9, 2013) (independent contractor agreement); Fantastic Sams Salons Corp. v. Maxie Enters., Inc., No. 3:11-CV-22 (CDL), 2012 WL 210889 (M.D. Ga. Jan. 24, 2012) (franchise agreement); Paragon Techs., Inc. v. Infosmart Techs., Inc., 312 Ga. App. 465, 718 S.E.2d 357 (2011) (independent contractor agreement); B & F Sys., Inc. v. LeBlanc, No. 7:07-CV-192 (HL), 2011 WL 4103576 (M.D. Ga. Sept. 14, 2011) (subjecting in-term restrictive covenant in distributorship agreement to strict scrutiny); Atlanta Bread Co. Int'l v. Lupton-Smith, 292 Ga. App. 14, 663 S.E.2d 743 (2008) (franchise agreement); Gandolfo's Deli Boys, 490 F. Supp. 2d at 1357 (franchise agreement); Allen v. Hub Cap Heaven, Inc., 225 Ga. App. 533, 538, 484 S.E.2d 259, 264 (1997) (franchise agreement); Rita Pers. Servs. v. Kot, 229 Ga. 314, 191 S.E.2d 79 (1972) (franchise agreement); see also Advance Tech., 250 Ga. App. 317, 551 S.E.2d 735 (distributorship agreement); Herndon v. Waller, 241 Ga. App. 494, 525 S.E.2d 159 (1999) (lease); Amstell, Inc. v. Bunge Corp., 213 Ga. App. 115, 443 S.E.2d 706 (1994) (independent contractor, manufacturing and distribution agreement); Jenkins v. Jenkins Irrigation, Inc., 244 Ga. 95, 259 S.E.2d 47 (1979) (independent contractor agreement); Fields Rainbow Int'l Carpet Dyeing & Cleaning Co., 259 Ga. 375, 380 S.E.2d 693 (1989) (franchise agreement); Owens v. RMA Sales, Inc., 183 Ga. App. 340, 358 S.E.2d 897 (1987) (distributorship agreement); Watson v. Waffle House, Inc., 253 Ga. 671, 672, 324 S.E.2d 175, 177 (1985) (lease); PCS Joint Venture, Ltd. v. Davis, 219 Ga. App. 519, 465 S.E.2d 713 (1995) (exclusive distribution agreement); Johnstone v. Tom's Amusement Co., 228 Ga. App. 296, 491 S.E.2d 394 (1998) (lease agreement). Cf. Swartz Invs., LLC v. Vion Pharm., Inc., 252 Ga. App. 365, 556 S.E.2d 460 (2001) (stating that the type of contract should not automatically determine the applicable level of scrutiny, but applying strict scrutiny to non-circumvention agreement under particular facts of the case; strict scrutiny applied because no consideration for covenant at issue, but expressing no opinion as to level of scrutiny applicable to non-circumvention clauses generally); see also O.C.G.A. § 13-8-52 (in addition to employment agreements, the new legislation applies to distributorship agreements, leases, partnership agreements, franchise agreements, agreements for the sale of a business, and agreements between two or more employers); O.C.G.A. § 13-8-57 (different presumptions of reasonableness for different agreements).

P. Covenants Ancillary to Professional Partnership Agreements

Under the old law, the Court of Appeals carved out a middle level of scrutiny for covenants ancillary to professional partnership agreements. See Physician Specialists in Anesthesia, P.C. v. MacNeill, 246 Ga. App.

398, 539 S.E.2d 216 (2000); Habif, Arogeti& Wynne, P.C. v. Baggett, 231 Ga. App. 289, 498 S.E.2d 346 (1998); McAlpin v. Coweta Fayette Surgical Assocs., P.C., 217 Ga. App. 669, 458 S.E.2d 499 (1995); Roberts v. Tifton Med. Clinic, P.C., 206 Ga. App. 612, 426 S.E.2d 188 (1992); Rash v. Toccoa Clinic Med. Assocs., 253 Ga. 322, 320 S.E.2d 170 (1984); see also Carson v. Obor Holding Co., LLC, 318 Ga. App. 645, 648-49, 734 S.E.2d 477, 481 (2012) (finding that covenants in operating agreement would fail mid-level scrutiny if it applies); Keeley v. Cardiovascular Surgical Assocs., P.C., 236 Ga. App. 26, 30-31, 510 S.E.2d 880, 885 (1999) (applying middle level of scrutiny to physician's covenant when physician was to become an equal owner within eighteen months); Delli-Gatti v. Mansfield, 223 Ga. App. 76, 477 S.E.2d 134 (1996) (construing physician's employment agreement more liberally than other employment agreements).

The Court of Appeals has held that where a party, in conjunction with the same transaction, has signed an employment agreement and a partnership agreement with his employer, both of which contain restrictive covenants, then the restrictive covenant in the employment agreement is subject to strict scrutiny, even when the covenants in the partnership agreement are subject to mid-level scrutiny. The Court relied on Russell Daniel Irrigation Co. v. Coram, 237 Ga. App. 758, 516 S.E.2d 804 (1999) and found that subjecting two restrictive covenants to different treatment, even though found in agreements executed as part of the same transaction, is consistent with the rationale behind the different levels of scrutiny. New Atlanta Ear, Nose & Throat Assocs., P.C. v. Pratt, 253 Ga. App. 681, 560 S.E.2d 268 (2002).

In the Pratt case, the Court seemed to imply that covenants in a professional partnership agreement can be "blue penciled," though the Court declined to do so on the grounds that "[t]he 'blue pencil' marks, but does not write." Id. at 687, 273 (alteration in original) (internal quotation mark omitted). The Court held, the "blue pencil" could limit an over broad territory, but it would not write in a territory, where none was stated. Id.

Covenants not to compete between or among physicians do not conflict with medical ethical principles or Georgia law requiring informed consent and do not injure the public in general. Pittman v. Harbin Clinic Prof'l Ass'n., 210 Ga. App. 767, 437 S.E.2d 619 (1993). Also, an employee's status as a physician should not affect the Court's scrutiny of restrictive covenants. See AGA, LLC v. Rubin, 243 Ga. App. 772, 533 S.E.2d 804 (2000) (rejecting argument individuals should receive less scrutiny because they are doctors). But see Shankman v. Coastal Psychiatric Assocs., 258 Ga. 294, 294-96, 368 S.E.2d 753, 753-54 (1988) (Smith, J., dissenting) (arguing that restrictive covenants in a medical contract should be illegal *per se*). Although Georgia courts have upheld restrictions against the general practice of medicine, see Delli-Gatti v. Mansfield, 223 Ga. App. 76, 79, 477 S.E.2d 134, 137 (1996) (concerning general

practitioner in rural county), an argument could be made that, given the large range of specialties, a specialized doctor's restrictive covenant should be tailored to the specialized medical services performed for the employer. See Saxton v. Coastal Dialysis & Med. Clinic, Inc., 220 Ga. App. 805, 809, 470 S.E.2d 252, 255 (1996) (upholding covenant that restricted physician from certain activities performed for employer, but not from general practice of medicine).

It should be noted that Georgia courts have held "that the level of scrutiny is not directly tied to the type of contract under consideration," and that the trial court must "look to the purposes behind the varying levels of scrutiny to determine which level is most appropriate . . . ." W. Coast Cambridge, Inc. v. Rice, 262 Ga. App. 106, 108, 584 S.E.2d 696, 698 (2003) (quoting Swartz Invs., LLC v. Vion Pharm., Inc., 252 Ga. App. 365, 368-69, 556 S.E.2d 460, 463 (2001)). In West Coast Cambridge, Inc., the Court of Appeals found that a doctor's covenant not to compete with a professional partnership was treated as being ancillary to the sale of a business rather than the "middle" level of scrutiny usually afforded professional partnerships. Id. at 109, 699 (doctor "benefited through passive investment [and] did not practice medicine with the Partnership"); see also OnBrand Media v. Codex Consulting, Inc., 301 Ga. App. 141, 607 S.E.2d 168 (2009) (applying middle-level scrutiny to non-disclosure agreements entered into as part of negotiations for a joint venture agreement, and finding that lack of territorial limitation and clear limits on the scope of the prohibited activity renders covenants not to compete unenforceable).

Q. Non-Recruitment Covenants

While many Georgia attorneys believe that covenants restricting solicitation or recruitment of employees have historically been scrutinized less strictly than customer non-solicitation or non-competition covenants – including many attorneys who practice in this area – a closer examination of the decisions in which these covenants have been scrutinized reveals that Georgia's old common law on this issue is in fact not at all that clear. The following timeline of decisions is intended to illustrate the divergent approaches which Georgia courts have taken when scrutinizing non-recruitment covenants:

- **1971**: Harrison v. Sarah Coventry, Inc., 228 Ga. 169, 171, 184 S.E.2d 448, 449 (1971) (rules for covenants against competition are not applicable where employee contractually agreed "not to interfere with the contractual relationships of the [employer] and its other employees"; restraint of trade cases have "no application" to cases involving non-recruitment covenants).

- **1985**: Lane Co. v. Taylor, 174 Ga. App. 356, 359-60, 330 S.E.2d 112, 117 (1985) (upholding non-recruitment covenant containing no geographical

limitation under "legitimate business interest" test) (physical precedent only).

- **1991**: U3S Corp. of Am. v. Parker, 202 Ga. App. 374, 376-77, 414 S.E.2d 513, 516 (1991) (covenant without a territorial limitation which prohibited solicitation or encouragement upheld).

- **1992**: ALW Mktg. Corp. v. Drunansky, No. CIV.A.1:91-CV-545RLV, 1991 WL 345313, at *7 (N.D. Ga. 1992) (denying preliminary injunction on non-recruitment provision because it contained no territorial limitation and was over broad in the employees it covered).

- **1994**: Sunstates Refrigerated Servs., Inc. v. Griffin, 215 Ga. App. 61, 63, 449 S.E.2d 858, 860-61 (1994) (upholding non-recruitment covenant without a territorial restriction which provided that for two years after termination of employment contract employee would not "employ, attempt to employ or assist anyone else in employing as a manager, executive or salesperson in any competing business any of the [employer's] managerial, executive or sales personnel.").

- **1996**: Club Props., Inc. v. Atlanta Offices-Perimeter, Inc., 180 Ga. App. 352, 354, 348 S.E.2d 919, 922 (1986) (as partial restraint of trade, no-hire provision in lease must meet "rule of reason" as to time, territory and proscribed activities; as covenant lacks a time limit, it is unenforceable).

- **2000 (June)**: Sanford v. RDA Consultants, Ltd., 244 Ga. App. 308, 311, 535 S.E.2d 321, 324 (2000) (upholding non-recruitment covenant without a territorial restriction which provided that for a period of one year from the date of termination the employee would not "attempt to employ or assist any other person in employing or soliciting for employment any employee employed by" the employer).

- **2000 (Dec.)**: Hulcher Servs., Inc. v. R.J. Corman R.R. Co., LLC, 247 Ga. App. 486, 491-92, 543 S.E.2d 461, 467 (2000) (non-solicitation of employees provision found unreasonable without restriction as to territory).

- **2001**: Capricorn Sys., Inc. v. Pednekar, 248 Ga. App. 424, 427, 546 S.E.2d 554, 558 (2001) (covenant restricting solicitation of customers and employees unenforceable without a territory).

- **2002**: Mathis v. Orkin Exterminating Co., 254 Ga. App. 335, 336, 562 S.E.2d 213, 214-15 (2002) (upholding non-recruitment covenant without a territorial restriction which prohibited "soliciting or in any manner attempting to solicit or induce any employees to leave their employment").

- **2005 (Mar.)**: Albany Bone & Joint Clinic, P.C. v. Hajek, 272 Ga. App. 464, 467, 612 S.E.2d 509, 512 (2005) (stating that a non-recruitment covenant is a restrictive covenant in partial restraint of trade).

- **2005 (Apr.)**: Palmer & Cay of Ga., Inc. v. Lockton Cos., 273 Ga. App. 511, 514-15, 615 S.E.2d 752, 756-57 (2005) (upholding covenant which contained no territorial restriction and prohibited employee from "attempting in any manner to cause or otherwise encourage any employee to leave").

- **2005 (Aug.)**: MacGinnitie v. Hobbs Grp., LLC, 420 F.3d 1234, 1242 (11th Cir. 2005) (stating that Georgia courts refuse to enforce employee non-solicitation provisions without territorial limitations)

- **2007**: Celtic Maint. Servs., Inc. v. Garrett Aviation Servs., LLC, No. CV 106-177, 2007 WL 4557775, at *5 (S.D. Ga. Dec. 21, 2007) ("[A]lthough Georgia courts have been quick to strike down broad non-competition agreements in employment contracts, broad non-recruitment and no-hire provisions are routinely enforced in Georgia.").

- **2011 (Jan.)**: Cox v. Altus Healthcare & Hospice, Inc., 308 Ga. App. 28, 30, 706 S.E.2d 660, 664 (2011) (non-recruitment covenant which bars unsolicited contact is void).

- **2011 (Sept.)**: Becham v. Synthes (U.S.A.), No. 5:11-CV-73 (MTT), 2011 WL 4102816, at *4 (M.D. Ga. Sept. 14, 2011) ("With regard to non-solicitation or non-recruitment of employees, covenants that have no territorial restriction are unenforceable.").

- **2014 (May)**: Wetherington v. Ameripath, Inc., Nos. 13-11925, 13-13436, 2014 WL 2016582, at *1 (11th Cir. 2014) (invalidating non-recruitment clause which barred former employee from hiring employees of former employer who have no confidential information and who resigned voluntarily as much as a year prior, regardless of whether the employees had any relationship with the plaintiff during his employment).

- **2014 (May)**: Wetherington v. Ameripath, Inc., Nos. 13-11925, 13-13436, 2014 WL 2016582, at *1 (11th Cir. 2014) (invalidating non-recruitment clause which barred former employee from hiring employees of former employer who have no confidential information and who resigned voluntarily as much as a year prior, regardless of whether the employees had any relationship with the plaintiff during his employment).

- **2017:** CMGRP, Inc. v. Gallant, 343 Ga. App. 91, 806 S.E.2d 16 (2017) (clarifying that a non-recruitment covenant does not need to have a

geographical limitation and does not have to be limited to the employees with whom the former employee had material contact or an established relationship).

Although the Georgia Court of Appeals' decision in Gallant provides some clarity on the common law rules governing the enforceability of non-recruitment covenants, the inconsistencies in the above cases leave it difficult to know definitively what rules a court will (or should) apply when scrutinizing a non-recruitment covenant entered into prior to the effective date of the Act.

III. Termination/Resignation

A. Severance/Post-Termination Agreement

Under the old law, restrictive covenants in agreements executed incident to the severance of the employment relationship were generally subject to the strict scrutiny applied to those within employment contracts. Kem Mfg. Corp. v. Sant, 182 Ga. App. 135, 355 S.E.2d 437 (1987).

B. Post-Termination Compensation

Even if restrictive covenants in employment or severance agreement are unenforceable, employer's contractual obligation to pay employee post-termination compensation is not void where the agreement contains a severability clause and there is consideration other than the covenants for the compensation. Kem Mfg. Corp. v. Sant, 182 Ga. App. 135, 355 S.E.2d 437 (1987).

IV. Litigation

A. General Requirements for Injunction

1. Temporary Restraining Orders ("TRO")

O.C.G.A. section 9-11-65 provides that a party may obtain a TRO if it clearly appears from the specific facts shown by affidavit or by verified complaint that immediate and irreparable injury, loss or damage will result.

Case law further requires that the party seeking a TRO demonstrate that it (1) will suffer irreparable harm if the injunction is not granted; (2) there is a substantial likelihood that it will prevail at

trial; and (3) the damage of not granting the injunction is greater than that to the defendant if the injunction is not granted.

2. Interlocutory and Permanent Injunctions

The purpose for granting interlocutory injunctions is to preserve the status quo, as well as balance the convenience of the parties, pending final adjudication of the case. Jackson v. Delk, 257 Ga. 541, 543-44, 361 S.E.2d 370, 373 (1987); Covington v. D.L. Pimper Grp., Inc., 248 Ga. App. 265, 269, 546 S.E.2d 37, 41 (2001).

In order to obtain a preliminary injunction in federal court, the movant must demonstrate (1) a substantial likelihood that he will ultimately prevail on the merits; (2) that he will suffer irreparable injury unless the injunction issues; (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) that the injunction, if issued, would not be adverse to the public interest. Morgan Stanley DW, Inc. v. Frisby, 163 F. Supp. 2d 1371 (N.D. Ga. 2001) (denying injunction to employer); see also Moorad v. Affordable Interior Sys., LLC, No. 1:11-CV-2580-RWS, 2012 WL 162289 (N.D. Ga. Jan. 18, 2012) (granting former employee a preliminary injunction against his employer's enforcement of over broad restrictive covenants).

Where an employee seeks an injunction prohibiting his or her former employer from seeking to enforce over broad restrictive covenants, irreparable harm can be established by the movant showing lost employment opportunities. Moorad v. Affordable Interior Sys., LLC, No. 1:11-CV-2580-RWS, 2012 WL 162289, *5 (N.D. Ga. Jan. 18, 2012) ("As that agreement would restrain trade, and was disfavored at the time it was signed, Plaintiff certainly would suffer irreparable harm if he were not granted an injunction on that matter."); Hix v. Aon Risk Servs. S., Inc., No. 1:11-CV-3141-RWS, 2011 WL 5870059, at *9 (N.D. Ga. Nov. 22, 2011).

In Keener v. Convergys Corp., 342 F.3d 1264 (11th Cir. 2003), the Eleventh Circuit found that the district court abused its discretion by entering a nationwide injunction against the enforcement of restrictive covenants. The Eleventh Circuit held that the territory of the injunction should have been limited to Georgia on grounds that "Georgia cannot in effect apply its public policy decisions nationwide" and that "[t]o permit a nationwide injunction would in effect interfere both with parties' ability to contract and their ability to enforce appropriately derived expectations." Id. at 1269. The Eleventh Circuit did not address the Full Faith and Credit issues

implicated in its decision.

However, in Hostetler v. Answerthink, Inc., 267 Ga. App. 325, 599 S.E.2d 271 (2004), the Georgia Court of Appeals rejected the Eleventh Circuit's holding regarding the scope of injunctive relief concerning the enforcement of restrictive covenants. Id. at 330, 276. In reversing a trial court that limited an injunction to the State of Georgia, the Court of Appeals expanded the injunction to have extra-territorial effect so that it would "prevent the relitigating of such issue[s] in other jurisdictions." Id. at 329, 275.

Although the Eleventh Circuit distinguished Hostetler from Keener with regard to injunctive relief in a subsequent case, the Eleventh Circuit did affirm that, under Georgia law, a declaratory judgment regarding the enforceability could have an extraterritorial effect. See Marsh & McClennan Cos., 404 F.3d 1297 (11th Cir. 2005). In Palmer & Cay, Inc. v. Marsh & McClennan Cos., 404 F.3d 1297 (11th Cir. 2005), the Eleventh Circuit held that the declaratory judgment could have an extraterritorial effect because "an enforcing court should apply the law of the state courts in the state where the rendering federal court sits, unless the state's law conflicts with federal interests," and "Georgia does not attempt to limit its declaratory judgments in cases involving non-competition agreements," so, therefore, "a federal district court sitting in Georgia and applying Georgia law should not do so either." Id. at 1310 (vacating district court's declaratory judgment to extent it attempted to limit relief to Georgia).

3. Wrongful Restraint

An employer who seeks and obtains an injunction based on illegal restrictive covenants exposes itself to potential liability for a counterclaim for wrongful restraint. Cox v. Altus Healthcare & Hospice, Inc., 308 Ga. App. 28, 30, 706 S.E.2d 660, 664 (2011) (finding that injunction entered against employee based on unreasonable covenants was unlawful and remanding for determination as to damages suffered by wrongfully restrained employee).

B. Corporation Code - Duties of Officers

1. A mere employee has no fiduciary obligation to former employer after termination of employment. See, e.g., Instrument Repair Serv., Inc. v. Gunby, 238 Ga. App. 138, 140, 518 S.E.2d 161, 163 (1999) (principles of agency pertinent to period when employee still employed, but will not sustain the grant of an injunction prohibiting competition after the agency relationship is terminated). An employee may make arrangements to enter a competing business while still employed and may immediately compete upon termination without breaching any fiduciary duties, but an employee may not solicit customers for a rival business before the end of his employment nor can he engage in other similar acts in direct competition with his employer during his employment. See, e.g., Ferrellgas Partners, Inc., No. 4-03-CV-107 (WDO), 2006 WL 372602 (M.D. Ga. Feb. 16, 2006).

2. O.C.G.A. section 14-2-831 allows for a derivative proceeding by a corporation against officers or directors (or former officers and directors) for appropriation, in violation of his/her duties, of any business opportunity of the corporation.

3. First it must be established that the employee was an officer. Sofate of Am., Inc. v. Brown, 171 Ga. App. 39, 318 S.E.2d 771 (1984); see also Vardeman v. Penn Mut. Life Ins. Co., 125 Ga. 117, 54 S.E. 66 (1906) (distinguishing corporate officer "elected by the directors or the stockholders" from agent who "is an employee"). But see Gresham & Assocs., Inc. v. Strianese, 265 Ga. App. 559, 560, 595 S.E.2d 82, 84 (2004) (finding there was a question of fact as to whether individual's "position as a vice president of [corporation in charge of a department] made him a corporate officer who had a fiduciary relationship with the corporation").

4. In Gresham & Assocs., Inc. v. Strianese, 265 Ga. App. 559, 595 S.E.2d 82 (2004), the Court of Appeals stated that "a corporate officer does not breach fiduciary duties owed to the corporation simply by making plans to start a competing company while still employed by the corporation." Id. at 560, 84. Under this rationale, the Court of Appeals affirmed that the corporate officer "[e]ven before termination of employment, . . . is entitled to make arrangements to compete [and] can properly purchase a rival business and upon termination of employment immediately compete." Id. at 560-61, 85 (third alteration in original) (internal quotation mark omitted) (quoting E.D. Lacey Mills, Inc. v. Keith, 183 Ga. App. 357, 362-63, 359 S.E.2d 148, 155 (1987)); see also Nilan's Alley v. Ginsburg, 208 Ga. App. 145, 430 S.E.2d 368 (1993).

However, the Court of Appeals reiterated, that despite being able to *prepare* to compete "during the term of employment with the corporation, the officer may not *solicit* customers for a competing company or otherwise *engage in direct competition* with the corporation's business." Id. (emphasis added); see also White v. Shamrock Bldg. Sys., Inc., 294 Ga. App. 340, 669 S.E.2d 168 (2008) (denying summary judgment where there was evidence that employee in fiduciary relationship with employer solicited contract for his own entity prior to termination); Continental Maritime Servs., Inc. v. Maritime Bureau, Inc, 275 Ga. App. 533, 621 S.E.2d 775 (2005) (letter sent by former officer to customers after termination not a breach of fiduciary duty); KEG Techs., Inc. v. Laimer, 436 F. Supp. 2d 1364 (N.D. Ga. 2006) (officer liable for actively soliciting customers and engaging in competition with employer only during period prior to termination).

5. Georgia has adopted a two step process for determining usurpation of a corporate opportunity. Se. Consultants, Inc. v. McCrary Eng'g Corp., 246 Ga. 503, 273 S.E.2d 112 (1980). First, the court must determine whether the appropriated opportunity was in fact a business opportunity rightfully belonging to the corporation. Id.; see also KEG Techs., Inc. v. Laimer, 436 F. Supp. 2d 1364 (N.D. Ga. 2006) (only sales made prior to termination of agency were illegally usurped corporate opportunities). A business opportunity arises from a "beachhead" consisting of a legal or equitable interest or an "expectancy" growing out of a pre-existing right or relationship. United Seal & Rubber Co. v. Bunting, 248 Ga. 814, 815, 285 S.E.2d 721, 722-23 (1982); see also Brewer v. Insight Tech., Inc., 301 Ga. App. 694, 689 S.E.2d 330 (2009) (evidence supported verdict where company was financially able to undertake new opportunity that had been presented to company's officer); Ins. Indus. Consultants, LLC v. Alford, 294 Ga. App. 747, 669 S.E.2d 724 (2008) (where no contractual relationship existed between company and prospective clients that company hoped to retain or acquire business with, or with whom it had to annually renew contracts with, such customers did not constitute business opportunity); Mau, Inc. v Human Techs., Inc., 274 Ga. App. 891, 619 S.E.2d 394 (2005) (no proof of a business opportunity to usurp). But see Quinn v. Cardiovascular Physicians, P.C., 254 Ga. 216, 326 S.E.2d 460 (1985) (factual question as to whether company's one-year contract constituted a business opportunity based on realistic and substantive expectation of its renewal, continuation or extension).

Then, the court must determine whether the corporate official violated a fiduciary duty in appropriating the opportunity. If the opportunity is found to be a corporate one, liability should not be imposed upon the acquiring officer if the evidence establishes that his acquisition did not violate his fiduciary duty of loyalty, good faith and fair dealing toward the corporation. Se. Consultants, Inc. v. McCrary Eng'g Corp., 246 Ga. 503, 273 S.E.2d 112 (1980); see also United Seal & Rubber Co. v. Bunting, 248 Ga. 814, 285 S.E.2d 721 (1982); Singer v. Habif, Arogeti & Wynne, P.C., 250 Ga. 376, 297 S.E.2d 473 (1982); Jenkins v. Smith, 244 Ga. App. 541, 542, 535 S.E. 2d 521, 523 (2000) (applying "good will" and "dealing of long standing 'with [a] certain customer'" as defense to misappropriation of corporate opportunity claim); Parks v. Multimedia Tech., Inc., 239 Ga. App. 282, 288-9, 520 S.E.2d 517, 524 (1999) (there is no liability if corporation is financially unable to undertake the appropriated opportunity); Sofate of Am., Inc. v. Brown, 171 Ga. App. 39, 318 S.E.2d 771 (1984).

C. Limited Liability Code - Duties of Members

Absent provisions otherwise in the operating agreement or articles of organization, non-managing members of manager-managed LLC's owe no fiduciary duties to the LLC or other members under O.C.G.A. section 14-11-305. ULQ, LLC v. Meder, 293 Ga. App. 176, 666 S.E.2d 713 (2008) (affirming summary judgment on breach of fiduciary claim by LLC against member).

11 LC 29 4563S/AP

House Bill 30 (AS PASSED HOUSE AND SENATE)

By: Representative Willard of the 49th

A BILL TO BE ENTITLED

AN ACT

To provide for legislative findings; to amend Chapter 8 of Title 13 of the Official Code of Georgia Annotated, relating to illegal or void contracts generally, so as to repeal Code Section 13-8-2.1, relating to contracts in partial restraint of trade; to change provisions relating to contracts contravening public policy; to repeal Article 4 of Chapter 8 of Title 13, relating to restrictive covenants in contracts; to provide a statement of legislative findings; to define certain terms; to provide for applicability; to provide for the enforcement of contracts that restrict or prohibit competition in certain commercial agreements; to provide for the judicial enforcement of such provisions; to provide for the modification of such provisions; to provide for rebuttable presumptions; to provide for enforcement by third-parties; to provide for construction; to provide for related matters; to provide for an effective date and applicability; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

During the 2009 legislative session the General Assembly enacted HB 173 (Act No. 64, Ga. L. 2009, p. 231), which was a bill that dealt with the issue of restrictive covenants in contracts and which was contingently effective on the passage of a constitutional amendment. During the 2010 legislative session the General Assembly enacted HR 178 (Ga. L. 2010, p. 1260), the constitutional amendment necessary for the statutory language of HB 173 (Act No. 64, Ga. L. 2009, p. 231), and the voters ratified the constitutional amendment on November 2, 2010. It has been suggested by certain parties that because of the effective date provisions of HB 173 (Act No. 64, Ga. L. 2009, p. 231), there may be some question about the validity of that legislation. It is the intention of this Act to remove any such uncertainty by substantially reenacting the substantive provisions of HB 173 (Act No. 64, Ga. L. 2009, p. 231), but the enactment of this Act should not be taken as evidence of a legislative determination that HB 173 (Act No. 64, Ga. L. 2009, p. 231) was in fact invalid.

SECTION 2.

Chapter 8 of Title 13 of the Official Code of Georgia Annotated, relating to illegal and void contracts generally, is amended by repealing subsection (a) of Code Section 13-8-2, relating to contracts contravening public policy, and enacting a new subsection (a) to read as follows:

"(a) A contract that is against the policy of the law cannot be enforced. Contracts deemed contrary to public policy include but are not limited to:

(1) Contracts tending to corrupt legislation or the judiciary;

(2) Contracts in general restraint of trade, as distinguished from contracts which restrict certain competitive activities, as provided in Article 4 of this chapter;

(3) Contracts to evade or oppose the revenue laws of another country;

(4) Wagering contracts; or

(5) Contracts of maintenance or champerty."

SECTION 3.

Said chapter is further amended by repealing Code Section 13-8-2.1, relating to contracts in partial restraint of trade.

SECTION 4.

Said chapter is further amended by repealing Article 4, relating to restrictive covenants in contracts, and enacting a new Article 4 to read as follows:

"ARTICLE 4

13-8-50.

The General Assembly finds that reasonable restrictive covenants contained in employment and commercial contracts serve the legitimate purpose of protecting legitimate business interests and creating an environment that is favorable to attracting commercial enterprises to Georgia and keeping existing businesses within the state. Further, the General Assembly desires to provide statutory guidance so that all parties to such agreements may be certain of the validity and enforceability of such provisions and may know their rights and duties according to such provisions.

13-8-51.

As used in this article, the term:

(1) 'Affiliate' means:

(A) A person or entity that directly, or indirectly through one or more intermediaries, controls or is controlled by or is under common control with another person or entity;

(B) Any entity of which a person is an officer, director, or partner or holds an equity interest or ownership position that accounts for 25 percent or more of the voting rights or profit interest of such entity;

(C) Any trust or other estate in which the person or entity has a beneficial interest of 25 percent or more or as to which such person or entity serves as trustee or in a similar fiduciary capacity; or

(D) The spouse, lineal ancestors, lineal descendants, and siblings of the person, as well as each of their spouses.

(2) 'Business' means any line of trade or business conducted by the seller or employer, as such terms are defined in this Code section.

(3) 'Confidential information' means data and information:

(A) Relating to the business of the employer, regardless of whether the data or information constitutes a trade secret as that term is defined in Code Section 10-1-761;

(B) Disclosed to the employee or of which the employee became aware of as a consequence of the employee's relationship with the employer;

(C) Having value to the employer;

(D) Not generally known to competitors of the employer; and

(E) Which includes trade secrets, methods of operation, names of customers, price lists, financial information and projections, route books, personnel data, and similar information;

provided, however, that such term shall not mean data or information (A) which has been voluntarily disclosed to the public by the employer, except where such public disclosure has been made by the employee without authorization from the employer; (B) which has been independently developed and disclosed by others; or (C) which has otherwise entered the public domain through lawful means.

(4) 'Controlling interest' means any equity interest or ownership participation held by a person or entity with respect to a business that accounts for 25 percent or more of the voting rights or profit interest of the business prior to the sale, alone or in combination with the interest or participation held by affiliates of such person or entity.

(5) 'Employee' means:

(A) An executive employee;

(B) Research and development personnel or other persons or entities of an employer, including, without limitation, independent contractors, in possession of confidential information that is important to the business of the employer;

(C) Any other person or entity, including an independent contractor, in possession of selective or specialized skills, learning, or abilities or customer contacts, customer

information, or confidential information who or that has obtained such skills, learning, abilities, contacts, or information by reason of having worked for an employer; or

(D) A franchisee, distributor, lessee, licensee, or party to a partnership agreement or a sales agent, broker, or representative in connection with franchise, distributorship, lease, license, or partnership agreements.

Such term shall not include any employee who lacks selective or specialized skills, learning, or abilities or customer contacts, customer information, or confidential information.

(6) 'Employer' means any corporation, partnership, proprietorship, or other business organization, whether for profit or not for profit, including, without limitation, any successor in interest to such an entity, who or that conducts business or any person or entity who or that directly or indirectly owns an equity interest or ownership participation in such an entity accounting for 25 percent or more of the voting rights or profit interest of such entity. Such term also means the buyer or seller of a business organization.

(7) 'Executive employee' means a member of the board of directors, an officer, a key employee, a manager, or a supervisor of an employer.

(8) 'Key employee' means an employee who, by reason of the employer's investment of time, training, money, trust, exposure to the public, or exposure to customers, vendors, or other business relationships during the course of the employee's employment with the employer, has gained a high level of notoriety, fame, reputation, or public persona as the employer's representative or spokesperson or has gained a high level of influence or credibility with the employer's customers, vendors, or other business relationships or is intimately involved in the planning for or direction of the business of the employer or a defined unit of the business of the employer. Such term also means an employee in possession of selective or specialized skills, learning, or abilities or customer contacts or customer information who has obtained such skills, learning, abilities, contacts, or information by reason of having worked for the employer.

(9) 'Legitimate business interest' includes, but is not limited to:

(A) Trade secrets, as defined by Code Section 10-1-761;

(B) Valuable confidential information that otherwise does not qualify as a trade secret;

(C) Substantial relationships with specific prospective or existing customers, patients, vendors, or clients;

(D) Customer, patient, or client good will associated with:

(i) An ongoing business, commercial, or professional practice, including, but not limited to, by way of trade name, trademark, service mark, or trade dress;

(ii) A specific geographic location; or

(iii) A specific marketing or trade area; and

(E) Extraordinary or specialized training.

(10) 'Material contact' means the contact between an employee and each customer or potential customer:

(A) With whom or which the employee dealt on behalf of the employer;

(B) Whose dealings with the employer were coordinated or supervised by the employee;

(C) About whom the employee obtained confidential information in the ordinary course of business as a result of such employee's association with the employer; or

(D) Who receives products or services authorized by the employer, the sale or provision of which results or resulted in compensation, commissions, or earnings for the employee within two years prior to the date of the employee's termination.

(11) 'Modification' means the limitation of a restrictive covenant to render it reasonable in light of the circumstances in which it was made. Such term shall include:

(A) Severing or removing that part of a restrictive covenant that would otherwise make the entire restrictive covenant unenforceable; and

(B) Enforcing the provisions of a restrictive covenant to the extent that the provisions are reasonable.

(12) 'Modify' means to make, to cause, or otherwise to bring about a modification.

(13) 'Products or services' means anything of commercial value, including, without limitation, goods; personal, real, or intangible property; services; financial products; business opportunities or assistance; or any other object or aspect of business or the conduct thereof.

(14) 'Professional' means an employee who has as a primary duty the performance of work requiring knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction or requiring invention, imagination, originality, or talent in a recognized field of artistic or creative endeavor. Such term shall not include employees performing technician work using knowledge acquired through on-the-job and classroom training, rather than by acquiring the knowledge through prolonged academic study, such as might be performed, without limitation, by a mechanic, a manual laborer, or a ministerial employee.

(15) 'Restrictive covenant' means an agreement between two or more parties that exists to protect the first party's or parties' interest in property, confidential information, customer good will, business relationships, employees, or any other economic advantages that the second party has obtained for the benefit of the first party or parties, to which the second party has gained access in the course of his or her relationship with the first party or parties, or which the first party or parties has acquired from the second party as the result of a sale. Such restrictive covenants may exist within or ancillary to contracts

between or among employers and employees, distributors and manufacturers, lessors and lessees, partnerships and partners, employers and independent contractors, franchisors and franchisees, and sellers and purchasers of a business or commercial enterprise and any two or more employers. A restrictive covenant shall not include covenants appurtenant to real property.

(16) 'Sale' means any sale or transfer of the good will or substantially all of the assets of a business or any sale or transfer of a controlling interest in a business, whether by sale, exchange, redemption, merger, or otherwise.

(17) 'Seller' means any person or entity, including any successor-in-interest to such an entity, that is:

(A) An owner of a controlling interest;

(B) An executive employee of the business who receives, at a minimum, consideration in connection with a sale; or

(C) An affiliate of a person or entity described in subparagraph (A) of this paragraph; provided, however, that each sale involving a restrictive covenant shall be binding only on the person or entity entering into such covenant, its successors-in-interest, and, if so specified in the covenant, any entity that directly or indirectly through one or more affiliates is controlled by or is under common control of such person or entity.

(18) 'Termination' means the termination of an employee's engagement with an employer, whether with or without cause, upon the initiative of either party.

(19) 'Trade dress' means the distinctive packaging or design of a product that promotes the product and distinguishes it from other products in the marketplace.

13-8-52.

(a) The provisions of this article shall be applicable only to contracts and agreements between or among:

(1) Employers and employees;

(2) Distributors and manufacturers;

(3) Lessors and lessees;

(4) Partnerships and partners;

(5) Franchisors and franchisees;

(6) Sellers and purchasers of a business or commercial enterprise; and

(7) Two or more employers.

(b) The provisions of this article shall not apply to any contract or agreement not described in subsection (a) of this Code section.

13-8-53.

(a) Notwithstanding any other provision of this chapter, enforcement of contracts that restrict competition during the term of a restrictive covenant, so long as such restrictions are reasonable in time, geographic area, and scope of prohibited activities, shall be permitted. However, enforcement of contracts that restrict competition after the term of employment, as distinguished from a customer nonsolicitation provision, as described in subsection (b) of this Code section, or a nondisclosure of confidential information provision, as described in subsection (e) of this Code section, shall not be permitted against any employee who does not, in the course of his or her employment:

(1) Customarily and regularly solicit for the employer customers or prospective customers;

(2) Customarily and regularly engage in making sales or obtaining orders or contracts for products or services to be performed by others;

(3) Perform the following duties:

(A) Have a primary duty of managing the enterprise in which the employee is employed or of a customarily recognized department or subdivision thereof;

(B) Customarily and regularly direct the work of two or more other employees; and

(C) Have the authority to hire or fire other employees or have particular weight given to suggestions and recommendations as to the hiring, firing, advancement, promotion, or any other change of status of other employees; or

(4) Perform the duties of a key employee or of a professional.

(b) Notwithstanding any other provision of this chapter, an employee may agree in writing for the benefit of an employer to refrain, for a stated period of time following termination, from soliciting, or attempting to solicit, directly or by assisting others, any business from any of such employer's customers, including actively seeking prospective customers, with whom the employee had material contact during his or her employment for purposes of providing products or services that are competitive with those provided by the employer's business. No express reference to geographic area or the types of products or services considered to be competitive shall be required in order for the restraint to be enforceable. Any reference to a prohibition against 'soliciting or attempting to solicit business from customers' or similar language shall be adequate for such purpose and narrowly construed to apply only to: (1) such of the employer's customers, including actively sought prospective customers, with whom the employee had material contact; and (2) products or services that are competitive with those provided by the employer's business.

(c)(1) Activities, products, or services that are competitive with the activities, products, or services of an employer shall include activities, products, or services that are the same as or similar to the activities, products, or services of the employer. Whenever a

description of activities, products, or services, or geographic areas, is required by this Code section, any description that provides fair notice of the maximum reasonable scope of the restraint shall satisfy such requirement, even if the description is generalized or could possibly be stated more narrowly to exclude extraneous matters. In case of a postemployment covenant entered into prior to termination, any good faith estimate of the activities, products, or services, or geographic areas, that may be applicable at the time of termination shall also satisfy such requirement, even if such estimate is capable of including or ultimately proves to include extraneous activities, products, or services, or geographic areas. The postemployment covenant shall be construed ultimately to cover only so much of such estimate as relates to the activities actually conducted, the products or services actually offered, or the geographic areas actually involved within a reasonable period of time prior to termination.

(2) Activities, products, or services shall be considered sufficiently described if a reference to the activities, products, or services is provided and qualified by the phrase 'of the type conducted, authorized, offered, or provided within two years prior to termination' or similar language containing the same or a lesser time period. The phrase 'the territory where the employee is working at the time of termination' or similar language shall be considered sufficient as a description of geographic areas if the person or entity bound by the restraint can reasonably determine the maximum reasonable scope of the restraint at the time of termination.

(d) Any restrictive covenant not in compliance with the provisions of this article is unlawful and is void and unenforceable; provided, however, that a court may modify a covenant that is otherwise void and unenforceable so long as the modification does not render the covenant more restrictive with regard to the employee than as originally drafted by the parties.

(e) Nothing in this article shall be construed to limit the period of time for which a party may agree to maintain information as confidential or as a trade secret, or to limit the geographic area within which such information must be kept confidential or as a trade secret, for so long as the information or material remains confidential or a trade secret, as applicable.

13-8-54.

(a) A court shall construe a restrictive covenant to comport with the reasonable intent and expectations of the parties to the covenant and in favor of providing reasonable protection to all legitimate business interests established by the person seeking enforcement.

(b) In any action concerning enforcement of a restrictive covenant, a court shall not enforce a restrictive covenant unless it is in compliance with the provisions of Code

Section 13-8-53; provided, however, that if a court finds that a contractually specified restraint does not comply with the provisions of Code Section 13-8-53, then the court may modify the restraint provision and grant only the relief reasonably necessary to protect such interest or interests and to achieve the original intent of the contracting parties to the extent possible.

13-8-55.

The person seeking enforcement of a restrictive covenant shall plead and prove the existence of one or more legitimate business interests justifying the restrictive covenant. If a person seeking enforcement of the restrictive covenant establishes by prima-facie evidence that the restraint is in compliance with the provisions of Code Section 13-8-53, then any person opposing enforcement has the burden of establishing that the contractually specified restraint does not comply with such requirements or that such covenant is unreasonable.

13-8-56.

In determining the reasonableness of a restrictive covenant that limits or restricts competition during or after the term of an employment or business relationship, the court shall make the following presumptions:

(1) During the term of the relationship, a time period equal to or measured by duration of the parties' business or commercial relationship is reasonable, provided that the reasonableness of a time period after a term of employment shall be as provided for in Code Section 13-8-57;

(2) A geographic territory which includes the areas in which the employer does business at any time during the parties' relationship, even if not known at the time of entry into the restrictive covenant, is reasonable provided that:

(A) The total distance encompassed by the provisions of the covenant also is reasonable;

(B) The agreement contains a list of particular competitors as prohibited employers for a limited period of time after the term of employment or a business or commercial relationship; or

(C) Both subparagraphs (A) and (B) of this paragraph;

(3) The scope of competition restricted is measured by the business of the employer or other person or entity in whose favor the restrictive covenant is given; provided, however, that a court shall not refuse to enforce the provisions of a restrictive covenant because the person seeking enforcement establishes evidence that a restrictive covenant has been violated but has not proven that the covenant has been violated as to the entire scope of

the prohibited activities of the person seeking enforcement or as to the entire geographic area of the covenant; and

(4) Any restriction that operates during the term of an employment relationship, agency relationship, independent contractor relationship, partnership, franchise, distributorship, license, ownership of a stake in a business entity, or other ongoing business relationship shall not be considered unreasonable because it lacks any specific limitation upon scope of activity, duration, or geographic area so long as it promotes or protects the purpose or subject matter of the agreement or relationship or deters any potential conflict of interest.

13-8-57.

(a) In determining the reasonableness in time of a restrictive covenant sought to be enforced after a term of employment, a court shall apply the rebuttable presumptions provided in this Code section.

(b) In the case of a restrictive covenant sought to be enforced against a former employee and not associated with the sale or ownership of all or a material part of:

(1) The assets of a business, professional practice, or other commercial enterprise;

(2) The shares of a corporation;

(3) A partnership interest;

(4) A limited liability company membership; or

(5) An equity interest or profit participation, of any other type, in a business, professional practice, or other commercial enterprise,

a court shall presume to be reasonable in time any restraint two years or less in duration and shall presume to be unreasonable in time any restraint more than two years in duration, measured from the date of the termination of the business relationship.

(c) In the case of a restrictive covenant sought to be enforced against a current or former distributor, dealer, franchisee, lessee of real or personal property, or licensee of a trademark, trade dress, or service mark and not associated with the sale of all or a part of:

(1) The assets of a business, professional practice, or other commercial enterprise;

(2) The shares of a corporation;

(3) A partnership interest;

(4) A limited liability company membership; or

(5) An equity interest or profit participation, of any other type, in a business, professional practice, or other commercial enterprise,

a court shall presume to be reasonable in time any restraint three years or less in duration and shall presume to be unreasonable in time any restraint more than three years in duration, measured from the date of termination of the business relationship.

(d) In the case of a restrictive covenant sought to be enforced against the owner or seller of all or a material part of:

(1) The assets of a business, professional practice, or other commercial enterprise;

(2) The shares of a corporation;

(3) A partnership interest;

(4) A limited liability company membership; or

(5) An equity interest or profit participation, of any other type, in a business, professional practice, or other commercial enterprise,

a court shall presume to be reasonable in time any restraint the longer of five years or less in duration or equal to the period of time during which payments are being made to the owner or seller as a result of any sale referred to in this subsection and shall presume to be unreasonable in time any restraint more than the longer of five years in duration or the period of time during which payments are being made to the owner or seller as a result of any sale referred to in this subsection, measured from the date of termination or disposition of such interest.

13-8-58.

(a) A court shall not refuse to enforce a restrictive covenant on the ground that the person seeking enforcement is a third-party beneficiary of such contract or is an assignee or successor to a party to such contract.

(b) In determining the enforceability of a restrictive covenant, it is not a defense that the person seeking enforcement no longer continues in business in the scope of the prohibited activities that is the subject of the action to enforce the restrictive covenant if such discontinuance of business is the result of a violation of the restriction.

(c) A court shall enforce a restrictive covenant by any appropriate and effective remedy available at law or equity, including, but not limited to, temporary and permanent injunctions.

(d) In determining the reasonableness of a restrictive covenant between an employer and an employee, as such term is defined in subparagraphs (A) through (C) of paragraph (5) of Code Section 13-8-51, a court may consider the economic hardship imposed upon an employee by enforcement of the covenant; provided, however, that this subsection shall not apply to contracts or agreements between or among those persons or entities listed in paragraphs (2) through (7) of subsection (a) of Code Section 13-8-52.

13-8-59.

Nothing in this article shall be construed or interpreted to allow or to make enforceable any restraint of trade or commerce that is otherwise illegal or unenforceable under the laws of the United States or under the Constitution of this state or of the United States."

SECTION 5.

This Act shall become effective upon its approval by the Governor or upon its becoming law without such approval and shall apply to contracts entered into on and after such date and shall not apply in actions determining the enforceability of restrictive covenants entered into before such date.

SECTION 6.

All laws and parts of laws in conflict with this Act are repealed.

The Game Has Changed:
What Will Litigation Under The New Restrictive Covenants Act Look Like?

by Benjamin I. Fink, Esq., Kenneth N. Winkler, Esq. and Neal F. Weinrich, Esq.
Berman Fink Van Horn P.C.

By now, almost everyone is aware of Georgia's new Restrictive Covenant Act, O.C.G.A. § 13-8-50 *et seq.* (the "Act"). Most people also know the Act overturns more than one hundred years of Georgia case law and drastically changes the dynamic between employers and employees in Georgia with respect to the enforcement of non-competes and other restrictive covenants in employment agreements. What we do not yet know is how disputes will be resolved under the Act.

With a new set of rules, non-compete litigation will likely look entirely different. It is essentially a new season with a whole new set of rules for litigators in this area, who will combat their opponents with an arsenal of new (and mostly untested) arguments and litigation strategies.

This article provides a hypothetical roadmap of how a matter involving restrictive covenants governed by the Act might unfold.

The Client Call ("It's Time to Play Ball")

Your secretary buzzes you. She tells you that Robert Cox, the general counsel of one of your best clients, Bravos Field Turf Corporation ("BravosTurf"), is on the telephone and needs to speak with you about an urgent matter. Mr. Cox tells you that Mason Heyward, BravosTurf's youngest, but most prolific salesperson, abruptly resigned two days ago and is now working for BravosTurf's primary competitor, Turf-for-Less Corporation ("Turf-for-Less"). He also tells you that BravosTurf has learned Mr. Heyward has been soliciting three of BravosTurf's biggest customers which he serviced while employed by BravosTurf and which collectively are responsible for 40% of BravosTurf's revenue. BravosTurf is concerned Mr. Heyward is soliciting or will likely solicit business from other BravosTurf customers. BravosTurf views Mr. Heyward's employment with Turf-for-Less and his solicitation of BravosTurf's customers as a potentially very serious threat to its business.

You recall that you met with Mr. Cox and BravosTurf's President after the Act went into effect to discuss revising the non-competes and other restrictive covenants in BravosTurf's employment agreements. You ask if Mr. Heyward signed a revised agreement. As you pose this question to Mr. Cox, you open the file on your computer containing the form restrictive covenant agreement that your firm drafted for BravosTurf. You see it has both a non-solicitation covenant as well as a non-competition covenant. You recall that BravosTurf chose to include non-competition covenants in their new agreements, whereas previously BravosTurf steered away from including non-competition covenants due to the risk that they could be found unenforceable and render the non-solicitation covenants in the agreements unenforceable as well. You note that the non-competition covenant states that it restricts the employee from working within one hundred fifty miles of BravosTurf's headquarters, which are in downtown Atlanta.

As you quickly scan the agreement on your computer, Mr. Cox confirms that Mr. Heyward signed a new agreement. A few follow-up questions also confirm the agreement Mr. Heyward signed is substantially similar to the one you are viewing on your computer.

You discuss BravosTurf's options with Mr. Cox. The two of you decide that you will send a stern letter to Mr. Heyward reminding him of his obligations under the restrictive covenants in his agreement and demanding that he immediately cease and desist from violating his covenants through his employment with Turf-for-Less. You draft such a letter. Among other things, the letter advises Mr. Heyward that BravosTurf will pursue litigation and seek an injunction against him if he does not comply with its demands and cease his unlawful conduct. The letter also advises Mr. Heyward that BravosTurf will pursue any other causes of action it has against him based on evidence it has obtained or may obtain. The letter is sent that evening to Mr. Heyward via overnight mail. You also send a letter to Turf-for-Less informing Turf-for-Less of Mr. Heyward's restrictive covenants with BravosTurf and explaining that BravosTurf believes Turf-for-Less is tortiously interfering with BravosTurf's contractual relationship with Mr. Heyward through its employment of him. Of course, your letters also remind both Mr. Heyward and Turf-for-Less of their obligations to preserve relevant evidence relating to BravosTurf's potential claims.

The Initial Response From Opposing Counsel ("Assessing the Other Team's Line-Up")

A few days later, you receive a letter from Scottie Boras, who represents Mr. Heyward. The letter states that Mr. Heyward will not comply with BravosTurf's demands for a variety of reasons. The letter reads as follows:

> *Your letter states that O.C.G.A § 13-8-50 et seq. (the "Act") will govern the enforceability of the restrictive covenants in Mr. Heyward's employment agreement. However, Mr. Heyward is not an employee within the meaning of O.C.G.A. § 13-8-51(5). He was not an executive employee for BravosTurf. O.C.G.A. § 13-8-51(5)(A). He also was not involved in research and development and he was not and is not in possession of any confidential information important to BravosTurf's business. O.C.G.A. § 13-8-51(5)(B). He also was not and is not in possession of selective or specialized skills, learning, abilities, customer contacts, customer information or confidential information which he obtained* ***by reason of having worked for BravosTurf****. O.C.G.A. § 13-8-51(5)(C). Indeed, Mr. Heyward disputes having such skills, learning, abilities, contacts or information; as such, he is expressly exempted from the definition of an "employee" under the Act.*
>
> *To the extent Mr. Heyward has any such skills, learning, abilities, contacts or information, he obtained such skills while he was employed with Acme Turf Corporation ("Acme"). He worked for Acme for several years before joining BravosTurf, and he learned all information relating to the industry as well as the customer relationships referred to in your letter while working for Acme. As such, Mr. Heyward is not an employee within the meaning of the Act. The Act therefore does not apply to the employment agreement between BravosTurf and Mr. Heyward. O.C.G.A § 13-8-52(a)(1) ("The provisions of this article shall be applicable only to contracts and agreements*

between or among: (1) [e]mployers and employees, as such terms are defined in Code Section 13-8-51").

Since the Act does not apply, preexisting Georgia case law governs the enforceability of the restrictive covenants in Mr. Heyward's agreement. H.B. 173 §4. Under such law, as I am certain a practitioner as experienced in this area as you would acknowledge, the restrictive covenants are patently unenforceable and constitute an illegal restraint of trade. Mr. Heyward therefore will not comply with your demands that he abide by these unlawful restrictive covenants.

Even assuming that Mr. Heyward was an "employee" such that the Act governs the enforceability of the restrictive covenants and assuming that the restrictive covenants are enforceable under the new law, a court would not enjoin Mr. Heyward based on the non-compete in the agreement because of the extreme economic hardship that enforcement of the covenants will impose on Mr. Heyward. Mr. Heyward has worked in the baseball field turf industry since he graduated from high school and would be unable to find work in a different industry. Mr. Heyward has three children to support and a mortgage to pay. His wife also recently lost her teaching job. He and his family have resided in the Atlanta area for many years and it would be extremely burdensome, both financially and emotionally, to relocate his family, if he were even able to find a position in the baseball field turf industry located outside of the extremely broad, restricted territory in the agreement. In light of these facts, we seriously doubt that a court would enter an injunction against Mr. Heyward to enforce the restrictive covenants, even if the new law applies to him. See O.C.G.A. § 13-8-58(d).

Further, even if the Act governs the restrictive covenants and even if a court determines that enforcement of the covenants would not impose an economic hardship on Mr. Heyward (which we dispute), a court will surely not enforce the non-competition covenant because the restricted territory is patently overbroad. The new law requires that the geographic territory in a non-competition covenant be reasonable. See O.C.G.A. § 13-8-53(a). The one hundred fifty-mile radius contained in the non-competition is grossly unreasonable as Mr. Heyward only worked for or represented BravosTurf in limited areas in close proximity to metropolitan Atlanta (while O.C.G.A. § 13-8-56(c)(3) states that the geographic "scope of competition restricted is measured by the business of the employer [rather than by where the employee worked for or represented the employer]…", this provision only applies "[i]n determining the reasonableness of a restrictive covenant that limits or restricts competition during the course of an employment or business relationship..." O.C.G.A § 13-8-56). As the Act does not address what constitutes a reasonable geographical restriction for post-employment restrictive covenants, preexisting case law requiring a territory to be limited to the area where an employee worked for or represented the employer remains in effect. See, e.g., Howard Schultz & Assocs., Inc. v. Broniec, 239 Ga. 181, 183, 236 S.E.2d 265, 267-8 (1977).

Even if the reasonableness test in O.C.G.A. § 13-8-56(c)(3) applies to post-employment restrictive covenants (which we dispute), because BravosTurf itself does not

and has not done business throughout the area encompassed by the restricted territory, the territory does not constitute a "good faith estimate" of the maximum reasonable restricted geographical area. O.C.G.A § 13-8-53(c)(1). Further, although the new law allows courts to "blue pencil" over broad restrictive covenants, because the restricted territory is defined as "the area within a one hundred fifty-mile radius of BravosTurf's headquarters", rather than by listing the restricted counties or zip codes, it would be impossible for a court to exercise the discretion it has to modify the covenant by striking portions of the restricted territory to make it reasonable. See O.C.G.A. §§ 13-8-53(d); 13-8-54(b); 13-8-51(11). As such, the non-competition covenant would not be enforced, in the unfortunate event BravosTurf sought an injunction against Mr. Heyward.

Notwithstanding all of these reasons why we believe BravosTurf would not obtain any injunctive relief if it pursues litigation against Mr. Heyward, Mr. Heyward wishes to resolve this matter amicably. Please let me know if there are certain customers BravosTurf wishes to propose that Mr. Heyward not solicit for a limited period of time. Perhaps this can be a starting point for discussions concerning resolution of this dispute.

Analyzing the Issues ("The Scouting Report")

After reviewing Mr. Boras' letter, you reach for your file containing your notes and marked-up version of the Act. You have litigated several restrictive covenant cases with Mr. Boras before, and you know he is not only very competent in this area, but he also has a reputation for being one of the most aggressive lawyers in town. However, you also know that the Act created more questions than answers, and you have doubts about some of the arguments Mr. Boras has raised. Nevertheless, you want to review the statute carefully before you discuss the letter with your client. You quickly type the following list of the issues you feel you and your associate need to get your arms around:

1) ***Was Mr. Heyward ever an "executive"?*** *I seem to recall Mr. Cox telling me that Mr. Heyward was recently named the Vice President of Sales. Is that correct? If so, this fact could quickly dispose of Mr. Boras' dubious argument that Mr. Heyward is not an "employee" under the Act. O.C.G.A. § 13-8-51(5)(A).*

2) ***Did Mr. Heyward have confidential information which is important to BravosTurf's business?*** *If so, what was the confidential information and does the information satisfy each paragraph in O.C.G.A. § 13-8-51(3)(A)-(E)? Further, in light of the statements in Mr. Boras' letter, we should specifically confirm that the information which Mr. Cox believes is "confidential information" was disclosed to Mr. Heyward or he become aware of it as a consequence of his relationship with BravosTurf (O.C.G.A. § 13-8-51(3)(C)). We also need to ask him why the information was important to BravosTurf's business. Depending on Mr. Cox's responses, Mr. Heyward may qualify as an "employee" under O.C.G.A § 13-8-51(5)(B). We should be sure to get as much detail as possible regarding these issues and others from Mr. Cox as we will want to include these facts in BravosTurf's Verified Complaint if BravosTurf decides to pursue litigation.*

*3) **Did Mr. Heyward have selective or specialized skills, learning, abilities, customer contacts, customer information or confidential information?** Assuming BravosTurf contends he did have such skills, learning, abilities, contacts, and/or information as I expect it will, we need to discuss with Mr. Cox what evidence we can use in the lawsuit and/or at an injunction hearing to establish these facts so we can prove Mr. Heyward was an "employee" under the Act.*

*4) **Does it matter whether Mr. Heyward obtained his skills, learning, abilities, contacts or information while at Acme and not at BravosTurf?** While O.C.G.A § 13-8-51(8) provides that a "key employee" means "an employee in possession of selective or specialized skills, learning, or abilities or customer contacts or customer information who has obtained such skills, learning abilities, contacts, or information by reason of having worked for **the** employer", O.C.G.A. § 13-8-53(C), provides that an employee is any other person "... who or that has obtained such skills, learning, abilities, contacts, or information by reason of having worked for **an** employer." O.C.G.A. § 13-8-53(C) (emphasis added). Thus, under the plain language of the statute, Mr. Heyward need not have obtained his skills, learning, abilities, contacts or information from BravosTurf – rather, he could have learned those things from any employer. While the drafters of the statute may have intended something different, the language in the statute is unambiguous. Thus, as long as Mr. Heyward had skills, learning, abilities, contacts or information which he obtained by reason of working for **an** employer – no matter which one – shouldn't the court consider him an "employee" within the meaning of the Act?*

*5) **Is Mr. Heyward able to show economic hardship?** I should consider retaining an expert to show that there are plenty of job opportunities for Mr. Heyward. I should also ask Mr. Cox what BravosTurf knows about Mr. Heyward's finances. Does BravosTurf have evidence we can use to disprove Mr. Heyward's "economic hardship" defense? Do any employees of BravosTurf know the size of his house? Does BravosTurf have any information about the vacations he and his family have taken in the last few years? Does BravosTurf know whether he or his wife own multiple cars, and if so, what kinds? It sure would help our case if Mr. Heyward lives in a big house in Buckhead, sends his kids to private school and drives a BMW 7-Series.*

*6) **Is Mr. Boras' "territorial" argument incorrect?** As to whether the one hundred fifty-mile radius constitutes a reasonable geographical territory under the new law for a post-employment restrictive covenant, is Mr. Boras trying to capitalize on some sloppiness in the statute? O.C.G.A. § 13-8-56(2) and (3) provide guidelines for the reasonableness of territories in covenants restricting competition during the **course** of an employment or business relationship. O.C.G.A. § 13-8-53(c)(1) and (2) provide how an employer may adequately describe territories in covenants restricting competition after the **term** of employment, but do they speak to what will constitute a reasonable territory in such covenants? Does the statute leave room for Mr. Boras' argument that it fails to instruct as to what constitutes a reasonable geographic restriction for post-term restrictive covenants and that therefore the rules from pre-existing case law must govern the court's analysis of this issue? Isn't it more likely that courts will interpret the Act as easing what constitutes and how a drafter can adequately describe a reasonable territorial*

restriction? Contrary to Mr. Boras' contention, isn't it unlikely a court will find the geographical restriction in BravosTurf's non-competition covenant with Mr. Heyward to be fatal to the covenant as a whole? See, generally, O.C.G.A. § 13-8-53(c)(1) ("...The postemployment covenant shall be construed ultimately to cover only so much of such estimate as relates to the ... geographic areas actually involved within a reasonable period of time prior to termination."). In any event, it will be important to gather information from Mr. Cox about where BravosTurf conducts business and where Mr. Heyward worked for and represented BravosTurf.

7) ***Is Mr. Boras' "blue pencil" argument incorrect?*** *The Act permits a court to "modify" a covenant that is otherwise void and unenforceable. O.C.G.A. § 13-8-53(d). Under the new law, to "modify" a covenant means to bring about a "modification", and a "modification" means the "limitation of a restrictive covenant to render it reasonable in light of the circumstances in which it was made. [A modification] shall include: (a) Severing or removing that part of a restrictive covenant that would otherwise make the entire restrictive covenant unenforceable; and (B) Enforcing the provisions of a restrictive covenant to the extent that the provisions are reasonable." O.C.G.A. § 13-8-51(11) and (12). Thus, while blue penciling may be one tool at a court's disposal to modify a covenant to make it reasonable, it does not seem to be the only one. A reasonable reading of the statute indicates the Act vests courts with authority to take steps to modify a covenant such that it is reasonable and can be enforced.*

Strategic Discussion with the Client ("The Meeting on the Mound")

Having carefully analyzed the issues raised in Mr. Boras' letter, you call Mr. Cox. You walk him through your analysis of Mr. Boras' letter and you obtain information from Mr. Cox to help you further analyze Mr. Boras' arguments. Based on information he provides, you are confident Mr. Heyward will be considered an "employee" under the statute as at a minimum he had access to names of customers and price lists, both of which are identified as potentially being confidential information under O.C.G.A. § 13-8-51(3)(E). You also learn from Mr. Cox that Mr. Heyward earned at least $250,000 per year for the last five years, received a $130,000 sales bonus two months before he left BravosTurf and took at least two international vacations per year the last few years. He also lives in a nice house in Alpharetta and drives a Mercedes E-class. Mr. Cox is thus justifiably skeptical that enforcement of the one-year non-competition covenant would cause Mr. Heyward any economic hardship.

Mr. Cox asks you his chances of obtaining an injunction against Mr. Heyward. He also lets you know that BravosTurf is not interested in resolving the matter unless Mr. Heyward and Turf-for-Less agree to discontinue their relationships with the BravosTurf customers he already solicited and Mr. Heyward agrees to enter into a Consent Order whereby he agrees to fully comply with the non-solicitation provision. You explain to Mr. Cox that while the Act is imperfect and untested and allows lawyers representing employees to assert some arguments against employers seeking to enforce restrictive covenants, just as Mr. Boras has, you are confident in BravosTurf's right to obtain at least some injunctive relief if it chooses to try to enforce Mr. Heyward's restrictive covenants (though this could also depend on what judge is

assigned to the case). Mr. Cox tells you to broach a resolution with Mr. Boras but to proceed with preparing and filing a lawsuit against Mr. Heyward.

Pre-litigation Negotiations ("Staring Down the Batter")

You call Mr. Boras and tell him that BravosTurf is willing to forego enforcement of the non-competition covenant if Mr. Heyward and Turf-for-Less will stop doing business with the BravosTurf customers that Mr. Heyward dealt with during his employment with BravosTurf and Mr. Heyward will agree to a Consent Order concerning the non-solicitation provision. Mr. Boras says he will relay your offer but expects that while Mr. Heyward remains open to agreeing not to solicit certain customers whom he and Turf-for-Less are not already doing business with, if that is unacceptable to BravosTurf and BravosTurf decides to file suit to try to enforce the covenants, Mr. Heyward will likely just "take his chances" on the outcome.

During the call, Mr. Boras states that if BravosTurf tries to enforce the restrictive covenants through legal action, in addition to the various reasons contained in his letter as to why the covenants should not be enforced, Mr. Heyward will also assert a challenge to the constitutionality of the amendment to the Georgia Constitution allowing the Act to take effect, on the grounds that the language of the enabling referendum was misleading and deceptive. You have been aware of potential challenges to the referendum language but what you have read in the non-compete blogosphere confirm your analysis that this argument is an uphill battle. As you are discussing this issue with Mr. Boras, you scribble a note on your legal pad to have your associate begin preparing a bench brief on this issue for the imminent TRO hearing.

Preparing the Pleadings ("Bringing the Heat")

You and your associate begin preparing a complaint, a motion for temporary restraining order and preliminary injunction, and a supporting brief. You pepper Mr. Cox and Mr. Heyward's supervisor at BravosTurf with e-mails about the details of Mr. Heyward's customer relationships, customer good will, and training. You explain to BravosTurf that the Act requires an employer to plead and prove the existence of one or more legitimate business interests to justify the restrictive covenants and that your questions are intended to gather information about how BravosTurf can establish in its complaint that it has legitimate business interests. O.C.G.A. § 13-8-55; O.C.G.A. § 13-8-51(9)(C), (D), and (E). You tell Mr. Cox one way that BravosTurf may establish it has a legitimate business interest in enforcing the covenants is by showing that BravosTurf has "substantial relationships with specific prospective or existing customers, patients, vendors, or clients." O.C.G.A. § 13-8-51(9)(C). You tell Mr. Cox that while the Act is unclear as to what is meant by a "substantial" relationship and while you know BravosTurf is reluctant to specifically identify its customers or the financial reasons why BravosTurf believes its relationships with its customers should be considered "substantial", you believe it is important that BravosTurf meet the prerequisites under the Act, particularly since Mr. Boras and Mr. Heyward appear bent on defending aggressively and will undoubtedly use whatever arguments they can conjure up based on the Act to try to capitalize on any potential loopholes in BravosTurf's pleadings. To address BravosTurf's concerns about disclosing its customer relationships and financial information regarding the relationships, you propose to Mr. Cox that you will request permission from the Court to have the Clerk file BravosTurf's pleadings under

seal. When he learns that including information in the complaint which will satisfy the prerequisites under the Act (including information showing that BravosTurf conducted business throughout the one hundred fifty-mile radius for its headquarters and that the geographic territory in the non-competition covenant is therefore reasonable), will shift the burden of proof to Mr. Heyward to demonstrate that the covenant is unreasonable, Mr. Cox approves of your decision to try to file the action under seal. O.C.G.A. § 13-8-55.

Having spent the weekend preparing and finalizing the complaint, motion, brief and supporting affidavits containing all of your evidence, and your evidence regarding the customers Mr. Heyward has taken, you send your associate to the courthouse on Monday morning to file everything and to attempt to get a TRO hearing scheduled. She also files the motion for expedited discovery you have prepared given that you are certain you will want to quickly conduct discovery regarding the defenses Mr. Boras has asserted that Mr. Heyward will raise, particularly if the case moves forward swiftly to a preliminary injunction hearing. Your associate returns from the courthouse and reports that Judge Fay Vincent's chambers called Mr. Boras while she was there to confirm his availability for a TRO hearing on that Friday.

The TRO Hearing ("The Payoff Pitch")

You begin preparing your outline for the hearing. You include in your outline responses to the various counter-arguments you know are coming from Mr. Boras concerning why the Act does not apply and why the Court should not enjoin Mr. Heyward. Mr. Boras files his opposition brief that Thursday. As you are fortunately prepared to address most of his arguments, the last-minute preparation is modest.

You arrive in Judge Vincent's courtroom on Friday morning. Judge Vincent starts by telling the parties that he has read the parties' briefs and that this case is not his "first rodeo" in the non-compete realm. He tells the attorneys he has handled many of these cases in his twenty years on the bench but none under the Act. As he says he is pleased that the Act finally allows him to require employees to honor and abide by the agreements they sign, you look out of the corner of your eye to gauge the reaction of Mr. Cox, who is attending the hearing with you. Judge Vincent also says he is equally concerned that the Act may encourage employers to overreach in their agreements because judges can blue-pencil covenants to make them more reasonable. Your optimism turns slightly out of fear that the Judge may think BravosTurf's covenants are unreasonable.

Judge Vincent then states that he does not want to hear anything further from the attorneys regarding the ballot referendum. He says he has briefly reviewed Mr. Heyward's arguments for why the referendum is unconstitutional and he has reviewed the order entered a week ago by his colleague a few floors below which declared the Act unconstitutional, a copy of which Mr. Heyward attached to his brief. He says he respectfully disagrees with his brother on the bench that the referendum was unconstitutional, but that he will not make a final ruling on that issue and would allow further argument and even evidence on it at a later stage in the case.

Judge Vincent hears the parties' arguments, including arguments based on the affidavit submitted by Mr. Heyward in support of his economic hardship defense. Judge Vincent says he

believes Mr. Heyward is clearly an employee within the meaning of the Act but has doubts that the geographical restriction in BravosTurf's non-competition covenant is reasonable. He believes some discovery and presentation of evidence is necessary before he can rule on whether it is over broad and if and how it should be modified. Picking up on an argument you made, Judge Vincent says he is reluctant to decide Mr. Heyward's economic hardship defense without giving you the opportunity to obtain financial documents from and depose Mr. Heyward regarding his financial wherewithal. After admitting he is unsure what the most appropriate interim relief to craft is, Judge Vincent decides to enter a temporary restraining order permitting Mr. Heyward to work for Turf-for-Less in a non-sales capacity and enjoining Mr. Heyward from directly or indirectly violating the non-solicitation covenant. Judge Vincent schedules a preliminary injunction hearing for three weeks later and authorizes the parties to conduct expedited discovery during that period.

Discovery ("Digging In")

You and your associate spend the next three weeks embroiled in expedited discovery. Mr. Boras takes depositions of two of Mr. Heyward's supervisors, one of whom makes some somewhat damaging admissions regarding the areas in which BravosTurf does business that you are concerned may pose a problem for enforcement of the one hundred fifty-mile radius. The other supervisor gives great testimony about the training, skills, and confidential information that Mr. Heyward obtained while at BravosTurf.

You depose representatives of two customers whom BravosTurf believes Mr. Heyward solicited and whom Mr. Cox says BravosTurf is unlikely to ever win back their business. One of them admits Mr. Heyward solicited them to move their business from BravosTurf to Turf-for-Less. The other testifies his company approached Mr. Heyward when they heard through the grapevine that he had left BravosTurf and taken a position at Turf-for-Less. As this customer offers this testimony, you recall that BravosTurf chose to have its new non-solicitation covenants prohibit employees from accepting unsolicited business. When you were revising the covenants for BravosTurf, you discussed with Mr. Cox how under Georgia's pre-existing case law, a non-solicitation covenant could not prohibit a former employee from accepting business from a customer without any prior solicitation by the former employer and the Act does not appear to have changed this rule. See, e.g., Waldeck v. Curtis 1000, Inc., 261 Ga. App. 590, 583 S.E.2d 266 (2003) ("…. a non-solicitation provision may not contain a bar on the acceptance of business from unsolicited clients"). However, you also advised BravosTurf that, if a court ever applied the Act and found that BravosTurf's non-solicitation covenant could not lawfully restrict its employee from accepting unsolicited business, the court could also simply blue pencil the "acceptance" language out of the agreement. BravosTurf therefore chose to have its non-solicitation covenants prohibit both solicitation and acceptance of business from former customers. Nevertheless, you do not probe deeply into this issue at the customer's deposition, as to date Mr. Boras has not raised this issue and you do not want to risk bringing it to his attention.

Of course, you also depose Mr. Heyward. When at Mr. Boras' instruction Mr. Heyward refuses to answer questions regarding his finances, savings, and spending patterns, you are forced to call Judge Vincent's chambers with a request for a telephone hearing in the middle of

the deposition. When Judge Vincent finally gets on the line and says he has only five minutes because he is in the middle of a hearing in a death penalty case, you explain the dispute and that you believe you are entitled to conduct a thorough examination of Mr. Heyward regarding his finances given that he has asserted that the court should not enforce his covenants due to the economic hardship that would be imposed on him. O.C.G.A. § 13-8-58(d). Judge Vincent says he will not give you carte blanche to examine Mr. Heyward regarding all of his finances and assets and he believes you should limit your examination to what finances and liquid assets Mr. Heyward has available to live off of in the event that the court enforced the year-long non-competition covenant. You and Mr. Boras spar over the meaning of Judge Vincent's ruling for the rest of Mr. Heyward's deposition. After the deposition, you promptly file a motion to compel Mr. Heyward to answer certain questions he refused to answer, but with the injunction hearing three days away, you are doubtful you will get answers to these questions prior to the hearing.

The Preliminary Injunction Hearing ("The Bottom of the Ninth")

The day of the injunction hearing arrives. Both parties present their evidence. Mr. Boras focuses his presentation on his arguments that the geographic territory in the non-competition covenant is unreasonable and that enforcement of the non-competition covenant would impose a severe economic hardship on Mr. Heyward and his family.

Judge Vincent expresses doubts that the one hundred fifty-mile radius in the non-competition covenant is reasonable and asks for additional briefing on the issue of whether its overbreadth would render the non-competition covenant unenforceable in its entirety because the territory cannot be "blue penciled" based on how it is drafted, or whether he can reform the territory to an area he finds is reasonable. The parties submit their post-hearing briefs and competing proposed orders.

The Order ("Post Game Wrap-Up")

A week later, you receive an order from the court. You call Mr. Cox to explain that Judge Vincent enjoined Mr. Heyward from violating the non-solicitation covenant but declined to enjoin him with respect to the non-competition covenant based on his ruling that he could not "blue pencil" the geographic territory, which he found to be overbroad. You tell Mr. Cox that you think Judge Vincent's ruling that he cannot "blue pencil" the geographic territory and that the Act does not permit him to judicially modify the territory to an area he finds is reasonable is erroneous. You explain that while you believe this error gives BravosTurf strong grounds to appeal the order (or to cross-appeal if Mr. Heyward appeals the injunction entered against him with respect to the non-solicitation covenant), given the discretion judges are afforded in entering injunctions, there is no guarantee of a reversal, as the Court of Appeals may find it was within Judge Vincent's discretion to deny BravosTurf any injunctive relief based on the non-competition covenant. You explain that until Georgia's appellate courts provide guidance on interpreting the Act, it is difficult to predict how the appellate courts will decide this issue and others.

You also ask Mr. Cox to begin thinking through BravosTurf's strategy for moving forward in this case. You remind him that since Judge Vincent has enforced the non-solicitation

covenant, if BravosTurf wishes to continue to litigate against Mr. Heyward, it may pursue claims for damages against him for the business lost from customers he has already taken.

You mention that while you believe Judge Vincent's ruling on whether he could have judicially modified the territory is wrong and that you are confident that the Georgia appellate courts will eventually vindicate your analysis of the Act with respect to this issue, if BravosTurf wishes to err on the cautious side by revising its agreements, it could revise its non-competition covenants to specifically list the counties, cities or zip codes in which post-employment competition is restricted. You explain to Mr. Cox that if the agreements are drafted in this manner, any extraneous areas could unquestionably be stricken if the territory was ever found to be overbroad. You ask Mr. Cox if he would like to schedule a time to meet to discuss further revisions to BravosTurf's employment agreements.

Finally, you also tell Mr. Cox that later that day you are sending him your firm's month-end invoice for the case. You let him know that the amount of the invoice is greater than invoices for the initial stages of non-compete litigation matters that you have handled for BravosTurf in the past. You explain to Mr. Cox that while the Act makes it substantially easier for employers like BravosTurf to obtain some injunctive relief against rogue employees like Mr. Heyward, unfortunately, litigating non-compete matters under the Act will more often than not be significantly more expensive than litigating under Georgia's pre-existing restrictive covenants case law.

As this hypothetical shows, litigating restrictive covenant cases under the Act will present a host of unknowns. There are numerous legal issues raised by the Act, many of which are not mentioned in this article, which will require appellate interpretation and clarification and/or legislative revision. Furthermore, while the Act makes it easier for employers to obtain some relief against former employees, results under the Act are going to be inherently unpredictable for quite some time. This lack of predictable outcomes for cases litigated under the Act also presents a challenge from a client management standpoint, as does the likely added cost associated with litigating cases under the Act.

In time, practitioners in the area of Georgia restrictive covenants law will of course know much more about litigation under the Act. In the interim, while this article attempts to provide a glimpse into what litigation under the Act might look like, practitioners should expect the unexpected and anticipate a few curve balls along the way.

Benjamin I. Fink and Kenneth N. Winkler are shareholders and Neal F. Weinrich is an associate in the Atlanta law firm Berman Fink Van Horn P.C. where they focus their practices on non-compete and other competition-related disputes and employment law.

State Bar of Georgia
INSTITUTE OF CONTINUING LEGAL EDUCATION

STATE BAR SERIES

Trade Secrets, Confidential Information And Computer Fraud And Abuse

Presented By:

Neal F. Weinrich
Berman Fink Van Horn PC, Atlanta, GA

Georgia Law of Trade Secrets and Confidential Information

R. Carl Cannon
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP
Suite 2400
230 Peachtree Street, N.W.
Atlanta, Georgia 30303
Telephone: (404) 525-8622
E-mail: ccannon@constangy.com

TABLE OF CONTENTS

Page

Page

TABLE OF AUTHORITIES

CASES

Page

Page

Page

Page

Page

Page

Page

Page

Page

Page

TREATISES

OTHER AUTHORITIES

Georgia Law of Trade Secrets and Confidential Information

I. Introduction

While it has become almost trite to say, we are indeed living in an information age. Information today is being created faster and disseminated more widely than ever before. It is virtually impossible to read a newspaper or magazine without finding some reference to the Internet and its World Wide Web. This paper will address the protection afforded information under Georgia law.

The value of information generally is derived from the knowledge it provides, not the physical form in which it is embodied. Unlike most tangible property, information can be appropriated from one who has it without depriving that person of its possession. Therefore, this paper will focus primarily on information as an intangible, without regard to the physical form in which it is recorded.

Common law protection of information has developed based on theories of property and contract rights. The concept of "trade secrets" was devised to recognize property rights in certain unique types of information. Contract law has evolved to extend protection by agreement to certain other types of information not regarded as trade secrets. Effective May 11, 2011, this category of information was given statutory recognition by being included in the definition of "confidential information" along with trade secrets. *See* O.C.G.A. § 13-8-51(3).

In 1990, Georgia's General Assembly enacted the Georgia Trade Secrets Act ("GTSA"), O.C.G.A. §§ 10-1-760, *et seq*., which refined the definition of "trade secret" and modified Georgia's common law of trade secrets. The GTSA is based upon, but differs in some respects from, the Uniform Trade Secrets Act ("UTSA"). A copy of the GTSA is provided in Appendix A, pages 56-61 *infra*, and a copy of the UTSA is provided in Appendix B, pages 62-66 *infra*. The GTSA did not affect the common law concerning confidential information.

By acknowledging and providing legal protection for trade secrets, the law recognizes the public interest in encouraging the creation and use of commercially valuable information. Conversely, by placing restrictions on what information qualifies for trade secret protection, the law recognizes the public interest in the free flow of information.

Similarly, by permitting contractual protection for confidential information, the law upholds fundamental freedom of contract principles. At the same time, however, the law limits the availability of contract protection in order to promote two other public interests: preventing unreasonable restraints on trade and allowing workers to enjoy the economic benefits that flow naturally from the increase in knowledge, skills and abilities that comes from experience.

II. Trade Secrets

A. General Definition

Under the GTSA, a trade secret is any information that meets the following three-pronged test: (1) the information is not commonly known by or available to the public; (2) the information has actual or potential economic value to its possessor because others who can obtain economic value by using or disclosing it (a) generally do not know it *and* (b) cannot readily ascertain it by proper means; and (3) the possessor has made reasonable efforts to keep the information secret. O.C.G.A. § 10-1-761(4). As long as information satisfies this three-pronged test, no contract is required to entitle its owner to trade secret protection. O.C.G.A. §§ 10-1-762(d) and 10-1-763(c).

Prior to the GTSA, a "trade secret" under Georgia law was defined as a " 'plan, process, tool, mechanism, or compound, known only to its owner and those of his employees to whom it must be confided in order to apply it to the uses intended.' " *American Buildings Co. v. Pascoe Building Systems, Inc.*, 260 Ga. 346, 349, 392 S.E.2d 860, 864 (1990) (citation omitted). A trade secret under this definition "was protectable as a property right where (1) it was sufficiently concrete in its development to be usable . . . ; (2) it was novel and original and of value . . . ; and (3) it was not generally known in the trade." *Union Carbide Corp. v. Tarancon Corp.*, 742 F. Supp. 1565, 1579 (N.D. Ga. 1990).

The GTSA's definition of a protectable trade secret seems more expansive than Georgia's common law definition. To date, however, the reported cases under the GTSA have not identified anything that is now a trade secret under the GTSA that would not have been a trade secret under common law.

B. Types of Information Potentially Covered

The plain language of the GTSA encompasses literally any type of information that meets the three-pronged test described above. Nevertheless, the statute recognizes particular types of information that can come within the definition of trade secret. They are: (1) technical or nontechnical data, (2) formulas, (3) patterns, (4) compilations, (5) programs, (6) devices, (7) methods, (8) techniques, (9) drawings, (10) processes, (11) financial data, (12) financial plans, (13) product plans, and (14) lists of actual or potential customers or suppliers. O.C.G.A. § 10-1-761(4).

It is significant that, of all the types of information listed in the statute, only information concerning customers and suppliers is preceded by the word "lists." The Georgia Supreme Court has held that this usage means the GTSA has not changed the general common law rule that the intangible information contained in such lists is not a trade secret, even though the lists themselves may be. *Avnet, Inc. v. Wyle Laboratories, Inc.*, 263 Ga. 615, 619-20, 437 S.E.2d 302, 305 (1993); *accord Allen v. Hub Cap Heaven, Inc.*, 225 Ga. App. 533, 536, 484 S.E.2d 259, 263 (1997); *Amerigas Propane, L. P. v. T-Bo Propane, Inc.*, 972 F. Supp. 685, 697-98 (S.D. Ga. 1997) (discussing the 1996 amendments to the

GTSA). Thus, the owner of such lists is entitled to an injunction for their return and, presumably, damages for their prior use, but not an injunction against a former employee's use of whatever he remembers about the lists. *DeGiorgio v. Megabyte International, Inc.*, 266 Ga. 539, 540, 468 S.E.2d 367, 369 (1996) (Disclosure or use of "personal knowledge [of customer and vendor information] may be forbidden through the use of restrictive covenants, but not under the Trade Secrets Act."). *But see Morgan Stanley DW, Inc. v. Frisby*, 163 F. Supp. 2d 1371, 1378-82 (N.D. Ga. 2001) (suggesting that customer lists may not be entitled to trade secret protection in the brokerage industry).

On its face, the *Avnet* decision, *supra*, seems to apply only to lists of actual or potential customers and suppliers. The court of appeals, however, apparently reads the decision more expansively. *See Stone v. Williams General Corp.*, 266 Ga. App. 608, 611, 597 S.E.2d 456, 460 (2004). In *Stone*, the court stated, albeit in *dicta*,

> In *Avnet* our Supreme Court held that an individual is free to use any information he can remember from his former employment, **including trade secrets**, in the absence of a valid and enforceable covenant.

Id. (emphasis added), *rev'd on other grounds*, 279 Ga. 428, 614 S.E.2d 758 (2005); *see also Manuel v. Convergys Corp.*, 430 F.3d 1132, 1140-41 (11th Cir. 2005). Given this decision, prudence dictates using written agreements to protect all intangible trade secrets unless or until this aspect of *Stone* is overruled.

C. Three-pronged Test

As stated above, the GTSA provides a three-pronged test for determining the existence of a trade secret. Prior to the GTSA, whether something qualified as a trade secret was considered a question of fact. *Outside Carpets, Inc. v. Industrial Rug Co.*, 228 Ga. 263, 267-68, 185 S.E.2d 65, 68 (1971). That remains the case under the GTSA. *Insight Technologies, Inc. v. Freightcheck, LLC*, 280 Ga. App. 19, 27, 633 S.E.2d 373, 380 (2006).

1. First Prong

The first statutory prong requires that the information not be commonly known by or available to the public. This prong was added by the 1996 amendments to the GTSA, but it is not clear how, if at all, it changed the law. As will be seen, prior to (and after) the 1996 amendments, the GTSA definition of trade secrets included a requirement that to be a trade secret information must not be readily ascertainable by proper means by others who can obtain economic value from it. O.C.G.A. § 10-1-761(4)(A). It is difficult to imagine how information that is commonly known by or available to the public could meet this requirement.

Nevertheless, while information in the public domain cannot be a trade secret, systems or processes that combine such information in a unique way may be a trade secret. An example of this is seen in the Supreme Court of Georgia's decision in *Essex Group, Inc. v. Southwire Company*, 269 Ga. 553, 501 S.E.2d 501 (1998). In that case, Southwire claimed that its logistics system was a trade

secret. Southwire had developed the system at considerable expense over a period of three years, but most of its components were commercially available. Rejecting a contention that a trade secret cannot be comprised of matters within the public domain, the court held that " 'a trade secret can include a system where the elements are in the public domain, but there has been accomplished an effective, successful and valuable integration of the public domain elements and the trade secret gave the [trade secret owner] a valuable competitive advantage which is protected from misappropriation.' " 269 Ga. at 555, 501 S.E.2d at 503, *quoting Rivendell Forest Products v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994).

Moreover, the fact that a system's function "can be reproduced with a combination of commercially available components and reverse engineering" does not necessarily preclude the system from being a trade secret if it is unique to its owner. *Tronitec, Inc. v. Shealy*, 249 Ga. App. 442, 449, 547 S.E.2d 749, 756 (2001), *rev'd on other grounds*, 277 Ga. 210, 586 S.E.2d 661 (2003).

2. Second Prong

(a) Economic Value

The second statutory prong requires that for information to be a trade secret it must have actual or potential economic value to its possessor *because* others who can obtain economic value by using or disclosing it (i) generally do not know it *and* (ii) cannot readily ascertain it by proper means.

The statute does not specify how much economic value the information must have. In *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337, 357 (M.D. Ga. 1992), the court found the requisite economic value in the fact that the plaintiff derived significant income from licensing the computer software at issue. Therefore, since the plaintiff also "made considerable efforts to maintain the secrecy" of its software, the court concluded that the software was a trade secret under the GTSA. *Id*. at 357-58.

Although neither the *CMAX/Cleveland* decision nor other published decisions have discussed the issue, the language of the GTSA suggests that it is not so much the magnitude of the economic value that is important as the reason for the economic value. The statute itself requires that the economic value be derived from the fact that others who can benefit from the trade secret generally do not know it and cannot readily ascertain it through proper means. This implies that the importance of economic value as a criterion is that it gives one who knows the information at issue a competitive advantage in business. Thus, the primary focus should be on the extent to which others know the information or can readily ascertain it by proper means.

In *CMAX/Cleveland*, for example, the economic value of the software at issue presumably derived primarily from the fact that others did not know its source code and would have had to expend substantial efforts to develop the equivalent by independent means. Until others could offer competitive products

through the results of their own efforts, CMAX/Cleveland's software enjoyed a competitive advantage and could command a higher license fee.

(b) Generally Unknown

In addition, the information must not be generally known to others who can benefit economically from it. The common law rule was essentially the same. *See Thomas v. Best Manufacturing Corp.*, 234 Ga. 787, 790, 218 S.E.2d 68, 71 (1975) (Trade secret protection "does not exist, however, with respect to matters which are generally known in the trade . . . ."); *Outside Carpets, Inc. v. Industrial Rug Co.*, 228 Ga. 263, 268, 185 S.E.2d 65, 68 (1971); *Taylor Freezer Sales Co. v. Sweden Freezer Eastern Corp.*, 224 Ga. 160, 164, 160 S.E.2d 356, 359 (1968); *Wilson v. Barton & Ludwig, Inc.*, 163 Ga. App. 721, 723, 296 S.E.2d 74, 77 (1982). The fact-intensive nature of this requirement is illustrated by Georgia Supreme Court's decision in *Outside Carpets, Inc. v. Industrial Rug Co.*, 228 Ga. 263, 185 S.E.2d 65 (1971).

The alleged trade secret in *Outside Carpets* was a "so-called vinyl fusing oven used to laminate vinyl backing to carpets, rugs and mats, and the process utilized by the plaintiff in connection therewith." 228 Ga. at 264, 185 S.E.2d at 66. The plaintiff presented evidence of the unique nature of its oven, including the testimony of its president that there were only four such ovens in existence, two in plaintiff's plant, one built at another company's plant under license from the plaintiff, and one at the defendant company's plant. The individual defendant, on the other hand, gave an affidavit to the effect that he had developed

the oven for the plaintiff using skills he had acquired from working at various plants for more than 20 years. He further averred that the plaintiff's oven involved no new principles or features not generally known in the industry and that similar ovens were in use at a number of other companies. The Georgia Supreme Court held that it was a question of fact whether the plaintiff's oven, together with the processes it used, was a trade secret. 228 Ga. at 266-67, 185 S.E.2d at 67-68.

(c) Not Readily Ascertainable

Finally, the information must not be readily ascertainable by proper means. Here, too, the common law rule probably was the same. *Cf. American Photocopy Equipment Co. v. Henderson*, 250 Ga. 114, 115, 296 S.E.2d 573, 575 (1982) (denying protection to customer lists not obtained by "improper means"); *Thomas v. Best Manufacturing Corp.*, 234 Ga. 787, 789, 218 S.E.2d 68, 71 (1975) ("Trade secrets are entitled to protection so long as competitors fail to duplicate them by legitimate, independent research.").

Proper means under the GTSA include "[r]everse engineering of a trade secret not acquired by misappropriation" and "independent development." O.C.G.A. § 10-1-761(1). The statute does not indicate what other means might be considered proper.

The Supreme Court of Georgia, however, has found that proper means also may include compiling information from published sources. *Leo Publications, Inc. v. Reid*, 265 Ga. 561, 562, 458 S.E.2d 651, 652 (1995). In *Leo Publications*, a

publisher sought trade secret protection for information concerning the names of its advertisers and the size and frequency of their advertisements. The court held that this information was not a trade secret because any of the publisher's readers could readily compile that information by simply reading the publication.

The GTSA's definition of "improper means" is reasonably comprehensive. "Improper means" include: (1) "theft," (2) "bribery," (3) "misrepresentation," (4) "breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use," or (5) "espionage through electronic or other means." O.C.G.A. § 10-1-761(1). This definition is essentially derived from common law. *See* Restatement of Torts, § 759, Comment (c) (defining "improper means" as "theft, trespass, bribing or otherwise inducing employees or others to reveal the information in breach of duty, fraudulent misrepresentations, threats of harm by unlawful conduct, wire tapping, procuring one's own employees or agents to become employees of the other for purposes of espionage and so forth"). In *AirWatch LLC v. Mobile Iron, Inc.*, Civil Action No. 1:12-cv-3571-JEC, 2013 WL 4757491, *5 (N.D. Ga. Sept. 4, 2013), the court held that the defendant's alleged "use of false identities, email addresses, phone numbers, and a fake business" to obtain access to the plaintiff's proprietary software satisfied the GTSA's definition of "improper means."

3. Third Prong

The third prong of the test requires that for information to qualify as a trade secret under the GTSA, the possessor must make reasonable efforts to keep

the information secret. No Georgia Supreme Court nor any Georgia Court of Appeals decisions could be found indicating that this requirement existed prior to the GTSA. The common law in other jurisdictions, however, has required efforts to maintain secrecy. *See* 1 R. Milgrim, *Milgrim on Trade Secrets* § 1.04, at 1-99 (1994). In addition, the Eleventh Circuit seems to have concluded that this requirement existed under Georgia common law. *See Roboserve, Ltd. v. Tom's Foods, Inc.*, 940 F.2d 1441, 1454-55 (11th Cir. 1991) (A plaintiff seeking trade secret protection under Georgia law "must demonstrate that access to the alleged trade secret has been strictly limited.").

Only a few cases have considered this requirement under the GTSA. In *Avnet, Inc. v. Wyle Laboratories, Inc.*, 263 Ga. 615, 437 S.E.2d 302 (1993), the Georgia Supreme Court addressed the plaintiff's efforts to maintain the secrecy of customer lists. The court noted that "[t]here was evidence that the customer lists were not freely or widely disseminated and that certain employees to whom the information contained in the lists had been disclosed were required to sign agreements to keep the information secret." 263 Ga. at 617, 437 S.E.2d at 304. The court concluded that this evidence was sufficient to support a finding that the plaintiff "had made a reasonable effort to maintain the secrecy" of the lists. *Id.* In the court's view, it was immaterial that not all employees were required to sign nondisclosure agreements because the law protects trade secrets even in the absence of a written agreement. *Id.*

Customer lists were also at issue in *Smith v. Mid-States Nurses, Inc.*, 261 Ga. 208, 403 S.E.2d 789 (1991). There, however, the only evidence that the plaintiff endeavored to maintain the secrecy with respect to any of its operations was testimony that it instructed the defendant "to maintain the confidentiality of written forms [the agency] had developed, including applications for nurses, contracts for nurses and health facilities, and [the agency's] price list and billing form." Since these written forms were not the lists at issue, the court concluded that there was "no evidence" that the plaintiff had "made reasonable efforts under the circumstances" to protect its alleged trade secrets. 261 Ga. at 209, 403 S.E.2d at 790; s*ee also Bacon v. Volvo Service Center, Inc.*, 266 Ga. App. 543, 545, 597 S.E.2d 440, 443-44 (2004) (rejecting trade secret protection for customer lists where there was no effort to protect secrecy).

Bid calculations were at issue in *Infrasource, Inc. v. Hahn Yalena Corp.*, 272 Ga. App. 144, 613 S.E.2d 144 (2005). The plaintiff in that case claimed its bid numbers were trade secrets; however, the plaintiff's bid disclosed the alleged trade secrets to the prospective customer without any confidentiality requirement. Therefore, the court held that any effort the plaintiff made to maintain secrecy was unreasonable as a matter of law. 272 Ga. App. at 149, 613 S.E.2d at 709-10.

In *Equifax Services, Inc. v. Examination Management Services, Inc.*, the court of appeals held that, under the circumstances in that case, simply requiring employees to sign an agreement prohibiting the disclosure of confidential

information did not constitute a reasonable effort to maintain the secrecy of the alleged trade secret. 216 Ga. App. 35, 40, 453 S.E.2d 488, 493 (1994). The court took care, however, to observe that it was not holding "that requiring employees to sign confidentiality agreements alone is never sufficient to constitute a reasonable step to maintain . . . secrecy" under the GTSA. *Id.* Indeed, the court noted that in some cases requiring employees to sign nondisclosure agreements "may well be the only reasonable step that can be taken . . . ." *Id.*

While the *Equifax* decision left open the possibility that only requiring employees to execute confidentiality agreements sometimes may satisfy the GTSA's requirement for taking reasonable steps to protect trade secrets, it would be unwise to rely on that possibility if any additional steps could be taken. For example, in *Diamond Power International, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007), the court found that Diamond Power's use of a general confidentiality agreement was insufficient to entitle it to trade secret protection for its Hardware Book file "in light of Diamond Power's demonstrated ability to be more restrictive over information which it wished to keep secret, and the availability of other measures to guard its secrecy . . . ." *Id.* at 1335. Moreover, at least one court has read *Diamond Power* to support the proposition that " 'Georgia law is well established that requiring employees "to sign a general confidentiality agreement upon the commencement of their employment does not alone demonstrate that [the employer's] efforts to maintain secrecy were reasonable." ' " *The B & F System, Inc. v. LeBlanc*, Civil Action No. 7:07-cv-192

(HL), 2011 WL 4103576, at *25 (M.D. Ga. Sept. 14, 2011), *quoting Diamond Power's* citation of *Equifax*.

In any event, requiring nondisclosure agreements of employees is not essential for obtaining judicial protection for trade secrets, *provided* the owner has taken other appropriate steps to preserve their secrecy. *See Sanford v. RDA Consultants, Ltd.*, 244 Ga. App. 308, 312, 535 S.E.2d 321, 325 (2000). *But see Stone v. Williams General Corp.,* 266 Ga. App. 608, 611, 597 S.E.2d 456, 459 (2004), *rev'd on other grounds*, 279 Ga. 428, 614 S.E.2d 758 (2005).

In *Servicetrends, Inc. v. Siemens Medical Systems, Inc.*, 870 F. Supp. 1042 (N.D. Ga. 1994), the defendant counterclaimed seeking trade secret protection for certain technical data used in servicing a lithotripter sold under the name "Lithostar." The defendant contended that one of its former employees had misappropriated its trade secrets by disclosing this technical data to his current employer, who was a competitor in servicing Lithostar machines. The court found that the defendant provided all of the technical data to its customers and at least some of the data to the plaintiff in conjunction with the plaintiff's purchase of spare parts from the defendant. Therefore, the court concluded that the defendant's "wide distribution of the allegedly confidential technical data remove[d] any legal protection it might otherwise have had as trade secrets." *Id.* at 1074.

In *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337, 357 (M.D. Ga. 1992), the district court found that the plaintiff had "made considerable efforts to

maintain the secrecy" of its computer software. There, the plaintiff (1) registered its software under the Copyright Act as an unpublished work containing trades secrets, (2) licensed the software under agreements that strictly prohibited reproduction or disclosure to third parties, (3) placed proprietary notices on the software's documentation, (4) required employees to sign confidentiality agreements and made them aware of the secrecy of the software, (5) required employees whose work necessitated printing the software's source code to shred the printout afterwards, and (6) limited disclosure of the software to those who licensed it or signed a nondisclosure agreement. This impressive showing led the court to conclude that the plaintiff had met the third prong's requirement for a trade secret. *Id*. at 357-58.

Elaborate steps to protect trade secrets from disclosure by state agencies to whom they are required to be disclosed technically is not required to preserve their trade secret status. *See Georgia Department of Natural Resources v. Theragenics Corp.*, 273 Ga. 724, 545 S.E.2d 904 (2001). Since the Georgia Open Records Act was amended in 2012, however, "[a]n entity submitting records containing trade secrets that wishes to keep such records confidential under [the Open Records Act exemption for trade secrets] shall submit and attach to the records an affidavit affirmatively declaring that specific information in the records constitute trade secrets pursuant to" the GTSA. O.C.G.A. § 50-18-72(a). Moreover, in any action against a state agency to enjoin the agency's release of a trade secret, the owner of the trade secret must present evidence that the

information in question meets all the requirements of the GTSA. *See State Road and Tollway Authority v. Electronic Transaction Consultants Corp.*, 306 Ga. App. 487, 490, 702 S.E.2d 486, 489 (2010). The procedure for doing so is specified in the Open Records Act as amended in 2012. O.C.G.A. § 50-18-72(a).

D. Duration of Protection

Under the GTSA, "trade secret information is protectable until it has been acquired by others by proper means." *Essex Group, Inc. v. Southwire Company*, 269 Ga. 553, 556, 501 S.E.2d 501, 504 (1998). This is consistent with prior law. *See Thomas v. Best Manufacturing Corp.*, 234 Ga. 787, 789, 218 S.E.2d 68, 71 (1975).

E. Relief for Actual or Threatened Misappropriation

1. Substantive Relief

Before addressing the specific types of relief which may be obtained under the GTSA, it should be noted that at least one court has held that relief was available against a former employee under prior law even for innocent misappropriation. *Union Carbide Corp. v. Tarancon Corp.*, 742 F. Supp. 1565, 1580 n. 6 (N.D. Ga. 1990). This should remain the case under the GTSA because its definition of misappropriation does not require that a former employee knowingly breached his duty not to disclose or use his former employer's trade secret. *See* O.C.G.A. § 10-1-761(2)(B)(ii)(II). It also should be noted that alleging misappropriation of trade secrets in terms of legal conclusions may not survive a motion to dismiss, at least in federal court. *See Southern Nuclear Operating Co.*

v. Electronic Data Systems Corp., Civil Action File No. 1:06-cv-1988-TCB, N.D. Ga., Docket No. 86, Order filed July 6, 2007, *aff'd* 273 Fed. Appx. 834 (11th Cir. 2008).

The GTSA affords a variety of relief for misappropriation of trade secrets. It authorizes courts to enjoin actual or threatened misappropriation. O.C.G.A. § 10-1-762(a). An injunction may even extend for some period after the trade secret loses its status as a trade secret, if the loss of that status is due to a defendant's misappropriation. *Id.* In a case decided under prior law, the Georgia Supreme Court held that it was not an abuse of discretion to grant an interlocutory injunction where the evidence was in conflict concerning whether the information at issue constituted a trade secret. *American Buildings Co. v. Pascoe Building Systems, Inc.*, 260 Ga. 346, 350, 392 S.E.2d 860, 864 (1990). More recently, the court of appeals stated that "[w]here the trial court, in ruling on an interlocutory injunction, makes findings of fact based upon conflicting evidence, this court will not disturb the ruling as an abuse of discretion unless the denial or granting of the injunction was based on an erroneous interpretation of law." *Covington v. D. L. Pimper Group, Inc.*, 248 Ga. App. 265, 267, 546 S.E.2d 37, 39 (2001). Nevertheless, while a plaintiff may obtain an interlocutory injunction based on conflicting evidence concerning whether particular information constitutes a trade secret, an absence of evidence with respect to any essential element of a trade secret will defeat a motion for injunctive relief. *See Merial Limited v. Roman*, Civil Action No. 1:10-CV-0760-RWS, 2010 WL

1249646, *1 (N.D. Ga. March 24, 2010) (plaintiff failed to "present evidence of reasonable efforts to maintain the secrecy of the information").

That injunctive relief under the GTSA can be quite creative is illustrated by the case of *Essex Group, Inc. v. Southwire Company*, 269 Ga. 553, 501 S.E.2d 501 (1998). In that case, Southwire Company sued a former employee and his new employer to protect Southwire's logistics system, which it contended was a trade secret. The former employee had overseen the development of Southwire's logistics system, and his new employer was a direct competitor of Southwire. The trial court ruled that Southwire's logistics system was a trade secret and granted creative relief. First, the court issued an injunction barring the former employee from working in his new employer's logistics department for five years, or sooner if the new employer independently developed its own logistics system before then. Second, the court appointed an impartial verifier to confirm compliance with the injunction and to determine when the new employer had independently developed its own system. 269 Ga. at 553, 501 S.E.2d at 502. The Georgia Supreme Court upheld the trial court's order. 269 Ga. at 557-59, 501 S.E.2d at 505-06.

One commentator has suggested that the *Southwire* decision, *supra*, may have signaled the Georgia Supreme Court's implicit adoption of the inevitable disclosure doctrine. Birg, *Application of the "Inevitable Disclosure" Doctrine in Georgia,* 6 Ga. B.J. 58 (April 1999). Whether or not the inevitable disclosure doctrine is viable in Georgia, the supreme court has made clear that it "is not an

independent claim under which a trial court may enjoin an employee from working for an employer or disclosing trade secrets." *Holton v. Physician Oncology Services, LP*, 292 Ga. 864, 870, 742 S.E.2d 702, 706 (2013). While the doctrine still may support a claim for threatened misappropriation, the supreme court expressly left that issue undecided in *Holton*. *Id*.

An injunction under the GTSA also may prohibit one who misappropriates a trade secret from benefiting from the misappropriation. For example, where an individual misappropriates from his or her former employer a client list constituting a trade secret and uses the list to obtain business from clients on it, the individual may be enjoined from providing competitive services to any clients so obtained. *See Paramount Tax & Accounting, LLC v. H & R Block Eastern Enterprises, Inc.*, 299 Ga. App. 596, 604, 683 S.E.2d 141, 148 (2009). The injunction may not, however, extend to clients on the list who were obtained by means other than use of the misappropriated list. *Id*.

To obtain an injunction, however, a trade secret owner must show either actual or threatened misappropriation. O.C.G.A. § 10-1-762(a); *American Software USA, Inc. v. Moore*, 264 Ga. 480, 484, 448 S.E.2d 206, 209 (1994). Such a showing does not necessarily require direct evidence. Circumstantial evidence may suffice, even in the face of sworn denial of misappropriation. *See Tronitec, Inc. v. Shealy*, 249 Ga. App. 442, 451-52, 547 S.E.2d 749, 758 (2001), *rev'd on other grounds*, 277 Ga. 210, 586 S.E.2d 661 (2003). On the other hand, where the circumstantial evidence can be construed as consistent with a denial of

misappropriation and other direct evidence, such circumstantial evidence will be insufficient to avoid summary judgment. *See Contract Furniture Refinishing & Maintenance Corp. v. Remanufacturing & Design Group, LLC*, 317 Ga. App. 47, 56-57, 730 S.E.2d 708, 714-15 (2012).

It also is important to note that to obtain an injunction against a non-party requires a showing that the non-party acted in concert with an enjoined party. *See Bea Systems, Inc. v. Webmethods, Inc.*, 265 Ga. 503, 509-11, 595 S.E.2d 87, 91-93 (2004).

Prior law did not require that the terms of an injunction disclose the trade secrets to which it related; the injunction "need only include a general description of the trade secrets sought to be protected." *Ward v. Process Control Corp.*, 247 Ga. 583, 584, 277 S.E.2d 671, 673 (1981). Presumably this remains true under the GTSA. However, an injunction against "using, reproducing, distributing, disclosing or otherwise disseminating [Plaintiffs'] trade secrets and proprietary information" has been held to be insufficiently specific to comply with the requirements of O.C.G.A. § 9-11-65(d). *Pregler v. C&Z, Inc.*, 259 Ga. App. 149, 575 S.E.2d 915 (2003).

In exceptional circumstances where it would be unreasonable for some reason to prohibit future use, a court may issue an injunction conditioning future use on payment of a reasonable royalty. O.C.G.A. § 10-1-762(b). The statute gives as an example of such an exceptional circumstance the situation where an infringer's "material and prejudicial change of position prior to acquiring

knowledge or reason to know of misappropriation . . . renders a prohibitive injunction inequitable." *Id.*

The statute also authorizes courts to order "affirmative acts to protect a trade secret." O.C.G.A. § 10-1-762(c).

Under the GTSA, the owner of a trade secret is entitled to recover damages for its misappropriation. O.C.G.A. § 10-1-763(a). Recovery of damages may be either in addition to or in lieu of injunctive relief. *Id.* Recoverable "[d]amages include *both* the actual loss caused by misappropriation *and* the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss." *Id.* (emphasis added); *see also White v. Arthur Enterprises, Inc.*, 219 Ga. App. 124, 464 S.E.2d 225 (1995). If a trade secret's owner fails to prove any damages caused by the misappropriation by a preponderance of the evidence, "the court may award damages caused by misappropriation measured in terms of a reasonable royalty . . . ." *Id.* In that case, the royalty may not be for longer "than the period of time for which use [of the trade secret] could have been prohibited." *Id.*

In addition to compensatory damages, the court may award exemplary damages if the misappropriation is found to have been "willful and malicious." O.C.G.A. § 10-1-763(b). Evidence of hiring a competitor's employees, stealing the competitor's software, and soliciting the competitor's customers has been held to support a finding of willful and malicious misappropriation. *Brandenburg v. All-Fleet Refinishing, Inc.*, 252 Ga. App. 40, 42-43, 555 S.E.2d 508, 512 (2001).

Exemplary damages may be awarded in any amount not exceeding twice the award of compensatory damage (*i.e.*, the amount awarded as actual and/or unjust enrichment damages, or as damages measured as a reasonable royalty). O.C.G.A. § 10-1-763(b). Exemplary damages may be awarded in an appropriate case even though no demand for such damages was made in the complaint. *Brandenburg v. All-Fleet Refinishing, Inc.*, 252 Ga. App. 40, 42, 555 S.E.2d 508, 512 (2001).

Finally, the GTSA authorizes courts to award reasonable attorneys' fees to trade secret owners who establish "willful and malicious misappropriation." O.C.G.A. § 10-1-764. Courts may also award attorneys' fees to prevailing parties if "a claim of misappropriation is made in bad faith [or] a motion to terminate an injunction is made or resisted in bad faith . . . ." *Id.*

The defendant in a recent federal case sought novel relief for the plaintiffs' alleged violation of the GTSA. The plaintiffs in that case, *Wells v. Daugherty Systems, Inc.*, Civil Action No. 1:14-CV-2655-WSD, 2014 WL 4545790 (N.D. Ga. Sept. 12, 2014), sought to enjoin the defendant, their former employer, from enforcing allegedly invalid covenants restricting their competition with the defendant. The defendant argued in response, based on the plaintiffs' alleged violations of the GTSA and Georgia's criminal trespass statute, that the doctrine of "unclean hands" barred the plaintiffs from obtaining injunctive relief. The district court rejected the argument, holding that, although the defendant's accusations could form the basis of separate claims against the plaintiffs, the

accusations did "not restrict the court's authority to grant equitable relief in the form of an injunction, enjoining Defendant from enforcing the Restrictive Covenants." *Id*. at *4.

2. Procedural Relief

The Georgia Civil Practice Act and the Federal Rules of Civil Procedure authorize protective orders to govern the extent and manner of disclosure relating to trade secrets. O.C.G.A. § 9-11-26(c)(7); Fed. R. Civ. P. 26(c)(7). A good example of a comprehensive protective order covering trade secrets and other confidential information may be found at *Abdallah v. The Coca Cola Co.*, No. 98-CV-3679-RWS, 1999 WL 527740 (N.D. Ga. June 23, 1999). Failure to obtain an appropriate protective order before disclosing a trade secret in discovery could result in its loss.

In addition, the GTSA expressly directs courts to protect the secrecy of trade secrets during litigation. O.C.G.A. § 10-1-765. The statute even authorizes courts to order "any person involved in the litigation not to disclose an alleged trade secret without prior court approval." *Id*. Therefore, it probably would be prudent to request that the court exercise this authority with respect to everyone who may be present during any hearing or trial in the case, including jurors. That is especially so because, to survive summary judgment (at least in federal court), a party seeking trade secret protection "needs to provide sufficient detail about the trade secret for the Court to ascertain whether there is a genuine issue of material fact regarding both the existence and the misappropriation of the trade

secret." *Purchasing Power, LLC v. Bluestream Brands, Inc.*, Civil Action No. 1:12-CV-258-WSD, 2014 WL 1870734, *6-*7 (N.D. Ga. May 9, 2014); *Ferco Enterprises, Inc. v. Taylor Recycling Facility LLC*, Civil Action No. 1:05-cv-2980-ODE, N.D. Ga., Docket No. 373, Order filed Oct. 16, 2007, pp. 42-43, *aff'd* 291 Fed. Appx. 304 (11th Cir. 2008).

It also would be prudent to disclose as little as possible during trial about the specifics of the trade secrets being litigated. Prior to the GTSA, it was held that a plaintiff seeking relief in equity is not "required to make public upon the record of the court the complete details of its trade secrets in order to protect them." *Taylor Freezer Sales Co. v. Sweden Freezer Eastern Corp.*, 224 Ga. 160, 165, 160 S.E.2d 356, 360 (1968); *accord Rollins Protective Services Co. v. Palermo*, 249 Ga. 138, 142 n. 1, 287 S.E.2d 546, 550 n. 1 (1982). Presumably that remains true under the GTSA.

Nevertheless, some trial courts insist that the trade secrets at issue be placed in the record so that the record will be complete in the event of an appeal. When faced with that situation, it would be prudent to request that the court order the trade secrets placed under seal. This procedure is expressly authorized under the GTSA. O.C.G.A. § 10-1-765 (court may order "sealing the records of the action"). A similar request should be made at the appellate court level in the event of an appeal, although the fact that the record initially is filed in the appellate court without being sealed may not destroy the trade secret status of information contained in it. *See Stone v. Williams General Corp.*, 266 Ga. App.

608, 611 n. 4, 597 S.E.2d 456, 459 n. 4 (2004), *rev'd on other grounds*, 279 Ga. 428, 614 S.E.2d 758 (2005); *Tronitec, Inc. v. Shealy*, 249 Ga. App. 442, 450-51, 547 S.E.2d 749, 757 (2001), *rev'd on other grounds*, 277 Ga. 210, 586 S.E.2d 661 (2003).

F. Statute of Limitations

The statute of limitations for actions under the GTSA is five years and runs from the time "the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered" (the "discovery rule"). O.C.G.A. § 10-1-765. The statute provides that "a continuing misappropriation by any person constitutes a single claim against that person . . . ." *Id.* It is unclear whether this means that the statute of limitations for a continuing misappropriation runs from the first or last act of misappropriation which the trade secret owner discovered or should have discovered. However, the concluding phrase of the GTSA's statute of limitations section states, "but this Code section shall be applied separately to the claim against each person who receives a trade secret from another person who misappropriated that trade secret." This qualifying phrase may mean that the statute of limitations with respect to the initial offender runs from the date of the first act of misappropriation that the trade secret owner discovered or should have discovered.

The Georgia Court of Appeals addressed the so-called "discovery rule" in *Porex Corp. v. Haldopoulos*, 284 Ga. App. 510, 644 S.E.2d 349 (2007). There,

the court pointed out that a claim accrues when the plaintiff has "knowledge of sufficient facts from which a reasonable jury could infer misappropriation," *i.e.*, when a plaintiff has sufficient information to make out a "meaningfully colorable" claim. 284 Ga. App. at 515, 644 S.E.2d at 353. Thus, suspicion alone of possible misappropriation is not sufficient to establish "objectively reasonable notice" that would trigger the running of the statute. *Id.* The court also held, however, that the plaintiff is required to exercise reasonable diligence to discover misappropriation of trade secrets. 284 Ga. App. at 516, 644 S.E.2d at 353. Accordingly, "when there is reason to suspect that a trade secret has been misappropriated, and a reasonable investigation would produce facts sufficient to confirm this suspicion (and justify bringing suit), the limitations period begins, even though the plaintiff has not conducted such an investigation." *Id.* If, however, "a person becomes aware of facts which would make a reasonably prudent person suspicious, he or she has a duty to investigate further and is charged with knowledge of matters which would have been revealed by such an investigation." 284 Ga. App. at 516, 644 S.E.2d at 353-54. The limitations period can be tolled, however, if "certain facts necessary to the claim are unavailable even to a reasonably diligent plaintiff." 284 Ga. App. at 516, 644 S.E.2d at 354. In that case, the period is tolled until those facts become available. *Id.*

Presumably, the statute of limitations for misappropriation of trade secrets prior to the GTSA was four years. *See* O.C.G.A. § 9-3-32 ("Recovery of personal property; damages for conversion or destruction").

When dealing with trade secrets, it is wise to act quickly regardless of how long the applicable statute of limitations may be. Failure to do so could make it impossible, as a practical matter, to obtain effective relief in some cases.

G. Effect on Common Law and Other Statutes

The GTSA supersedes conflicting laws providing civil remedies for misappropriation of trade secrets. O.C.G.A. § 10-1-767(a); *Robbins v. Supermarket Equipment Sales, LLC*, 290 Ga. 462, 465, 722 S.E.2d 55, 58 (2012); *Servicetrends, Inc. v. Siemens Medical Systems, Inc.*, 870 F. Supp. 1042, 1073 (N.D. Ga. 1994). For example, the statute supersedes actions for conversion, breach of confidential relationship and duty of good faith, unjust enrichment, and *quantum meruit* that are based on the alleged misappropriation of trade secrets. *RMS Titanic, Inc. v. Zaller*, 978 F. Supp. 2d 1275, 1296 (N.D. Ga. 2013); *Tronitec, Inc. v. Shealy*, 249 Ga. App. 442, 447, 547 S.E.2d 749, 755 (2001), *rev'd on other grounds*, 277 Ga. 210, 586 S.E.2d 661 (2003); *Penalty Kick Management Ltd. v. The Coca Cola Co.*, 164 F. Supp. 2d 1376, 1379 (N.D. Ga. 2001); *Diamond Power International, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1345 (N.D. Ga. 2007). The GTSA also supersedes actions for breach of fiduciary duty to the extent based on misappropriation of trade secrets. *Putters v. Rmax Operating, LLC,* No. 1:13-cv-3382-TWT, 2014 WL 1466902, *2 (N.D. Ga. April 15, 2014); *Keg*

Technologies, Inc. v. Lamier, 436 F. Supp. 2d 1364, 1377 (N.D. Ga. 2006). Furthermore, a plaintiff claiming misappropriation of trade secrets under the GTSA "cannot be allowed to plead a lesser alternate theory of restitution simply because the information does not qualify as a trade secret." *Robbins v. Supermarket Equipment Sales, LLC*, 290 Ga. 462, 465, 722 S.E.2d 55, 58 (2012).

Earlier this year, the Northern District of Georgia held that the GTSA preempts an action for computer theft under the Georgia Computer Systems Protection Act where the alleged theft (misappropriation of allegedly confidential and proprietary information) was accomplished by the unauthorized use of an employer's computer system to download the information. *RLI Insurance Co. v. Banks*, No. 1:14–CV–1108–TWT, 2015 WL 400540, *2 (N.D. Ga. Jan. 28, 2015). *RLI Insurance* seems inconsistent with a subsequent Georgia Court of Appeals case and two earlier cases in the Northern District of Georgia, but it does not appear that the GTSA preemption issue was raised in those cases. *Lyman v. Cellchem International, LLC*, No. A15A1282, 2015 WL 7291213, *5-*6 (Ga. App. Nov. 19, 2015); *Putters v. Rmax Operating, LLC,* No. 1:13-cv-3382-TWT, 2014 WL 1466902, *4 (N.D. Ga. April 15, 2014*); Vurv Technology LLC v. Kenexa Corp.*, No. 1:08-cv-3442-WSD, 2009 WL 2171042, *3-4 (N.D. Ga. July 20, 2009) . While at first blush the *RLI Insurance* decision also might seem inconsistent with the decision in *DuCom v. State*, 288 Ga. App. 555, 654 S.E.2d 670 (2008) , it is not, because *DuCom* was a criminal case and did not involve civil remedies.

The GTSA does not, however, affect contractual duties or remedies. O.C.G.A. § 10-1-767(b)(1). Nor does it affect other civil remedies that are not based on trade secret misappropriation. O.C.G.A. § 10-1-767(b)(2). With respect to contract actions, it is important to note that the GTSA provides that "a contractual duty to maintain a trade secret or limit use of a trade secret shall not be deemed void or unenforceable solely for lack of a durational or geographic limitation on the duty." O.C.G.A. § 10-1-767(b)(1). This savings provision was applied in *Wright v. Power Industry Consultants, Inc.*, 234 Ga. App. 833, 508 S.E.2d 191 (1998). The nondisclosure provision at issue in *Wright* contained no durational limit and its scope appears clearly to have included confidential business information that would not have qualified as a trade secret under the GTSA. 234 Ga. App. at 837-38, 508 S.E.2d at 195. Without discussing the provision's failure to distinguish between trade secrets and other types of confidential information, the court invoked O.C.G.A. § 10-1-767(b)(1) to uphold the provision insofar as it pertained to trade secrets. *Id.*; *see also* O.C.G.A. § 13-8-53(e).

When the exception for contractual remedies is taken into account, the scope of the GTSA's supersession may be stated as follows: the GTSA supersedes all non-contractual civil remedies for the misappropriation of intangible information, whether or not the information meets the GTSA's definition of trade secret. *See Meyn America, LLC v. Tarheel Distributors, Inc.*, Civil Action No. 5:14-CV-41(MTT), 2014 WL 3824313, *9-*11 (M.D. Ga. Aug. 4, 2014); *Robbins v.*

Supermarket Equipment Sales, LLC, 290 Ga. 462, 465-67, 722 S.E.2d 55, 58 (2012); *Professional Energy Management, Inc. v. Necaise*, 300 Ga. App. 223, 224-25, 684 S.E.2d 374, 377 (2009); *Dial HD, Inc., v. ClearOne Communications, Inc.*, No. CV 109-100, 2010 WL 3732115, *10-12 (S.D. Ga. Sept. 7, 2010); *PHA Lighting Design, Inc. v. Kosheluk*, No. 1:08-cv-01208-JOF, 2010 WL 1328754, *10-11 (N.D. Ga. March 30, 2010); *Diamond Power International, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1345 (N.D. Ga. 2007). Nevertheless, "[a] claim for fraud, which involves willful misrepresentation or deception, may be viable even if the allegedly-misrepresented information was a trade secret or a public record. " *RMS Titanic, Inc. v. Zaller*, 978 F. Supp. 2d 1275, 1296 (N.D. Ga. 2013).

III. Confidential Information

A. Introduction

The main distinction between trade secrets and "confidential information" is that the law generally will not provide protection for "confidential information" in the absence of an enforceable contract prohibiting its use or disclosure. *Durham v. Stand-by Labor of Georgia, Inc.*, 230 Ga. 558, 563, 198 S.E.2d 145, 149 (1973). The only exception to this requirement for a contract appears to be situations in which confidential information is "procured by improper means or otherwise disclosed without privilege, as in violation of relations of confidence." *Id.*; *accord Wesley-Jessen, Inc. v. Armento*, 519 F. Supp. 1352, 1361 (N.D. Ga.

1981); *TDS Healthcare Systems Corp. v. Humana Hospital Illinois, Inc.*, 880 F. Supp. 1572, 1582 (N.D. Ga. 1995).

Prior to May 11, 2011, contracts prohibiting the use or disclosure of an employer's confidential information by an employee or former employee ("nondisclosure agreements") were governed solely by common law. That continues to be the case for nondisclosure agreements entered into prior to May 11, 2011.

For nondisclosure agreements entered into on or after May 11, 2011, Act 99 of the 2011 Georgia Laws (codified at O.C.G.A. §§ 13-8-50 through 13-8-59 and referred to hereafter as "Act 99") now applies. While Act 99 governs these more recent nondisclosure agreements, it does not necessarily supersede the common law in every instance. The following discussion of Georgia's law of confidential information will endeavor to point out those instances in which Act 99 changes the common law.

B. Definition of "Confidential Information"

Act 99 defines the term "Confidential Information" as follows:

"Confidential Information" means data and information:

> (A) Relating to the business of the employer, regardless of whether the data or information constitutes a trade secret as that term is defined in Code Section 10-1-761;
>
> (B) Disclosed to the employee or of which the employee became aware of (*sic*) as a consequence of the employee's relationship with the employer;

> (C) Having value to the employer;
>
> (D) Not generally known to competitors of the employer; and
>
> (E) Which includes trade secrets, methods of operation, names of customers, price lists, financial information and projections, route books, personnel data, and similar information;
>
> provided, however, that such term shall not mean data or information (A) which has been voluntarily disclosed to the public by the employer, except where such public disclosure has been made by the employee without authorization from the employer; (B) which has been independently developed and disclosed by others; or (C) which has otherwise entered the public domain through lawful means.

O.C.G.A. §13-8-51(3).

Georgia common law's definition of "confidential information" is not as precise. Indeed, the Northern District of Georgia appears to be the only court to have attempted to define what Georgia common law regards to be protectable "confidential information." That court identified the characteristics of "confidential information" as follows:

> Although Georgia law does not conclusively define "confidential information," it appears that the information must (1) be the plaintiff's property; (2) be peculiar to its business; and (3) the disclosure or use of which by the defendant causes injury to the plaintiff. *See Taylor Freezer Sales Co. v. Sweden Freezer Eastern Corp.*, 224 Ga. 160, 165, 160 S.E.2d 356 (1968). Further, the information must possess an element of secrecy peculiar to the

> complaining party, known only to it, not general secrets of the trade. *Id*. at 165, 160 S.E.2d 356.

TDS Healthcare Systems Corp. v. Humana Hospital Illinois, Inc., 880 F. Supp. 1572, 1585 (N.D. Ga. 1995). Unfortunately, the district court's definition is *dicta* and was not subjected to rigorous analysis.

Aside from the Northern District's definition, about all that can be said generally concerning what can constitute protectable "confidential information" for nondisclosure agreements not covered by Act 99 is that it must be information which a business has a "legitimate need" to protect. *See Durham v. Stand-by Labor of Georgia, Inc.*, 230 Ga. 558, 565, 198 S.E.2d 145, 150 (1973); *Nationwide Advertising Service, Inc. v. Thompson Recruitment Advertising, Inc.*, 183 Ga. App. 678, 686, 359 S.E.2d 737, 744 (1987); *Kem Manufacturing Corp. v. Sant*, 182 Ga. App. 135, 139, 355 S.E.2d 437, 443 (1987); *Lane Co. v. Taylor*, 174 Ga. App. 356, 359, 330 S.E.2d 112, 117 (1985).

Whether a business has a legitimate need to protect particular information is a question of fact under Georgia common law. *Id*. Factors to be considered in determining the legitimacy of the need to maintain the confidentiality of customer information covered by a nondisclosure agreement include: (1) the time and effort the plaintiff expended amassing its customers and building its goodwill, (2) the need to protect its economic advantage through confidential customer connections and confidential personnel data, (3) the efforts made to protect the information, and (4) the overall aspects of the business indicating a

legitimate need to protect the information. *Durham v. Stand-by Labor of Georgia, Inc.*, 230 Ga. 558, 565, 198 S.E.2d 145, 150 (1973).

Act 99 does not appear to require any inquiry into whether a business has a legitimate need to protect information that meets the statute's definition of confidential information. Presumably, any information meeting that definition may be protected by a nondisclosure agreement without any additional showing of a legitimate need for protection.

C. Types of Information Potentially Protectable

As noted above, for nondisclosure agreements subject to Act 99, it appears that any information meeting the statute's definition of confidential information is potentially protectable. For agreements not covered by Act 99, we must look to prior case law.

In *Durham v. Stand-by Labor of Georgia, Inc.*, 230 Ga. 558, 198 S.E.2d 145 (1973), the court addressed a nondisclosure agreement covering (1) the names and/or addresses of the company's customers, (2) any other information whatsoever concerning the company's customers, and (3) the company's methods of doing business. In essence, the court held that this information could be protected by the nondisclosure agreement if the company could show a legitimate business need to protect it. 230 Ga. at 559, 198 S.E.2d at 147. If there is a legitimate need for protection, it is of no consequence whether the information to be protected consists of written lists or information committed to memory. 230 Ga. at 564, 198 S.E.2d at 150.

In *Lane Co. v. Taylor*, 174 Ga. App. 356, 330 S.E.2d 112 (1985), the court considered a nondisclosure agreement covering (1) the names of current or past customers, and (2) any information acquired from the employer concerning the employer's methods of doing business, price structures, systems of operation, "know-how," documents, records, forms or any other confidential information. The court found that the use of the term "confidential information" in the nondisclosure agreement had the effect of modifying all the terms so as to cover only information that was in fact confidential. Therefore, the court concluded that the information could be protected if the company established a legitimate need to maintain its confidentiality. 174 Ga. App. at 359, 330 S.E.2d at 117.

In *Nasco, Inc. v. Gimbert*, 239 Ga. 675, 238 S.E.2d 368 (1977), however, the Georgia Supreme Court held that a nondisclosure agreement covering "'any information concerning any matters affecting or relating to the business of the employer'" was too broad as a matter of law to be enforceable. The court observed that "[t]here is a great deal of public information concerning matters which would affect or relate to the business of the employer; e.g., interest rates or minimum wage legislation." 239 Ga. at 676-77, 238 S.E.2d at 369-70.

On the other hand, Georgia appellate courts have upheld nondisclosure agreements as a matter of law in at least two reported cases. In *Wiley v. Royal Cup, Inc.*, the court addressed an agreement prohibiting disclosure of "any of [the company's] business methods, sales, service, or distribution techniques, selling prices, or the names or addresses of its present or prospective customers." 258

Ga. 357, 370 S.E.2d 744, 745 (1988). The agreement also contained a provision in which the former employee acknowledged that the information covered constituted confidential information. 258 Ga. at 359-60, 370 S.E.2d at 746. Without stating how, if at all, this acknowledgment influenced its decision, the court concluded that the nondisclosure agreement was enforceable. 258 Ga. at 360, 370 S.E.2d at 746. The lesson of this case would seem to be that all nondisclosure agreements should contain an acknowledgment that the information covered is confidential. *See also Palmer & Cay of Georgia, Inc. v. Lockton Companies, Inc.*, 273 Ga. App. 511, 515, 615 S.E.2d 752, 757 (2005) (by signing the employment agreement, the employees "acknowledged that names of customers are considered confidential business information and 'constitute [ ] valuable, special and unique property of the Company.' [citation omitted]").

Similarly, in *Sunstates Refrigerated Services, Inc. v. Griffin*, 215 Ga. App. 61, 449 S.E.2d 858 (1994), the court of appeals held a nondisclosure agreement enforceable as a matter of law. In that case, the agreement prohibited the use, disclosure and exploitation of confidential business information. In an unusually well-drafted provision, the company had defined such information as

> data and information relating to the business of the Company (whether constituting a trade secret or not) which is or has been disclosed to the Employee or of which the Employee became aware as a consequence of or through his relationship to the Company and which has value to the Company and is not generally known to its competitors. Confidential information shall not include any data or information that has been voluntarily disclosed to the public by the

> Company (except where such public disclosure has been made by Employee without authorization) or that has been independently developed and disclosed by others, or that otherwise enters the public domain through lawful means.

215 Ga. App. at 63, 449 S.E.2d at 860.

D. Enforceability of Nondisclosure Agreements

Act 99 appears to make two significant changes to Georgia's common law concerning confidential information. First, nondisclosure agreements covered by Act 99 may protect confidential information (as defined by the statute) for as long as the information remains confidential. In that regard, Act 99 provides

> Nothing in this article shall be construed to limit the period of time for which a party may agree to maintain information as confidential or as a trade secret, or to limit the geographic area within which such information must be kept confidential or as a trade secret, for so long as the information or material remains confidential or a trade secret, as applicable.

O.C.G.A. § 13-8-53(e).

Second, Act 99 authorizes a court to modify a nondisclosure agreement that otherwise would cover information not meeting the statute's definition of confidential information or extend coverage to a time when the information is no longer confidential. The authorization is found in two separate provisions of Act 99 as follows:

> Any restrictive covenant not in compliance with the provisions of this article is unlawful and is void and unenforceable; provided, however, that a court may modify a covenant that is otherwise void

> and unenforceable so long as the modification does not render the covenant more restrictive with regard to the employee than as originally drafted by the parties.

O.C.G.A. § 13-8-53(d).

> In any action concerning enforcement of a restrictive covenant, a court shall not enforce a restrictive covenant unless it complies with the provisions of Code Section 13-8-53; provided, however, that if a court finds that a contractually specified restraint does not comply with the provisions of Code Section 13-8-53, then the court may modify the restraint provision and grant only the relief reasonably necessary to protect such interest or interests and to achieve the original intent of the contracting parties to the extent possible.

O.C.G.A. § 13-8-54(b).

Nondisclosure agreements entered into prior to the effective date of Act 99 (May 11, 2011) are governed by prior case law. The following is a discussion of that case law, which is unaffected by Act 99.

Nondisclosure agreements entered into prior to the effective date of Act 99 (May 11, 2011) are generally enforceable if reasonable. According to an often quoted decision of the Georgia Supreme Court,

> their reasonableness turns on factors of time and the nature of the business interest sought to be protected . . . . In determining whether restraints on disclosure are reasonable, two factors are of importance: (1) whether the employer is attempting to protect confidential information relating to the business, such as trade secrets, methods of operation, names of customers, personnel data, and so on — even though the information does not rise to the stature of a trade secret; and (2) whether the restraint is reasonably related to the protection of the information.

Durham v. Stand-by Labor of Georgia, Inc., 230 Ga. 558, 563-64, 198 S.E.2d 145, 149-50 (1973); *see also Lee v. Environmental Pest & Termite Control, Inc.*, 271 Ga. 371, 374, 516 S.E.2d 76, 78 (1999). Whether a nondisclosure agreement is enforceable will often present a question of fact. *See, e.g., Physician Specialists in Anesthesia, P.C. v. MacNeill*, 246 Ga. App. 398, 408, 539 S.E.2d 216, 225 (2000). However, a nondisclosure agreement prohibiting disclosure of publicly available information is unenforceable as a matter of law. *Nasco, Inc. v. Gimbert*, 239 Ga. 675, 238 S.E.2d 368 (1977); *MacGinnitie v. Hobbs Group, LLC*, 420 F.3d 1234, 1242 (11th Cir. 2005).

As suggested by the foregoing quotation from *Durham,* nondisclosure agreements not governed by Act 99 must contain a time limit to survive the strict scrutiny applicable to cases involving the employer-employee relationship. Otherwise, they are unenforceable as a matter of law, at least as to information not constituting a trade secret. *Carson v. Obor Holding Co.,* 318 Ga. App. 645, 649-50, 734 S.E.2d 477, 482 (2012); *Howard Schultz & Associates of the Southeast, Inc. v. Broniec*, 239 Ga. 181, 188, 236 S.E.2d 265, 270 (1977); *Thomas v. Best Manufacturing Corp.*, 234 Ga. 787, 788, 218 S.E.2d 68, 70 (1975); *Pregler v. C&Z, Inc.*, 259 Ga. App. 149, 151, 575 S.E.2d 915, 917 (2003); *Stahl Headers, Inc. v. MacDonald*, 214 Ga. App. 323, 324, 447 S.E.2d 320, 322 (1994); *U3S Corp. v. Parker*, 202 Ga. App. 374, 378, 414 S.E.2d 513, 517 (1991); *TDS Healthcare Systems Corp. v. Humana Hospital Illinois, Inc.*, 880 F. Supp. 1572, 1585 (N.D. Ga. 1995); *Wesley-Jessen, Inc. v. Armento*, 519 F. Supp. 1352, 1362

(N.D. Ga. 1981). Where a nondisclosure agreement not governed by Act 99 covers both trade secrets and other types of confidential information, its failure to include a time limit will not preclude its enforcement with respect to trade secrets. *Wright v. Power Industry Consultants, Inc.*, 234 Ga. App. 833, 837-38, 508 S.E.2d 191, 195 (1998). Trade secrets, unlike mere confidential information covered by agreements not governed by Act 99, may be protected by agreement without temporal limitation. *The Variable Annuity Life Ins. Co. v. Joiner*, 454 F. Supp. 2d 1297, 1304 (S.D. Ga. 2006).

In addition, a nondisclosure agreement ancillary to employment that does contain a time limit but also contains a provision tolling the time limit during periods of breach is similarly unenforceable. *ALW Marketing Corp. v. McKinney*, 205 Ga. App. 184, 188, 421 S.E.2d 565, 568 (1992). That is because tolling tied to periods of breach could extend indefinitely. On the other hand, tolling provisions that are triggered by a lawsuit brought within a limited period of time may be enforceable. *Paul Robinson, Inc. v. Haege*, 218 Ga. App. 578, 579, 462 S.E.2d 396, 398 (1995).

A nondisclosure agreement extending two years after termination of employment has been upheld as reasonable. *Sunstates Refrigerated Services, Inc. v. Griffin*, 215 Ga. App. 61, 63, 449 S.E.2d 858, 860 (1994). Although only in *dicta*, the Georgia Supreme Court in *American Software USA, Inc. v. Moore* expressed the view that the nondisclosure agreement in that case, which

extended ten (10) years after termination of employment, was not unreasonable. 264 Ga. 480, 483-84, 448 S.E.2d 206, 209 (1994).

For nondisclosure restrictions contained in agreements subject to mid-level scrutiny, such as partnership and shareholder agreements, the temporal limitation requirement may not be as stringent as in the case of agreements ancillary to employment. For example, in *Carson v. Obor Holding Co.*, 318 Ga. App. 645, 734 S.E.2d 477 (2012), the court of appeals ruled that a nondisclosure provision was unenforceable under either strict scrutiny or mid-level scrutiny because it purported to extend in perpetuity **and** failed to define confidential information. *Id.* at 649, 734 S.E.2d at 482. This suggests that nondisclosure restrictions in an agreement subject to mid-level scrutiny may be deemed reasonable even in the absence of a temporal limitation if the information to which they apply is carefully limited by definition to only cover information that clearly deserves protection against disclosure.

The enforceability of a nondisclosure agreement does not depend on the enforceability of any covenant not to compete that may be contained in the same agreement. As the Georgia Supreme Court has stated, "a claim for breach of covenant not to compete and one for wrongful disclosure and use of confidential information in violation of contract may be maintained separately and independently under the same or distinct provisions of the employment agreement." *Durham v. Stand-by Labor of Georgia, Inc.*, 230 Ga. 558, 562-63, 198 S.E.2d 145, 149 (1973); *accord Wiley v. Royal Cup, Inc.*, 258 Ga. 357, 360,

370 S.E.2d 744, 746 (1988). Presumably this will remain the case for nondisclosure agreements covered by Act 99.

As in the case of covenants against competition, Georgia courts will not apply another state's law to render enforceable a nondisclosure agreement that would not be enforceable under Georgia law. *Enron Capital & Trade Resources, Inc. v. Pokalski,* 227 Ga. App. 727, 730, 490 S.E.2d 136, 139 (1997). There is no reason to believe that this will not continue to be the case for nondisclosure agreements governed by Act 99.

E. Relief for Breach of Nondisclosure Agreement

Nondisclosure agreements being contracts at law, the usual remedies for breach of contract are available. These would include damages and specific performance. The availability of such remedies should be the same for all nondisclosure agreements regardless of whether Act 99 applies.

Additional remedies may be available in the case of agreements covered by Act 99. In that regard, Act 99 provides that "[a] court shall enforce a restrictive covenant by any appropriate and effective remedy available at law or equity, including, but not limited to, temporary and permanent injunctions." O.C.G.A. § 13-8-58(c).

F. Miscellaneous

While it may seem illogical at first blush, it is possible for an individual to violate a nondisclosure agreement without ever revealing covered information to another person. This possibility is illustrated by the case of *Kuehn v. Selton &*

Associates, Inc., 242 Ga. App. 662, 530 S.E.2d 787 (2000). In that case, the defendant was bound by a nondisclosure agreement that prohibited only disclosure of covered information, and not the use of such information. After leaving the plaintiff's employ, the defendant formed a corporation and began competing with the plaintiff as the sole officer and employee of that corporation. In the process of competing, the defendant used information covered by his nondisclosure agreement with the plaintiff, but he did not disclose it to any other person. Noting that a corporation "possesses a legal existence separate and apart from that of its officers and shareholders," the court of appeals held that the defendant was not entitled to summary judgment on the issue of whether he had in fact violated the nondisclosure agreement. 242 Ga. App. at 666, 530 S.E.2d at 791.

G. Statute of Limitations

The applicable statute of limitation for written nondisclosure agreements is six years. O.C.G.A. § 9-3-24.

IV. Criminal Statutes

A. Georgia Theft of Trade Secrets Statute

O.C.G.A. § 16-8-13 makes "theft of a trade secret" a crime and provides for punishment "by imprisonment for not less than one nor more than five years and by a fine of not more than $50,000.00," if the value of the stolen trade secret exceeds $100. O.C.G.A. § 16-8-13(b). Theft of a trade secret having a value of $100 or less is punishable as a misdemeanor. *Id.*

The statute defines the offense of "theft of a trade secret" as follows:

> Any person who, with the intent to deprive or withhold from the owner thereof the exclusive use of a trade secret, or with an intent to appropriate a trade secret to his or her own use or to the use of another, does any of the following:
>
> (1) Takes, uses, or discloses such trade secret to an unauthorized person;
>
> (2) Acquires knowledge of such trade secret by deceitful means or artful practice; or
>
> (3) Without authority, makes or causes to be made a copy of an article representing such trade secret
>
> commits the offense of theft of a trade secret . . . .

O.C.G.A. § 16-8-13(b).

The statute's definition of "trade secret" is the same as under the GTSA. O.C.G.A. § 16-8-13(a)(4).

In *DuCom v. State*, 288 Ga. App. 555, 654 S.E.2d 670 (2008), the court addressed the Georgia theft of trade secrets statute. In that case, the defendant had been the manager of a real estate brokerage, development and property management company. After about six years in that position, she quit to start a competing company. Prior to quitting, however, she copied her former employer's property management master client list from the computer on which it was maintained and removed it from the premises to use in obtaining clients for her new business. The client list had been maintained with the requisite secrecy in that the computer from which the defendant copied it was password protected, and employees were not permitted to copy the list for use away from

the office. Also, the defendant, as a licensed real estate agent, owed a duty of loyalty to her former employer and supervised the other employees who had access to the computer. The prosecutor established that the list had economic value by proving that the defendant had made an unaccepted offer to purchase it shortly before she quit and that her former employer later sold it. The court of appeals found the client list to be a trade secret and upheld the defendant's conviction for its theft.

A copy of the Georgia theft of trade secrets statute is provided in Appendix C, pages 67-69 *infra*.

B. Georgia Computer Systems Protection Act

While the Georgia Computer Systems Protection Act, O.C.G.A. §§ 16-9-90, *et seq.*, ("GCSPA") does not appear to have been enacted with trade secrets and confidential information in mind, its provisions seem broad enough to provide substantial protection where such information is maintained in computer files. There is a question, however, concerning whether the GTSA preempts the GCSPA to the extent that the latter provides relief for the misappropriation of information.

The GTSA specifically states that it does not affect "[o]ther civil remedies that are not based upon misappropriation of a trade secret . . . ." O.C.G.A. § 10-1-767(b)(2) (Act). Moreover, the GCSPCA was enacted after the GTSA. Nevertheless, the Northern District of Georgia has held that the GTSA preempts the GCSPCA, in an action seeking relief for the misappropriation of allegedly

confidential and proprietary information. *RLI Insurance Co. v. Banks*, No. 1:14-CV-1108-TWT, 2015 WL 400540, *2 (N.D. Ga. Jan. 28, 2015). Neither the Georgia Supreme Court nor the Georgia Court of Appeals has addressed this specific issue.

Among other things, the GCSPA authorizes companies and individuals whose "property" is "injured by reason of a violation" of the statute to "sue therefor and recover for any damages sustained and the cost of the suit." O.C.G.A. §§ 16-9-93(g)(1). The term "property" is defined broadly to include computer programs. *Automated Drawing Systems, Inc. v. Integrated Network Services, Inc.*, 214 Ga. App. 122, 123-24, 447 S.E.2d 109, 111 (1994). The term also includes "data," which the statute defines to include "any representation of information . . . or data in any fixed medium, including documentation, computer printouts, magnetic storage media, . . . , storage in a computer, or transmission by computer network." O.C.G.A. § 16-9-92(5).

Violations of the GCSPA include the commission of "computer theft" and the commission of "computer trespass." "Computer theft" is committed whenever a person "uses a computer or computer network *with knowledge that such use is without authority* and with the intention of . . . [t]aking or appropriating any property of another, *whether or not with the intention of depriving the owner of possession*." O.C.G.A. § 16-9-93(a)(1) (emphasis added). In *DuCom v. State*, 288 Ga. App. 555, 654 S.E.2d 670 (2008), the court upheld a defendant's conviction of computer theft where she copied her employer's

computer data for use in a competing business she was forming. The defendant was authorized to copy the data for use on her home computer in performing duties for her employer. She was not, however, authorized to copy the data for use on behalf of a competing company. Thus, her use of the employer's computer for that purpose was without authority and constituted computer theft. 288 Ga. App. at 562-63, 654 S.E.2d 675-76; *accord Putters v. Rmax Operating, LLC,* No. 1:13-cv-3382-TWT, 2014 WL 1466902, *4 (N.D. Ga. April 15, 2014*); Vurv Technology LLC v. Kenexa Corp.*, No. 1:08-cv-3442-WSD, 2009 WL 2171042, *3-*4 (N.D. Ga. July 20, 2009).

"Computer trespass" is committed whenever a person "uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) [d]eleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer system; (2) [o]bstructing, interrupting, or in any way interfering with the use of a computer program or data; or (3) [a]ltering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists . . . ." O.C.G.A. § 16-9-93(b).

The court of appeals addressed the definition of "computer trespass" in *Ware v. American Recovery Solution Services, Inc.*, 324 Ga. App. 187, 749 S.E.2d 775 (2013). In that case a dispute arose between the plaintiff company ("ARSS") and defendant Ware, a computer programmer who had been engaged

to create certain applications software. Resorting to self-help when he became upset by ARSS's failure to make an expected payment, Ware logged into ARSS's computer server using the login and password of ARSS's CFO. He then proceeded to disable the login for the server so that ARSS could not access its database of 36,000 accounts and emailed ARSS's owners demanding immediate payment. ARSS had to engage a software expert to restore access to the server and sustained certain lost profits.

The trial court found that Ware had committed computer trespass and entered judgment for ARSS. On appeal, Ware argued that he did not access ARSS's computer server " 'without authority' because he owned the software that he tampered with and because he 'restored the application and gave them the previous package that they had paid for.' " *Id.* at 191, 749 S.E.2d at 779. The court of appeals found Ware's claimed ownership irrelevant to whether he had committed computer trespass. According to the court, "[t]he statute only requires that the intruder use a computer or a network knowing that he was without authority and either temporarily or permanently remove data, interfere with the use of a computer program, or cause a computer program to malfunction." *Id.*

In *Sitton v. Print Direction, Inc.*, 312 Ga. App. 365, 718 S.E.2d 532 (2011), the court of appeals affirmed the trial court's finding that an employer's inspection of emails on an employee's personal laptop computer was not "without authorization" so as to violate the GCSPA. By choice, the employee routinely

connected his own laptop computer to his employer's computer network and used it in his work for the employer. Under those circumstances, the court found in the employer's broad computer usage policy the authority for the employer's inspection of the emails in question, even though the emails were on a separate email address from the employee's company-issued email address. *Id*. at 367-69, 718 S.E.2d at 535-38.

Two other cases addressed whether one who remotely accesses a computer system located in Georgia from outside the state is subject to personal jurisdiction in Georgia in an action brought under the GCSPA. In *John Gallup & Associates, LLC v. Conlow*, Civil Action No. 1:12-CV-03779-RWS, 2013 WL 3191005 (N.D. Ga. June 21, 2013), the defendant used her computer located in California to delete certain programs and data from the plaintiff's computer server located in Georgia. The defendant was a resident of California and had never worked in Georgia or traveled to Georgia (other than for layovers at the Atlanta airport while in transit to destinations outside of Georgia). The court held that the defendant did not have sufficient contacts with Georgia to subject her to jurisdiction here under the Georgia Long Arm Statute.

In *LabMD, Inc. v. Tiversa, Inc.*, 509 Fed. Appx. 842 (11th Cir. 2013), the defendants used a computer located outside of Georgia to search the plaintiff's computer located in Georgia and download a computer file from it. The Eleventh Circuit held that this contact was not sufficient to subject the defendants to jurisdiction in Georgia under the Georgia Long Arm Statute. The court likened

the defendants' use of an out-of-state computer to access the plaintiff's computer to contacting someone in Georgia by email or telephone from another state, which Georgia courts have held not to constitute sufficient contact with Georgia to subject one to personal jurisdiction under the Georgia Long Arm Statute. *Id.* at 844.

A copy of the GCSPA is provided in Appendix D, pages 70-81 *infra*.

C. Georgia Racketeer Influenced & Corrupt Organizations Act

The Georgia Court of Appeals, in ruling on claims under the Georgia Racketeer Influenced & Corrupt Organizations Act ("RICO"), has made clear that the misappropriation of a trade secret can constitute at least one of the two predicate offenses necessary to sustain a civil cause of action under RICO. *Tronitec, Inc. v. Shealy*, 249 Ga. App. 442, 447, 547 S.E.2d 749, 755 (2001), *rev'd on other grounds*, 277 Ga. 210, 586 S.E.2d 661 (2003); *see also Stone v. Williams General Corp.*, 266 Ga. App. 608, 612, 597 S.E.2d 456, 460 (2004), *rev'd on other grounds*, 279 Ga. 428, 614 S.E.2d 758 (2005). This ruling is consistent with the plain language of RICO [specifically O.C.G.A. § 16-14-3(9)(A)(ix)], but *Tronitec* is the first reported decision to address the issue. A violation of the Georgia Computer Systems Protection Act also can serve as a predicate offense under RICO. O.C.G.A. § 16-14-3(9)(A)(xxviii).

The civil remedies provisions of RICO make its possible applicability to trade secrets cases intriguing. For example, persons injured as a consequence of a RICO violation may recover three times their actual damages as well as

attorneys' fees and costs. O.C.G.A. § 16-14-6(c). Punitive damages may also be awarded "where appropriate." *Id.*

Query whether the GTSA preempts RICO's civil remedies insofar as the misappropriation of trade secrets is concerned. See *RLI Insurance Co. v. Banks*, No. 1:14–CV–1108–TWT, 2015 WL 400540, *2 (N.D. Ga. Jan. 28, 2015).

D. Economic Espionage Act of 1996

Under the Economic Espionage Act of 1996 (the "EEA"), 18 U.S.C. §§ 1831, *et seq*., it is a federal crime to misappropriate another's trade secret. Under 18 U.S.C. § 1831, an individual who misappropriates a trade secret for the benefit of a foreign government, instrumentality or agent may be fined up to $500,000 and imprisoned for up to 15 years, or both. Organizations that do so may be fined up to the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

Under 18 U.S.C. § 1832, an individual who misappropriates a trade secret for the benefit of any person or entity other than the owner may be fined up to $250,000 [18 U.S.C. § 3571(b)(3)] and imprisoned for up to 10 years, or both. Organizations that do so may be fined up to $5,000,000.

The EEA includes a broad criminal forfeiture provision as well as criminal penalties. It also authorizes the Attorney General to bring a civil action in federal court to obtain appropriate injunctive relief. The EEA does not, however, provide

for a private right of action. *Auto-Opt Networks, Inc. v. GTL USA, Inc.*, Civil Action No. 3:14-CV-1252-D, 2014 WL 2719219 (N.D. Tex. June 16, 2014).

The EEA defines the term "trade secret" expansively to include all information, regardless of form or type, that the owner has taken reasonable measures to keep secret and that derives actual or potential economic value because it is not generally known to, and not readily ascertainable through proper means by, the public. The "actual or potential economic value" element does not require proof that the owner of the trade secret actually lost money as a result of the misrepresentation. *United States v. Hanjuan*, 733 F.3d 718, 721 (7th Cir. 2013).

On its face, the EEA appears to provide powerful protection for trade secrets. Its actual effectiveness, however, may depend on whether trade secrets must be disclosed to defendants who are prosecuted under the statute. In *United States v. Hsu*, 982 F. Supp. 1022 (E.D. Pa. 1997), the district court ruled that the alleged trade secrets in question in that case had to be disclosed to defendants charged with stealing them. The Third Circuit reversed because the defendants were not charged with stealing the alleged trade secrets (the district court had been mistaken), but only with conspiring and attempting to steal them. *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998). The appellate court declined to address whether disclosure would have been required had actual theft been charged. It remains to be seen whether the disclosure issue will detract from the EEA's effectiveness.

The First Circuit has subsequently held that proof of the actual existence of trade secrets is unnecessary in a prosecution for conspiracy under the EEA. *United States v. Martin*, 228 F.3d 1, 13 (1st Cir. 2000).

The decisions in *Hsu* and *Martin* provide some comfort that prosecutions under the EEA do not necessarily require disclosure of trade secrets (or other confidential information) to defendants. Disclosure to law enforcement officials and prosecutors, however, may be unavoidable. While such disclosure has not yet been held to forfeit the trade secret status of proprietary information, it would be advisable to obtain at least verbal assurances of confidentiality before voluntarily revealing confidential business information in support of a criminal investigation or prosecution. *See United States v. Yang*, No. 1:97-cr-00288-PCE, 1999 U.S. Dist. LEXIS 7130 (N.D. Ohio, March 18, 1999).

Indeed, the victim of trade secret theft may be entitled to protection from an accused's public disclosure of his trade secrets in federal court proceedings. *See* Crime Victims' Rights Act, 18 U.S.C. § 3771, *et seq*. This proposition was suggested in the government's motion *in limine* in *United States v. Williams*, No. 1:06-CR-313-03-JOF, N.D. Ga., Docket Entry No. 91, filed Jan. 4, 2007, n. 1 at p. 4. That motion and the defense response (Docket Entry No. 94) are enlightening with respect to the considerations at issue. The docket in that case does not reflect the court's ruling on the government's motion; however, a subsequent exhibit list filed by the government after trial indicates that the government was permitted to introduce some redacted exhibits at trial. *Id*., Docket Entry No. 124.

The issue was not raised on appeal. *See United States v. Williams*, 526 F.3d 1312 (11th Cir. 2008).

More recently, a court has invoked the provisions of 18 U.S.C. § 1835 to grant the government's request for a protective order to safeguard from public disclosure during trial seven photographs allegedly depicting trade secrets. *U. S. v. Roberts*, No. 3:08-CR-175, 2010 WL 1010000 (E.D. Tenn. March 17, 2010). Section 1835 provides for the court to

> enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws.

The court rejected the defendants' argument that Section 1835 did not apply unless it was first established that the photographs actually depicted bona fide trade secrets. *Id*. at *6-*8.

A copy of the EEA is provided in Appendix E, pages 82-87 *infra*.

December 18, 2015.

Georgia Trade Secrets Act of 1990, As Amended

§ 10-1-760 Short title.

This article shall be known as the "Georgia Trade Secrets Act of 1990."

§ 10-1-761 Definitions.

As used in this article, the term:

(1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means. Reverse engineering of a trade secret not acquired by misappropriation or independent development shall not be considered improper means.

(2) "Misappropriation" means:

(A) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) Disclosure or use of a trade secret of another without express or implied consent by a person who:

(i) Used improper means to acquire knowledge of a trade secret;

(ii) At the time of disclosure or use, knew or had reason to know that knowledge of the trade secret was:

(I) Derived from or through a person who had utilized improper means to acquire it;

(II) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(iii) Before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

(3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other for profit or not for profit legal or commercial entity.

(4) "Trade secret" means information, without regard to form, including, but not limited to, technical or nontechnical data, a formula, a pattern, a compilation, a program, a device, a method, a technique, a drawing, a process, financial data, financial plans, product plans, or a list of actual or potential customers or suppliers which is not commonly known by or available to the public and which information:

(A) Derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(B) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

§ 10-1-762 Injunctive relief.

(a) Actual or threatened misappropriation may be enjoined. Upon application to the court, an injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in appropriate circumstances for reasons including, but not limited to, an elimination of commercial advantage that otherwise would be derived from the misappropriation or where the trade secret ceases to exist due to the fault of the enjoined party or others by improper means.

(b) In exceptional circumstances, if the court determines that it would be unreasonable to prohibit future use, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited. Exceptional circumstances include, but are not limited to, a material and prejudicial change of position prior to acquiring

knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.

(c) In appropriate circumstances, affirmative acts to protect a trade secret may be compelled by court order.

(d) In no event shall a contract be required in order to maintain an action or to obtain injunctive relief for misappropriation of a trade secret.

§ 10-1-763 Recovery of damages.

(a) In addition to or in lieu of the relief provided by Code Section 10-1-762, a person is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. If neither damages nor unjust enrichment caused by the misappropriation are proved by a preponderance of the evidence, the court may award damages caused by misappropriation measured in terms of a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret for no longer than the period of time for which use could have been prohibited.

(b) If willful and malicious misappropriation exists, the court may award exemplary damages in an amount not exceeding twice any award made under subsection (a) of this Code section.

(c) In no event shall a contract be required in order to maintain an action or to recover damages for misappropriation of a trade secret.

§ 10-1-764 Award of attorneys' fees.

If a claim of misappropriation is made in bad faith, a motion to terminate an injunction is made or resisted in bad faith, or willful and malicious misappropriation exists, the court may award reasonable attorneys' fees to the prevailing party.

§ 10-1-765 Protection of trade secret during action.

In an action under this article, a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.

§ 10-1-766 Limitation of action.

An action for misappropriation must be brought within five years after the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered. For the purposes of this Code section, a continuing misappropriation by any person constitutes a single claim against that person, but this Code section shall be applied separately to the claim against each person who receives a trade secret from another person who misappropriated that trade secret.

§ 10-1-767 Effect on other laws.

(a) Except as provided in subsection (b) of this Code section, this article shall supersede conflicting tort, restitutionary, and other laws of this state providing civil remedies for misappropriation of a trade secret.

(b) This article shall not affect:

(1) Contractual duties or remedies, whether or not based upon misappropriation of a trade secret; provided, however, that a contractual duty to maintain a trade secret or limit use of a trade secret shall not be deemed void or unenforceable solely for lack of a durational or geographical limitation on the duty;

(2) Other civil remedies that are not based upon misappropriation of a trade secret; or

(3) The definition of a trade secret contained in Code Section 16-8-13, pertaining to criminal offenses involving theft of a trade secret or criminal remedies, whether or not based upon misappropriation of a trade secret.

Uniform Trade Secrets Act

(Drafted by the National Conference of Commissioners on Uniform State Laws, as amended 1985)

§ 1. Definitions

As used in this Act, unless the context requires otherwise:

(1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.

(2) "Misappropriation" means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason

to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

(3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity.

(4) "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

§ 2. Injunctive Relief

(a) Actual or threatened misappropriation may be enjoined. Upon application to the court an injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation.

(b) In exceptional circumstances, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited.

Exceptional circumstances include, but are not limited to, a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.

(c) In appropriate circumstances, affirmative acts to protect a trade secret may be compelled by court order.

§ 3. Damages

(a) Except to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.

(b) If willful and malicious misappropriation exists, the court may award exemplary damages in the amount not exceeding twice any award made under subsection (a).

§ 4. Attorney's Fees

If (i) a claim of misappropriation is made in bad faith, (ii) a motion to terminate an injunction is made or resisted in bad faith, or (iii) willful and

malicious misappropriation exists, the court may award reasonable attorney's fees to the prevailing party.

§ 5. Preservation of Secrecy

In action under this Act, a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.

§ 6. Statute of Limitations

An action for misappropriation must be brought within 3 years after the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered. For the purposes of this section, a continuing misappropriation constitutes a single claim.

§ 7. Effect on Other Law

(a) Except as provided in subsection (b), this [Act] displaces conflicting tort, restitutionary, and other law of this State providing civil remedies for misappropriation of a trade secret.

(b) This [Act] does not affect: (1) contractual remedies, whether or not based upon misappropriation of a trade secret; or (2) other civil remedies that are not based upon misappropriation of a trade secret; or (3) criminal remedies, whether or not based upon misappropriation of a trade secret.

§ 8. Uniformity of Application and Construction

This act shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this Act among states enacting it.

§ 9. Short Title

This Act may be cited as the Uniform Trade Secrets Act.

§ 10. Severability

If any provision of this Act or its application to any person or circumstances is held invalid, the invalidity does not affect other provisions or applications of the Act which can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

§ 11. Time of Taking Effect

This [Act] takes effect on _____, and does not apply to misappropriation occurring prior to the effective date. With respect to a continuing misappropriation that began prior to the effective date, the [Act] also does not apply to the continuing misappropriation that occurs after the effective date.

§ 12. Repeal

The following Acts and parts of Acts are repealed:

Georgia Theft of Trade Secrets Statute

§ 16-8-13. Theft of trade secrets

(a) As used in this Code section, the term:

(1) “Article” means any object, material, device, substance, or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint, or map.

(2) “Copy” means any facsimile, replica, photograph, or other reproduction of an article and any note, drawing, or sketch made of or from an article.

(3) “Representing” means describing, depicting, containing, constituting, reflecting, or recording.

(4) “Trade secret” means information, without regard to form, including, but not limited to, technical or nontechnical data, a formula, a pattern, a compilation, a program, a device, a method, a technique, a drawing, a process, financial data, financial plans, product plans, or a list of actual or potential customers or suppliers which is not commonly known by or available to the public and which information:

(A) Derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(B) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

(b) Any person who, with the intent to deprive or withhold from the owner thereof the exclusive use of a trade secret, or with an intent to appropriate a trade secret to his or her own use or to the use of another, does any of the following:

(1) Takes, uses, or discloses such trade secret to an unauthorized person;

(2) Acquires knowledge of such trade secret by deceitful means or artful practice; or

(3) Without authority, makes or causes to be made a copy of an article representing such trade secret

commits the offense of theft of a trade secret and, upon conviction thereof, shall be punished by imprisonment for not less than one nor more than five years and by a fine of not more than $50,000.00, provided that, if the value of such trade secret, and any article representing such trade secret that is taken, is not more than $100.00 such person shall be punished as for a misdemeanor.

(c) In a prosecution for any violation of this Code section, a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.

(d) For the purposes of this Code section, a continuing theft by any person constitutes a single claim against that person, but this Code section shall be applied separately to the claim against each person who receives a trade secret from another person who committed the theft.

(e) This Code section shall not affect:

(1) Contractual duties or remedies, whether or not based on theft of a trade secret; or

(2) The provisions of Code Sections 10-1-761 through 10-1-767, pertaining to civil offenses and remedies involving the misappropriation of a trade secret, or other civil or criminal laws that presently apply or in the future may apply to any transaction or course of conduct that violates this Code section.

Georgia Computer Systems Protection Act

§ 16-9-90 Short title.

This article shall be known and may be cited as the "Georgia Computer Systems Protection Act."

§ 16-9-91 Legislative findings.

The General Assembly finds that:

(1) Computer related crime is a growing problem in the government and in the private sector;

(2) Such crime occurs at great cost to the public, since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) The opportunities for computer related crimes in state programs, and in other entities which operate within the state, through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets are great;

(4) Computer related crime operations have a direct effect on state commerce;

(5) Liability for computer crimes should be imposed on all persons, as that term is defined in this title; and

(6) The prosecution of persons engaged in computer related crime is difficult under previously existing Georgia criminal statutes.

§ 16-9-92 Definitions.

As used in this article, the term:

(1) "Computer" means an electronic, magnetic, optical, hydraulic, electrochemical, or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve, or communicate computer programs, computer data, or the results of computer operations to or from a person, another computer, or another device. This term specifically includes, but is not limited to, mail servers and e-mail networks. This term does not include a device that is not used to communicate with or to manipulate any other computer.

(2) "Computer network" means a set of related, remotely connected computers and any communications facilities with the function and purpose of transmitting data among them through the communications facilities.

(3) "Computer operation" means computing, classifying, transmitting, receiving, retrieving, originating, switching, storing, displaying, manifesting, measuring, detecting, recording, reproducing,

handling, or utilizing any form of data for business, scientific, control, or other purposes.

(4) "Computer program" means one or more statements or instructions composed and structured in a form acceptable to a computer that, when executed by a computer in actual or modified form, cause the computer to perform one or more computer operations. The term "computer program" shall include all associated procedures and documentation, whether or not such procedures and documentation are in human readable form.

(5) "Data" includes any representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network.

(6) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects interstate or foreign commerce, but does not include:

(A) Any wire or oral communication;

(B) Any communication made through a tone-only paging device;

(C) Any communication from a tracking device; or

(D) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

(7) “Electronic communication service" means any service which provides to its users the ability to send or receive wire or electronic communications.

(8) “Electronic communications system” means any wire, radio, electromagnetic, photoelectronic, photo-optical, or facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

(9) “Electronic means” is any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:

(A) Any telephone or telegraph instrument, equipment, or facility, or any component thereof,

(i) Furnished to the subscriber or user by a provider of electronic communication service in the ordinary course of its business and used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(ii) Used by a provider of electronic communication service in the ordinary course of its business or by

an investigative or law enforcement officer in the ordinary course of his or her duties; or

(B) A hearing aid or similar device being used to correct subnormal hearing to better than normal.

(10) "Electronic storage" means:

(A) Any temporary, intermediate storage of wire or electronic communication incidental to its electronic transmission; and

(B) Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

(11) "Financial instruments" includes any check, draft, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction-authorizing mechanism, or marketable security, or any computer representation thereof.

(12) "Law enforcement unit" means any law enforcement officer charged with the duty of enforcing the criminal laws and ordinances of the state or of the counties or municipalities of the state who is employed by and compensated by the state or any county or municipality of the state or who is elected and compensated on a fee basis. The term shall include, but not be limited to, members of the Department of Public Safety, municipal police, county police, sheriffs, deputy sheriffs, and agents and investigators of the Georgia Bureau of Investigation.

(13) "Property" includes computers, computer networks, computer programs, data, financial instruments, and services.

(14) "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

(15) "Services" includes computer time or services or data processing services.

(16) "Use" includes causing or attempting to cause:

(A) A computer or computer network to perform or to stop performing computer operations;

(B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; or

(C) A person to put false information into a computer.

(17) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner to verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.

(18) "Without authority" includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network.

§ 16-9-93 Criminal liability and penalties for crimes of computer theft, trespass, invasion of privacy, forgery, and password disclosure.

(a) Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

(2) Obtaining property by any deceitful means or artful practice; or

(3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

(b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or

(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of

how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

(c) Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

(d) Computer Forgery. Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

(e) Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

(f) Article not Exclusive. The provisions of this article shall not be construed to preclude the applicability of any other law which presently applies or

may in the future apply to any transaction or course of conduct which violates this article.

(g) Civil Relief; Damages.

(1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, “damages” shall include loss of profits and victim expenditure.

(2) At the request of any party to an action brought pursuant to this Code section, the court shall by reasonable means conduct all legal proceedings in such a way as to protect the secrecy and security of any computer, computer network, data, or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under this Code section must be brought within four years after the violation is discovered or by exercise of reasonable diligence should have been discovered. For purposes of this article, a continuing violation of any one subsection of this Code section by any person constitutes a single violation by such person.

(h) Criminal Penalties.

(1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

(2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

§ 16-9-93.1 Transmission of data through computer network, etc., using name, trade name, trademark, etc., to falsely identify person, organization, or representative transmitting such data[1/]

(a) It shall be unlawful for any person, any organization, or any representative of any organization knowingly to transmit any data through a computer network or over the transmission facilities or through the network facilities of a local telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data or which would falsely state or imply that such person, organization, or representative has permission or is

legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted symbol for such purpose when such permission or authorization has not been obtained; provided, however, that no telecommunications company or Internet access provider shall violate this Code section solely as a result of carrying or transmitting such data for its customers.

(b) Any person violating subsection (a) of this Code section shall be guilty of a misdemeanor.

(c) Nothing in this Code section shall be construed to limit an aggrieved party's right to pursue a civil action for equitable or monetary relief, or both, for actions which violate this Code section.

§ 16-9-94 Venue.

For the purpose of venue under this article, any violation of this article shall be considered to have been committed:

(1) In the county of the principal place of business in this state of the owner of a computer, computer network, or any part thereof;

(2) In any county in which any person alleged to have violated any provision of this article had control or possession of any proceeds of the violation or of any books, records, documents, or property which were used in furtherance of the violation;

(3) In any county in which any act was performed in furtherance of any

transaction which violated this article; and

(4) In any county from which, to which, or through which any use of a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.

Economic Espionage Act of 1996

18 U.S.C. §§ 1831, *et seq*.

§ 1831 Economic espionage.

(a) In general.--Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.

(b) Organizations.--Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

§ 1832 Theft of trade secrets.

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

§ 1833 Exceptions to prohibitions.

This chapter does not prohibit--

(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

§ 1834 Criminal forfeiture.

Forfeiture, destruction, and restitution relating to this chapter shall be subject to section 2323, to the extent provided in that section, in addition to any other similar remedies provided by law.

§ 1835 Orders to preserve confidentiality

In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

§ 1836 Civil proceedings to enjoin violations.

(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this chapter.

(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this section.

§ 1837 Applicability to conduct outside the United States.

This chapter also applies to conduct occurring outside the United States if--

(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

(2) an act in furtherance of the offense was committed in the United States.

§ 1838 Construction with other laws.

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

§ 1839 Definitions.

As used in this chapter--

(1) the term “foreign instrumentality” means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

(2) the term “foreign agent” means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

(3) the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or

how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

(4) the term “owner”, with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

114TH CONGRESS
2D SESSION

S. 1890

AN ACT

To amend chapter 90 of title 18, United States Code, to provide Federal jurisdiction for the theft of trade secrets, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Defend Trade Secrets Act of 2016''.

SEC. 2. FEDERAL JURISDICTION FOR THEFT OF TRADE SECRETS.

(a) IN GENERAL.—Section 1836 of title 18, United States Code, is amended by striking subsection (b) and inserting the following:

''(b) PRIVATE CIVIL ACTIONS.—

''(1) IN GENERAL.—An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.

''(2) CIVIL SEIZURE.—

''(A) IN GENERAL.—

''(i) APPLICATION.—Based on an affidavit or verified complaint satisfying the requirements of this paragraph, the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.

''(ii) REQUIREMENTS FOR ISSUING ORDER.—The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that—

''(I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order;

''(II) an immediate and irreparable injury will occur if such seizure is not ordered;

''(III) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;

"(IV) the applicant is likely to succeed in showing that—

"(aa) the information is a trade secret; and

"(bb) the person against whom seizure would be ordered—

"(AA) misappropriated the trade secret of the applicant by improper means; or

"(BB) conspired to use improper means to misappropriate the trade secret of the applicant;

"(V) the person against whom seizure would be ordered has actual possession of—

"(aa) the trade secret; and

"(bb) any property to be seized;

"(VI) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;

''(VII) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and

''(VIII) the applicant has not publicized the requested seizure.

''(B) ELEMENTS OF ORDER.—If an order is issued under subparagraph (A), it shall—

''(i) set forth findings of fact and conclusions of law required for the order;

''(ii) provide for the narrowest seizure of property necessary to achieve the purpose of this paragraph and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;

''(iii)(I) be accompanied by an order protecting the seized property from disclosure by prohibiting access by the applicant

or the person against whom the order is directed, and prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court; and

''(II) provide that if access is granted by the court to the applicant or the person against whom the order is directed, the access shall be consistent with subparagraph (D);

''(iv) provide guidance to the law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including—

''(I) the hours during which the seizure may be executed; and

''(II) whether force may be used to access locked areas;

''(v) set a date for a hearing described in subparagraph (F) at the earliest possible time, and not later than 7 days after the order has issued, unless the party against whom the order is directed and

others harmed by the order consent to another date for the hearing, except that a party against whom the order has issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the applicant who obtained the order; and

''(vi) require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or wrongful or excessive attempted seizure under this paragraph.

''(C) PROTECTION FROM PUBLICITY.—The court shall take appropriate action to protect the person against whom an order under this paragraph is directed from publicity, by or at the behest of the person obtaining the order, about such order and any seizure under such order.

''(D) MATERIALS IN CUSTODY OF COURT.—

''(i) IN GENERAL.—Any materials seized under this paragraph shall be taken

into the custody of the court. The court shall secure the seized material from physical and electronic access during the seizure and while in the custody of the court.

''(ii) STORAGE MEDIUM.—If the seized material includes a storage medium, or if the seized material is stored on a storage medium, the court shall prohibit the medium from being connected to a network or the Internet without the consent of both parties, until the hearing required under subparagraph (B)(v) and described in subparagraph (F).

''(iii) PROTECTION OF CONFIDENTIALITY.—The court shall take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized pursuant to this paragraph unless the person against whom the order is entered consents to disclosure of the material.

''(iv) APPOINTMENT OF SPECIAL MASTER.—The court may appoint a special master to locate and isolate all misappropriated trade secret information and to fa-

cilitate the return of unrelated property and data to the person from whom the property was seized. The special master appointed by the court shall agree to be bound by a non-disclosure agreement approved by the court.

''(E) SERVICE OF ORDER.—The court shall order that service of a copy of the order under this paragraph, and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order. The court may allow State or local law enforcement officials to participate, but may not permit the applicant or any agent of the applicant to participate in the seizure. At the request of law enforcement officials, the court may allow a technical expert who is unaffiliated with the applicant and who is bound by a court-approved non-disclosure agreement to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure.

''(F) SEIZURE HEARING.—

''(i) DATE.—A court that issues a seizure order shall hold a hearing on the date set by the court under subparagraph (B)(v).

''(ii) BURDEN OF PROOF.—At a hearing held under this subparagraph, the party who obtained the order under subparagraph (A) shall have the burden to prove the facts supporting the findings of fact and conclusions of law necessary to support the order. If the party fails to meet that burden, the seizure order shall be dissolved or modified appropriately.

''(iii) DISSOLUTION OR MODIFICATION OF ORDER.—A party against whom the order has been issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the party who obtained the order.

''(iv) DISCOVERY TIME LIMITS.—The court may make such orders modifying the time limits for discovery under the Federal Rules of Civil Procedure as may be necessary to prevent the frustration of the

purposes of a hearing under this subparagraph.

''(G) ACTION FOR DAMAGE CAUSED BY WRONGFUL SEIZURE.—A person who suffers damage by reason of a wrongful or excessive seizure under this paragraph has a cause of action against the applicant for the order under which such seizure was made, and shall be entitled to the same relief as is provided under section 34(d)(11) of the Trademark Act of 1946 (15 U.S.C. 1116(d)(11)). The security posted with the court under subparagraph (B)(vi) shall not limit the recovery of third parties for damages.

''(H) MOTION FOR ENCRYPTION.—A party or a person who claims to have an interest in the subject matter seized may make a motion at any time, which may be heard ex parte, to encrypt any material seized or to be seized under this paragraph that is stored on a storage medium. The motion shall include, when possible, the desired encryption method.

''(3) REMEDIES.—In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may—

''(A) grant an injunction—

''(i) to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not—

''(I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or

''(II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business;

''(ii) if determined appropriate by the court, requiring affirmative actions to be taken to protect the trade secret; and

''(iii) in exceptional circumstances that render an injunction inequitable, that conditions future use of the trade secret upon payment of a reasonable royalty for

no longer than the period of time for which such use could have been prohibited;

''(B) award—

''(i)(I) damages for actual loss caused by the misappropriation of the trade secret; and

''(II) damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss; or

''(ii) in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret;

''(C) if the trade secret is willfully and maliciously misappropriated, award exemplary damages in an amount not more than 2 times the amount of the damages awarded under subparagraph (B); and

''(D) if a claim of the misappropriation is made in bad faith, which may be established by circumstantial evidence, a motion to terminate an injunction is made or opposed in bad faith,

or the trade secret was willfully and maliciously misappropriated, award reasonable attorney's fees to the prevailing party.

''(c) JURISDICTION.—The district courts of the United States shall have original jurisdiction of civil actions brought under this section.

''(d) PERIOD OF LIMITATIONS.—A civil action under subsection (b) may not be commenced later than 3 years after the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered. For purposes of this subsection, a continuing misappropriation constitutes a single claim of misappropriation.''.

(b) DEFINITIONS.—Section 1839 of title 18, United States Code, is amended—

(1) in paragraph (3)—

(A) in subparagraph (B), by striking ''the public'' and inserting ''another person who can obtain economic value from the disclosure or use of the information''; and

(B) by striking ''and'' at the end;

(2) in paragraph (4), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(5) the term 'misappropriation' means—

''(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

''(B) disclosure or use of a trade secret of another without express or implied consent by a person who—

''(i) used improper means to acquire knowledge of the trade secret;

''(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—

''(I) derived from or through a person who had used improper means to acquire the trade secret;

''(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

''(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy

of the trade secret or limit the use of the trade secret; or

''(iii) before a material change of the position of the person, knew or had reason to know that—

''(I) the trade secret was a trade secret; and

''(II) knowledge of the trade secret had been acquired by accident or mistake;

''(6) the term 'improper means'—

''(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and

''(B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition; and

''(7) the term 'Trademark Act of 1946' means the Act entitled 'An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes, approved July 5, 1946 (15 U.S.C. 1051 et seq.) (commonly re-

ferred to as the ''Trademark Act of 1946'' or the ''Lanham Act'')'.''.

(c) EXCEPTIONS TO PROHIBITION.—Section 1833 of title 18, United States Code, is amended, in the matter preceding paragraph (1), by inserting ''or create a private right of action for'' after ''prohibit''.

(d) CONFORMING AMENDMENTS.—

(1) The section heading for section 1836 of title 18, United States Code, is amended to read as follows:

''§ 1836. Civil proceedings''.

(2) The table of sections for chapter 90 of title 18, United States Code, is amended by striking the item relating to section 1836 and inserting the following:

''1836. Civil proceedings.''.

(e) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to any misappropriation of a trade secret (as defined in section 1839 of title 18, United States Code, as amended by this section) for which any act occurs on or after the date of the enactment of this Act.

(f) RULE OF CONSTRUCTION.—Nothing in the amendments made by this section shall be construed to modify the rule of construction under section 1838 of title

18, United States Code, or to preempt any other provision of law.

(g) APPLICABILITY TO OTHER LAWS.—This section and the amendments made by this section shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress.

SEC. 3. TRADE SECRET THEFT ENFORCEMENT.

(a) IN GENERAL.—Chapter 90 of title 18, United States Code, is amended—

(1) in section 1832(b), by striking ''$5,000,000'' and inserting ''the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided''; and

(2) in section 1835—

(A) by striking ''In any prosecution'' and inserting the following:

''(a) IN GENERAL.—In any prosecution''; and

(B) by adding at the end the following:

''(b) RIGHTS OF TRADE SECRET OWNERS.—The court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a sub-

mission under seal that describes the interest of the owner in keeping the information confidential. No submission under seal made under this subsection may be used in a prosecution under this chapter for any purpose other than those set forth in this section, or otherwise required by law. The provision of information relating to a trade secret to the United States or the court in connection with a prosecution under this chapter shall not constitute a waiver of trade secret protection, and the disclosure of information relating to a trade secret in connection with a prosecution under this chapter shall not constitute a waiver of trade secret protection unless the trade secret owner expressly consents to such waiver.''.

(b) RICO PREDICATE OFFENSES.—Section 1961(1) of title 18, United States Code, is amended by inserting ''sections 1831 and 1832 (relating to economic espionage and theft of trade secrets),'' before ''section 1951''.

SEC. 4. REPORT ON THEFT OF TRADE SECRETS OCCURRING ABROAD.

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office.

(2) FOREIGN INSTRUMENTALITY, ETC.—The terms ''foreign instrumentality'', ''foreign agent'', and ''trade secret'' have the meanings given those terms in section 1839 of title 18, United States Code.

(3) STATE.—The term ''State'' includes the District of Columbia and any commonwealth, territory, or possession of the United States.

(4) UNITED STATES COMPANY.—The term ''United States company'' means an organization organized under the laws of the United States or a State or political subdivision thereof.

(b) REPORTS.—Not later than 1 year after the date of enactment of this Act, and biannually thereafter, the Attorney General, in consultation with the Intellectual Property Enforcement Coordinator, the Director, and the heads of other appropriate agencies, shall submit to the Committees on the Judiciary of the House of Representatives and the Senate, and make publicly available on the Web site of the Department of Justice and disseminate to the public through such other means as the Attorney General may identify, a report on the following:

(1) The scope and breadth of the theft of the trade secrets of United States companies occurring outside of the United States.

(2) The extent to which theft of trade secrets occurring outside of the United States is sponsored by foreign governments, foreign instrumentalities, or foreign agents.

(3) The threat posed by theft of trade secrets occurring outside of the United States.

(4) The ability and limitations of trade secret owners to prevent the misappropriation of trade secrets outside of the United States, to enforce any judgment against foreign entities for theft of trade secrets, and to prevent imports based on theft of trade secrets overseas.

(5) A breakdown of the trade secret protections afforded United States companies by each country that is a trading partner of the United States and enforcement efforts available and undertaken in each such country, including a list identifying specific countries where trade secret theft, laws, or enforcement is a significant problem for United States companies.

(6) Instances of the Federal Government working with foreign countries to investigate, arrest, and prosecute entities and individuals involved in the theft of trade secrets outside of the United States.

(7) Specific progress made under trade agreements and treaties, including any new remedies enacted by foreign countries, to protect against theft of trade secrets of United States companies outside of the United States.

(8) Recommendations of legislative and executive branch actions that may be undertaken to—

(A) reduce the threat of and economic impact caused by the theft of the trade secrets of United States companies occurring outside of the United States;

(B) educate United States companies regarding the threats to their trade secrets when taken outside of the United States;

(C) provide assistance to United States companies to reduce the risk of loss of their trade secrets when taken outside of the United States; and

(D) provide a mechanism for United States companies to confidentially or anonymously report the theft of trade secrets occurring outside of the United States.

SEC. 5. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) trade secret theft occurs in the United States and around the world;

(2) trade secret theft, wherever it occurs, harms the companies that own the trade secrets and the employees of the companies;

(3) chapter 90 of title 18, United States Code (commonly known as the ''Economic Espionage Act of 1996''), applies broadly to protect trade secrets from theft; and

(4) it is important when seizing information to balance the need to prevent or remedy misappropriation with the need to avoid interrupting the—

(A) business of third parties; and

(B) legitimate interests of the party accused of wrongdoing.

SEC. 6. BEST PRACTICES.

(a) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Federal Judicial Center, using existing resources, shall develop recommended best practices for—

(1) the seizure of information and media storing the information; and

(2) the securing of the information and media once seized.

(b) UPDATES.—The Federal Judicial Center shall update the recommended best practices developed under subsection (a) from time to time.

(c) CONGRESSIONAL SUBMISSIONS.—The Federal Judicial Center shall provide a copy of the recommendations developed under subsection (a), and any updates made under subsection (b), to the—

(1) Committee on the Judiciary of the Senate; and

(2) Committee on the Judiciary of the House of Representatives.

SEC. 7. IMMUNITY FROM LIABILITY FOR CONFIDENTIAL DISCLOSURE OF A TRADE SECRET TO THE GOVERNMENT OR IN A COURT FILING.

(a) AMENDMENT.—Section 1833 of title 18, United States Code, is amended—

(1) by striking ''This chapter'' and inserting ''(a) IN GENERAL.—This chapter'';

(2) in subsection (a)(2), as designated by paragraph (1), by striking ''the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation'' and inserting ''the disclosure

of a trade secret in accordance with subsection (b)'';
and

(3) by adding at the end the following:

''(b) IMMUNITY FROM LIABILITY FOR CONFIDENTIAL DISCLOSURE OF A TRADE SECRET TO THE GOVERNMENT OR IN A COURT FILING.—

''(1) IMMUNITY.—An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that—

''(A) is made—

''(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and

''(ii) solely for the purpose of reporting or investigating a suspected violation of law; or

''(B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

''(2) USE OF TRADE SECRET INFORMATION IN ANTI-RETALIATION LAWSUIT.—An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use

the trade secret information in the court proceeding, if the individual—

"(A) files any document containing the trade secret under seal; and

"(B) does not disclose the trade secret, except pursuant to court order.

"(3) NOTICE.—

"(A) IN GENERAL.—An employer shall provide notice of the immunity set forth in this subsection in any contract or agreement with an employee that governs the use of a trade secret or other confidential information.

"(B) POLICY DOCUMENT.—An employer shall be considered to be in compliance with the notice requirement in subparagraph (A) if the employer provides a cross-reference to a policy document provided to the employee that sets forth the employer's reporting policy for a suspected violation of law.

"(C) NON-COMPLIANCE.—If an employer does not comply with the notice requirement in subparagraph (A), the employer may not be awarded exemplary damages or attorney fees under subparagraph (C) or (D) of section

1836(b)(3) in an action against an employee to whom notice was not provided.

''(D) APPLICABILITY.—This paragraph shall apply to contracts and agreements that are entered into or updated after the date of enactment of this subsection.

''(4) EMPLOYEE DEFINED.—For purposes of this subsection, the term 'employee' includes any individual performing work as a contractor or consultant for an employer.

''(5) RULE OF CONSTRUCTION.—Except as expressly provided for under this subsection, nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access of material by unauthorized means.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—Section 1838 of title 18, United States Code, is amended by striking ''This chapter'' and inserting ''Except as provided in section 1833(b), this chapter''.

Passed the Senate April 4, 2016.

Attest:

Secretary.

114TH CONGRESS
2D SESSION

S. 1890

AN ACT

To amend chapter 90 of title 18, United States Code, to provide Federal jurisdiction for the theft of trade secrets, and for other purposes.

THE DEFEND TRADE SECRETS ACT: TRADE SECRET PROTECTION GOES FEDERAL

Benjamin I. Fink
Neal F. Weinrich
Daniel H. Park
Ashley M. Bowcott
Berman Fink Van Horn P.C.
Atlanta, Georgia 30305
www.bfvlaw.com
www.gatradesecrets.com
www.georgia-noncompete.com

Table of Contents

A Federal Cause of Action for Trade Secret Misappropriation

Introduction

Trade secret theft is a very serious concern for employers. According to a recent report by the Center for Responsible Enterprise and Trade and PricewaterhouseCoopers, LLP, trade secret theft has an estimated economic impact of 1% to 3% of the United States' Gross Domestic Product.[1] Hundreds of billions of dollars per year are lost through trade secret theft.[2]

Trade secret litigation has also multiplied in the last fifteen years. And in the digital era, it is significantly easier for employees to misappropriate company data, which in turn makes it more challenging for companies to prevent trade secret theft.

The importance of trade secrets and the need to protect them got Congress's attention. In early 2016 the Defend Trade Secrets Act (DTSA) passed the Senate and House, with widespread support across the aisles. On May 11, 2016, President Obama signed the DTSA into law.

---

[1] CREATE.ORG & PWC, ECONOMIC IMPACT OF TRADE SECRET THEFT: A FRAMEWORK FOR COMPANIES TO SAFEGUARD TRADE SECRETS AND MITIGATE POTENTIAL THREATS (Feb. 2014), available at https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.

[2] *See also* THE IP COMMISSION, THE REPORT OF THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY (May 2013), available at http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf (estimating that annual losses to the American economy caused by trade secret theft are over $300 billion).

A Brief History of Trade Secret Law in the United States

While technology has made it easier than ever for employees to misappropriate trade secrets, trade secret protection is not a new issue. Courts in the United States have been addressing trade secret theft since at least the 19th century.[3]

Trade secrets were originally considered property and were analyzed under a "strict property view," but courts eventually moved away from this viewpoint.[4] In 1939, trade secrets were included in the Restatement (First) of Torts in the section on Interference with Advantageous Economic Relations.[5] This arguably represented a shift from a property-based view of trade secrets to a view rooted more directly in concerns about unfair competition.[6]

In 1979, the Uniform Trade Secrets Act (UTSA) was approved by the National Conference of Commissions on Uniform State Law. The purpose of the UTSA was to centralize the law surrounding trade secrets by creating a model statute available for adoption by the states.

Almost every state has adopted the UTSA in some form. However, because many states have not adopted the UTSA verbatim, and also because many state appellate

---

[3] Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 3, 13 (2007), available at http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=1089&context=iplr (citing *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 493 n.23 (1974); *Warner-Lambert Co. v. Execuquest Corp.*, 691 N.E. 2d 545, 547 (Mass. 1998); *Peabody v. Norfolk*, 98 Mass. 452, 458 (1868)).
[4] *Id.*, at 13-15.
[5] *Id.*
[6] *Id.*

courts interpret the same provisions of the UTSA differently, trade secret law varies from state to state.

What is the DTSA?

Before the passage of the DTSA, trade secret misappropriation was a federal crime under the Economic Espionage Act: Chapter 90 of Title 18 of the United States Code. However, a private party could not bring a civil cause of action based on trade secret theft.

The DTSA amends the Economic Espionage Act. It creates a civil cause of action for the owner of a trade secret that has been misappropriated "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[7]

The DTSA thus attempts to create a more uniform federal system to protect innovations and intellectual property as trade secrets through civil remedies. Many of the provisions of the DTSA are similar to those in the UTSA. The DTSA does not preempt state trade secret laws, so the law functions as a supplement to the many state law versions of the UTSA, rather than as a replacement.[8]

---

[7] DTSA § 2(b)(1). A copy of the DTSA is attached to this article.
[8] As amended by the DTSA, 18 U.S.C. section 1836(f) states that "[n]othing in the amendments made by this section shall be construed to modify the rule of construction under section 1838 of title 18, United States Code, or to preempt any other provision of law."

What is a "Trade Secret" and "Misappropriation" under the DTSA?

The amended definition of a trade secret is contained in Title 18, Section 1839 of the United States Code.[9] A trade secret is defined as

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if – (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of information.[10]

"Misappropriation" of a trade secret is defined under the DTSA as:

> (A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

[9] 18 U.S.C.A. § 1839 (3)(A)-(B).
[10] 18 U.S.C.A. § 1839 (3)(A)-(B).

(B) disclosure or use of a trade secret of another without express or implied consent by a person who – (i) used improper means to acquire knowledge of a trade secret; (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was –(I) derived from or through a person who had used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii) before a material change of the position of the person, knew or had reason to know that – (I) the trade secret was a trade secret; and (II) knowledge of the trade secret had been acquired by accident or mistake.[11]

Remedies Under the DTSA

The typical remedies for trade secret theft are available under the DTSA. The district court can issue an injunction and award damages for the misappropriation of a trade secret. Damages can include the actual losses from misappropriation, unjust enrichment, or a reasonable royalty.[12] In addition, if the trade secret was willfully and maliciously appropriated, the court can award exemplary damages up to two times the

[11] 18 U.S.C.A. § 1839 (5)(A)-(B).
[12] DTSA § 2(b)(3)(B)(i)(I–III).

amount of actual damages and reasonable attorney's fees.[13] As discussed in more detail below, the DTSA also allows for ex parte seizure of materials related to a misappropriated trade secret. The DTSA contains a three-year statute of limitation.[14]

The Ex Parte Seizure Provision

The most controversial provision in the DTSA is the ex parte seize provision. The DTSA empowers district courts to order, upon ex parte application, "the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[15] To address concerns discussed during the Senate Judiciary Committee hearing, an amendment was added to expressly provide that an ex parte seizure order may only be granted in "extraordinary circumstances."[16]

In order to issue an ex parte seizure order, the court is required to find, based on specific facts, that a temporary restraining order issued under Rule 65(b) of the Federal Rules of Civil Procedure would be inadequate to prevent disclosure and that immediate and irreparable injury will occur without seizure.[17] The court also must find that the harm to the moving party if the seizure is not ordered outweighs the harm to the "legitimate interests" of the party against whom the seizure would be ordered, and

---

[13] DTSA § 2(b)(3)(C) and (D). An earlier version of the bill provided for exemplary damages that were three times the amount of actual damages.
[14] DTSA § 2(d). The statutes of limitations in state trade secret statutes vary. An earlier version of the DTSA provided for a five-year statute of limitation.
[15] DTSA § 2(b)(2)(A)(i).
[16] DTSA § 2(b)(2)(A)(i).
[17] DTSA § 2(b)(2)(A)(ii)(I-II).

"substantially outweighs" the harm to any third parties.[18] In addition, the court must find that the applicant for seizure is likely to succeed in showing that the information in question is a trade secret and was misappropriated by the other party.[19]

The applicant must also not have publicized the material on which seizure is sought and must describe "with reasonable particularity" what must be seized to protect the trade secret, and the court must find that the party against whom the seizure is sought would seek to "destroy, move, hide, or otherwise make such matter inaccessible" without seizure.[20] The target of the seizure must also be in "actual" possession of the trade secret and any property to be seized.[21]

If an ex parte seizure order is granted, the court is required to make specific findings of fact and conclusions of law showing why the issuance of the order is required.[22] The order must also be as narrowly tailored as is possible to protect the trade secret, while not interfering with the legitimate business interests of the party accused of misappropriating the trade secret that are unrelated to the trade secret that has allegedly been misappropriated.[23]

The seizure must be executed by a federal law enforcement officer.[24] The court may permit state or local law enforcement officials to participate.[25] The court's order must provide guidance to the law enforcement officials regarding the scope of their

[18] DTSA § 2(b)(2)(A)(ii)(III).
[19] DTSA § 2(b)(2)(A)(ii)(IV).
[20] DTSA § 2(b)(2)(A)(ii)(VI–VIII).
[21] DTSA § 2(b)(2)(A)(ii)(V).
[22] DTSA § 2(b)(2)(B)(i).
[23] DTSA § 2(b)(2)(B)(ii).
[24] DTSA § 2(b)(2)(E).
[25] DTSA § 2(b)(2)(E).

authority, including when the seizure may be executed and whether force may be used to access locked areas.[26]

Law enforcement officials may request the court permit an independent technical expert to assist in the seizure.[27] However, the independent technical expert must sign a non-disclosure agreement. [28] The applicant may not participate in the seizure.[29]

Any materials seized are to be taken into the custody of the court, and no copies or disclosures can be made.[30] After the seizure, the court may appoint a special master to locate and isolate all misappropriated trade secret information and to return data and information that belongs to the person from whom the property was seized and is not a trade secret.[31]

The court must hold a hearing no later than seven days after the order is issued, unless the party against whom the order is directed and others harmed by the order consent to a later date for the hearing.[32] A party who has had information seized may move for a modification or dissolution of the seizure order at any time, and if they suffered damage due to a wrongful or overly broad seizure, they are entitled to relief from the party that moved for seizure.[33] The court's seizure order must require the

[26] DTSA § 2(b)(2)(B)(iv).
[27] DTSA § 2(b)(2)(E).
[28] DTSA § 2(b)(2)(E).
[29] DTSA § 2(b)(2)(E).
[30] DTSA § 2(b)(2)(B)(iii) and (D).
[31] DTSA § 2(b)(2)(B)(iii) and (D).
[32] DTSA § 2(b)(2)(B)(v).
[33] DTSA § 2(b)(2)(F)(iii) and (G).

person obtaining the order to post a bond that the court determines is accurate for the payment of damages as a result of a wrongful or excessive seizure.[34]

The Inevitable Disclosure Doctrine and Employee Mobility

One concern discussed during Senate Judiciary Committee hearings relates to the controversial inevitable disclosure doctrine. Some thought there was a risk that injunctions under the DTSA which were based on "threatened misappropriation", rather than actual misappropriation, could negatively impact employee mobility, given that the DTSA authorizes federal judges to enjoin employees from starting positions with competitors based on the *threat* of misappropriation. An earlier version of the bill addressed this concern by stating that an injunction could not "prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation."

Some believed this provision was insufficient. The DTSA was therefore amended to provide that an injunction may not "prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows."[35] While an injunction based on threatened disclosure is still permitted, the determination of whether there is a "threat" will turn on the misconduct of the employee that shows he or she is likely to misappropriate information, rather

[34] DTSA § 2(b)(2)(B)(vi).
[35] DTSA § 2(b)(3)(A)(i)(I).

than the fact that the employee has information in his or her head that the former employer contends the employee will inevitably disclose if allowed to work for a competitor. The DTSA was also amended to provide that an injunction must not "otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."[36]

Whistleblower Protections

The DTSA provides that an individual is immune from civil or criminal liability under any federal or state trade secret law for the disclosure of a trade secret that is made in confidence to a government official or to an attorney for the sole purpose of reporting or investigating a suspected violation of the law, or is made in a complaint or other document filed in a lawsuit or other proceeding if such filing is made under seal. [37] Similar protections apply to the disclosure of a trade secret in a retaliation lawsuit.[38]

The DTSA requires employers to notify their employees of these immunities in any contract or agreement that governs the use of a trade secret or other confidential information.[39] The failure to comply with the notice requirement precludes the recovery of exemplary damages or attorney fees.[40]

[36] DTSA § 2(b)(3)(A)(i)(II).
[37] DTSA § 7(b)(1).
[38] DTSA § 7(b)(2).
[39] DTSA § 7(b)(3)(A).
[40] DTSA § 7(b)(3)(C).

Reactions to the DTSA

There has been extensive discussion in academia and the bar about the pros and cons of federalizing trade secret law, as well as analysis of the efforts to federalize trade secret law, including the DTSA. A group of law professors opposed prior efforts to implement federal trade secret legislation, arguing that doing so would weaken state trade secret law and create uncertainty.[41] The professors also argued that a federal trade secrets law could be used for anti-competitive purposes.[42] Others have questioned whether federalizing trade secret law is within Congress' power under the Commerce Clause, given that some material traditionally considered trade secrets—such as customer lists—may be in some instances confined intra-state.[43] Another frequently raised concern is that the ex parte seizure provision could be abused. Some have also raised the prospect of "trade secret trolls," similar to "patent trolls," or non-practicing entities, which own patents and assert rights against infringers.

Notwithstanding these critiques, the DTSA attracted many supporters and had bipartisan backing in both legislative chambers. The business community was also reportedly fully behind the idea of federal trade secrets legislation, and a number of intellectual property counsel for major corporations testified before Congress in favor of

---

[41] *See* Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2014" (S.2267) and the "Trade Secrets Protection Act of 2014" (H.R. 5233), available at http://infojustice.org/wp-content/uploads/2014/08/Professor-Letter-Opposing-Trade-Secret-Legislation.pdf.
[42] *Id.*
[43] *See* Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2014," *supra* note 41.

the bill.[44] Many practitioners and businesspeople alike justifiably believe that the increasingly national and international nature of trade secret theft warrants heightened protection through a federal scheme.[45]

Federal trade secret legislation will also likely make the laws governing trade secret protection increasingly uniform throughout the United States (although the fact that state trade secret laws are not preempted raises questions about the level of uniformity that can be achieved). Finally, in response to concerns about the ex parte seizure provisions, many believe these provisions are necessary to allow for recovery of stolen trade secrets in unique, egregious circumstances, and that the statute provides reasonable protections to guard against abuse. Those defending the ex parte seizure provision note that federal judges entrusted with enforcement of these provisions will undoubtedly exercise due caution and reserve ex parte relief for very limited situations.

Survey of Opinions Discussing the DTSA

Not surprisingly, many employers are taking advantage of this new law when former employees and/or competitors take their valuable trade secret information. This section of this article surveys a number of the court opinions involving claims brought under the DTSA. The opinions surveyed in this article touch on a variety of issues

---

[44] *Report of the Senator Judiciary Committee on the Defend Trade Secrets Act of 2016*, available at https://www.congress.gov/congressional-report/114th-congress/senate-report/220/1.
[45] *Trade Secret Practitioner Letter of Support*, available at http://www.beckreedriden.com/wp-content/uploads/2015/12/Trade-Secret-Practitioner-Letter-of-Support-Final.pdf.

germane to the DTSA, including whether a misappropriation that occurred prior to the enactment of the DTSA but continued after its passage is actionable, obtaining TROs and preliminary injunctions, the definitions of a "trade secret" and "misappropriation" under the DTSA, and the relationship between the DTSA and state non-compete law.

Cases Discussing Continuous Misappropriation of Information Taken Prior to Passage of the DTSA

One issue that arose frequently in cases litigated shortly following the DTSA's passage was how courts should treat trade secret violations that occurred prior to the passage of the DTSA, but that continued after the DTSA was in effect. The following cases illustrate how courts have dealt with this issue.

Syntel Sterling Best Shores Mauritius, Ltd. v. TriZetto Group, Inc.

In September 2016, the United States District Court for the Southern District of New York granted TriZetto Group, Inc. ("TriZetto") and Cognizant Technology Solutions leave to amend their counterclaims against Syntel Sterling Best Shores Mauritius, Ltd. ("Syntel"), specifically to include "new claims and allegations of trade secret theft under the [DTSA]."[46]

[46] *Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc.*, 15-CV-211 (LGS) (RLE), 2016 WL 5338550 (S.D.N.Y. Sept. 23, 2016).

TriZetto developed software products for the healthcare industry and hired Syntel as a contractor.[47] The two parties executed a Master Services Agreement ("MSA"), which contained a clause that prevented the use of one's confidential information by the other for their individual benefit.[48] When TriZetto was acquired by a competitor, Cognizant, Syntel elected to use their option to terminate the MSA on February 18, 2015.[49]

The defendants asserted that Syntel employees systematically accessed and downloaded confidential information and intended to use it to compete against TriZetto because it was acquired by a Syntel competitor.[50] The litigation began in January 2015.[51] The court had initially set March 23, 2015 as "the deadline to amend the pleadings without leave of the court."[52] However, because the DTSA was passed during the proceedings, the defendants sought to add a DTSA claim to their counterclaims.[53] The court determined that the defendants' confidential information and Syntel's downloading of that information sufficed to meet the elements for relief under the DTSA.[54] Specifically, the court determined that defendants successfully alleged that they proved they "took reasonable measures to keep the information secret . . . the information [was] valuable and crucial to business functions . . . [and that] Syntel [] without their consent [] downloaded TriZetto's Intellectual Property from their

[47] *Id.* at *1.
[48] *Id.*
[49] *Id.* at *6.
[50] *Id.* at *2.
[51] *Id.* at *2-3.
[52] *Id.* at *3.
[53] *Id.*
[54] *Id.* at *6.

Customer Exchange and other repositories and used it for Syntel's own use and financial gain, in breach of the MSA's prohibition on each party using the other's confidential information for its own benefit."[55]

More significantly, the court allowed the DTSA counterclaim because the "wrongful act continue[d] to occur after the date of the enactment of DTSA."[56] Thus, under *Syntel*, a misappropriation which initially occurred prior to the enactment of the DTSA but continues after its passage can be actionable under the DTSA.

Adams Arms LLC v. Unified Weapon Systems, Inc.

The United States District Court for the Middle District of Florida also decided a case involving a continuing misappropriation that began prior to the DTSA's enactment in *Adams Arms, LLC v. United Weapon Systems*.[57]

Adams Arms produced weapons for law enforcement officers around the world.[58] Adams Arms was approached in 2014 by Aguieus and United Weapons Systems, Inc. ("UWS"), a subsidiary of Aguieus, to collaborate on a bid to provide the Peruvian government with rifles.[59]

The collaboration to win the bid required that Adams Arms provide products and trade secrets to UWS.[60] Adams Arms and Aguieus then executed a Mutual

---

[55] *Id.*
[56] *Id.*
[57] *Adams Arms, LLC v. Unified Weapon Sys. Inc.*, No. 8:16-cv-1503-T-33AEP, 2016 WL 5391394, at *1 (M.D. Fla. Sept. 27, 2016).
[58] *Id.*
[59] *Id.*
[60] *Id.*

Confidentiality and Nondisclosure Agreement, which prevented trade secret use for any purpose other than those related to the project.[61] A non-binding Letter of Intent to order 3,000 units from Adams Arms was then executed.[62] General Parker, a director and advisor for UWS, then met with the president and CEO of Adams Arms in attempt to offer his help in negotiating the contract with the Peruvian government.[63] General Parker did not disclose that he worked with UWS when he was asked about possible conflicts of interest, and then executed a Confidential/Nondisclosure Agreement with Adams Arms.[64]

While Adams Arms took great care to protect its trade secrets, it disclosed trade secrets to the defendants after the various confidentiality agreements were signed.[65] Throughout the manufacturing process of the arms for the Peruvian government, various trade secrets were disclosed at the defendants' request.[66] Eventually, UWS was announced as the winner of the bid for providing the weapons to the Peruvian government.[67] However, after the announcement UWS effectively excluded Adams Arms entirely from the deal.[68]

Adams Arms filed a complaint on June 10, 2016 against UWS that included a cause of action for violation of the DTSA and the Florida Trade Secrets Act ("FTSA").[69]

---

[61] *Id.*
[62] *Id.* at *2.
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.* at *3.
[67] *Id.*
[68] *Id.*
[69] *Id.*

Defendants moved to dismiss the DTSA claim on the grounds that the DTSA was not in effect at the time of the misappropriation.[70] The defendants argued that 18 U.S.C. Section 1836(b), the three year statute of limitations provision, should bar the DTSA claim because the provision means that "any continuity of a misappropriation shall be treated as one misappropriation."[71] The court rejected this argument.[72] The court interpreted the statute of limitations provision in the DTSA to apply "only when a claim accrues for statute of limitation purposes."[73] The issue before the court was whether the DTSA could apply when the misappropriation of trade secrets occurred both before and after the DTSA's effective date.[74] The court looked to Section 2(e) of the DTSA, which states that the law applies to "any misappropriation . . . for which any act occurs after the effective date."[75] The court interpreted this to mean that under the DTSA, "when an 'act' occurs after the effective date, a partial recovery is available on a misappropriation claim."[76] The court therefore denied the defendants' motion to dismiss.[77]

Mission Measurement Corporation v. Blackbaud, Inc.

In October 2016, the United States District Court for the Northern District of Illinois decided a case involving misappropriation that occurred prior to the enactment

[70] *Id.* at *5.
[71] *Id.* at *6 (quoting Doc. #46 at 2).
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.* (quoting Pub. L. No. 114-153, Section 2(e)).
[76] *Id.* at *6.
[77] *Id.*

of the DTSA, although it did not specifically address whether this fact impacted the viability of the claim, unlike *Adams Arms* and *Syntel*.[78]

Mission Measurement Corporation ("Mission") provides data to non-profits and other entities with the goal of predicting the success of social impact programs.[79] Mission developed a proprietary database called "Outcome Taxonomy" to help in these predictions.[80] At the time of the litigation, a patent was pending for Outcome Taxonomy.[81] In 2012, Vista Equity Partners ("Vista") reached out to Mission in an attempt to obtain a method for measuring outcomes for their client, MicroEdge.[82] After a series of discussions, MicroEdge and Mission Measurement agreed to jointly design a software application.[83]

Concerned with protecting trade secret information, Mission and MicroEdge executed a Confidentiality and Non-Disclosure Agreement and negotiated the terms of a Joint Development Agreement, but never signed it.[84] In 2013, both parties executed a Letter of Intent, which "explicitly acknowledged the joint nature of the product in terms of joint product development, joint technology development, and joint sales pitch meetings . . . [and] clearly stated that the Outcomes Taxonomy is Mission Measurement's sole property."[85] Mission worked closely with and continued to share

---

[78] *Mission Measurement Corp. v. Blackbaud, Inc.*, 216 F. Supp. 3d 915 (N.D. Ill. 2016).
[79] *Id.* at 917.
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.* at 918.
[84] *Id.*
[85] *Id.*

confidential information with MicroEdge until the summer of 2014, when MicroEdge abruptly stopped communicating with Mission.[86]

Unbeknownst to Mission, MicroEdge had been in acquisition discussions with Blackbaud, Inc. ("Blackbaud") for several months.[87] After Blackbaud purchased MicroEdge for $160 million, Mission was informed of the acquisition and assured that the joint product would be more successful as a result of the deal.[88] MicroEdge did not revoke or terminate any of the executed Agreements with Mission.[89] In October 2015, the defendants issued a press release that introduced a product very similar to the joint product with no mention of Mission.[90] Soon after, the product entered the market.[91]

Mission alleged that MicroEdge and Vista had initially planned to "pump up MicroEdge's value" by developing the joint product with Mission, and that Mission's eventual exclusion was also deliberately engineered.[92] Further, the product introduced in a February 2016 press release called "Blackbaud Outcomes" possessed nearly identical characteristics of the joint product.[93]

Mission brought causes of action under both the DTSA and the Illinois Trade Secrets Act ("ITSA").[94] After providing an overview of both laws, the court analyzed the defendants' argument that the Mission's claims failed because they "failed to specifically

---

[86] *Id.* at 919.
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.* at 919-20.

identify the exact trade secrets at issue in this lawsuit."[95] The court, applying the applicable pleading standards, found that when a complaint does not directly specify the trade secrets at issue, "'allegations [are] adequate in instances where the information and the efforts to maintain its confidentiality are described in general terms.'"[96] The court found Mission's allegations were sufficient.[97] Throughout the course of their discussions and the development of the joint project, Mission allegedly disclosed a wealth of confidential information to MicroEdge, and Mission and MicroEdge entered into a Confidentiality and Non-Disclosure Agreement before the information was shared.[98] After the Letter of Intent was signed in 2013, Mission shared more confidential information.[99] The defendants allegedly used this confidential information in "marketing and selling BlackBaud outcomes, which embodies most, if not all, of the joint product offerings."[100] The court found that these allegations were sufficient, but did not address the import of the alleged misappropriation initially taking place prior to the enactment of the DTSA.[101]

Brand Energy & Infrastructure Services, Inc. v. Irex Contracting Group

In March 2017, the United States District Court for the Eastern District of Pennsylvania held that the DTSA applies to misappropriation that began before its May

[95] *Id.* at 920.
[96] *Id.* (quoting *Covenant Aviation Sec., LLC v. Berry*, 15 F. Supp. 3d 813, 818 (N.D. Ill. 2014)).
[97] *Id.* at 921.
[98] *Id.* at 921-22.
[99] *Id.* at 921.
[100] *Id.* at 921-22(citing Compl. ¶ 48).
[101] *Id.* (citing Compl. ¶ 48).

11, 2016 enactment, so long as the misappropriation continued after the effective date.[102] Plaintiff, Brand Energy & Infrastructure Services, Inc. ("Brand"), a construction company, alleged that three of its former employees stole its trade secrets and equipment and misappropriated its proprietary information.[103] Brand claimed that these former employees had been using its stolen equipment and trade secrets to benefit their new employer, Irex Corporation ("Irex").[104] As such, Brand brought claims against Irex and the defendant-employees under the DTSA, as well as various state law claims.[105]

The events giving rise to this lawsuit started in 2014 when employees at Brand began leaking Brand's protected business information to the three defendant-employees who had already moved to Irex.[106] One specific item Brand alleges the defendant-employees stole is Brand's "Market Playbook" which is a database only accessible on Brand-network computers that allegedly contains billions of dollars in proprietary information, including Brand's future business plans and targets.[107] Brand further contended that the defendant-employees were continuing to use the information up until the time of the instant lawsuit.[108] Brand claimed that it had lost millions of dollars

---

[102] *Brand Energy & Infrastructure Servs., Inc. v. Irex Contracting Grp.*, No. 16-2499, 2017 WL 1105648 (E.D. Pa. Mar. 24, 2017)
[103] *Id.* at *1.
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*

as a result of the misappropriation and theft. [109] Irex filed a motion to dismiss Brand's claims.[110]

The court ultimately denied Irex's motion to dismiss, holding that the "use" of another's trade secret explicitly qualifies as an act of misappropriation under the DTSA, and Brand's complaint alleges various times, after the enactment of the DTSA, that Irex "used" its alleged trade secrets.[111]

The court also found that applying the DTSA to this case does not violate the Ex Post Facto Clause of the United States Constitution and therefore is not impermissibly retroactive.[112] The court concluded that the statutory language and legislative history of the DTSA reveal Congress's intent to apply the DTSA to continuing misappropriations that began prior to its enactment but continue post-enactment.[113] The court reasoned that Congress' close adherence to the UTSA as a model for drafting most of the DTSA means that its exclusion of a few select UTSA provisions was intentional and therefore quite revealing.[114] The UTSA "effective date" provision stipulates, "[w]ith respect to a continuing misappropriation that began prior to the effective date, the [Act]…does not apply to the continuing misappropriation that occurs after the effective date."[115] The DTSA's "effective date" provision is very different because Congress specifically omitted the language that would have precluded the DTSA from applying to misappropriations

[109] *Id.* at *2.
[110] *Id.* at *1.
[111] *Id.* at *4.
[112] *Id.* at *5.
[113] *Id.* at *7.
[114] *Id.* at *8.
[115] *Id.* (quoting UTSA § 11).

that began before, but continued after, enactment.[116] If Congress had wanted to keep UTSA's "effective date" provision, it could have done so with more ease than drafting a new provision.[117] Thus, the court found no reason to dismiss Brand's DTSA claim and Irex's motion to dismiss was denied.[118]

Avago Technologies U.S., Inc. v. NanoPrecision Products, Inc.

In January 2017, the United States District Court for the Northern District of California dismissed a DTSA claim finding that it did not allege misappropriation prior to the effective date of the statute.[119] The plaintiff and counter-defendant, Avago Technologies U.S., Inc. ("Avago"), is a global supplier of "fiber optic communications modules."[120] Lawrence McColloch was employed as an engineer at Avago and worked for many years developing the design of single mode optical benches.[121] Defendant, nanoPrecision Products, Inc. ("nPP"), began communicating with Avago in 2010 regarding its capabilities to precision stamp various components for fiber optic applications, including optical benches.[122] After Avago and nPP entered into a non-disclosure agreement in 2012, they continued to communicate about the possibility of

[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Avago Techs. U.S. Inc. v. NanoPrecision Prods., Inc.*, No. 16-cv-03737-JCS, 2017 WL 412524 (N.D. Cal. Jan. 31, 2017).
[120] *Id.* at *1.
[121] *Id.*
[122] *Id.*

working together and shared confidential designs back and forth for a few years before such communications led to the dispute.[123]

While discussions about working together were still underway, McColloch filed various patent applications assigning ownership thereof to Avago.[124] Alleging that one patent contained proprietary information that nPP had disclosed to Avago during their discussions under the NDA, nPP filed a complaint in the Superior Court of California in early 2015.[125] Shortly thereafter, in April 2015, nPP filed a patent application.[126] Avago alleged that nPP's application used inventions that were previously disclosed in Avago's application.[127]

In the instant action, initiated on July 1, 2016, Avago sought a declaratory judgment of correct inventorship of the two patents which it had been issued as of that date.[128] In nPP's counterclaim, nPP asserted a DTSA claim against Avago, alleging that Avago used nPP's proprietary and confidential information to prepare its patent application.[129]

Avago contended that nPP's DTSA claim must be dismissed because all the actionable conduct alleged in nPP's counterclaim occurred *before* the DTSA came into effect.[130] The court agreed and found for Avago.[131] nPP contended that Avago's

---

[123] *Id.* at *2.
[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.* at *3.
[129] *Id.* at *8.
[130] *Id.*
[131] *Id.*

continued use of its confidential information in the prosecution of the "Avago Applications" allowed it to seek a partial recovery for misappropriation from the date the DTSA came into effect.[132] To be clear, nPP did not suggest that any new information was disclosed in the course of the patent prosecutions that had not been disclosed prior to DTSA's effective date, rather it alleged that "Avago *again disclosed such information to the world by its continued prosecution of the Avago Applications*."[133]

The court found that nPP did not cite any authority suggesting that the DTSA allows a misappropriation claim to be asserted based on the continued use of information that was disclosed prior to the effective date of the statute.[134] Simply alleging that the same information was disclosed "again" is not sufficient to meet the definition of "disclosure" because "disclosure," by definition, implies that the information was previously secret.[135] Additionally, nPP failed to allege any facts showing that acts of misappropriation occurred after the DTSA came into effect.[136] Accordingly, the court dismissed nPP's DTSA claim, with leave to amend to include allegations showing that the DTSA claim is based on misappropriation that occurred after the effective date of the statute.[137]

---

[132] *Id.* at *9.
[133] *Id.* (emphasis added).
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.*

Cave Consulting Group, Inc. v. Truven Health Analytics, Inc.

In May 2015, Cave Consulting Group, Inc ("CCGroup") sued Truven Health Analytics, Inc. ("Truven"), alleging infringement of two patents.[138] In February 2017, CCGroup filed a third amended complaint adding claims for misappropriation under the DTSA, among other state statutory and common law claims.[139] In April 2017, the United States District Court for the Northern District of California dismissed the DTSA claim for failure to allege specific acts of misappropriation after the enactment date of the DTSA.[140]

The events giving rise to the misappropriation claims occurred in December 2016 when Truven produced discovery emails in connection with the patent litigation that allegedly showed that in 2014, when CCGroup was competing for a Truven client, a Truven vice president had reached out to a contact who worked at a business that had formerly used CCGroup's services to acquire a copy of CCGroup's confidential presentation materials.[141] According to CCGroup, the confidential presentation materials contained trade secret information about CCGroup's software products, and Truven used them to prepare for a meeting with the client who ultimately chose to remain with Truven.[142] After said client meeting, CCGroup alleged specifically that the Truven vice president shared the confidential materials with another Truven employee, and generally that Truven continued to use the alleged trade secrets as of the date of the

---

[138] *Cave Consulting Grp., Inc. v. Truven Health Analytics, Inc.*, No. 15-cv-02177-SI, 2017 WL 1436044 (N.D. Cal. Apr. 24, 2017).
[139] *Id.* at *1.
[140] *Id.*
[141] *Id.*
[142] *Id.*

instant lawsuit to compete with CCGroup for potential customers and to develop and modify its products to be more competitive with CCGroup.[143]

The DTSA only covers acts occurring "on or after the date of the enactment of this Act."[144] Thus, Truven contended, CCGroup failed to state a claim under the DTSA because the alleged misappropriation occurred before the DTSA's passage.[145] However, CCGroup argued that it can still pursue claims under the DTSA alleging "use" and "disclosure" of trade secrets *after* the enactment of the DTSA for there are three theories of liability under the DTSA: acquisition, disclosure, and use.[146] Nonetheless, the court found for Truven and dismissed the DTSA claim.[147]

The court held that the specific conduct regarding the use and disclosure of trade secrets (i.e. the use of the materials in preparation for a client meeting, and the forwarding of the presentation materials from the vice president to another employee) predated the enactment of the DTSA.[148] As for Truven's conduct after the enactment of the DTSA, CCGroup generally alleged that Truven was continuing to use its intellectual property to develop and modify products to be more competitive with CCGroup.[149] The court found this general allegation insufficient to state a claim because it lacked specific allegations that Truven used or disclosed the alleged trade secrets after the enactment of

---

[143] *Id*. at *2.
[144] *Id*. (citing Pub. L. No. 114-153 § 2(e), 130 Stat. 376 (2016)).
[145] *Id*. at *3.
[146] *Id*. at *3-4.
[147] *Id*. at *5.
[148] *Id*.
[149] *Id*.

the DTSA.[150] Accordingly, the court dismissed the DTSA claim, granting leave to amend with more particularity.[151]

Agilysys, Inc. v. Hall

In May 2017, the United States District Court for the Northern District of Georgia mirrored the reasoning of the court in *Adams Arms* regarding continued misappropriation when it denied a former employee's motion to dismiss the DTSA claim against him and found that "an owner may recover under the DTSA if any act of misappropriation occurs after the [Act's] effective date" even if the information was taken prior to the DTSA's enactment.[152]

Agilysys, Inc. ("Agilysys") brought several claims against its former employee Ken Hall and his new employer Solutions II, Inc. ("Solutions II"), including claims for violation of the CFAA and DTSA.[153] Both defendants filed various motions to dismiss all of the claims against them.[154]

Hall had worked for Agilysys as a Major Account Executive for several decades.[155] Because Hall had access to proprietary information, including Agilysys's sales force, marketing programs, sales strategies, customer acquisition methods, sales figures, pricing information, existing contracts, and customer lists, he entered into a non-

[150] *Id.*
[151] *Id.*
[152] *Agilysys, Inc. v. Hall*, 258 F. Supp. 3d 1331, 1349 (N.D. Ga. 2017).
[153] *Id.* at 1339.
[154] *Id.*
[155] *Id.* at 1338.

disclosure agreement with the company and was also bound by its code of conduct and policies.[156]

Agilysys alleged that from March 29 through March 31, 2016, "Hall emailed Agilysys' trade secret, confidential, and/or proprietary information from his Agilysys email account to his personal email account."[157] Furthermore, Agilysys alleged that Hall then resigned from Agilysys by email on the afternoon of March 31.[158] Minutes after sending his resignation, Agilysys alleged that Hall sent additional customer information from his Agilysys email account to his personal email account.[159] Thereafter, Hall began working for Solutions II: a direct competitor of Agilysys.[160] Agilysys also continued to receive messages from customers to Hall at his Agilysys email account regarding proposals he had sent the customers after his resignation.[161]

In his motion to dismiss the DTSA claim, Hall argued that since the DTSA was not enacted until May 11, 2016 and continuing misappropriations are treated as a single misappropriation, his March 2016 actions were not in the ambit of the DTSA.[162] In response, Agilysys argued that Hall's "continued use, possession, and disclosure of Plaintiff's proprietary information after May 11, 2016, constitute[d] actionable misappropriation."[163] The court agreed.[164]

---

[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.*
[162] *Id.* at 1348.
[163] *Id.*
[164] *Id.*

The court found that based on the time of acquisition of confidential information alone, Agilysys's claim against Hall would be barred.[165] However, Hall's argument that under 18 U.S.C. section 1836(d), "a continuing misappropriation constitutes a single claim of misappropriation" failed because that provision referred solely to the determination of the DTSA's statute of limitations.[166] The court held that it was clear the DTSA was intended to apply to any misappropriation of a trade secret occurring on or after the effective date.[167]

Wang v. Golf Tailor, LLC

Later in the summer of 2017, the United States District Court for the Northern District of California examined the extinguishment of continuing misappropriation claims for products made available to the public before the DTSA was enacted.[168]

Jonathan Wang and Golf Tailor, LLC ("Golf Tailor") each claimed to have created the same golf club and golf training aid, and each alleged that the other had stolen the design.[169] The parties had filed suit over these products in multiple federal courts before Wang initiated litigation in the Northern District of California.[170]

---

[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Wang v. Golf Tailor, LLC*, No. 17-cv-00898-LB, 2017 WL 2861111, at *1 (N.D. Cal. July 5, 2017).
[169] *Id.*
[170] *Id.* at *3.

Golf Tailor asserted a counterclaim that Wang had misappropriated Golf Tailor's trade secrets by selling the golf club and training aid.[171] The court held that Golf Tailor had no DTSA claim against Wang for the golf club because Golf Tailor had already lost any trade secrets it had in the product before the DTSA was enacted.[172] Because Golf Tailor was selling the clubs in 2015, there could be no continuing misappropriation because any design-related trade secrets embodied in the clubs would have been available to the public before May 11, 2016: the DTSA's effective date.[173] Under California state trade secret law, public disclosure, even by simply selling a product, "'is fatal to the existence of a trade secret.'"[174] Therefore, Tailor Golf's misappropriation claim for the golf club was extinguished.[175]

The beginning sale date for the training aid was less clear, and the court found it was possible that Golf Tailor's training aid sales did not begin until after the enactment of the DTSA.[176] If true, Golf Tailor could have asserted its counterclaim against Wang for misappropriation of the training aid. However, Wang presented admissions from Golf Tailor at a hearing that sale dates for the training aid preceded the DTSA's enactment.[177] Golf Tailor then agreed to withdraw its DTSA counterclaim without prejudice to its right

---

[171] *Id. at *4.*
[172] *Id.*
[173] *Id.*
[174] *Id.* (quoting *In re Providian Credit Card Cases*, 96 Cal. App. 4th 292, 304 (2002)).
[175] *Id.* at *5.
[176] *Id.* at *6.
[177] *Id.*

to assert a trade secrets claim under California law if it could demonstrate in the future that Wang appropriated the training aid before it was available for sale.[178]

Dazzle Software II, LLC v. Kinney

In *Dazzle*, John Kinney allegedly downloaded the contents of one of the plaintiff's computers.[179] The computer allegedly contained trade secret information about the Dazzle Software program, which was used by pawnshops to manage sales and customer information.[180] Dazzle Software was developed by Derek Best, who passed away in 2016.[181] Mr. Best managed the company himself, and when he died, he left the assets to his wife.[182] According to the record, Mrs. Best was not able to manage the business, and litigation after Mr. Best's death allowed Dazzle Software II, LLC ("Dazzle") to purchase the business assets.[183] Three computers contained the program, and Mrs. Best was required to turn them over to Dazzle.[184] However, she had not turned over the third computer at the time of the alleged misappropriation.[185]

---

[178] *Id.*
[179] *Dazzle Software II, LLC v. Kinney*, No. 16-cv-12191, 2016 WL 6248906, at *1 (E.D. Mich. Aug. 22, 2016); Plaintiff's Response in Opposition to Defendant's Motion to Dismiss Count IV of Plaintiff's Complaint with Prejudice at1.
[180] *Dazzle Software*, 2016 WL 6248906, at *1.
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] Plaintiff's Response in Opposition to Defendant's Motion to Dismiss Count IV of Plaintiff's Complaint with Prejudice at 1.
[185] *Dazzle Software*, 2016 WL 6248906, at *1.

Kinney contacted Mrs. Best under the pretext of attempting to obtain a license to allow him and his employer to keep using the software.[186] Mrs. Best allowed him to use the third computer, but he then downloaded the computer's entire contents.[187] He then made the contents available to his employer, Central Ohio Scrap Metal Co.[188]

Dazzle filed a complaint in the United States District Court for the Eastern District of Michigan, alleging multiple causes of action, including one for violation of the DTSA. Dazzle sought ex parte relief, which the court declined to grant in a brief order. The defendants moved to dismiss the DTSA claim because the alleged misappropriation took place before the DTSA's enactment.[189] In August 2016, the Eastern District of Michigan ruled in a very brief opinion that Dazzle's cause of action under the DTSA failed because Dazzle had not alleged misappropriation occurring after the enactment of the DTSA.[190] The court did allow Dazzle to amend its Complaint to assert violations of the DTSA based on post-enactment conduct.[191]

Cases Discussing the Elements and Scope of TRO's and Preliminary Injunctions Based on the DTSA

Not surprisingly, many cases interpreting the DTSA do so in the context of adjudicating a request for injunctive relief. This section discusses cases where courts

---

[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Id.*
[191] *Id.*

have addressed temporary restraining orders and preliminary injunctions under the DTSA.

Henry Schein, Inc. v. Cook

In *Henry Schein, Inc. v. Cook,* the United States District Court for the Northern District of California issued some of the first rulings in a case involving a DTSA claim in June 2016.[192] Henry Schein, Inc. ("HSI") markets, distributes, and sells healthcare supplies and equipment to healthcare providers.[193] Jennifer Cook was hired by HSI as a Field Sales Consultant in April 2005.[194] She signed a Confidentiality and Non-Solicitation Agreement when she was hired. Additionally, in 2011, she signed a Letter Agreement that "required her to hold 'in strictest confidence' any confidential information 'concerning the products, processes, services, business, suppliers, and customers of HSI,' and 'to neither copy nor take any such material upon leaving the Company's employ.'"[195] She also agreed not to solicit any of HSI's past or present customers for a 12-month period following the end of her employment.[196]

On May 13, 2016, Cook resigned from HSI to begin a position at a competitor.[197] Prior to her resignation, Cook had forwarded emails containing confidential company

---

[192] *Henry Schein, Inc. v. Cook*, No. 16-cv-03166-JST, 2016 WL 3418537, at *1 (N.D. Cal. June 22, 2016).
[193] *Id.*
[194] *Id.*
[195] *Id.* (quoting ECF No. 2-1 at 9-10).
[196] *Id.* (quoting ECF No. 1 at 24).
[197] *Id.* (quoting ECF No. 1 at 24).

reports that constituted trade secrets from her work account to her personal account.[198] On the day of her resignation, Cook used HSI's proprietary software to transfer confidential customer information to her company laptop.[199] She then downloaded the customer information to her iPad.[200] HSI further alleged that Cook had visited its customers' offices prior to her resignation and attempted to persuade them to switch their business to her new employer.[201]

On June 9, 2016 HSI filed suit against Cook and sought a temporary restraining order.[202] HIS's complaint included a claim under the DTSA.[203] On June 10, the Northern District of California granted HSI's application for a TRO in part, because "Plaintiff was likely to succeed on its trade secret claims, brought under the DTSA, CUTSA, and UCL, among others, because 'customer information such as sales history and customer needs and preferences constitute trade secrets.'"[204] The TRO required Cook to refrain from destroying or altering materials related to the case, accessing or using any of HSI's confidential information, and contacting or communicating with any of her assigned clients while she was employed with HSI.[205]

The court subsequently took up HSI's request for a preliminary injunction.[206] The court considered the definitions of trade secrets under both the DTSA and

---

[198] *Id.*
[199] *Id.* Cook also failed to return the company laptop for two weeks.
[200] *Id.*
[201] *Id.* at *2.
[202] *Id.*
[203] *Id.*
[204] *Id.* at *3-*4. (quoting ECF No. 12 at 5).
[205] *Id.*
[206] *Id.*

California's trade secrets act (CUTSA).[207] The court then focused on whether customer information at issue was protectable as a trade secret under California law.[208] HSI argued the information was protectable as a trade secret because "the customer information at issue was developed by HSI and kept confidential in order to give HSI an advantage over its competitors in obtaining business from those customers" and HSI took reasonable measures to ensure that the information was kept confidential.[209] Cook alleged that the information was not protectable as a trade secret because the information was already known to others in the industry and also available from public sources, such as a Google search.[210] The court disagreed with Cook, holding that the information was protectable as a trade secret because HSI's proprietary software contained information such as customer buying patterns that would not be readily available to others in the industry.[211] Ultimately, the court held that Cook had misappropriated the documents and information she e-mailed to herself under both the DTSA and the CUTSA.[212]

In examining HSI's allegation that Cook had violated the Letter Agreement by soliciting customers prior to and immediately after her resignation, the court applied Cal. Bus. & Prof. Code section 16600.[213] Section 16600 states that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of

---

[207] *Id.* at *4.
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *Id.* at *5.
[213] *Id.* at *6.

any kind is to that extent void."[214] The court determined that the non-solicitation clause in the Letter Agreement fell under the type of contract governed by section 16600.[215] HSI's argument that the clause fell under the "trade secret exception" sometimes recognized by California courts failed.[216] In order for the non-solicitation clause to meet the exception, HSI had to show that it was "necessary to protect the trade secrets at hand."[217] The court ruled HSI did not show the non-solicitation clause was necessary to protect the trade secrets, as there were "separate clauses in the same agreements that independently require[d] Cook to refrain from revealing or otherwise misusing trade secrets."[218] Further, HSI did not demonstrate that the materials Cook downloaded pertained to a specific HSI customer.[219]

The court further concluded that HSI did not prove that enjoining Cook from contacting HSI customers was necessary to protect its trade secrets.[220] Prior California case law established that "a court may not enjoin solicitation of a business based on a contractual clause – which would violate section 16600 – [but] it may do so based on tortious conduct – such as violation of the CUTSA or the UCL . . . thus, 'a former employee may be barred from soliciting existing customers to redirect their business

---

[214] *Id.* (quoting Cal. Bus. & Prof. Code section 16600).
[215] *Id.*
[216] *Id.*
[217] *Id.* at *6 (quoting *Asset Mktg. Sys., Inc. v. Gagnon*, 542 F. 3d 748, 758 (9thCir. 2008)).
[218] *Id.* (quoting *Gatan, Inc. v. Nion Co.*, No. 15-CV-1862-PJH, 2016 WL 1243477, at *3 (N.D. Cal. Mar. 30, 2016) (invalidating a clause under section 16600 preventing a reseller from marketing, selling or distributing any products similar to Gatan's products within one year after entering into a purchase agreement)).
[219] *Id.*
[220] *Id.* at *8.

away from the former employer and to the employee's new business if the employee is utilizing trade secret information to solicit those customers."[221] The court thus concluded that because Cook did not demonstrate a lack of cooperation with court orders and HSI failed to demonstrate through specific evidence that Cook was using trade secret information from HSI in order to solicit customers, HIS was not entitled to an injunction preventing Cook from having contact with customers.[222]

Earthbound Corporation v. MiTek USA

Earthbound Corporation ("Earthbound") is a manufacturer of products used to prepare buildings for earthquakes during construction. Earthbound filed a complaint against several former employees of Intact Structural Supply ("ISS"). ISS was a company affiliated with Earthbound that sold its products, services, and systems.[223] As members of the sales team of ISS, the former employees had access to Earthbound's trade secret information, financial goals, and planning information, including the "Super-Template," which Earthbound considered "a priceless trade secret."[224] Although Earthbound did use password protection for access to company information, none of the former employees had signed any type of confidentiality agreement while employed at ISS.[225]

---

[221] *Id.* (quoting *Ret. Grp. v. Galante*, 176 Cal. App. 4th 1226, 1238, 1238, 1237 (2009)).
[222] *Id.*
[223] *Earthbound Corp. v. MiTek USA, Inc.*, No. C16-1150 RSM, 2016 WL 4418013, at *1 (W.D. Wash. Aug. 19, 2016).
[224] *Id.*
[225] *Id.* at *2.

MiTek USA ("MiTek") was one of two Earthbound competitors.[226] MiTek had twice been in unsuccessful negotiations to buy Earthbound.[227] During those negotiations, the parties had executed a Non-Disclosure Agreement.[228] In June 2016, the former employees resigned from their positions and accepted positions at MiTek.[229]

After the employees turned in their company laptops and devices, it was discovered that some devices had been restored to factory settings.[230] Earthbound hired a forensic expert, who determined that on June 13, 2016, one of the employees accessed a large number of Earthbound files and a USB drive was inserted into the computer on the same day.[231] The forensic expert further identified evidence suggesting Defendants misappropriated Earthbound trade secrets prior to their resignations and continued to use them to work on bids and projects for MiTek customers.[232]

Earthbound filed suit in the United States District Court for the Western District of Washington, asserting claims for breach of duty of loyalty and for misappropriation of trade secrets under both the DTSA and the Washington Uniform Trade Secrets Act ("WUTSA").[233] Earthbound sought injunctive relief, arguing that that "if the individual Defendants are not immediately enjoined, and if MiTek is not ordered to return

---

[226] *Id.*
[227] *Id.*
[228] *Id.* at *2.
[229] *Id.*
[230] *Id.*
[231] *Id.* at *3.
[232] *Id.* at *3-7.
[233] *Id.*

Earthbound's data and allow Earthbound to conduct expedited discovery, ISS will likely close its doors and Earthbound may never recover."[234]

The court first examined Earthbound's misappropriation claim under the WUTSA.[235] Washington uses the Uniform Trade Secrets Act's definitions of trade secret and misappropriation, and the court determined that because both federal and state courts "have found that customized compilations of data, which may come from both public and private sources, constitute trade secrets," the data at issue was a trade secret under the WUTSA.[236] Without much discussion, the court also found that there was enough evidence to support a finding that the Defendants misappropriated the trade secrets.[237] The court did not devote much separate discussion to determining whether a trade secret existed under the DTSA and whether misappropriation had occurred, as "the [DTSA] defines trade secrets similarly but even more broadly than the UTSA."[238]

Based on these findings, the court concluded that Earthbound was entitled to a TRO and expedited discovery.[239]

Panera LLC v. Nettles

In July 2016, Panera, LLC ("Panera") filed suit in the United States District Court for the Eastern District of Missouri and sought a TRO against Michael Nettles: a former

---

[234] *Id.* at *7.
[235] *Id.*
[236] *Id.* at *9-10 (quoting *United States v. Nosal,* 844 F.3d 1024 (9th Cir. 2016)).
[237] *Id.* at *10.
[238] *Id.*
[239] *Id.* at *11-12.

employee.[240] Nettles was the former Vice President of Architecture in Panera's Information Technology Department, and during his time with Panera was privy to confidential information involving technology and strategy.[241] Nettles signed two Confidentiality and Non-Competition Agreements during his time with Panera.[242] Under the agreements, Nettles was bound to not work for competitors for one year following termination of his employment with Panera.[243] Papa John's was specifically listed as a competitor.[244]

In June 2016, Nettles requested a waiver of his agreement so that he could accept a role with Papa John's.[245] Panera refused.[246] Nonetheless, Nettles opted to resign from his position at Panera and accept a position with Papa John's as Senior Vice President, Chief Information and Digital Officer in July.[247] Panera filed suit, asserting several causes of action, including for violation of the Defend Trade Secrets Act.[248] Panera also moved for a TRO.

The court's analysis focused on the Missouri Uniform Trade Secrets Act ("MUTSA").[249] Under the MUTSA, Panera was "likely to succeed on the merits" because

---

[240] *Panera, LLC v. Nettles*, No. 4:16-cv-1181-JAR, 2016 WL 4124114 (E.D. Mo. Aug. 3, 2016).
[241] *Id.*
[242] *Id.*
[243] *Id.*
[244] *Id.* at *1.
[245] *Id.*
[246] *Id.*
[247] *Id.*
[248] *Id.* at *2.
[249] *Id.* at *2-6.

Nettles had knowledge of trade secrets due to his position at the company.[250] The court also noted that when Nettles left Panera, he returned his laptop to a "factory state" which erased any information that would allow Panera to track who he sent documents to on the laptop.[251] The court found these facts created "a strong inference of irreparable harm."[252] Although Missouri had not formally adopted the inevitable disclosure doctrine, the court found that if Nettles worked for Papa John's, his duties would almost certainly require him to draw upon and use trade secrets to which he was privy at Panera.[253] This further demonstrated irreparable harm.[254] The court thus granted Panera's TRO.[255] It specifically noted that "[a]lthough the court's analysis has focused on Panera's Missouri trade secrets claim, an analysis under the Defend Trade Secrets Act would likely reach a similar conclusion."[256]

CrowdStrike, Inc. v. NSS Labs. Inc.

In February 2017, the United States District Court for the District of Delaware denied a request from CrowdStrike, Inc. ("CrowdStrike, Inc.") for a TRO and preliminary injunction under the DTSA against NSS Labs. Inc. ("NSS").[257] CrowdStrike is a cybersecurity company that developed a software called the Falcon software to

---

[250] *Id.* at *4.
[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] *Id.*
[255] Id. at *6.
[256] *Id.*, n.2.
[257] *CrowdStrike, Inc. v. NSS Labs. Inc.*, No. 17-146-GMS, 2017 WL 588713 (D. Del. Feb. 13, 2017).

provide "threat detection to clients."[258] NSS tests cybersecurity software and tools available in the marketplace to determine how well they stand up to attacks.[259]

In April 2016, CrowdStrike and NSS executed a Private Engagement Agreement whereby NSS was to conduct a private test of CrowdStrike's Falcon cybersecurity platform.[260] CrowdStrike alleged that NSS failed to perform the tests in a way that CrowdStrike deemed accurate and acceptable.[261] In response, NSS conducted additional testing to attempt to remedy the failure CrowdStrike identified.[262] As part of this additional testing, NSS performed a public test of the Falcon software.[263] It is the results of this public test that CrowdStrike sought to enjoin NSS from disclosing during an upcoming technology gathering known as the RSA Conference.[264]

CrowdStrike alleged that NSS misappropriated its trade secrets in violation of the DTSA by using CrowdStrike's confidential information obtained through its private testing of the Falcon software that revealed the methods of threat detection used in the software.[265] The court did not doubt that this information was a trade secret.[266] However, the court found that CrowdStrike did not adequately allege that a misappropriation of said trade secret had occurred or would occur.[267] First, the court did not find that any trade secrets were revealed in NSS's report because NSS conducted

---

[258] *Id.* at *1.
[259] *Id.*
[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] *Id.*
[264] *Id.*
[265] *Id.* at *4.
[266] *Id.*
[267] *Id.*

"black box" testing on the Falcon software and such testing does not disclose the method by which the software detects threats.[268] Moreover, upon review of the report to be presented at the RSA Conference, the court confirmed that NSS did not plan to disclose any trade secrets to the public.[269] Thus, the court found no basis for CrowdStrike's assertion that NSS's disclosures would cause irreparable harm to its reputation.[270] The court went on to consider the balance of hardships, and held that NSS's business would be in jeopardy if it could be restrained from publishing the results of a test every time a customer questioned the methods by which the test was conducted.[271] Thus, upon finding no basis for awarding injunctive relief, the court denied CrowdStrike's requests for a TRO and preliminary injunction.[272]

Trulite Glass & Aluminum Solutions, LLC v. Smith

In October 2016, the United States District Court for the Eastern District of California granted Trulite Glass and Aluminum Solution's ("Trulite") motion for a preliminary injunction against Nathan Witkin and Bryan McNabb.[273] Trulite had filed causes of action for misappropriation of trade secrets by the Defendants in violation of Cal. Civ. Code Section 3426.1 and the DTSA.[274] The alleged trade secret information "consist[ed] of Trulite's customer, pricing, financial, and other sensitive business

---

[268] *Id.*
[269] *Id.*
[270] *Id.*
[271] *Id.* at *5.
[272] *Id.*
[273] *Trulite Glass & Aluminum Sols., LLC v. Smith,* No. 2:16-01798-cv-JAM-CKD, 2016 WL 5858498, at *1 (E.D. Cal. Oct. 6, 2016)
[274] *Id.*

data."[275] The court determined that the information derived independent economic value from not being readily available to others, and that Trulite took reasonable steps to keep the information confidential.[276] The trade secrets were acquired by unlawful means because Witkin sent confidential information from his work to his personal email, and McNabb sent confidential information to his new employer: a Trulite competitor.[277] Both Witkin and McNabb disclosed and used the confidential information illegally acquired from Trulite to compete with the company.[278] As such, the court determined that Trulite was entitled to a preliminary injunction as the defendants had violated the DTSA and California's trade secret law.[279] The court ordered Witkin and McNabb to return all Trulite documents within ten days of the order and to provide written certification to Trulite that the documents were either destroyed or returned to Trulite.[280] Further, the Witkin and McNabb were enjoined for a six month period from indirectly and directly initiating contact with Trulite customers that they were responsible for while employed by Trulite.[281] The court did allow the defendants to accept business from these customers during the period only if they were contacted by the customers first.[282] The court also ordered an independent computer expert to

[275] *Id.*
[276] *Id.*
[277] *Id.*
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] *Id.*
[282] *Id.*

oversee the destruction of documents and other confidential information on Witkin's computer.[283]

Phyllis Schlafly Revocable Trust v. Cori

This action arose in conjunction with two other cases in other jurisdictions.[284] The Phyllis Schlafly Revocable Trust and Missouri Eagle Forum asserted that two employees of the trust misappropriated trade secrets concerning a proprietary database ("the Database"), copied a partial list of the Database, misrepresented themselves as employees of the Eagle Forum, and refused to return passwords.[285] The plaintiffs sought an injunction prohibiting the defendants from using the likeness of Schlafly, using confidential information from the Database, and that the defendants be required to return confidential information.[286] The defendants argued that the intellectual property did not belong to the trust and was already subject to an injunction in another case.[287]

The United States District Court for the Eastern District of Missouri determined that the TRO should be denied because the plaintiffs had not met their burden of establishing a likelihood of success on the merits.[288] The court stated that the elements to prove misappropriation under both the DTSA and Missouri Uniform Trade Secrets

---

[283] *Id.*
[284] *Phyllis Schlafly Revocable Trust v. Cori*, No. 4:16CV01631JAR, 2016 WL 6611133 (E.D. Mo. Nov. 9, 2016).
[285] *Id.* at *2.
[286] *Id.*
[287] *Id.*
[288] *Id.*

Act ("MUTSA") were the same, and consisted of "(1) the existence of a protectable trade secret; (2) misappropriation of those trade secrets by the defendant; and (3) damages."[289] However, the court noted that in order to prove any of those elements, ownership of the trade secret must be established.[290] The ownership of both the Database and Phyllis Schlafly's likeness and image was heavily disputed due to a question regarding the validity of an Assignment of Rights executed by Schlafly.[291] Because of this significant factual dispute over ownership of the alleged trade secrets, the court determined that the plaintiffs had not met their burden of establishing a likelihood of success on the merits of the DTSA claim.[292] As such, the court denied the request for injunctive relief.[293]

Engility Corporation v. Daniels

In December 2016, the United States District Court for the District of Colorado issued a ruling addressing the intersection of the DTSA and Colorado's state law prohibiting noncompete provisions.[294] Engility Corporation ("Engility") brought suit against Charles Daniels and Rutherford "Chip" Surber after they formed a competing company called Deployable Technology Solutions ("DTS").[295] The complaint alleged

[289] *Id.*
[290] *Id.* at *3.
[291] *Id.*
[292] *Id.*
[293] *Id.*
[294] *Engility Corp. v. Daniels*, No. 16-cv-2473-WJM-MEH, 2016 WL 7034976 (D. Colo. Dec. 2, 2016).
[295] *Id.* at *1.

several causes of action, including violations of the DTSA and the Colorado Uniform Trade Secrets Act ("CUTSA").[296]

Engility provided two business programs, the DCCS and MUOS, to military entities.[297] Specifically, Engility provided DCCS to U.S. Northern Command ("USNORTHCOM").[298] Daniels was the Technical Program Manager for DCCS and MUOS and worked closely with USNORTHCOM.[299] Daniels had signed a Confidentiality Agreement while employed with L-3 Communications, which eventually merged with Engility.[300] The Agreement covered L-3's successors, and thus was applicable to Daniels at the time of his resignation from Engility.[301] At issue were materials Engility contended Daniels copied from a company laptop to an external hard drive.[302]

Engility sought an injunction to prevent the Defendants from "disclosing, using, and/or otherwise making publicly available for any purpose any documents they obtained as a result of their employment with Engility . . . destroying, erasing or otherwise making unavailable for further proceedings in this matter, the Materials . . . [and] accepting any award of USNORTHCOM business opportunities obtained by the Defendants since their misappropriation of the materials."[303] Daniels did not contest that the information he obtained was a trade secret under both the DTSA and the

---

[296] *Id.*
[297] *Id.*
[298] *Id.*
[299] *Id.*
[300] *Id.* at *2.
[301] *Id.*
[302] *Id.* at *2-6.
[303] *Id.* at *7.

CUTSA.[304] The court further found that the trade secrets were misappropriated and that the evidence supported enjoining the defendants from disclosing the trade secrets.[305]

The court also addressed whether the defendants could be enjoined from accepting USNORTHCOM business in light of the DTSA provision that "forbids an injunction that would 'conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."[306] In Colorado, noncompete agreements are generally not enforced.[307] As such, the DTSA provision prohibiting an injunction that conflicts with applicable state law was arguably implicated.[308] However, an exception exists under Colorado law for "any contract for the protection of trade secrets."[309] This case did not invoke that exception directly because there was no non-compete agreement at issue.[310] However, the court determined it could enjoin the defendants from accepting USNORTHCOM business because the Colorado statute allowed noncompete agreements if necessary to protect trade secrets.[311] Because the court noted that it could not trust Daniels' representations that he no longer had trade secret information, because his stories about possessing the data changed several times

---

[304] *Id.*
[305] *Id.* at *10.
[306] *Id.* (quoting 18 U.S.C.A. Section 1836(b)(3)(A)(i)(II)).
[307] *Id.*
[308] *Id.*
[309] *Id.* (quoting Colo. Rev. Stat. §8-2-113(2)).
[310] *Id.*
[311] *Id.* at *10.

throughout the proceedings, the court enjoined the defendants from accepting or soliciting USNORTHCOM business for a one year period.[312]

Protection Technologies, Inc. v. Ribler

In March 2017, the United States District Court for the District of Nevada temporarily restrained Kenneth Ribler from disclosing any information he may have taken from his former employer, Protection Technologies ("Protech").[313] Protech brought suit against Ribler for violations of the DTSA and Nevada's codification of the Uniform Trade Secrets Act ("UTSA"), as well as other Nevada common law claims.[314] Protech alleged that Ribler, a regional sales manager for Protech, exported "confidential, proprietary, and trade secret documents and information" from the customer-management system to a private drive and emailed the information to himself.[315] Ribler subsequently deleted the emails from his company account, which Protech claimed was evidence of attempt to conceal his conduct.[316]

The court found that the act of downloading company data immediately following termination, coupled with attempts to hide this act, indicated an intent to disclose or exploit company data, satisfying the first requirement for granting a TRO.[317] Furthermore, the court found that the TRO would not harm any of Ribler's interests,

---

[312] *Id.* at *14.
[313] *Prot. Techs., Inc. v. Ribler*, 3:17-cv-00144-LRH-WGC, 2017 WL 923912 (D. Nev. Mar. 8, 2017).
[314] *Id.* at *2.
[315] *Id.* at *1.
[316] *Id.*
[317] *Id.*

and there was a strong public interest in protecting trade secrets.[318] Finally, the court found that Protech was likely to succeed on the merits of its DTSA and UTSA claims.[319] The court thus granted a TRO ordering that Ribler not destroy or tamper with any of the data or information he downloaded, emailed, or otherwise transmitted to himself or other parties, or solicit business from Protech's customers or assist another person or entity in soliciting such business.[320]

The court did, however, reserve until the preliminary-injunction hearing Protech's request for an expedited discovery order. The court found the expedited discovery sought to be overly extensive and stated that the purpose of a TRO is to prevent evidence destruction, thereby eliminating the need for expedited discovery.[321]

T&S Brass & Bronze Works, Inc. v. Slanina

In May 2017, the United States District Court for the District of South Carolina decided *T&S Brass & Bronze Works,* finding that broad restrictive covenants, including those prohibiting conduct outside of the United States, do not violate a prohibition on restraining employment.[322]

In 2009, James Slanina and his wife, Linda Basinger, started a company called EnviroPure Systems, Inc. ("ESI") to manufacture and sell a food waste disposal system

[318] *Id.*
[319] *Id.*
[320] *Id.* at *3.
[321] *Id.*
[322] *T&S Brass & Bronze Works, Inc. v. Slanina*, No. 6:16-03687-MGL, 2017 WL 1734362 (D.S.C. May 4, 2017).

developed by Slanina for commercial facilities.[323] In 2012, plaintiff T&S Brass and Bronze Works, Inc. ("T&S") created EnviroPure Systems, LLC ("EnviroPure") to acquire ESI.[324] Slanina then became president of EnviroPure.[325] Basinger did not become an employee of EnviroPure, but instead, in February 2015, doing business as Advantagreen, she entered into a National Market Sales Agreement whereby Advantagreen would serve as a sales representative and distributor for EnviroPure.[326] As part of the acquisition, Slanina and Basinger signed Covenant Agreements with T&S prohibiting them from disclosing confidential information, soliciting customers, and competing with the business of T&S.[327] Slanina's non-compete provisions expired two years after the termination of his employment, and Basinger's expired two years after T&S' acquisition of ESI. The confidentiality provisions had no expiration date.[328]

In November 2016, CEO of T&S, Claude Theisen, suspended Slanina's employment.[329] Shortly thereafter, T&S requested an ex parte TRO which was granted by a magistrate judge.[330] T&S also filed a motion for preliminary injunction.[331] A few months later, T&S filed an amended complaint asserting a claim for violation of the DTSA, the South Carolina Trade Secrets Act, the Racketeer Influenced and Corrupt

---

[323] *Id.* at *1.
[324] *Id.*
[325] *Id.*
[326] *Id.* at *2.
[327] *Id.* at *1.
[328] *Id.*
[329] *Id.* at *2.
[330] *Id.*
[331] *Id.*

Organizations Act (RICA), and various common law claims.[332] About a month later, Basinger filed a Motion to Compel Arbitration, asserting that all of T&S's claims against her were subject to mandatory arbitration.[333]

The magistrate judge's grant of the TRO was only a recommendation, and thus the court had to make a de novo determination as to T&S' motion for preliminary injunction.[334] In the first of fourteen objections Slanina offered in opposition to the preliminary injunction, Slanina claimed that the Magistrate Judge improperly granted the initial TRO on an ex parte basis.[335] The court overruled this objection holding that the granting of an initial TRO has no bearing on the propriety of a preliminary injunction.[336] The remaining relevant objections are discussed below.[337]

Slanina, in his third objection, contended that the defendants' disclosure of EnviroPure's financial information to prospective investors was intended to benefit T&S by attracting parties to invest in EnviroPure, the disclosures were accompanied by nondisclosure agreements, and there was no evidence any of the entities to whom Slanina disclosed the confidential information had ever misused it.[338] The court was unpersuaded by Slanina's claims given evidence that Slanina said in an email that he

---

[332] *Id.* at *4.
[333] *Id.*
[334] *Id.* at *8.
[335] *Id.*
[336] *Id.*
[337] *Id.*
[338] *Id.* at *9.

was attempting to "move the company away from the existing management," and evidence that he disclosed T&S trade secrets to third parties without permission.[339]

In their fifth objection, the defendants contended that the magistrate judge's assertion that they harmed T&S by pursuing their own business interests with a company in the U.K. called X-Met, was unsupported.[340] Slanina stated that X-Met had a distributorship agreement with EnviroPure that did not violate EnviroPure's preexisting distributorship agreement with another U.K. company.[341] Thus, defendants maintained they were acting for the benefit of T&S and not in their own personal interests.[342] However, there was abundant evidence that the defendants were pursuing their own interests.[343] For instance, defendants provided the operator of X-Met with EnivroPure's logo and confidential information without informing T&S and while EnviroPure already had a distributor in the U.K.[344]

The court was similarly unpersuaded by the defendants' eighth objection that OMPECO, an Italian company with whom defendants interacted, was not competitive with EnviroPure.[345] The defendants claimed that the magistrate judge found OMPECO was a competitor of EnviroPure solely based on a brochure which showed that it manufactures machines to treat food waste.[346] The court held that it was reasonable for the magistrate judge to rely on the brochure in assuming OMPECO was in the food

---

339 *Id.*
340 *Id.* at *10.
341 *Id.*
342 *Id.*
343 *Id.*
344 *Id.*
345 *Id.* at *11.
346 *Id.*

disposal business because the defendants did not suggest a reason that the court's assumption based on the brochure was unreasonable.[347]

In their ninth objection, the defendants objected to the magistrate judge's conclusion that Slanina greatly diminished his credibility with his representations that his contact with OMPECO was solely to help his wife, Linda Basinger, in negotiations on behalf of her company, Advantagreen.[348] Based on ample evidence that Slanina was misrepresenting his actions to the court, the court agreed with the magistrate judge's conclusion.[349]

In their eleventh objection, the defendants asserted that enjoining them from conducting business with companies outside of the United States is improper because, they alleged, their non-compete was expressly limited to the United States.[350] The court found that it was irrelevant whether the non-compete agreement applies to conduct outside the United States because the DTSA applies to such international conduct when defendants are citizens or permanent resident aliens of the United States or organizations existing under the laws of the United States.[351] Thus, the court held that T&S may enjoin conduct outside the United States under the DTSA.[352]

The defendants' twelfth objection opposed the magistrate judge's recommendation that the defendants be enjoined from "(i) conducting any business with, assisting, consulting with, or communicating about the food disposal industry

---

[347] *Id.*
[348] *Id.*
[349] *Id.*
[350] *Id.* at *12.
[351] *Id.* (citing 18 U.S.C. § 1837).
[352] *Id.*

with . . . X-Met . . .or OMPECO, or any [of their] employees . . . or affiliates, [and] (ii) entering into any employment relationship with any person or entity [both within and outside of the United States] for the purpose of designing, manufacturing, or selling food disposal systems or related products without leave of court."[353] The court held that the injunction was not a blanket prohibition preventing defendants from entering any employment relationships competitive with T&S.[354] Rather, it enjoined the defendants from certain employment with companies that were competitive with T&S, which is permitted by the DTSA.[355]

The thirteenth objection was the only one the court found persuasive.[356] Slanina claimed and the court agreed that enjoining him and the other defendants from "[d]isparaging the plaintiffs . . . in regard to the issues presented in this case" was inappropriate since the defendants had not entered into a non-disparagement agreement with the plaintiffs.[357]

Finally, Basinger's Motion to Compel Arbitration was granted.[358] Thus, the defendants were enjoined pursuant to the preliminary injunction pending arbitration.[359]

Waymo LLC v. Uber Technologies, Inc.

---

[353] *Id.* at *13.
[354] *Id.*
[355] *Id.*
[356] *Id.* at *14.
[357] *Id.*
[358] *Id.* at *15.
[359] *Id.* at *16.

In the highly publicized May 2017 case of *Waymo LLC v. Uber Technologies, Inc.*, the United States District Court for the Northern District of California granted injunctive relief to a company that demonstrated that at least some of the thousands of files taken by a former employee contained misappropriated trade secrets, but denied an injunction in the corresponding patent infringement claim.[360] The parties to this case were competitors in the budding self-driving car industry and each company sought to develop Light Detection and Radar Technology to advance the industry.[361]

In filing for a preliminary injunction on its trade secret misappropriation and patent infringement claims, Waymo LLC ("Waymo") presented compelling evidence that its former engineer Anthony Levandowski downloaded "over 14,000 confidential files from Waymo immediately before leaving his employment there" to spearhead its competitors' efforts to develop self-driving cars.[362] Waymo further demonstrated that Uber Technologies, Inc. ("Uber") planned to acquire Levandowski's own companies and hire Levandowski while he was still employed with Waymo.[363]

In December 2015, Levandowski accessed Waymo's password-protected intranet and used his work laptop to download the files before connecting a portable data transfer device to the laptop.[364] Days later, Levandowski installed a new operating system and wiped his computer clean.[365] In early 2016, Levandowski formed his own

---

[360] *Waymo LLC v. Uber Techs., Inc.*, No. C 17-00939 WHA, 2017 WL 2123560, at *1 (N.D. Cal. May 15, 2017).
[361] *Id.*
[362] *Id.*
[363] *Id.*
[364] *Id.* at *2.
[365] *Id.*

company, Ottomotto, and continued communicating with Uber while employed by Waymo.[366] On January 27, 2016, Levandowski resigned from Waymo without notice.[367] Two additional Waymo employees exported some documents and left the company to join Levandowski's business.[368]

Throughout the following months, Uber obtained legal advice and had a firm prepare a due diligence report of the files Levandowski took from Waymo.[369] Then, in August 2016, Uber bought Levandowski's company and hired Levandowski to head its self-driving car project.[370] Also in the summer of 2016, Waymo grew suspicious of its employees' departing and hired a forensics security engineer who discovered the exported documents.[371]

On March 10, 2017, after filing the action, Waymo sought provisional relief.[372] The court found Waymo's patent theories insufficient to grant provisional relief.[373] In its patent infringement claim, Waymo alleged there was a fundamental common lens design between the companies' systems.[374] However, the court found the system Uber was using at the time of the suit did not use a fundamental common lens design, and that Uber's other system had been abandoned in October 2016 and was never developed

---

[366] *Id.*
[367] *Id.*
[368] *Id.* at *3.
[369] *Id.*
[370] *Id.*
[371] *Id.*
[372] *Id.* at *4.
[373] *Id.* at *6.
[374] *Id.*

as a working prototype.[375] Since the system was defunct, there was no need to enjoin it from operations.[376]

In contrast, the court found that Waymo had met its burden to be granted provisional relief on the misappropriation claim under the DTSA.[377] Despite having doubts about the accuracy of the quantity of Waymo's asserted trade secrets (121 trade secrets were claimed in the pleadings), the court found it likely that at least some information in the 14,000 downloaded files was worthy of trade secret protection and pointed to at least two processes that were trade secrets.[378]

Ultimately, the court concluded that Uber knew or should have known that Levandowski had these thousands of Waymo files, that at least some of them were used in Uber's development efforts, and that at least some of them merited trade secret protection.[379] The court also examined the likely harm in Levandowski possessing these files given that he had hidden behind his Fifth Amendment privilege and that Uber could simply mimic the technologies in the files whilst claiming the system was independently developed.[380] Additionally, the court reasoned that it would be difficult to assign monetary value to the injury suffered by the destruction of these trade secrets.[381] The court found that the public interest was better served by legitimate competition in a

---

375 *Id.*
376 *Id.*
377 *Id.* at *7.
378 *Id.* at *8.
379 *Id.* at *10.
380 *Id.* at *11.
381 *Id.*

highly innovative field driven by trade secrets.[382] Also, despite Uber's argument that an injunction would thwart the company's self-driving technology developments, the injunction did not prevent Uber from continuing to develop its own technology.[383] The "ever-present danger" of Levandowski's possession of at least 14,000 confidential files containing trade secrets made injunctive relief particularly appropriate.[384] However, the court emphasized that the circumstances of this case demanded "narrow and carefully-tailored relief."[385] The court declined to enjoin Uber from using all 121 alleged trade secrets and even refused to enjoin them from using those specific trade secrets the court believed had merit.[386] Thus, the injunction primarily prohibited Levandowski from working on Uber's system, which minimized the hardship on the company and protected Waymo from further disclosure and use of its information.[387]

GTAT Corporation v. Fero

In May 2017, the United States District Court for the District of Montana found that a trade secret misappropriation claim was not sufficiently alleged as to warrant a preliminary injunction.[388] GTAT Corporation ("GTAT") is a technology company that offers technology and equipment utilized in the polysilicon process, a raw material used

[382] *Id.* at *12.
[383] *Id.*
[384] *Id.* at *11.
[385] *Id.* at *12.
[386] *Id.*
[387] *Id.* at *13.
[388] *GTAT Corp. v. Fero*, CV 17-55-M-DWM, 2017 WL 2303973, at *1 (D. Mont. May 25, 2017).

primarily in the solar industry.[389] The polysilicon portion of its business was based out of Missoula, Montana.[390] Chad Fero worked as an engineer for GTAT and was involved with the research and development of GTAT's polysilicon technology.[391] While general processes for producing polysilicon are generally known, GTAT had invested almost a decade of research and development to create its own proprietary polysilicon process.[392] GTAT provided clients with blueprints of equipment and works with fabricators around the world to produce the equipment.[393] GTAT treated all of the information, materials, and equipment surrounding its polysilicon process as confidential and proprietary, and requires sales material be labeled accordingly.[394]

At the time Fero was hired, he signed a Confidentiality Agreement, agreeing to keep technical GTAT information confidential, even after his employment ended.[395] In September 2016, Fero left his employment with GTAT.[396] Shortly thereafter, he entered into a consulting agreement with GTAT until January 2017.[397] Since leaving GTAT, Fero operated a polysilicon technology business under the name "Ferosilicon."[398] Fero was not bound by a non-compete covenant, but GTAT alleged that Fero could not have "independently developed the chemical processes, equipment designs, and engineering

---

[389] *Id.*
[390] *Id.*
[391] *Id.*
[392] *Id.*
[393] *Id.*
[394] *Id.*
[395] *Id.* at *2.
[396] *Id.*
[397] *Id.*
[398] *Id.*

specifications" he offered without using any of GTAT's trade secret information.[399] In support of this allegation, GTAT presented evidence that when it arrived to close a $10 million deal with a Chinese company that had been in development since October 2015, the Chinese company informed GTAT that it could no longer proceed at that price because Fero had offered "essentially the same technology and equipment at a much lower price."[400] As a result, GTAT was not able to make a sale of their entire technology and equipment package.[401]

GTAT brought claims against Fero for trade secret misappropriation under the DTSA and state law, as well as other common law claims.[402] In the instant case, the issue before the court was whether GTAT had shown that Fero was likely to use its trade secrets and that a preliminary injunction was warranted while the case progressed.[403] The court found that it was faced with the difficult task of determining where GTAT's confidential information and trade secrets ended and where Fero's experience and ability began.[404] GTAT presented evidence that it took measures to protect its trade secrets but testimony revealed that some of the security measures GTAT had in place may not have been regularly enforced including the fact that employees used DropBox and USBs despite a GTAT policy against it and Fero was not given an exit interview during which GTAT recovered Fero's laptop.[405]

---

399 *Id.*
400 *Id.*
401 *Id.*
402 *Id.*
403 *Id.*
404 *Id.* at *3.
405 *Id.* at *4.

The court found that even assuming GTAT had taken reasonable measures to protect its trade secrets, it had not demonstrated a likelihood of success as to the remaining requirements of its claim.[406] GTAT had to show that its trade secrets derive independent economic value by not being widely known.[407] GTAT identified trade secrets that fell into three general "buckets": (1) materials of construction, (2) internal components, and (3) specific processes involved in the polysilicon process.[408] The court found that many of the over sixty trade secrets GTAT identified may either be known by others in the field, disclosed in patent applications, or previously disclosed by GTAT itself.[409]

The court found that even assuming GTAT had identified its trade secrets as not being generally known, GTAT had failed to make a preliminary showing as to misappropriation.[410] It found that although GTAT was able to create suspicion as to what Fero could have uploaded onto DropBox or taken on his laptop, it failed to show that any information was actually taken by either means.[411] Additionally, no exit interview was conducted in which GTAT requested return of the laptop and there were disputes as to the enforcement of the no-DropBox policy.[412] GTAT argued that Fero's business offerings could not have been developed without using GTAT's proprietary technology, but Fero testified that he had invested over $70,000 in his company, set up

---

406 *Id.*
407 *Id.*
408 *Id.*
409 *Id.*
410 *Id.*
411 *Id.*
412 *Id.*

his own lab, relied extensively on publicly-available articles, and was not offering the same type of product as GTAT.[413] The court held that although further discovery may show that Fero's business was not proceeding with organic information, the existing record did not persuasively show otherwise.[414] The court thus found that GTAT failed to establish a sufficient threat of misappropriation.[415]

North American Deer Registry, Inc. v. DNA Solutions, Inc.

In June 2017, the United States District Court for the Eastern District of Texas granted a preliminary injunction under the DTSA.[416] In 2007, two deer breeder associations joined forces to create the North American Deer Registry, Inc. ("NADR").[417] NADR hired DNA Solutions, Inc. ("DNAS") to perform DNA analysis on its deer and host its database of deer lineages.[418] As part of this business arrangement, DNAS would perform most of NADR's client outreach, and would preserve the confidentiality of NADR's information and return such information upon termination of DNAS's services.[419] In 2014, the parties revised their agreement so that upon termination of the agreement on January 1, 2017, NADR would retain ownership of all biological materials, genetic information, genotype analysis data, membership directory, and any other

---

[413] *Id.* at *5.
[414] *Id.*
[415] *Id.*
[416] *N. Am. Deer Registry, Inc. v. DNA Sols., Inc.*, No. 4:17-CV-00062, 2017 WL 2402579, at *1 (E.D. Tex. June 2, 2017).
[417] *Id.*
[418] *Id.*
[419] *Id.*

information provided by NADR, and DNAS would return all information provided by NADR.[420]

On January 27, 2017, NADR filed a complaint alleging misappropriation of trade secrets under the DTSA, among other claims.[421] NADR moved for a preliminary injunction, and the court found in favor of NADR, holding that DNAS misappropriated NADR's trade secrets when it did not return the information following the termination of their business relationship as stipulated in the agreement.[422] DNAS argued that it did return the information while also retaining a copy as a part of its "database."[423] The court, however, was not persuaded by this strained reading of the word "return."[424] The court held that the "Return of Information" provision of the agreement required a complete return of information, without any retention.[425] In addition to this violation, DNAS also admitted to contacting certain NADR customers to offer DNAS as an alternative service to NADR.[426] DNAS obtained this information under a duty to maintain its secrecy, but then used it without permission.[427]

Having found that DNAS likely misappropriated NADR's trade secrets in multiple ways, the court found that NADR had a substantial likelihood of prevailing on its trade secret claim.[428] The court also found that the balance of hardships favored

---

[420] *Id.*
[421] *Id.*
[422] *Id.* at *8.
[423] *Id.*
[424] *Id.*
[425] *Id.*
[426] *Id.*
[427] *Id.*
[428] *Id.* at *9.

NADR because if DNAS was allowed to operate with NADR's trade secrets, NADR would lose its advantage because once its trade secrets are used by a competitor, they become public, and lose their secret status.[429] Accordingly, the court granted NADR's application for preliminary injunction under the DTSA enjoining DNAS from the use and disclosure of NADR's trade secrets until a final decision is ordered in the case.[430]

Compulife Software, Inc. v. Newman

In June 2017, the United States District Court for the Southern District of Florida denied preliminary injunctive relief for failure to establish irreparable injury.[431] Compulife Software, Inc. ("Compulife") creates software products that allow individuals to compare term life insurance products and rates.[432] Compulife's software included HTML code that allowed an individual to visit a website and enter certain information—age, sex, amount of insurance desired—in order to request life insurance quotes.[433] The HTML submitted that information to the host-based software, which looks up the rates and product information for various insurance companies, calculates premiums, and produces quotes that are ultimately displayed on the website.[434] The purpose of the HTML code was to communicate with the host-based software containing specific

[429] *Id.* at *10.
[430] *Id.*
[431] *Compulife Software, Inc. v. Newman*, NO. 9:16-CV-81942-ROSENBERG/BRANNON, 2017 WL 2537357, at *1 (S.D. Fla. June 12, 2017).
[432] *Id.*
[433] *Id.*
[434] *Id.*

variables created by Compulife which communicate with the host-based software.[435] The server on which the host-based software resides also housed Compulife's database of digital information about the products and rates.[436] Compulife obtained this information from insurance companies, but does not own this information.[437] In fact, the information was public and provided to other companies offering competing software.[438] Compulife compiled the information into an encrypted database to prevent reverse engineering.[439] Compulife contended that the way it stored its information was a trade secret, claiming that its quotes are unique because of the way information is stored on its database and based on the procedures it used to calculate premiums.[440] Compulife had registered its software with the United States Copyright Office.[441]

The National Association of Accredited Insurance Professionals ("NAAIP") maintains a website which offers a life insurance quote engine as does the website www.beyondquotes.com ("BeyondQuotes").[442] Compulife maintains that Moses Newman, Aaron Levy, David Rutstein, and Binyomin Rutstein controlled or contributed to the operation of both NAAIP and BeyondQuotes.

In April 2015, Compulife discovered that NAAIP and BeyondQuotes had copied Compulife's HTML code onto their websites and had accessed Compulife's database of

---

435 *Id.*
436 *Id.* at *2.
437 *Id.*
438 *Id.*
439 *Id.*
440 *Id.*
441 *Id.*
442 *Id.*

information.[443] None of the Defendants had Compulife's permission to access Compulife's database of information or copy its HTML code.[444] After learning of their use, Compulife disabled access and both the NAAIP and BeyondQuotes websites ceased producing life insurance quotes.[445]

Compulife filed suit against the Defendants for misappropriation under the DTSA, and other federal and state law claims.[446] Subsequent to the filing of the lawsuit, Compulife discovered NAAIP and BeyondQuotes were still using Compulife's information.[447] Despite discovering this use in September 2016, Compulife waited nearly three months before filing a motion for preliminary injunction and did not turn off NAAIP and BeyondQuotes' access to the information.[448]

The court denied Compulife's motion for a preliminary injunction for failure to show it would suffer irreparable injury unless the injunction issues.[449] Compulife presented evidence of injuries, including the cost of measures take to stop further misappropriation and loss of business and revenue.[450] Additionally, while a loss of customers and goodwill is considered an irreparable injury, Compulife presented no evidence that it lost any customers to NAAIP or Beyondquotes.[451] Finally, the court found that Compulife delayed in seeking a preliminary injunction, militating against a

---

[443] *Id.* at *3.
[444] *Id.*
[445] *Id.*
[446] *Id.*
[447] *Id.* at *3-4.
[448] *Id.*
[449] *Id.* at *6.
[450] *Id.*
[451] *Id.* at *7.

finding of irreparable harm. For these reasons, the court concluded that Compulife would not suffer irreparable harm in the absence of an injunction and denied the motion.

Art & Cook, Inc. v. Haber

In October 2017, the United States District Court for the Eastern District of New York district court denied a preliminary injunction to a cookware company in a suit against its former employee because it found the company had not demonstrated likelihood of success on the merits of its trade secret misappropriation claim.[452]

Art & Cook, Inc. ("Art") filed suit against Abraham Haber for DTSA violations as well as common law claims.[453] On March 23, 2017, Art also sought a TRO and preliminary injunction to prevent Haber from using or disclosing Art's trade secrets, selling or buying cookware with any of Art's contacts, using or disclosing any information developed by Haber while employed with Art, and using a mark for commercial purposes.[454] Following a hearing, the district court entered a TRO.[455] The court held an evidentiary hearing for the preliminary injunction on April 7, 2017 and denied the motion.[456]

Art is a cookware company that sells products to large retailers.[457] In 2012, Haber began working for Art as a salesperson.[458] During his employment, Haber was asked to

---

[452] *Art & Cook, Inc. v. Haber*, 17-cv-1634 (LDH) (CLP), 2017 WL 4443549 (E.D.N.Y. Oct. 3, 2017).
[453] *Id.* at *1
[454] *Id.*
[455] *Id.*
[456] *Id.*
[457] *Id.*

sign an employee handbook and nondisclosure agreement, but he refused to do so.[459] Art inspected Haber's computer while he was still employed by the company.[460] Art's search revealed that Haber had emailed documents to his personal email account.[461] These documents included a spreadsheet with buyer contacts at seventy-two companies and another with "logos, branding/marketing strategies, target customer lists, and sales projections for an anticipated line of cleaning supplies called 'Gripps.'"[462] Haber also allegedly sent a PowerPoint presentation with a marketing business plan for Gripps.[463] Haber's employment was terminated on January 13, 2017.[464] Art alleged that following his termination, Haber contacted one of Art's suppliers and requested supplies similar to those sold to Art.[465]

In examining likelihood of success on the merits, the court found that the contacts from the spreadsheet were generally known and therefore not trade secrets.[466] The design and marketing strategies, on the other hand, were "the sort of business information that the DTSA was designed to protect."[467] However, in addition to showing that information derives independent economic value from not being generally known, to show likelihood of success on the merits, the moving party must also show it took

---

458 *Id.*
459 *Id.*
460 *Id.* at *2.
461 *Id.*
462 *Id.*
463 *Id.*
464 *Id.* at *1.
465 *Id.* at *2.
466 *Id.* at *3.
467 *Id.*

reasonable measures to keep the information secret.[468] Art presented some evidence that Haber was told about confidentiality several times and that he was asked to sign a nondisclosure agreement.[469] The court was unpersuaded by these efforts, finding that Art did not even attempt to get Haber to sign a confidentiality agreement until three years into employment and that his access to confidential information was in no way limited following his refusal to sign the agreement.[470] Despite taking other measures to protect the information, including using password protections, the court found Art had not significantly safeguarded its information and therefore was unlikely to succeed on the merits at trial.[471] Because the customer contacts were not trade secrets and the design and marketing strategies had not been protected enough to warrant trade secret classification, the court denied Art's motion for preliminary injunction under the DTSA.[472]

Sapienza v. Trahan

The United States District Court for the Western District of Louisiana also examined likelihood of success on the merits in a motion for preliminary injunction stemming from a claim under the DTSA.[473]

---

[468] *Id.*
[469] *Id.*
[470] *Id.*
[471] *Id.*
[472] *Id.* at *4.
[473] *Sapienza v. Trahan,* NO. 16-CV-01701, 2017 WL 6012658 (W.D. La. Oct. 23, 2017), report and recommendation adopted, NO. 16-1701, 2017 WL 6008076 (W.D. La. Dec. 4, 2017).

In October 2015, Richard Sapienza was a consultant with EnerSciences Holdings, LLC ("EnerSciences"): a company owned by Ben Davis and David Trahan.[474] Sapienza assisted in development of a low temperature gel breaker for another company called Chem Rock.[475] When EnerSciences shut down, Sapienza and the owners wanted to keep the research team intact and replicate the business model for a new company.[476] The three created a new company, Advanced Applied Research, LLC ("AAR"), and relied on Rapid Specialty Products ("Rapid Specialty") to sell and manufacture AAR's technologies.[477] EnerSciences was shut down in October 2015 and the research team began working for Rapid Specialty with the intention of working for AAR when the company was formed.[478]

AAR was formed in late October 2015.[479] The Articles of Organization and other documents relating to AAR were unclear as to who the company's members were.[480] Nonetheless, Sapienza, Trahan, and Davis made contributions in exchange for a one-third membership interest in AAR.[481] Although Rapid Specialty was supposed to sell AAR's products, a new company ("Chem Advances") was formed to sell AAR's

474 *Id.* at *1.
475 *Id.*
476 *Id.*
477 *Id.*
478 *Id.*
479 *Id.* at *2.
480 *Id.*
481 *Id.*

products.[482] Sapienza was not a member of Chem Advances, but both Trahan and Davis were.[483]

A business opportunity arose with a distributor of chemical products and services that had previously had a distribution agreement with Rapid Specialty.[484] Discussions began with that company through AAR and Chem Advances.[485] Chem Advances also began to pursue other business opportunities around that time.[486] The research team from EnerSciences continued developing technologies that were essential to these deals.[487] Sapienza brought this action to enjoin Davis and Trahan from misappropriating and misusing AAR's trade secrets by disclosing them to potential customers.[488]

Sapienza contended that trade secrets were misappropriated by Trahan and Davis through improper means "because they breached their fiduciary duties to AAR by forming Chem Advances" rather than handling distribution and sales efforts through AAR directly.[489] Furthermore, Sapienza alleged misappropriation because Chem Advances manufactured and sold the trade secrets to third parties.[490]

---

[482] *Id.*
[483] *Id.*
[484] *Id.* at *3.
[485] *Id.*
[486] *Id.*
[487] *Id.*
[488] *Id.* at *5.
[489] *Id.* at *8.
[490] *Id.*

The court held that the DTSA "does not contemplate a breach of a fiduciary duty" as an improper means that would qualify as misappropriating a trade secret.[491] Specifically, the court did not believe that forming a separate company in which Sapienza did not have an interest would be "improper means" under the DTSA.[492] Furthermore, the court reasoned that there was no evidence of "theft, bribery, misrepresentation, or an inducement of a breach of duty to maintain secrecy to acquire AAR's trade secrets."[493] Because the individuals always intended for another entity to manufacture and sell the products developed by the research team, the court found that the use of Chem Advances—rather than AAR—was aligned with that intent.[494] Although unfortunate for Sapienza that the entity selling its products was not one in which Sapienza had a membership interest, the court found that Davis and Trahan's breach of fiduciary duty as members of AAR could not be considered misappropriation of AAR's trade secrets.[495] Because this burden was not met, the court found no likelihood of success on the merits and denied Sapienza's injunction.[496]

First Western Capital Management Co. v. Malamed

The Tenth Circuit Court of Appeals addressed the critical issue of whether a plaintiff seeking injunctive relief under the DTSA must still meet the prerequisites for injunctive relief under F.R.C.P. 65. First Western Capital Management ("First

[491] *Id.*
[492] *Id.*
[493] *Id.*
[494] *Id.*
[495] *Id.* at *9.
[496] *Id.* at *10.

Western") sought a preliminary injunction in the district court against its former employee Kenneth Malamed.[497] Malamed sold his investment firm to First Western in 2008 and was employed by First Western from that time.[498] In early 2016, First Western began considering a sale of the business, which Malamed opposed.[499] Malamed then had his assistant make copies of his client book with nearly 5,000 contacts in addition to financial and pricing information.[500] On September 1, 2016, First Western fired Malamed.[501] On the same day, First Western served Malamed with a federal court complaint filed a month earlier alleging misappropriation of trade secrets under the DTSA, among other claims.[502] The company also sought injunctive relief to prevent solicitation of First Western's clients.[503]

The district court issued the injunction, which prevented Malamed from soliciting or accepting business from any First Western client.[504] However, the court excused First Western from one of the four requirements to obtain injunctive relief: a showing of irreparable harm.[505] The court reasoned that because the DTSA provides for injunctive relief to prevent misuse of trade secrets and because Malamed was misusing or threatening to misuse First Western's trade secrets, there was a presumption of

---

[497] *First W. Capital Mgmt. Co. v. Malamed,* 874 F.3d 1136, 1139 (10th Cir. 2017).
[498] *Id.*
[499] *Id.*
[500] *Id.*
[501] *Id.*
[502] *Id.*
[503] *Id.*
[504] *Id.*
[505] *Id.*

irreparable harm.[506] The district court nonetheless noted that without this presumption, the injunction would be improper because money damages were readily ascertainable and could have made First Western whole.[507] The court relied on an earlier Tenth Circuit case, *Star Fuel Marts, LLC v. Sam's East, Inc.*, in which the court detailed narrow circumstances where a presumption of irreparable injury may apply.[508]

However, just weeks after the district court's decision, the Tenth Circuit Court of Appeals clarified that irreparable harm may only be presumed where a statute *mandates* rather than permits injunctive relief.[509] Because the DTSA authorizes but does not require injunctive relief, the party seeking injunctive relief must prove each element, including irreparable harm.[510] In light of the *Fish* decision, the Tenth Circuit reversed the district court's grant of the injunction.

Broker Genius, Inc. v. Zalta

In December 2017, the United States District Court for the Southern District of New York denied a TRO after finding that Broker Genius, Inc. ("Broker Genius") was unlikely to succeed on the merits of its DTSA claim because it failed to take reasonable measures to protect its alleged trade secrets.[511]

---

[506] *Id.* at 1140.
[507] *Id.*
[508] *Id.*
[509] *Fish v. Kobach,* 840 F.3d 7120 (10th Cir. 2016).
[510] *First W. Capital Mgmt. Co.*, 874 F.3d at 1142-43.
[511] *Broker Genius, Inc. v. Zalta,* 280 F. Supp. 3d 495 (S.D.N.Y. 2017).

Broker Genius—a software development company for the ticket broker industry—sued former licensees Nathan Zalta and Michael Shamah and their company.[512] Broker Genius alleged that Zalta and Shamah used their access to Broker Genius's AutoPricer v.3 software to obtain information to aid in creating a competitor product, TickPricer.[513] After filing suit, Broker Genius sought to preliminarily enjoin Zalta, Shamah, and their company from using the newly developed TickPricer or making the software available to any third party.[514]

Broker Genius alleged that it had expended serious money and other resources to develop its software by developing trade secrets that encompassed the "core functionalities and user interface of the AutoPricer software."[515] Although the court agreed with Zalta and Shamah that Broker Genius had failed to describe certain software components with sufficient specificity to determine whether they warranted trade secret protection, the court did find three types of information that may be eligible for trade secret protection: "software architecture, UX/UI, and specific solutions to addressing the scalability problems in an automatic ticket pricing software."[516] The court nonetheless expressed some doubt regarding the extent to which this information was known outside the business.[517]

The court found that even if those three categories of information were not general knowledge in the industry, they are still not entitled to trade secret protection

---

[512] *Id.* at 498.
[513] *Id.*
[514] *Id.*
[515] *Id.* at 514.
[516] *Id.* at 515.
[517] *Id.* at 516.

unless Broker Genius took reasonable measures to protect their secrecy.[518] The court noted the particular importance in this case for Broker Genius to demonstrate reasonable measures of secrecy because "the UX/UI of AutoPricer v.3 is made readily apparent to every single user of the software."[519]

The court found that Broker Genius had taken some measures to protect its information.[520] For example, Broker Genius did not advertise AutoPricer v.3 on the company website or in promotional videos.[521] Additionally, the software was only accessible via password.[522] Broker Genius employees were also required to sign both non-disclosure agreements and employee handbooks referencing the duty to keep information confidential.[523]

However, the court also found that Broker Genius regularly disclosed information to its customers without notifying them of the information's confidential nature or requiring them to sign any type of confidentiality agreement.[524] Broker Genius had also disclosed the alleged trade secrets in a published patent or patent application, which extinguishes all trade secret protection unless the information's owner can successfully demonstrate that the trade secret exceeds the scope of the information disclosed in the patent process.[525] The court did believe Broker Genius had met this burden, reasoning that the patent application did not disclose each claimed secret of the software's features

[518] *Id.* at 517.
[519] *Id.*
[520] *Id.*
[521] *Id.*
[522] *Id.*
[523] *Id.*
[524] *Id.*
[525] *Id.*

and published screenshots of an AutoPricer v.3 predecessor did not include all architecture, scalability solutions, or the entire UX/UI.[526] The court also found that product demonstrations to new customers—lasting between three and eight minutes—could not possibly have disclosed all of Broker's Genius alleged trade secret information.[527]

Nonetheless, the court found that Broker Genius's public disclosures of the software indicated that "Broker Genius did not consider AutoPricer v.3's software architecture or user interface to be trade secrets prior to initiating this litigation."[528] In fact, the court noted that Broker Genius had seemingly opted to protect its information through patent law as opposed to trade secret law.[529] Also, Broker Genius's sales representatives did not follow a script when demonstrating the software to potential clients, which the court believed demonstrated that Broker Genius did not believe any particular information to be confidential.[530]

Ultimately, however, the fatal blow to Broker Genius's argument that it took reasonable measures to keep its information secret was the fact that customers were granted unfettered access, including use of "the software itself, as well as extensive training sessions, user manuals, explanatory videos, and feature update emails that explain how the software works and how to take advantage of each of its

[526] *Id.* at 518.
[527] *Id.* at 519.
[528] *Id.*
[529] *Id.*
[530] *Id.* at 520.

functionalities."[531] The court found that it was through these resources that Zalta and Shamah were able to duplicate much of the software.[532] Furthermore, Broker Genius's total failure to make any oral representations or mark any specific material as confidential led the court to find that reasonable measures to protect secrecy were not taken.[533] Importantly, Broker Genius's argument that the Terms of Use licensees had to accept in order to use the software did classify some information as confidential was unpersuasive because it was not sufficiently obvious.[534] Therefore, Broker Genius's motion for preliminary injunction was denied.

Digital Mentor, Inc. v. Ovivo USA, LLC

Yet another motion for preliminary injunction under a DTSA claim was denied by a the United States District Court for the Western District of Seattle in February 2018 based on the court's finding that the plaintiff had not met its burden to establish the information in dispute contained trade secrets.[535] Digital Mentor, Inc. ("Digital") is an engineering consulting service that developed a waste and wastewater industry mobile computing system.[536] Ovivo USA, LLC ("Ovivo") is a provider of water and wastewater treatment facility equipment.[537] Digital licensed its system to Ovivo in March 2014, and

---

[531] *Id.*
[532] *Id.*
[533] *Id.* at 521.
[534] *Id.*
[535] *Digital Mentor, Inc. v. Ovivo USA, LLC,* No. C17-1935-RAJ, 2018 WL 993944, at *1 (W.D. Wash. Feb. 21, 2018).
[536] *Id.*
[537] *Id.*

Ovivo granted Digital a limited license to its company documents.[538] The parties also executed a non-disclosure agreement.[539] Digital alleged that Ovivo developed a product that was virtually identical in appearance, design, and functionality to its own mobile computing system and filed this action.[540]

Digital argued that Ovivo had misappropriated its trade secrets in violation of the DTSA.[541] However, in arguing the existence of trade secrets, Digital simply stated that its system as "the first mobile digital software system that provided intuitive, interactive and comprehensive access to maintenance, troubleshooting and support information relating to equipment and assets within a water and wastewater treatment facility or plant."[542] The court held that Digital did not indicate with any specificity why its information would qualify as a trade secret under the DTSA.[543] A preliminary injunction was therefore not warranted given that Digital had not shown it was likely to succeed on the merits.[544]

Allstate Insurance Co. v. Rote

In August 2016, the United States District Court for the District of Oregon granted a modified preliminary injunction to Allstate Insurance Company ("Allstate") based in part on the DTSA, as well as the Oregon Uniform Trade Secrets Act

---

[538] *Id.*
[539] *Id.*
[540] *Id.* at *3.
[541] *Id.* at *2.
[542] *Id.*
[543] *Id.*
[544] *Id.*

("OUTSA").[545] Tanya Rote was a former Exclusive Allstate Agent.[546] During her employment with Allstate, she had access to Allstate's confidential information that included "customers' contact information, the type and value of policies carried by those customers, and the location and description of assets insured through Allstate."[547] The parties had executed an "Exclusive Agency Agreement," which provided that upon termination of the Agreement, Rote was required to "immediately return all property belonging to the Company, or dispose of it in such a manner as the Company specifies.'"[548] Rote was also bound by a noncompete for one year after the termination of the agreement.[549]

After her employment ended, Rote retained Allstate's confidential information and sold competing products from her former Allstate agency location.[550] She also solicited business from Allstate customers using confidential information she obtained while employed with Allstate.[551]

Allstate filed suit, asserting—among others—claims for trade secret misappropriation.[552] The court cited *Henry Schein, Inc. v. Cook* in its ruling on Allstate's request for injunctive relief, stating that "customer information such as sales

---

[545] *Allstate Ins. Co. v. Rote*, No. 3:16-cv-01432-HZ, 2016 WL 4191015 (D. Or. Aug. 7, 2016).
[546] *Id.*
[547] *Id.*
[548] *Id.*
[549] *Id.* at *1-2.
[550] *Id.* at *2.
[551] *Id.*
[552] *Id.* at *3.

history and customer needs and preferences constitute trade secrets."[553] The court then briefly noted that under both the DTSA and the OUTSA, "[injunctions can be issued] to provide for the sanctity of trade secrets."[554]

The court granted an injunction in Allstate's favor which "require[d] Rote to immediately return all confidential information to Allstate and refrain from using or disclosing such information."[555] Notably, the alleged misappropriation took place prior to the enactment of the DTSA, but the court did not address that issue in its opinion.[556]

Cases Discussing Pleading Requirements under the DTSA

Because the DTSA is federal law, pleadings alleging DTSA violations must meet the pleadings requirements under the Federal Rules of Civil Procedure. Courts have attempted to strike a balance between the need for specificity in pleadings with the plaintiff's interest in protecting alleged trade secrets from further public disclosure.

Aggreko, LLC v. Barreto, LLC

In March 2017, the United States District Court for the District of North Dakota denied a motion to dismiss a complaint alleging misappropriation of trade secrets in violation of the DTSA.[557] Plaintiff, Aggreko, LLC, ("Aggreko"), and Defendant, Elite

---

[553] *Id.* (quoting *Henry Schein, Inc. v. Cook*, 191 F. Supp. 3d 1072, 1077 (N.D. Cal. 2016)).
[554] *Id.*
[555] *Id.* at *7.
[556] *Id.*
[557] *Aggreko, LLC v. Barreto, LLC*, No. 1:16-cv-353, 2017 WL 963170 (D.N.D. Mar. 13, 2017).

Power, LLC ("Elite Power"), were both in the business of renting generators to customers in North Dakota.[558] In 2014, Elite Power hired Guillermo Barreto, the former Business Development Manager for Aggreko.[559] In his capacity at Aggreko, Barreto had access to Aggreko's confidential information and trade secrets.[560] After giving his notice of resignation, Barreto began downloading Aggreko's trade secrets and confidential information from their internal computer.[561] Subsequently, Barreto used Aggreko's confidential and proprietary information and trade secrets to win business away from Aggreko on behalf of Elite Power.[562]

Elite Power filed a motion to dismiss Aggreko's claims alleging that Aggreko had not pled its misappropriation claims, including its DTSA claim, with sufficient particularity.[563] The court denied the motion to dismiss holding that "[a]ll that is required at this stage of the proceedings is an allegation that Barreto misappropriated Aggreko's trade secrets sufficient to put the defense on notice as to the nature of the claim."[564] It was undisputed that Barreto downloaded information from Aggreko's network onto his personal computer.[565] The court held that given this undisputed allegation, and Aggreko's specific description of its trade secrets as including operations, customers, business proposals, pricing strategy, client preferences and history, and

---

[558] *Id.* at *1.
[559] *Id.*
[560] *Id.*
[561] *Id.*
[562] *Id.* at *2.
[563] *Id.*
[564] *Id.*
[565] *Id.*

proprietary pricing models, Aggreko's misappropriation of trade secrets claims were plausible and not subject to dismissal under Rule 12(b)(6).[566]

Chubb INA Holdings, Inc. v. Chang

In February 2017, the United States District Court for the District of New Jersey denied a motion to dismiss a DTSA claim.[567] Plaintiff, Chubb INA Holdings, Inc. ("Chubb") was a competitor of defendants, Endurance Services, Endurance Holdings, and Endurance Assurance (collectively, "Endurance") in the business of property and casualty insurance.[568] Michael Chang worked for Chubb for over nineteen years before joining Endurance.[569] Chubb alleged that Chang willfully and maliciously targeted and solicited twelve of Chubb's employees for employment at Endurance.[570] Chubb further alleged that Chang and Endurance used Chubb's confidential information to identify specific employees and present them with employment offers at Endurance.[571]

Chubb alleged that Chang and several of the employees he poached had access to and removed confidential information from Chubb's computer systems, which included information regarding the client's key contact persons, its pricing and discounting preferences and tolerances, insurance policies, insureds, pending projects and proposals, claims experience and handling practices, sales and marketing strategies, revenues,

---

[566] *Id.*
[567] *Chubb INA Holdings Inc. v. Chang*, No. 16-2354-BRM-DEA, 2017 WL 499682 (D.N.J. Feb. 7, 2017).
[568] *Id.* at *1.
[569] *Id.*
[570] *Id.*
[571] *Id.*

compensation, personal information and other non-public business information.[572] Chubb further provided that "access to [the] Confidential Information…[was] strictly limited to Chubb employees" and could be retrieved only through use of a password assigned to employees.[573] In addition, Chubb had numerous internal rules and regulations—which Chang violated—that prohibited the forwarding of emails containing confidential information to personal email accounts, among other things.[574]

The defendants argued that Chubb's allegations were insufficient to state a claim under the DTSA because their alleged acquisition of Chubb's confidential information all occurred prior to the May 11, 2016 effective date of the DTSA.[575] Defendants added that mere "retention" of the confidential information after the effective date, without its "use" or "disclosure," is not an actionable misappropriation under the DTSA.[576] Finally, defendants argued that Chubb alleged a purported inevitable disclosure, which is not actionable under the DTSA.[577]

The court disagreed with defendants' arguments and denied the motion to dismiss.[578] In their complaint and amended complaint, the Chubb set forth factual allegations supporting an inference that defendants did, in fact, use the confidential information they had acquired.[579] Chubb further alleged that Chang retained large volumes of documents containing confidential information after May 11, 2016, with the

---

[572] *Id.* at *2.
[573] *Id.* at *2.
[574] *Id.*
[575] *Id* at *9.
[576] *Id.*
[577] *Id.*
[578] *Id.*
[579] *Id.*

intent to disclose and/or use it to Endurance's benefit in the future.[580] The court found that the Chubb had alleged "more than the mere possibility of misconduct," and that Chubb "need not make out specific allegations as to exactly how defendants used or disclosed plaintiff[s'] trade secrets."[581] Therefore, accepting as true Chubb's allegations, the court denied defendants' motion to dismiss the DTSA claim.[582]

Raben Tire Co., LLC v. McFarland

In February 2017, the United States District Court for the Western District of Kentucky granted a motion to dismiss claims brought under the DTSA.[583] Plaintiff, Raben Tire Co., LLC ("Raben Tire Co.") filed an action against two of its former employees, Dennis R. McFarland and Christopher Bates and their new employer, CBA Tire Inc. and Antioch Tire, Inc. ("Tredroc Tire").[584] The complaint alleged misappropriation of trade secrets under the DTSA and the Kentucky Uniform Trade Secrets Act (KUTSA), along with common law claims.[585] McFarland, Bates, and Tredroc

[580] *Id.*
[581] *Id.* (quoting *Osteotech, Inc. v. Biologic, LLC*, No. 07-1296 (JAP), 2008 WL 686318, at *5 (D.N.J. Mar. 7, 2008)).
[582] *Id.*
[583] *Raben Tire Co. v. McFarland*, NO. 5:16-CV-00141-TBR, 2017 WL 741569 (W.D. Ky. Feb. 24, 2017).
[584] *Id.* at *1.
[585] *Id.*

Tire moved to dismiss Raben Tire Co.'s complaint.[586] The court granted the motion to dismiss, finding that Raben Tire Co. had not plausibly alleged that the information in question qualified as a "trade secret" under the DTSA.[587]

Raben Tire Co. alleged that prior to their resignations and for some time after, McFarland and Bates transferred "confidential and proprietary information" to Tredroc Tire, including (1) sales commission reports showing sales from Raben Tire Co.'s customers who were assigned to Bates, (2) the names of customers of Raben Tire Co., and (3) a possible location for a new service center which Raben Tire Co. had disclosed to Bates after his resignation during negotiations to possibly retain him in some different capacity.[588] Although Raben Tire Co. labeled this information "confidential" in its complaint, it did not allege that it took reasonable efforts to protect the information from disclosure.[589] Because of this omission, the complaint failed to plausibly allege that the "confidential and proprietary information" qualified as a "trade secret" under the DTSA.[590] A complaint must support more than a "mere possibility of misconduct" to survive a motion to dismiss.[591] Without allegations that Raben Tire Co. took steps to protect the information in question, the court found that its complaint did nothing more than create a "mere possibility" that the defendants had violated the DTSA.[592]

---

[586] *Id.*
[587] *Id.*
[588] *Id.*
[589] *Id.*
[590] *Id* at *2.
[591] *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).
[592] *Id.*

SleekEZ, LLC v. Horton

In April 2017, the United States District Court for the District of Montana granted a motion to amend an employer's complaint to add a claim under the DTSA.[593] Plaintiff, SleekEZ, LLC ("SleekEZ") brought an action against Hal Horton for various business torts, including misappropriation of trade secrets relating to animal grooming products that it developed and sold.[594]

Previously, the court had issued an original Scheduling Order setting a "motions to amend pleadings" deadline of July 20, 2016.[595] The order was subsequently amended three times with the last amendment extending the deadline to October 21, 2016.[596] SleekEZ filed an amended complaint on that deadline.[597] On November 3, 2016, they filed a motion to amend, requesting that the court find they were allowed to amend the complaint until October 21, 2016 pursuant to the amended Scheduling Order, or alternatively that the court grant them leave to amend under Federal Rule of Civil Procedure Rule 15(a)(2).[598] Horton filed a motion to strike the amended complaint on the grounds SleekEZ failed to comply with the Scheduling Order.[599]

Horton was in a relationship with SleekEZ owner, Jennifer Tipton, from 2002 until 2014.[600] Horton was also employed by SleekEZ to create a marketing strategy for

---

[593] *SleekEZ, LLC v. Horton*, CV 16-09-BLG-SPW-TJC, 2017 WL 1906957 (D. Mont. Apr. 21, 2017).
[594] *Id.* at *1.
[595] *Id.* at *2.
[596] *Id.*
[597] *Id.*
[598] *Id.*
[599] *Id.* at *1-2.
[600] *Id.* at *1.

the company and, in that capacity, learned confidential and proprietary information about the business and its products.[601] SleekEZ asserted that Horton was aware that he had an obligation to keep the information confidential.[602] In May 2014, Horton's employment was terminated and thereafter, SleekEZ alleged, Horton began selling knockoffs of SleekEZ's products, used stolen blade components from the company in his product called the "Groom Ninja," copied SleekEZ's handle design, used his own knowledge of SleekEZ's manufacturers, distributors, and retailers to advance his products, and misrepresented himself as being affiliated with SleekEZ.[603]

When considering whether to grant leave to amend, courts consider the following five factors: "(1) bad faith, (2) undue delay, (3) prejudice to opposing party, (4) futility of amendment, and (5) whether plaintiff has previously amended his complaint."[604] The only factor disputed by Horton was futility.[605] Horton alleged that SleekEZ's DTSA claim failed as a matter of law and therefore the amendment was futile and should not be allowed.[606] Horton contended that (1) SleekEZ failed to allege the specific efforts that were made to maintain the secrecy of the trade secrets, (2) SleekEZ failed to impose a duty on Horton to maintain secrecy, and (3) some of the conduct in question occurred before the implementation date of the DTSA.[607] SleekEZ countered that its pleading was sufficient because it (1) identified efforts it made to maintain secrecy, (2) imposed a duty

---

[601] *Id.*
[602] *Id.*
[603] *Id.*
[604] *Id.* at *3 (quoting *Allen v. City of Beverly Hills*, 911 F.2d 367, 373 (9th Cir. 1990)).
[605] *Id.*
[606] *Id.* at *4.
[607] *Id.*

on Horton to maintain secrecy, and (3) the conduct in question continued after the May 11, 2016 DTSA implementation date.[608]

The court found for the plaintiffs holding that trade secret allegations are adequate "in instances where the information and the efforts to maintain its confidentiality are described in general terms"[609] and the question of whether a duty to maintain secrecy was imposed is highly fact-specific seeing as a lack of confidentiality agreement is not dispositive evidence of failure to maintain secrecy.[610] The court noted that a duty to maintain confidentiality can be based on a close personal relationship which gives rise to a fiduciary relationship and eliminates the need to take affirmative steps to ensure secrecy of the information.[611] Finally, the court found that under a "disclosure theory," SleekEZ's DTSA claim is actionable because the disclosure or use of the trade secret continued after the effective date of the DTSA.[612] The fact that the trade secrets were acquired prior to the law's enactment is immaterial.[613] Thus, the court found that the proposed amended complaint was not futile, and therefore recommended SleekEz's leave to amend be granted and Horton's motion to strike be denied.[614]

Lifesize, Inc. v. Chimene

---

[608] *Id.*
[609] *Id.* at *4 (quoting *Covenant Aviation Sec., LLC*, 15 F. Supp. 3d at 818).
[610] *Id.* at *5 (citing *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1201 (S.D. Cal. 2008)).
[611] *Id.* (citing *Elm City Cheese Co. v. Federico*, 752 A.2d 1037, 1052 (Conn. 1999)).
[612] *Id.*
[613] *Id.*
[614] *Id.*

In April 2017, the United States District Court for the Western District of Texas denied a motion to dismiss, holding that proper acquisition of trade secrets can result in misappropriation through improper use or disclosure of the same.[615] Lifesize, Inc. develops equipment for audio, web, and video conferencing.[616] Beau Chimene was employed as a senior engineer by Lifesize Communications, Inc. ("LCI").[617] LCI was subsequently acquired as a division of Logitech but Chimene continued working for LCI and leading the effort to make developments on LCI's speakerphone.[618] At some point thereafter, Lifesize, Inc. spun off from Logitech, leaving LCI fully owed by Logitech, though Lifesize, Inc. carried on largely the same business as LCI.[619] Chimene then became employed by Logitech working on its conference room products.[620] Lifesize, Inc. was concerned he might use its confidential information to develop competing products, so they requested written confirmation from Logitech that Chimene would not retain or disclose Lifesize, Inc.'s confidential information.[621]

On May 4, 2016, Logitech's outside counsel contacted Lifesize, Inc. revealing that Chimene had retained the laptop and two engineering notebooks containing trade secrets that had been provided to him while working at LCI.[622] Logitech returned the notebooks, but refused Lifesize, Inc.'s requests to reassign Chimene to work in an area

---

[615] *Lifesize, Inc. v. Chimene*, 1:16-CV-1109-RP, 2017 WL 1532609 (W.D. Tex. Apr. 26, 2017).
[616] *Id.* at *1.
[617] *Id.*
[618] *Id.*
[619] *Id.* at *2.
[620] *Id.*
[621] *Id.*
[622] *Id.*

that would not risk the disclosure of Lifesize, Inc.'s trade secrets.[623] Accordingly, Lifesize, Inc. filed a complaint against Chimene alleging misappropriation of trade secrets in violation of the DTSA and Texas Uniform Trade Secrets Act ("TUTSA"), among other claims.[624]

Unpersuaded by Chimene's arguments, the court found that Lifesize, Inc. had stated a proper claim for misappropriation under the TUTSA and DTSA.[625] The court held that it is not necessary for the defendant's acquisition to be wrongful; the plaintiff may instead show that the defendant permissibly acquired the information within a relationship of confidence and later disclosed or used the information in violation of that confidence.[626] In this case, Chimene claimed a confidentiality agreement he signed was never assigned to Lifesize, Inc., making his acquisition of their trade secrets proper.[627] Nevertheless, the court found that even though Chimene had access to his company-owned laptop as an employee, and therefore acquired the trade secrets lawfully, he could still be liable for their misappropriation if he used or disclosed them without authorization and with the knowledge that he was under a duty to maintain their secrecy.[628] The court held that Lifesize, Inc. plausibly alleged that Chimene was engaged in such misappropriation and had therefore stated a viable misappropriation

---

[623] *Id.*
[624] *Id.* at *3, *13 n.4 ("The definitions of misappropriation and improper means under the federal DTSA are identical to those under TUTSA in all respects material to the analysis here.").
[625] *Id.* at *9.
[626] *Id.*
[627] *Id.*
[628] *Id.*

claim.[629] Accordingly, the court denied Chimene's motion to dismiss the DTSA and TUTSA claims.[630]

Singer v. Stuerke

In June 2017, the United States District Court for the District of Nevada examined the consequences of insufficient pleadings of misappropriation claims under the DTSA and their effect on subject matter jurisdiction.[631] In 2015, Simon Singer and Leroy Stuerke formed the financial services company Tax Planning Institute, LLC ("TPI").[632] Singer alleged that Stuerke had used TPI's trade secret customer information for a competing business and filed a request to compel arbitration pursuant to TPI's Operating Agreement.[633] Stuerke filed a motion to dismiss, denying the validity of trade secrets, challenging the court's subject matter jurisdiction, and challenging the court's personal jurisdiction over him.[634]

Under the Federal Arbitration Act, the court had to determine: (1) if there exists a valid agreement to arbitrate between the parties; (2) if the dispute is within the scope of the arbitration agreement; and (3) whether the court would have subject matter jurisdiction over the controversy if not for the arbitration agreement.[635] After finding that there was a valid agreement to arbitrate, the scope of the arbitration agreement

---

[629] *Id.*
[630] *Id.*
[631] *Singer v. Stuerke*, No. 2:16-cv-02526-KJD-GWF, 2017 WL 2603305 (D. Nev. June 14, 2017).
[632] *Id.* at *1.
[633] *Id.*
[634] *Id.*
[635] *Id.* at *2.

included the trade secret dispute, and that Stuerke was subject to personal jurisdiction in Nevada courts, the court turned to an analysis of its subject matter jurisdiction based on Singer's pleading.[636] Singer alleged the court had both federal question and diversity jurisdiction over the parties.[637]

The court found that Singer's misappropriation claim under the DTSA did not set forth any provisions in the TPI Operating Agreement or elsewhere that detailed reasonable measures to protect the alleged trade secrets from improper disclosure.[638] Since this is an essential element of a trade secret claim under the DTSA and the complaint was devoid of factual assertions that the disclosure or use of a trade secret without consent by a person who knew of "'a duty to maintain the secret of the trade secret or limit the use of the trade secret,'" the pleading—as written—was insufficient to allow for relief.[639] The court allowed Singer fourteen days to file an amended petition including the key element that Stuerke had obligations to prevent disclosure of the trade secrets pursuant to an agreement between the parties.[640] If properly pled, the court would have subject matter jurisdiction over the underlying controversy and Singer would be able to proceed with binding arbitration.[641] If the defect could not be cured, Singer's request would be dismissed.

---

[636] *Id.*
[637] *Id.*
[638] *Id.*
[639] *Id.*
[640] *Id.*
[641] *Id.*

Wells Lamont Industry Group LLC v. Mendoza

In July 2017, the United States District Court for the Northern District of Illinois held that general identification of misappropriated trade secrets under a claim for violation of the DTSA meets the federal court pleading standards.[642]

Wells Lamont Industry Group LLC ("Wells Lamont") sued Richard Mendoza for violation of the DTSA and Illinois Trade Secrets Act, as well as his new employer, Radians, Inc. ("Radians") for various common law claims.[643] Wells Lamont designs, manufactures, and sells industrial gloves.[644] Mendoza worked as a Director of Sales for Wells Lamont before resigning in August 2016 and taking a similar position with Radians: a direct competitor of Wells Lamont.[645]

While with Wells Lamont, Mendoza signed a confidentiality agreement due to his exposure to confidential information, including product designs and prototypes.[646] The confidentiality agreement included trade secrets pertaining to financial information and forbade Mendoza from communicating the information or using it for the benefit of any other person or firm.[647] Additionally, an information technology agreement prevented Mendoza from disclosing trade secrets for any purpose other than in the capacity of his official duties with Wells Lamont.[648]

---

[642] *Wells Lamont Indus. Grp. LLC v. Mendoza*, 17 C 1136, 2017 WL 3235682, at *1 (N.D. Ill. July 31, 2017).
[643] *Id.*
[644] *Id.*
[645] *Id.*
[646] *Id.*
[647] *Id.*
[648] *Id.*

Before and after his resignation, Mendoza forwarded confidential information to his personal email address.[649] Mendoza then reached out to some of his former Wells Lamont customers to convince them to do business with Radians.[650] In September 2016, Wells Lamont sent a demand letter to both Mendoza and Radians seeking return of the confidential information and reminding Mendoza of his continuing obligations to the company.[651] Mendoza admitted to forwarding the information to his personal email and also to providing a Radians employee with a copy of Wells Lamont's confidential pricing list.[652] The following month, Mendoza contacted a Wells Lamont client, traveled to the client's office, and presented the client with replicas of several Wells Lamont products.[653] Following the presentation, the client cancelled its meeting with a Wells Lamont salesman.[654] Wells Lamont alleged Mendoza was utilizing confidential information to divert other Wells Lamont customers to Radians.[655]

After Wells Lamont initiated litigation, Mendoza moved to dismiss the DTSA claim against him.[656] He argued that Wells Lamont had not sufficiently alleged its information was a trade secret protected under the DTSA.[657] Wells Lamont's complaint referred to trade secrets such as "business models, business plans, and product development plans" and confidential information including "customer account

---

[649] *Id.* at *2.
[650] *Id.*
[651] *Id.*
[652] *Id.*
[653] *Id.*
[654] *Id.*
[655] *Id.*
[656] *Id.*
[657] *Id.*

information, product summaries, pricing sheets, product prototypes, product designs, and detailed sales reports."[658] The court found that general identification of the trade secrets that Wells Lamont alleged had been misappropriated was sufficient to survive a motion to dismiss.[659] The court also emphasized that general pleadings regarding misappropriation under the DTSA are typically adequate given the plaintiff's interest in avoiding public disclosure of trade secrets in court filings.[660]

Steves & Sons, Inc. v. JELD-WEN, Inc.

In September 2017, the United States District Court for the Eastern District of Virginia held that the DTSA does not create an express or implied private right of action for redress for conspiracy to engage in theft of trade secrets.[661]

John Pierce was a Senior Executive Vice President with JELD-WEN, Inc. ("JELD-WEN") and oversaw JELD-WEN's molded door skins operations.[662] In 1988, Pierce entered a management employment contract with JELD-WEN, in which he acknowledged that he was exposed to confidential data in his role with the company.[663] Steves and Sons, Inc. ("Steves") purchased door skins from JELD-WEN during Pierce's employment and Pierce often worked directly with Steves to complete these purchases. In June 2012, Pierce retired from JELD-WEN.

---

[658] *Id.* at *3.
[659] *Id.*
[660] *Id.*
[661] *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 271 F. Supp. 3d 835 (E.D. Va. 2017).
[662] *Id.* at 838.
[663] *Id.*

Around February 2015, Steves reached out to Pierce seeking confidential information relating to JELD-WEN's door skin business.[664] Steves and Pierce entered a Mutual Confidentiality and Non-Disclosure Agreement on March 15, 2015 in which Pierce would acquire JELD-WEN trade secrets and other confidential information by traveling to the JELD-WEN facilities and communicating with employees to elicit the information.[665] Steves agreed to pay for Pierce's expenses on this trip.[666] Pierce then sold Steves confidential information regarding finances and primer costs, JELD-WEN's future plans, and manufacturing processes.[667]

John Ambruz was also a former executive of JELD-WEN who worked as the Executive Vice President of Corporate Development from 2012 through 2014.[668] Ambruz similarly signed an employment contract with JELD-WEN.[669] Upon termination, Ambruz signed an acknowledgment of his ongoing duty to maintain confidentiality regarding JELD-WEN's trade secrets.[670]

Ambruz then started a consulting firm called Global Strategic Partners ("GSP").[671] Steves retained GSP as a consultant in July 2015 to evaluate the feasibility in developing its own molded door skin plant.[672] JELD-WEN alleged that Steves provided confidential information to Ambruz obtained through the parties' Long Term Supply Agreement and

---

[664] *Id.*
[665] *Id.* at 839.
[666] *Id.*
[667] *Id.*
[668] *Id.*
[669] *Id.*
[670] *Id.*
[671] *Id.*
[672] *Id.*

that Steves planned to use and continued to use JELD-WEN's trade secrets and confidential information in determining the feasibility of opening its own plant.[673]

JELD-WEN brought several claims against Steves, including conspiracy to violate the DTSA.[674] Steves sought dismissal of this claim and argued that 18 U.S.C. section 1832 did not create a private cause of action for conspiracy to violate the DTSA.[675] JELD-WEN argued that because an individual can apply for a civil seizure order under the DTSA against those conspiring to improperly use trade secrets, there must be a private right of action.[676]

The court noted that following the DTSA's enactment, district courts recognized a private right of action under the civil seizure provision.[677] However, the court pointed out that JELD-WEN relied on an inference from the civil seizure provision, that JELD-WEN cited no decision finding a private right of action, and that this case was therefore one of first impression.[678]

The court found that Section 1832(a) did not mention a private right of action regarding conspiracy to steal trade secrets.[679] Furthermore, since the statute established the crime and punishments for committing the crime, the court held there is no private civil action unless Congress specifies so.[680] Prior to the DTSA's enactment, courts did

---

673 *Id.*
674 *Id.* at 840.
675 *Id.*
676 *Id.* at 840-41.
677 *Id.* at 841.
678 *Id.*
679 *Id.*
680 *Id.*

not find a private right of action to redress this criminal conduct.[681] After the DTSA was enacted, plaintiffs continued to rely upon state law for conspiracy claims.[682] The court found all of these to be strong indicators that the DTSA did not create a private right of action for conspiracy.[683] Ultimately, the court held that Section 1832(a) does not imply a private right of action and instead only lessens the burden of obtaining a seizure order.[684]

Dichard v. Morgan

In November 2017, the United States District Court for the District of New Hampshire granted a motion for judgment on the pleadings with regard to a DTSA claim.[685] Michael Dichard brought action against his former employer, Jay-Mor Enterprises ("Jay-Mor"), alleging claims originating from his termination.[686] Jay-Mor then asserted counterclaims against Dichard alleging that Dichard misappropriated Jay-Mor's trade secrets in violation of the DTSA.[687] This court granted Dichard's motion for judgment on the pleadings with regard to Jay-Mor's DTSA claims.[688]

Jay-Mor is a family-owned demolition contracting business.[689] Dichard was employed by Jay-Mor as a senior-level business developer.[690] He, along with other

---

[681] *Id.*
[682] *Id.*
[683] *Id.*
[684] *Id.* at 843.
[685] *Dichard v. Morgan*, No. 17-CV-00338-AJ, 2017 WL 5634110 (D.N.H. Nov. 22, 2017).
[686] *Id.* at *1.
[687] *Id.*
[688] *Id.*
[689] *Id.*

employees, developed two large demolition projects estimated to produce over $1 million in revenues.[691] After Dichard resigned in March of 2017, Jay-Mor discovered that Dichard had absconded with the confidential project files for both aforementioned projects as well as additional confidential information and trade secrets.[692] He also offered both projects to additional demolition contractors, including his new employer.[693]

Dichard moved for judgment on the pleadings asserting that Jay-Mor failed to sufficiently allege (1) Dichard has disclosed any confidential information to a third party, (2) Jay-Mor took reasonable steps to protect its information, and (3) that the information in question constituted a trade secret.[694] The court addressed Dichard's second allegation, and finding it conclusive, did not address the other two.[695] With regard to the "reasonable steps" element of a DTSA claim, the court referred to ample case law stating that "at the pleading stage, plaintiffs need only describe the . . . efforts to maintain the confidentiality of the information in general terms,"[696] but this requires some affirmative step beyond merely "[i]ntending to keep the information secret."[697] Here, the only allegation Jay-Mor made which could be construed as an affirmative act to maintain secrecy of information is that the information was that it was "stored in

---

[690] *Id.*
[691] *Id.* at *2.
[692] *Id.*
[693] *Id.*
[694] *Id.*
[695] *Id.*
[696] *Id.* (quoting *Mission Measurement Corp.*, 216 F. Supp. 3d at 921).
[697] *Id.* (quoting *Singer*, 2017 WL 2603305, at *3).

files."[698] This act could seemingly apply to confidential and non-confidential information alike, and thus the court found that it did not support a plausible inference that Jay-Mor took any affirmative measures to maintain secrecy of the alleged trade secret and confidential information.[699] The court granted the motion without prejudice to Jay-Mor amending its counterclaim within fourteen days.[700]

Prominence Advisors, Inc. v. Dalton

In December 2017, the United States District Court for the Northern District of Illinois granted a former employee's motion to dismiss a DTSA claim when it held the former employer had failed to allege facts that could plausibly show the employee had misappropriated trade secrets.[701]

Prominence Advisors, Inc. ("Prominence") provides tools and services related to health care software.[702] In April 2016, Prominence entered an employment agreement with Joseph Dalton, who was to be employed as Director of Technology.[703] The agreement contained several restrictive covenants as well as a requirement to return confidential information upon termination.[704] Prominence's confidential information

[698] *Id.* at *3.
[699] *Id.*
[700] *Id.*
[701] *Prominence Advisors, Inc. v. Dalton,* No. 17 C 4369, 2017 WL 6988661, at *1 (N.D. Ill. Dec. 18, 2017).
[702] *Id.*
[703] *Id.*
[704] *Id.*

included "customer and potential customer information, employee agreements, training and review programs and techniques, personnel data, and other electronic data."[705]

Dalton was responsible for migrating Prominence's confidential information to a new cloud-based platform and backing up copies on an external hard drive.[706] Shortly after entering the employment agreement, relations between the two parties became strained and Dalton was terminated on May 13, 2016.[707] Prominence then filed suit, alleging that Dalton had breached his employment agreement through various actions as well as bringing a claim for trade secret misappropriation under the DTSA.[708] Dalton filed a motion to dismiss, arguing that Prominence failed to allege any facts to support its trade secret misappropriation claim and had also not indicated what confidential information was the subject of this claim.[709]

The court noted that "[f]or a DTSA claim to survive a motion to dismiss, a complaint need only identify the alleged trade secret in a general sense."[710] Therefore, the court found that Prominence had adequately alleged the existence of a trade secret when it referred to Dalton's possession of customer information, prospect information, employee agreements, personnel data, and electronic data.[711] Although the allegations

---

[705] *Id.*
[706] *Id.* at *2.
[707] *Id.*
[708] *Id.* at *1.
[709] *Id.*
[710] *Id.* at *3 (citing *Wells Lamont Indus. Grp. LLC*, 2017WL3235682, at *3).
[711] *Id.* at *4.

were "high-level and general in nature," the court found they were sufficient to allege the existence of a trade secret.[712]

However, Prominence's DTSA claim did not survive the motion to dismiss because the court found that misappropriation had not been properly alleged.[713] Prominence alleged that Dalton retained access to the cloud-based software on two personal devices as well as the external hard drive where he was backing up the information.[714] The court found that none of these allegations indicated improper acquisition or improper disclosure or use under the DTSA.[715] In fact, the court noted that Prominence's complaint showed Dalton had "acquired the information while performing his official duties while employed by Prominence."[716] Additionally, Prominence failed to allege any facts to support its allegation that the information had been disclosed or used.[717] Because Dalton had acquired the information through his job with the company and Prominence had not indicated any improper use or disclosure of the information, the court dismissed the DTSA claim without prejudice.[718]

---

[712] *Id.*
[713] *Id.*
[714] *Id.*
[715] *Id.*
[716] *Id.*
[717] *Id.* at *5.
[718] *Id.*

Ultradent Products, Inc. v. Spectrum Solutions LLC

In January 2018, the United States District Court for the District of Utah examined pleading requirements and emphasized the importance of including dates of alleged misappropriation to survive a motion to dismiss a DTSA claim.[719]

An Ultradent Products, Inc. ("Ultradent") subsidiary entered an agreement with Spectrum Solutions LLC ("Spectrum") to manufacture DNA test kits.[720] The agreement, which was set to run through September 24, 2017, had an automatic renewal provision unless proper notice was given regarding non-renewal.[721] Spectrum provided late notice in June 2017 that it did not intend to renew, but Ultradent had already extended the agreement when the notice deadline passed.[722] Spectrum indicated it did not want to renew the agreement because it planned to manufacture its own DNA test kits, and it would not pay royalties to Ultradent for doing so.[723]

Neil Johnson worked for Ultradent as a Manager of Production for the DNA test kits until his termination on November 2, 2015.[724] In the course of his employment, Johnson signed an employment agreement that prohibited him from using Ultradent's trade secrets or other confidential information during or after his employment.[725] In its complaint, Ultradent alleged that Johnson violated his employment agreement "by

---

[719] *Ultradent Prods., Inc. v. Spectrum Sols. LLC*, No. 2:17-CV-890, 2018 WL 324868 (D. Utah Jan. 8, 2018).
[720] *Id.* at *1.
[721] *Id.*
[722] *Id.*
[723] *Id.*
[724] *Id.*
[725] *Id.*

consulting or being employed by Spectrum and by disclosing Ultradent's trade secrets or confidential, proprietary, technical, or business information to Spectrum."[726]

Spectrum filed a motion to dismiss the DTSA claim and argued that Ultradent had failed to allege misappropriation under the DTSA.[727] Importantly, Spectrum pointed to Ultradent's failure to state when any alleged misappropriation occurred and argued for dismissal because nothing in the pleadings alleged misappropriation *after* the DTSA's enactment.[728] Ultradent argued the misappropriation occurred during the time period "when Spectrum was preparing to manufacture DNA test kits itself."[729]

The court was not persuaded by this argument and noted that the paragraphs in the complaint that Ultradent cited for support did not mention Johnson at all.[730] The court held that all allegations relating to the DTSA claim failed to "indicate when the alleged misappropriation occurred."[731] Furthermore, Ultradent's allegation that Spectrum was currently using or threatening to use its trade secrets to set up a manufacturing facility for the DNA test kits was insufficient because it was a conclusory allegation "wholly devoid of any well-pled facts."[732] The court held that "a mere recitation of the elements of a cause of action is insufficient to state a claim under DTSA."[733]

---

[726] *Id.* at *2.
[727] *Id.*
[728] *Id.*
[729] *Id.*
[730] *Id.*
[731] *Id.* at *3.
[732] *Id.*
[733] *Id.*

Elsevier Inc. v. Doctor Evidence, LLC

In January 2018, the United States District Court for the Southern District of New York dismissed a DTSA counterclaim after it found the company had failed to demonstrate an understanding of the distinction between confidential information and trade secrets.[734]

Elsevier Inc. ("Elsevier") and Doctor Evidence, LLC ("DRE") entered an agreement on July 18, 2014 for DRE to use its software for data analysis on articles identified by Elsevier.[735] The agreement obligated Elsevier to keep DRE's information confidential.[736] Once DRE began performing the data analysis, the parties started engaging in regular teleconferences regarding the activity.[737] In a counterclaim following Elsevier's filing of a breach of contract claim, DRE alleged that Elsevier used the teleconferences are a pretext to gain access to DRE's information and that Elsevier intended to use DRE's confidential information to develop its own similar products.[738]

In its DTSA counterclaim, DRE listed nine categories of confidential information it disclosed to Elsevier.[739] DRE alleged that Elsevier's representatives used the teleconferences to gain insight to DRE's processes so the company could develop its own services substantially similar to those offered by DRE.[740] DRE further alleged this information was obtained by improper means because of the agreement in place

---

[734] *Elsevier Inc. v. Doctor Evidence, LLC*, 17-cv-5540 (KBF), 2018 WL 557906 (S.D.N.Y. Jan. 23, 2018).
[735] *Id.* at *1.
[736] *Id.*
[737] *Id.*
[738] *Id.*
[739] *Id.* at *2.
[740] *Id.*

between the parties at the time the information was misappropriated.[741] Elsevier filed a motion to dismiss the DTSA claim as well as common law claims.[742]

The court found the categories of confidential information listed by DRE in its counterclaim were "extraordinarily general."[743] These categories included clinical methods relating to executing projects, data configuration protocols, interpretation of data, the process to asses quality of evidence, risk of bias assessments, analytics, and other processes.[744] The court held that alleging the existence of *categories* of confidential information without providing any details of the actual trade secrets did not "give rise to a plausible allegation of a trade secret's existence."[745] Furthermore, the court noted that DRE had conflated confidential information and trade secrets throughout its counterclaim, indicating a possible lack of understanding of the standard required by the DTSA.[746]

Although the court acknowledged that a party need not divulge each detail of an alleged trade secret in its pleadings, it held the party "must do more than simply list general categories of information."[747] Furthermore, DRE's pleading failed to discuss the information's value, the extent to which it is known by those within and outside the industry, the amount of money or effort expended to develop the information, and the ease by which the information could be used or acquired by those outside the

---

[741] *Id.*
[742] *Id.* at *1.
[743] *Id.* at *5.
[744] *Id.*
[745] *Id.*
[746] *Id.*
[747] *Id.* at *6.

company.[748] The court believed all of these "contours" necessary to support a trade secrets claim under the DTSA, but such information was lacking in this case.[749] Because a DTSA violation must be pled with more specificity than simply restating the elements of a trade secret, DRE's counterclaim was dismissed.[750]

M.C. Dean, Inc. v. City of Miami Beach, Florida

In August 2016, the United States District Court for the Southern District of Florida granted a motion to dismiss a subcontractor's action under the DTSA and the Florida Uniform Trade Secrets Act ("FUTSA") for failure to state a claim on which relief could be granted.[751] M.C. Dean, a city subcontractor, brought suit against the City of Miami Beach and International Brotherhood of Electrical Workers, Local 349, alleging violations of the DTSA and the FUTSA.[752] M.C. Dean, an electrical design-build and systems integration firm, was a subcontractor for Clark Construction Group, LLC ("Clark").[753] Clark was the general contractor for the Miami Beach Convention Center renovation project, and employed M.C. Dean as a subcontractor on that project.[754] As part of the city's wage ordinance law, Clark was required to provide the city with payroll information.[755] The payroll requirement also applied to subcontractors, and M.C. Dean

[748] *Id.*
[749] *Id.*
[750] *Id.* at *7.
[751] *M.C. Dean, Inc. v. City of Miami Beach*, 199 F. Supp. 3d 1349 (S.D. Fla. 2016).
[752] *Id.* at 1352.
[753] *Id.* at 1350.
[754] *Id.*
[755] *Id.* at 1351.

was contractually obligated to provide Clark with certified copies of its payroll.[756] M.C. Dean's payroll listed the names of its employees.[757]

The names of M.C. Dean's employees and training practices were valuable, and the International Brotherhood of Electrical Workers, Local 349's ("349") sought copies of the payroll from the city under the Florida Public Records Act.[758] After M.C. Dean objected, claiming that the payrolls were trade secrets, the city agreed to disclose only redacted copies of the payroll to 349.[759] After learning that a city clerk had inadvertently disclosed un-redacted copies of the payroll to 349 on March 22, 2016, M.C. Dean demanded that 349 return or destroy the copies.[760] 349 refused, and M.C. Dean filed a complaint on May 16, 2016 alleging violations of the DTSA and the FUTSA.[761]

The City of Miami Beach and 349 filed a motion to dismiss.[762] The court took up two of the defendants' arguments: "M.C. Dean failed to allege that it (1) it took reasonable steps to protect its trade secret, and (2) any acts of misappropriation."[763] The court first addressed the issue of whether M.C. Dean took reasonable steps to protect its trade secret.[764] Neither party disputed that the payrolls had independent economic value because they contained information not generally known or readily

---

[756] *Id.* at 1350.
[757] *Id.*
[758] *Id.*
[759] *Id.* at 1350-51.
[760] *Id.* at 1351.
[761] *Id.*
[762] *Id.* at 1350.
[763] *Id.* at 1353.
[764] *Id.* at 1355

ascertainable to others.[765] Because the payrolls had independent economic value, they satisfied the first element of the definition of a trade secret.[766]

However, the court determined that that because M.C. Dean did not take reasonable steps to keep the information secret, they did not satisfy the second element of a trade secret.[767] M.C. Dean was required to provide the payroll information to Clark, who was required to release the information to the City.[768] When M.C. Dean released the payroll information to Clark, it did not "impose any restriction on Clark's use of it, be it through contract or any other protective mechanism."[769] Because M.C. Dean failed to properly place restrictions on the payroll information, it could not successfully argue that it took reasonable steps to keep the information secret.[770]

The court then examined the defendant's allegation that M.C. Dean failed to prove any acts of misappropriation.[771] Under both the DTSA and the FUTSA, liability only attaches when there is evidence of misappropriation of the information.[772] The court noted that the information at issue in this case was acquired as a result of a City clerk's error, not as a result of an act of wrongdoing.[773] Further, M.C. Dean's subcontractor contract "required Clark to provide [the payroll information] to the City without restriction . . . [t]he described contractual provisions make abundantly clear the

---

[765] *Id.*
[766] *Id.*
[767] *Id.* at 1356.
[768] *Id.* at 1355.
[769] *Id.*
[770] *Id.* at 1357.
[771] *Id.*
[772] *Id.*
[773] *Id.*

information at issue is the property of [the] City and may be used by [the] City without restriction."[774] As such, the court determined that there was no evidence of misappropriation of the information because M.C. Dean "consented to disclosure of the information by entering the subcontract."[775]

M.C. Dean is thus a good reminder that in order to succeed on a DTSA claim (or a trade secret claim under state law), the plaintiff must take reasonable steps to protect the information at issue. Here, M.C. Dean did not take the reasonable steps and thus did not meet either the DTSA or the FUTSA standard for trade secret protection. The opinion notably does not address whether the fact that the alleged misappropriation at issue occurred prior to the DTSA's enactment had any bearing on the viability of the DTSA claim.

HealthBanc International, LLC v. Synergy Worldwide, Inc.

In September 2016, the United States District Court for the District of Utah decided *HealthBanc International, LLC v. Synergy Worldwide, Inc.*[776] HealthBanc manufactured a greens powder that could be mixed with water to create a nutritional supplement.[777] Synergy, a marketing company, agreed under a royalty contract to distribute HealthBanc's product and to pay HealthBanc royalties for each bottle of the

[774] *Id.*
[775] *Id.*
[776] *HealthBanc Int'l, LLC v. Synergy Worldwide, Inc.*, 208 F. Supp. 3d 1193 (D. Utah 2016).
[777] *Id.* at 1195.

supplement sold.[778] As part of the royalty contract, Synergy had to calculate the royalties for HealthBanc's reference.[779] After Synergy did not make royalty payments to HealthBanc and did not make the royalty records available, HealthBanc sued, asserting claims for breach of contract and for violations of the DTSA and Utah's state trade secret protection act.[780] In support of the causes of action based on trade secret claims, HealthBanc alleged that Synergy had "print[ed] portions of the greens formula on the packaging of the product and [used] the greens formula without paying royalties."[781]

The court determined that the trade secret claims failed as a matter of law because at the time of the misappropriation, HealthBanc did not have title to the trade secrets.[782] The court noted that pursuant to the DTSA, only "an owner of a trade secret that is misappropriated may bring a civil action under this subsection."[783] Both the DTSA and the Utah Uniform Trade Secrets Act ("UUTSA") contain identical provisions regarding bringing a valid misappropriation claim.[784] The provisions require that "a party may not be liable for misappropriation under either Act unless it takes, discloses, or uses a trade secret belonging to someone else."[785]

The court noted that the royalty agreement contained a provision that "transferred all intellectual property rights – including trade secret rights – to

---

[778] *Id.*
[779] *Id.*
[780] *Id.*
[781] *Id.* at 1195-96.
[782] *Id.* at 1201.
[783] *Id.* (quoting 18 U.S.C.A. Section 1836(b)(1)).
[784] *Id.*
[785] *Id.*

Synergy."[786] HealthBanc was not the rightful owner of the trade secret rights at the time of the misappropriation.[787] Synergy lawfully owned the trade secret rights, and therefore HealthBanc could not bring a valid misappropriation claim against Synergy.[788] The District Court of Utah therefore granted Synergy's motion to dismiss the trade secret causes of action with prejudice.[789]

Cases Discussing Amending Pleadings to Add a DTSA Claim

Particularly in lawsuits that were ongoing at the time of the DTSA's passage, courts have had to consider whether to permit plaintiffs to amend their complaints to add a DTSA claim. This section discusses some of those cases.

VIA Technologies, Inc. v. ASUS Computer International

In February 2017, the United States District Court for the Northern District of California addressed a procedural issue with regard to a DTSA claim.[790] VIA Technologies, Inc. ("VIA") brought suit against ASUS Computer International ("ASUS") for alleged infringement of VIA's patents and misappropriation of intellectual property

[786] *Id.*
[787] *Id.*
[788] *Id.*
[789] *Id.*
[790] *VIA Techs., Inc. v. ASUS Comput. Int'l*, No. 14-cv-03586-BLF, 2017 WL 491172 (N.D. Cal. Feb. 7, 2017).

relating to USB technology.[791] VIA filed a motion for leave to amend the complaint to add a claim under the DTSA.[792] The court granted the motion.[793]

The DTSA went into effect before fact discovery closed and before expert disclosure deadlines.[794] Moreover, VIA was not made aware of pertinent sales data evidencing continuing trade secret misappropriation until December 22, 2016 when ASUS made its production of documents.[795] According to ASUS, the sales data was produced on November 16, 2016 and December 22, 2016 in supplemental productions, but VIA had inadvertently overlooked that data, thinking it was a mere "re-produc[tion]."[796]

The court noted that when a court's scheduling order does not set a deadline for amendments to the pleadings, a motion for leave to amend is evaluated under Federal Rule of Civil Procedure Rule 15, which provides that "[t]he court should freely grant leave [to amend] when justice so requires."[797] In deciding whether to grant leave to amend, the court must consider the factors set forth by the Supreme Court in *Foman v. Davis*.[798] A district court must grant leave to amend unless one or more of the *Foman* factors is present: (1) undue delay, (2) bad faith or dilatory motive, (3) repeated failure

---

[791] *Id.* at *1.
[792] *Id.*
[793] *Id.*
[794] *Id.*
[795] *Id.*
[796] *Id.*
[797] *Id.* (citing F.R.C.P. 15).
[798] *Id.* (citing *Foman v. Davis*, 371 U.S. 178 (1962); *Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d 1048 (9th Cir. 2009)).

to cure deficiencies by amendment, (4) undue prejudice to the opposing party, and (5) futility of amendment.[799]

Dismissing the "repeated failure to cure deficiencies" factor as irrelevant in this case, the court considered the remaining four factors.[800] First, it found neither undue delay nor bad faith on VIA's part.[801] Although VIA could have raised the DTSA issue in November had it known about the sales data, the additional four weeks did not make the delay undue.[802] There was also no demonstration of bad faith as VIA represented that it had misunderstood the November production as "re-production."[803]

With regard to the fourth factor, the court held that ASUS did not meet the burden of showing prejudice because "the proposed DTSA claim is based on the same nucleus of facts" as the existing claim under the California Uniform Trade Secret Act ("CUTSA").[804] The court found unpersuasive ASUS's argument that prejudice results from the fact that the DTSA provides for "an ex parte seizure remedy" that is not available under the CUTSA.[805] Although the court found that some additional discovery may be required, ASUS's admission that "VIA would be seeking the same relief that it is currently seeking under the CUTSA, under the same set of facts" undercut the argument that the additional discovery would be substantial.[806]

---

[799] *Id.*
[800] *Id.*
[801] *Id.*
[802] *Id.*
[803] *Id.*
[804] *Id.* at *2.
[805] *Id.*
[806] *Id.* at *3.

Finally, the court held that the proposed DTSA claim is not futile.[807] The mere fact that a claim is duplicative of existing claims, does not make it futile.[808] In order to be futile, the claim would have to be insufficient under Federal Rules of Civil Procedure Rule 12(b)(6).[809] The court was further persuaded by VIA's explanation as to why the DTSA claim was not added originally, which was a combination of the fact that the DTSA was not enacted until May 2016 and the data supporting the DTSA claim was not made available to VIA until November 2016.

High 5 Games, LLC v. Marks

In January 2017, the United States District Court for the District of New Jersey considered an amendment to add a claim under the DTSA.[810] Plaintiff, High Five Games ("H5G"), develops slot machine games for casinos and this case involves two of its gaming inventions known as "Super Symbols" and "Super Stacks."[811] Defendants, Daniel Marks, Joseph Masci, and Brian Kavanagh, were prior employees of H5G and privy to confidential information during their employment.[812] Marks resigned and founded Marks Studios, LLC, hiring the other two defendants as employees.[813] H5G subsequently discovered that another game distributor was featuring two of Marks' games which had "the same look and feel" and used similar names as its own "Super

[807] *Id.*
[808] *Id.*
[809] *Id.*
[810] *High 5 Games, LLC v. Marks*, No. 13-7161 (JMV), 2017 WL 349375 (D.N.J. Jan. 24, 2017).
[811] *Id.* at *1.
[812] *Id.*
[813] *Id.*

Symbols" and "Super Stacks" games.[814] H5G alleged that this game distributor had received these games by working with Marks and the other defendants who had misappropriated H5G's trade secrets.[815]

In the instant case, H5G filed a motion for leave to file a second amended complaint adding a DTSA claim.[816] Defendants claimed that H5G's DTSA claim was futile because it supposedly was based entirely on acts that occurred prior to its enactment on May 11, 2016.[817] The court disagreed with the defendants, finding that it would be premature to deem the DTSA claim futile when the parties had not yet sufficiently examined the issue.[818] The court acknowledged that there are various theories under which one may be liable for misappropriation under the DTSA.[819] For example, though a trade secret may have been acquired prior to the Act, allegations of *continuing* misappropriation are also colorable under the Act.[820] Thus, the court held that the adequacy of this claim under the DTSA required delving into fact questions and therefore was more appropriate for a full Rule 12(b)(6) motion, as opposed to a Rule 15 motion to amend.[821]

---

[814] *Id.*
[815] *Id.*
[816] *Id.* at *2.
[817] *Id.* at *5.
[818] *Id.* at *6.
[819] *Id.*
[820] *Id.*
[821] *Id.*

Chubb INA Holdings, Inc. v. Chang

In another ruling in *Chubb INA Holdings, Inc. v. Chang*, the United States District Court for the District of New Jersey considered whether to grant Chubb INA Holdings and Federal Insurance Company leave to file a Second Amended Complaint.[822] The plaintiffs had several reasons for seeking to file a Second Amended Complaint, one of which was to add a claim under the new DTSA.[823]

At issue was Chubb's contention that Chang and Endurance Services, along with several sub-holdings of Endurance, specifically sought to recruit Chubb employees and hire them for positions at Endurance.[824] Chubb's Amended Complaint asserted that the defendants used Chubb's confidential information to complete this process, eventually hiring 12 Chubb employees.[825] The Chubb employees were instructed to notify Chubb of their resignation on April 22, 2016, which was prior to the enactment of the DTSA.[826] Chubb also asserted that some of its former employees took confidential information from Chubb computers and did not return them.[827]

An Amended Complaint was filed on May 3, 2016 to "remove an allegation of diversity of citizenship and reflect[] additional facts purportedly learned during the course of [Chubb's] ongoing investigation and the limited discovery exchanged between

---

[822] *Chubb INA Holdings Inc. v. Chang*, No. 16-2354-BRM-DEA, 2016 WL 6841075, at *1 (D.N.J. Nov. 21, 2016).
[823] *Id.*
[824] *Id.*
[825] *Id.* at *2.
[826] *Id.*
[827] *Id.*

the parties."[828] On May 16, 2016, Chubb informed the defendants that they intended to move to amend to assert a claim under the DTSA.[829] The defendants opposed the amendment.[830]

The court determined that "[i]n the absence of unfair prejudice, futility of amendment, undue delay, bad faith, or dilatory motive, the court must grant a request for leave to amend."[831] The court thus granted the motion for leave to amend, without addressing the issue of the application of the DTSA to pre-enactment conduct.[832]

The Interstate Commerce Requirement under the DTSA

For subject matter jurisdiction over a DTSA claim to exist, the alleged trade secrets must relate "to a product or service used in, or intended for use in, interstate or foreign commerce."[833] Some defendants have challenged jurisdiction in DTSA cases based on a failure to meet this interstate commerce requirement. This section discusses several of those cases.

---

[828] *Id.*
[829] *Id.*
[830] *Id.* at *2-3.
[831] *Id.* at *6 (citing *Grayson v. Mayview State Hosp.*, 292 F.3d 103, 108 (3d Cir. 2002)).
[832] *Id.*
[833] 18 U.S.C.A. § 1836(b)(1).

Hydrogen Master Rights, Ltd. v. Weston

In January 2017, the United States District Court for the District of Delaware examined the interstate commerce requirement and found it did not have subject matter jurisdiction over the DTSA claim.[834]

Tracy Coats, Carl Le Souef, and Dr. Pravansu Mohanty were partners who used Hydrogen Master Rights, Ltd. ("HMR") "as an acquisition vehicle to purchase certain hydrogen technology."[835] HMR and the sellers executed a purchase agreement on December 12, 2011.[836] Dean Weston was an assignee of some of the sellers' rights under the purchase agreement.[837]

After the purchase agreement was executed, Weston told Dr. Mohanty that he knew the secret formula for the hydrogen technology and that he owned a partial interest in the technology itself.[838] In the purchase agreement, the sellers had made representations and warranties to HMR that the hydrogen technology formula had been kept confidential and that no one other than the sellers had any interest in it.[839] Therefore, HMR and Weston entered a mutual cooperation agreement that allowed both parties to pursue claim against the sellers regarding ownership of the hydrogen technology.[840] As part of the mutual cooperation agreement, Weston agreed "'to

[834] *Hydrogen Master Rights, Ltd. v. Weston*, 228 F. Supp. 3d 320, 338 (D. Del. 2017).
[835] *Id.* at 324-25.
[836] *Id.* at 325.
[837] *Id.*
[838] *Id.*
[839] *Id.*
[840] *Id.*

maintain the technology in the strictest of confidence and to not make any disclosure [sic] use thereof for any purpose without HMR's express written consent.'"[841]

HMR then began to pursue resolution with the sellers, and the sellers filed suit against Weston on March 23, 2012.[842] The sellers filed an affidavit, which indicated that Weston had extensive experience with the hydrogen technology and had made "'persistent attempts to learn the formula.'"[843] Based on the affidavit, HMR believed that the sellers had never told or revealed the formula to Weston and entered an agreement with sellers to toll the statute of limitations on the dispute.[844]

Coats withdrew from the partnership that had used HMR to purchase the hydrogen technology in 2014.[845] After she left the partnership, HMR alleged that Coats entered into a conspiracy with Weston and the sellers to extort HMR.[846] The sellers had settled litigation with Weston by agreeing to assign their rights under the HMR purchase agreement to Weston and his company.[847] On March 23, 2016, Weston used recordings made by Coats to threaten HMR to pay Weston $9.4 million and assign him the hydrogen technology rights.[848] As a result of those threats, this case was initiated and the alleged trade secrets of the recordings, the hydrogen technology, the purchase

[841] *Id.*
[842] *Id.* at 326.
[843] *Id.*
[844] *Id.*
[845] *Id.*
[846] *Id.* at 327.
[847] *Id.*
[848] *Id.*

agreement, and the mutual cooperation agreement formed the basis of the DTSA claims.[849]

The court held that HMR had failed to "allege any nexus between interstate or foreign commerce and the . . . [recordings], [h]ydrogen [t]echnology, [p]urchase [a]greement, or [m]utual [c]ooperation [a]greement."[850] The claims were therefore dismissed without prejudice.[851]

Government Employees Insurance Co. v. Nealey

In June 2017, the United States District Court for the Eastern District of Pennsylvania dismissed DTSA and unjust enrichment claims and issued sanctions when it found that the reasonable measures to protect a trade secret requirement under the DTSA had not been adequately pled.[852] The court also addressed the interstate commerce requirement.

This case stemmed from an extensive history of litigation arising from class actions filed against Government Employees Insurance Co. ("GEICO"). A dispute arose regarding the use of documents in the class actions and GEICO subsequently filed suit in the Pennsylvania district court against the class action plaintiffs' lawyers, expert witness, and the expert witness' company, asserting claims for trade secret misappropriation and

[849] *Id.*
[850] *Id.* at 338.
[851] *Id.*
[852] *Gov't Emps. Ins. Co. v. Nealey*, 262 F. Supp 3d 153, 158 (E.D. Pa. 2017).

unjust enrichment.[853] Attorney Scott Nealey and the other defendants filed a motion to dismiss.[854]

Some background on the history of litigation provides context for the court's ruling. In 2015, lawyer Stephen Hansen filed a class action against GEICO in Washington state court alleging that GEICO was failing to fully reimburse customers involved in accidents.[855] GEICO tried to remove the case to federal court and filed motions try to delay the litigation.[856] Hansen had filed an additional class action around the same time alleging that GEICO failed to reimburse customers for loss of use of their vehicle.[857] GEICO similarly attempted removal in that case.[858]

In October 2015, a Washington state court (after the case had apparently been remanded) entered a stipulated Protective Order to protect confidential information that may be disclosed through the course of litigation.[859] The Protective Order required the parties to designate and clearly mark information that was "confidential" and "highly confidential."[860]

In the second case, GEICO filed an affidavit proving how many insurance claims GEICO receives and how much they pay out per claim.[861] Although GEICO redacted the

---

[853] *Id.*
[854] *Id.*
[855] *Id.* at 159.
[856] *Id.*
[857] *Id.*
[858] *Id.* at 160.
[859] *Id.*at 159.
[860] *Id.* at 159-60.
[861] *Id.* at 160.

document, it failed to mark the document as required by the Protective Order.[862] Months later, despite GEICO's failure to follow the labeling instructions of the Protective Order, the court in the second class action granted GEICO's motion to seal the affidavit.[863] Two days after the affidavit was filed without any confidential designation, Nealey attended a deposition for a case in which GEICO was not a party.[864] The deponent was an expert statistician whom Nealey retained for the GEICO case.[865]

GEICO alleged that Nealey provided the expert witness with the unredacted affidavit from the class action and that the affidavit contained trade secrets, which had been misappropriated by Nealey's dissemination of them.[866] Nealey and the other defendants filed a motion to dismiss, including for failure to state a claim.[867] The court found that GEICO's DTSA claim failed to state a claim because GEICO did not take reasonable measures to protect the information.[868]

The court noted that pleading standards for reasonable measures to protect trade secrets were uncertain because the DTSA had only been enacted the year before.[869] GEICO argued that at the motion to dismiss stage of litigation, there were insufficient facts to determine whether reasonable measures had been taken and that the case needed to progress to make that judgment.[870] The court disagreed, finding that the

---

[862] *Id.*
[863] *Id.* at 161.
[864] *Id.* at 160.
[865] *Id.*
[866] *Id.*
[867] *Id.* at 162.
[868] *Id.* at 167.
[869] *Id.*
[870] *Id.*

factual information was "black-and-white" because GEICO had not followed the terms of its own stipulated Protective Order in regards to the affidavit.[871] Although the court did not doubt that GEICO took reasonable measures *within* the company to protect its trade secrets, it found it did not do so in the class action lawsuits.[872]

Additionally, the court found that GEICO itself had disclosed many of its alleged trade secrets when it attempted to prove the amounts in controversy to remove the cases to federal court.[873] Ultimately, it was GEICO's failure to follow the terms of the Protective Order or to properly follow court rules to subsequently seal the document that was fatal to its DTSA claim in Pennsylvania.[874] The court viewed this case as "not a trade secrets case" but one "about a company that improperly responded to a class action filed against it by suing the lawyers who filed the class action in a faraway forum."[875] Because this was an abuse of the judicial process, the court imposed sanctions in addition to dismissing GEICO's claims.[876]

Furthermore, even if the complaint had not been dismissed due to the aforementioned deficiencies, the court also held that it did not have subject matter jurisdiction over the claim.[877] Specifically, the court found that GEICO's complaint had failed to allege any nexus between interstate or foreign commerce and the alleged trade

[871] *Id.*
[872] *Id.* at 168.
[873] *Id.*
[874] *Id.*
[875] *Id.* at 178.
[876] *Id.*
[877] *Id.* at 172-73.

secrets regarding how much GEICO paid out on insurance claims.[878] The court cited *Hydrogen Master Rights, Ltd.* for the proposition that it has no jurisdiction over a claim where a party fails to allege any nexus between the trade secrets and interstate commerce.[879] However, the court found it possible that GEICO could allege how the payouts on insurance claims were involved in interstate or foreign commerce so it dismissed the claim without prejudice, giving the company leave to file a pleading that fulfilled the interstate commerce requirement.[880]

Cases Discussing Ex Parte Seizure under the DTSA

As mentioned, the DTSA's ex parte seizure provision was the most controversial aspect of the new law. Although there are limited decisions dealing with ex parte seizure relief under the DTSA, the decisions that exist strongly suggest that courts considering ex parte seizure requests are carefully weighing the considerations of all parties and are narrowly tailoring any orders they decide to grant.

OOO Brunswick Rail Management v. Sultanov

In January 2017, the United States District Court for the Northern District of California granted OOO Brunswick Rail Management's ("Brunswick") request for a

878 *Id.* at 160.
879 *Id.* at 173.
880 *Id.*

TRO.[881] In addition to the TRO, Brunswick sought a seizure order under the DTSA and a seizure and preservation order under Federal Rules of Civil Procedure Rules 64 and 65.[882]

While employed by Brunswick, Richard Sultanov allegedly sent several confidential documents to his personal email account without authorization, then subsequently deleted the messages and emptied them from his trash folder.[883] Paul Ostling, another former Brunswick employee, had received confidential emails from his former personal assistant who was still employed by Brunswick, which he then forwarded to Sultanov.[884] Sultanov also refused to return any company-issued mobile phone or laptop.[885]

Brunswick sought a preservation order claiming that Sultanov and Ostling had disclosed and planned to continue to disclose trade secrets to creditors to disadvantage Brunswick in negotiations regarding its debt restructuring.[886] To determine whether a preservation order is necessary, courts consider (1) threats to preservation of the evidence, (2) irreparable harm likely to result to the party seeking preservation, and (3) the capability of the custodian to maintain the evidence sought to be preserved.[887]

---

[881] *OOO Brunswick Rail Mgmt. v. Sultanov*, No. 5:17-cv-00017-EJD, 2017 WL 67119 (N.D. Cal. Jan. 6, 2017).
[882] *Id.* at *1.
[883] *Id.*
[884] *Id.*
[885] *Id.*
[886] *Id.*
[887] *Id.* (citing *Echostar Satellite LLC v. Freetech, Inc.,* No. C-07-06124 JW, 2009 WL 8399038, at *2 (N.D. Cal. Jan. 22, 2009)).

The court found that Brunswick had satisfied all three requirements.[888] First, there was a risk that Sultanov and Ostling would delete relevant material from their email accounts or it would be automatically deleted.[889] Second, deletion of this material would cause irreparable harm to Brunswick.[890] Third, it is within the reasonable capabilities of Google and Rackspace (Sultanov and Ostling's email providers, respectively) to preserve material in both defendants' accounts, but they are not required to do so absent a court order.[891] Thus, Google and Rackspace were each required to preserve all data from the respective employee's account within seventy-two hours of receiving the Order.[892]

In addition, Brunswick sought an order directing ex parte seizure of the sensitive information on Sultanov and Ostling's accounts by requiring Google and Rackspace to deliver copies of their accounts to the court.[893] The court found that a seizure was unnecessary because Google and Rackspace were required to preserve the data in any case.[894]

Brunswick also sought an order under the DTSA to seize Sultanov's company-issued laptop and mobile phone.[895] A court may issue a seizure order only if, among other requirements, an order under Federal Rules of Civil Procedure Rule 65 or another

---

[888] *Id.* at *1.
[889] *Id.*
[890] *Id.*
[891] *Id.*
[892] *Id.* at *3.
[893] *Id.* at *2.
[894] *Id.*
[895] *Id.*

form of equitable relief would be inadequate.[896] The court found that seizure under the DTSA was unnecessary because it found that equitable relief was adequate, as the court ordered that Sultanov must deliver the laptop and mobile phone at the time of the hearing and, in the meantime, the devices could not be accessed or modified under the preservation order.[897]

Finally, the court granted Brunswick's application for a TRO, finding all four elements satisfied.[898] First, Brunswick's evidence of improperly disseminated confidential information demonstrated a likeliness that Brunswick would succeed on the merits of its trade secrets claim.[899] Second, Brunswick had shown that it would likely suffer irreparable harm if the court did not grant injunctive relief since dissemination of the confidential information to Brunswick's creditors and others would cause irreparable harm.[900] Finally, the court found that the balance of equities weighed in Brunswick's favor and a TRO would serve the public interest.[901] In addition, an ex parte TRO application must satisfy Federal Rules of Civil Procedure Rule 65(b)(1), under which a TRO may issue only if "the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required."[902] Brunswick

[896] *Id.* (citing 18 U.S.C. § 1836(b)(2)(A)(ii)).
[897] *Id.* at *2.
[898] *Id.* at *3.
[899] *Id.*
[900] *Id.*
[901] *Id.*
[902] *Id.*

asserted that "notice would render the requested relief ineffective," and that district courts in the Ninth Circuit have granted relief in similar circumstances.[903]

Digital Assurance Certification, LLC v. Pendolino

In January 2017, the United States District Court for the Middle District of Florida determined that a certain customer list was not a trade secret.[904] Digital Assurance Certification, LLC ("DAC") employed Alex Pendolino, Jr. as a broker-dealer liaison.[905] Pursuant to his employment, Pendolino signed a confidentiality agreement acknowledging that he would be receiving confidential, trade secret information, and that he would maintain the confidentiality of the information during and after his employment.[906]

Pendolino left DAC on October 10, 2016 to work for a competitor.[907] A forensic computer expert engaged by DAC determined that prior to his departure, Pendolino attached a USB drive to his work computer and accessed every file in DAC's shared-network drive, including files containing the names of DAC's former, current, and potential customers.[908]

As a result, relying on the DTSA, DAC filed an ex parte application for the seizure of the documents, computers, and computer storage devices that DAC believed

---

[903] *Id.*
[904] *Digital Assurance Certification, LLC v. Pendolino*, No. 6:17-cv-72-Orl-31TBS, 2017 WL 320830 (M.D. Fla. Jan. 23, 2017).
[905] *Id.* at *1.
[906] *Id.*
[907] *Id.*
[908] *Id.*

unlawfully contain its customer list.[909] DAC also sought leave of court to file said confidential information under seal, or alternatively, to redact the confidential information contained in the documents obtained by Pendolino.[910]

The law states that customer lists are generally considered trade secrets provided that "(1) the list was acquired or compiled through the industry of the owner of the list and is not just a compilation of information commonly available to the public; and (2) the owner shows that it has taken reasonable efforts to maintain the secrecy of the information."[911] The court found that DAC had satisfied the second prong of the law by restricting employee access to its network by requiring a complex password that had to be updated every ninety days, restricting remote access to its servers, and requiring employees to sign confidentiality agreements regarding customer lists.[912] However, the court found that the first prong was not satisfied.[913] DAC did not adequately explain the method by which the list was created or otherwise show that the information is not readily available from a public source.[914] Thus, the court found that DAC had not met its burden of showing that the customer lists Pendolino allegedly misappropriated were, in fact, trade secrets, and did not grant DAC an order to seal.[915]

---

[909] *Id.*
[910] *Id.*
[911] *Id.* at *2 (quoting *E. Colonial Refuse Serv., Inc. v. Velocci*, 416 So. 2d 1276, 1278 (Fla. 5th DCA 1982)).
[912] *Id.*
[913] *Id.*
[914] *Id.*
[915] *Id.*

Magnesita Refactories Co. v. Mishra

In December of 2016, the United States District Court for the Northern District of Indiana issued a TRO in favor of Magnesita Refactories Company ("Magnesita") after the company alleged its former employee, Surendra Mishra, had violated the DTSA and the Indiana Uniform Trade Secrets Act.[916]

The court had emphasized the severity of a TRO as a form of equitable relief, but ultimately entered the order, which authorized the seizure of a laptop computer owned by Mishra that he used for both business and personal purposes.[917] The court based its decision on a finding that (1) there was a strong likelihood Mishra was conspiring to steal Magnesita's trade secrets contained on the laptop, and (2) the seizure was necessary to prevent impending harm.

To obtain the TRO, Magnesita presented to the court an affidavit from its Vice President of Sales & Marketing detailing emails between Mishra and a former Magnesita employee: Zelber Dettogne do Nasciemento.[918] The emails demonstrated Mishra and Dettogne's intent to create an independent refractory business with a Magnesita supplier, Xiangrong, and at least one individual at a company that had a business cooperation agreement with Magnesita.[919] The emails included discussion points and arrangements for a "kick-off meeting" to take place during the week of December 19,

[916] *Magnesita Refractories Co. v. Mishra*, NO. 2:16-CV-524-PPS-JEM, 2017 WL 655860 (N.D. Ind. Feb. 17, 2017).
[917] *Id.* at *1.
[918] *Id.* at *2.
[919] *Id.*

2016.[920] Furthermore, an email to Mishra stated, "I have just finished [the] company registration paper…using your passport copies."[921]

Mishra claimed that Dettogne was a personal friend and that they were considering forming a company so that Dettogne could obtain a residency work permit to continue living in Dubai and avoid taking his daughter out of her school there.[922] Mishra also claimed that when he saw the email saying that the company had been registered, he called Dettogne and told him he did not want to be part of the company.[923] Ultimately, the court was not persuaded and entered the TRO as requested by Magnesita.

Then, in January 2017, Mishra filed a motion to vacate and argued that the TRO allowing the seizure of his computer was improper under Federal Rules of Civil Procedure Rule 64.[924] Mishra asserted that Magnesita was required to follow the due process requirements in the DTSA's seizure provision and failed to do so.[925] Mishra thus requested that the court vacate all seizure orders and return his computer.[926]

The court held that Rule 64 was inapplicable because it does not apply to the seizure of *property for the purpose of preservation of evidence*.[927] Rule 64 authorizes

---

[920] *Id.*
[921] *Id.* at *3.
[922] *Id.* at *5.
[923] *Id.*
[924] *Magnesita Refractories Co. v. Mishra*, NO. 2:16-CV-524-PPS-JEM, 2017 WL 365619, at *1 (N.D. Ind. Jan. 25, 2017).
[925] *Id.* at *1.
[926] *Id.*
[927] *Id.*

"seizure of a person or property *to secure satisfaction of [a] potential judgment*."[928] The purpose of requesting seizure of Mishra's property—the computer—in this case was so it could be imaged and then returned to Mishra.[929] Therefore, the seizure had nothing to do with securing assets to satisfy a judgment so Federal Rule of Civil Procedure 64 did not apply.[930]

Furthermore, the court recognized that since the DTSA went into effect in May 2016, at least two other courts presiding over cases involving DTSA claims had issued TROs under Federal Rules of Civil Procedure Rule 65 ordering the seizure of property.[931] The DTSA's seizure provision would only apply if seizure could not be accomplished by way of equitable relief under Rule 65, and here the court found that Rule 65 was sufficient.[932] Thus, the court denied Mishra's motion to vacate the orders of seizure.[933]

Following denial of the motion to vacate, Mishra filed a motion to dissolve the TRO in February 2017.[934] In his motion, Mishra argued that the ex parte proceedings were improperly conducted, the scope of the TRO was overly broad and the TRO was facially defective.[935]

The court noted that in an effort to achieve its goal of maintaining the status quo while considering the interests of both parties, it initially granted the TRO authorizing

---

[928] *Id.*
[929] *Id.*
[930] *Id.*
[931] *Id.* at *2 (citing *Earthbound Corp.,* 2016 WL 4418013, at *11; *Panera, LLC*, 2016 WL 4124114, at *2-4).
[932] *Id.*
[933] *Id.*
[934] *Magnesita Refractories Co. v. Mishra*, NO. 2:16-CV-524-PPS-JEM, 2017 WL 655860, at *1 (N.D. Ind. Feb. 17, 2017).
[935] *Id.*

seizure of Mishra's laptop, but left it in the secured custody of the court.[936] The court considered this a "middle ground," which struck a balance between protecting the public interest in preventing trade secret dissemination while taking into account Mishra's privacy interest.[937] Therefore, the court held the TRO was proper in scope.

Finally, Mishra requested that Magnesita be ordered to post a bond because of the risk that some of Mishra's personal information may be disclosed if the device storing the images of his laptop was connected to the Internet.[938] The court denied this request on three grounds.[939] First, Mishra did not offer support for his request.[940] Second, his request was unreasonable given that the imaging would be stored on a closed working system, which posed a much lower risk of exposure than Mishra's everyday online activities.[941] Third, Federal Rules of Civil Procedure Rule 65(c) states that a TRO may only be issued "if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained," whereas, here, Mishra suffered no costs or damages if it was determined that the laptop was improperly seized.[942]

---

[936] *Id.* at *4.
[937] *Id.*
[938] *Id.* at *6.
[939] *Id.*
[940] *Id.*
[941] *Id.*
[942] *Id.*

Cases Discussing the Inevitable Disclosure Doctrine under the DTSA

Another issue courts assessing trade secrets claims regularly confront is the doctrine of inevitable disclosure, which, where applicable, allows for a finding of a trade secret violation based on *threatened* as opposed to actual misappropriations. DTSA cases involving claims of inevitable disclosure are discussed below.

Molon Motor & Coil Corp. v. Nidec Motor Corp.

In May of 2017, the United States District Court for the Northern District of Illinois denied Nidec Motor Corporation's ("Nidec") motion to dismiss as it found Molon Motor and Coil Corporation's ("Molon") allegations presented at least circumstantial evidence that Desai could have inevitably disclosed trade secrets to Nidec in violation of the DTSA.[943]

Molon sued Nidec for violation of the DTSA in addition to other claims.[944] Both companies manufactured fractional and sub-fractional electric motors and generators for various industries and were direct competitors.[945]

Manish Desai ("Desai") was Molon's former Head of Quality Control.[946] Because Desai was responsible for product liability testing, he had access to all of Molon's trade

[943] *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545, 2017 WL 1954531, at *1 (N.D. Ill. May 11, 2017).
[944] *Id.*
[945] *Id.*
[946] *Id.*

secrets and confidential information.[947] While at Molon, Desai was required to sign an employment agreement with a restrictive covenant that banned his unauthorized use of company data.[948] Desai left Molon in June 2013 and began working for a predecessor of Nidec: a competitor of Molon.[949]

Molon alleged that Desai had copied confidential information, including motor design and engineering drawings, motor production inspection protocols, data on motor production tools, quality control test protocols, quality control testing data and reports, and customer communications files, on a portable data drive before beginning employment with Nidec.[950] Molon further alleged that since Desai copied the information, Nidec had continued to use it.[951]

Nidec moved to dismiss the federal and state trade secret claims.[952] Nidec argued that Desai was not prohibited from copying the information while he was still employed by Molon.[953] Furthermore, Nidec argued there was no proof that the company had used any of the information on the drive.[954]

After determining Molon had "plausibly alleged that Desai breached a duty to maintain secrecy" of confidential information, the court then turned to the issue of whether Molon had adequately alleged that Nidec acquired or used the information.[955]

---

947 *Id.*
948 *Id.*
949 *Id.* at *2.
950 *Id.* at *1.
951 *Id.*
952 *Id.*
953 *Id.*
954 *Id.*
955 *Id.* at *5.

Nidec argued that Molon had not shown its ability to prove at trial that Nidec had obtained the information.[956] Molon argued it need not demonstrate this at the pleadings stage because the inevitable disclosure doctrine "allows a plaintiff to 'prove a claim of trade secret misappropriation by demonstrating that defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets.'"[957]

To determine whether the inevitable disclosure doctrine applies, courts look to: (1) the level of competition between the new and former employers; (2) whether the employee held comparable positions with the employers; and (3) the actions the new employer has taken to prevent the former employee from using or disclosing trade secrets.[958]

The court found that Molon had adequately pled that Nidec was a serious competitor.[959] Furthermore, the court found that Desai's responsibilities at the two companies were sufficiently similar; Nidec had even implicitly acknowledged this in its motion to dismiss.[960] Nidec nonetheless emphasized Desai's position in *quality control* as opposed to design in its argument that inevitable disclosure was inapplicable because Desai had no control over the actual design process and only tested the products as they were presented to him.[961] The court found that Desai's extensive responsibilities and access to information made it plausible he could have misappropriated design secrets

---

[956] *Id.*
[957] *Id.* (quoting *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995)).
[958] *Id.* (citing *Saban v. Caremark Rx, LLC*, 780 F. Supp. 2d 700, 734-35 (N.D. Ill. 2001)).
[959] *Id.*
[960] *Id.* at *6.
[961] *Id.*

even if he did not work in design himself.[962] Finally, the court found it was unlikely—particularly at the motion to dismiss stage of litigation—for the new employer to disclose steps it took to safeguard disclosure of the former employer's trade secrets.[963] Therefore, this was not a fatal flaw to Molon's case.

Ultimately, the court denied Nidec's motion to dismiss as it found Molon's allegations presented at least circumstantial evidence that Desai could have inevitably disclosed trade secrets to Nidec in violation of the DTSA.[964]

Mickey's Linen v. Fischer

In September 2017, the United States District Court for the Northern District of Illinois examined the impact of employee deceit on presumptions for and against issuing an injunction based on a violation premised on inevitable disclosure.[965]

Mickey's Linen ("Mickey's") sued its former employee Donald Fischer for misappropriation of trade secrets under the DTSA, as well as other claims.[966] Mickey's leases and launders linens for the hospitality and food service industries.[967] Fischer signed an Employment Agreement with Mickey's when he was hired, which included a Non-Competition provision, a Non-Solicitation provision, and a Confidentiality provision.[968] In his entry-level position as a route representative, Fischer had extensive

---

962 *Id.*
963 *Id.* at *7.
964 *Id.*
965 *Mickey's Linen v. Fischer,* No. 17 C 2154, 2017 WL 3970593 (N.D. Ill. Sept. 8, 2017).
966 *Id.* at *1
967 *Id.*
968 *Id.*

access to customer contacts.[969] Fischer was promoted through the company, but continued to deal primarily with information regarding customer relationships, including pricing plans.[970] In addition, Fischer oversaw a territory reroute due to his familiarity with the customer base.[971] With each promotion, Fischer had access to increasingly more confidential company information, including customer challenges, strategies, plans, and issues.[972]

After being promoted to Key Account Representative in December 2016, Fischer began discussions with one of Mickey's competitors, Alsco.[973] Fischer resigned from Mickey's on January 9, 2017.[974] When asked if he was going to work for Alsco, Fischer denied that he was.[975] Because of this denial, Mickey's made no attempt to shield Fischer from confidential information or to require that he return company property immediately.[976] Instead, Fischer continued to work for Mickey's in his regular capacity for several weeks following notice of his resignation.[977] Before Fischer returned his company cell phone, he wiped all information from it.[978] Additionally, Fischer returned only a fraction of the paperwork he had amassed in his office over the years and failed to return additional company documents from his car.[979]

---

[969] *Id.* at *3.
[970] *Id.*
[971] *Id.*
[972] *Id.* at *4.
[973] *Id.*
[974] *Id.* at *5.
[975] *Id.*
[976] *Id.*
[977] *Id.*
[978] *Id.*
[979] *Id.*

On February 20, 2017, Fischer began working for Alsco and soliciting Mickey's customers.[980] Thereafter, Mickey's filed suit and sought injunctive relief against Fischer.[981] In examining the likelihood of success on the merits of the DTSA claim, the court analyzed Fischer's arguments that the information did not comprise trade secrets and that he did not or would not misappropriate or inevitably disclose the information.[982]

Fischer argued that in order to find a violation based on the doctrine of inevitable disclosure, there must be a "high probability" that the trade secrets will be used rather than just a threatened misappropriation.[983] The court found that the first two factors to determine inevitable disclosure, level of competition between the employers and the employee working in comparable positions with each employer, were not seriously in dispute.[984] Therefore, the court only analyzed whether the actions the new employer took prevented the former employee from using or disclosing trade secrets of the former employer.[985]

In examining the third factor, the court noted that although Alsco did attempt to carve out a territory for Fischer that would not violate the covenants in his Employment Agreement with Mickey's, Alsco had never actually seen the Employment Agreement.[986] Alsco made little attempt to actually discover the terms of the Employment Agreement

---

[980] *Id.* at *6.
[981] *Id.* at *8.
[982] *Id.*
[983] *Id.* at *12.
[984] *Id.*
[985] *Id.*
[986] *Id.*

aside from asking Fischer for a copy, which he failed to provide.[987] Furthermore, the court found that Alsco did nothing to prevent Fischer from soliciting Mickey's customers or using Mickey's trade secrets to do so.[988]

Additionally, given Fischer's "history of deceit," the court was not convinced by Fischer's claim that he would not use Mickey's trade secrets in his job with Alsco.[989] The court cited a similar case where the Seventh Circuit held the district court improperly accepted defendant's assurances not to use trade secrets because the employee had lied about his reason for leaving employment before accepting employment with a competitor.[990]

Fischer also argued that he could not inevitably disclose Mickey's trade secrets because they were too complex to disclose without exact copies.[991] The court found that because Fischer wiped all information from his company cellphone, there was a reasonable presumption that he had misappropriated trade secrets: a rule set forth in *Liebert v. Mazur*.[992] In addition to Fischer's secrecy regarding his plans for employment, the court found that Fischer would use or disclose Mickey's trade secrets to Alsco if he was not enjoined from doing so.[993] Because Mickey's had demonstrated likelihood of

---

[987] *Id.*
[988] *Id.*
[989] *Id.* at *13.
[990] *Lakeview Tech., Inc. v. Robinson,* 446 F.3d 655, 656-58 (7th Cir. 2006).
[991] *Mickey's Linen,* 2017 WL 3970593, at *13.
[992] *Liebert Corp. v. Mazur,* 827 N.E.2d 909, 929 (Ill. App. Ct. 2005).
[993] *Mickey's Linen,* 2017 WL 3970593, at *13.

success on the merits, the motion for preliminary injunction was granted as to the DTSA claims.[994]

UCAR Technology (USA) Inc. v. Li

This case arose after employees, Yan Li, Hua Zhong, Da Huo, and Zhenzhen Kou, resigned from UCAR Technology (USA) Inc. ("UCAR") and allegedly misappropriated its trade secrets and intellectual property.[995] UCAR, a large chauffeured car services provider in China, filed claims against the four former employees—residents of California—for violation of the DTSA and the Computer Fraud and Abuse Act (CFAA), in addition to various common law causes of action.[996] In their answer, defendants claimed that UCAR failed to state a viable DTSA claim and filed various counterclaims.[997] In December 2017, the United States District Court for the Northern District of California granted in part and denied in part a motion to dismiss filed by the defendant-employees, and granted UCAR's motion to dismiss the employees' counterclaims.[998]

The employees alleged that UCAR's DTSA claim was too vague and speculative to support a claim for trade secret misappropriation, because it was based solely on the "inevitable disclosure" doctrine.[999] California courts have been unwavering in their

---

994 *Id.* at *20.
995 *UCAR Technology (USA) Inc. v. Li*, No. 5:17-cv-01704-EJD, 2017 WL 6405620 (N.D. Cal. Dec. 15, 2017).
996 *Id.* at *1.
997 *Id.*
998 *Id.*
999 *Id.* at *3.

rejection of claims based on the "inevitable disclosure" doctrine.[1000] Nonetheless, the court found this case was distinguishable because UCAR's complaint contained additional allegations to support the misappropriation claim that did not rely on the "inevitable disclosure" doctrine.[1001] UCAR alleged that the defendants disclosed trade secrets to third parties to entice third parties to invest in a new company to compete with UCAR.[1002] Specifically, UCAR alleged that Li "effectively conceded" that the defendants had taken UCAR's confidential information and found at least $10 million worth of investment funds for them to start a competing venture that would be worth $70 million.[1003] The court found that UCAR's allegations were sufficient to state a claim at the pleading stage and denied defendants' motion to dismiss UCAR's DTSA claim.[1004] Under a similar rationale, the court also denied defendants' motion to dismiss UCAR's claim under California's Uniform Trade Secrets Act (CUTSA).[1005]

The court also denied defendants' motion to dismiss UCAR's claim of violation of the CFAA.[1006] Defendants argued that the CFAA only prohibits improper "access" to information but does not prohibit "misuse" or "misappropriation" of the information.[1007] Therefore, defendants argued, they had "access" to the information when they were employees and their "access" was not improper.[1008] The court was

---

[1000] *Id.* (citing *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1463 (2002)).
[1001] *Id.*
[1002] *Id.*
[1003] *Id.*
[1004] *Id.*
[1005] *Id.* at *4.
[1006] *Id.*
[1007] *Id.*
[1008] *Id.*

unpersuaded by this argument, especially considering UCAR's allegation that defendants accessed computers after their resignation.[1009]

Case Discussing the Whistleblower Provisions of the DTSA

We are aware of case that has addressed the applicability of the whistleblower provisions in the DTSA. That case is discussed below.

Unum Group v. Loftus

In *Unum Group v. Loftus*, the United States District Court for the District of Massachusetts addressed the whistleblower immunity protections in the DTSA in a December 2016 opinion.[1010] Unum Group ("Unum") brought suit against Timothy Loftus for misappropriation of trade secrets under the DTSA and the Massachusetts Trade Secrets Act, as well as conversion.[1011] Loftus was the Director of Individual Disability Insurance Benefits at Unum. In September 2016, Loftus was caught on tape on three separate occasions leaving the company building with company documents and a laptop.[1012] The laptop was not returned to the company even after numerous requests.[1013] The incidents occurred shortly after Loftus was interviewed by in-house counsel at Unum during the company's investigation into claims practices.[1014]

[1009] *Id.*
[1010] *Unum Grp. v. Loftus*, 220 F. Supp. 3d 143 (D. Mass. 2016).
[1011] *Id.* at 145.
[1012] *Id.* at 146.
[1013] *Id.*
[1014] *Id.*

Unum filed suit and sought injunctive relief.[1015] Unum sought to "(i) enjoin Loftus from copying the documents, (ii) compel Loftus and his counsel to return all of the documents and any of Unum's other trade secret or confidential information in his possession, and (iii) enjoin Loftus from receiving a mirrored copy of the hard drive of his company laptop until Unum has removed or redacted files containing trade secrets or confidential information."[1016] Loftus argued that he was entitled to whistleblower protection under Section 1836(b) of the DTSA, and that Unum therefore was not entitled to relief under the DTSA. Loftus further argued that because the court's jurisdiction over the case was predicated on the DTSA claim, dismissal of the DTSA claim would necessitate dismissal of the complaint, as the court would no longer have jurisdiction over the state law claims.[1017]

Although Loftus asserted that he was entitled to immunity because his trade secret misappropriation was solely for the purpose of informing an attorney of Unum's wrongdoing, the court held that the record lacked facts to support this contention.[1018] At the time of the opinion, Loftus had not filed a lawsuit against Unum and no discovery had revealed the potential legal significance of the documents Loftus took.[1019] The court found this was not enough to qualify for whistleblower immunity under the DTSA.[1020]

[1015] *Id.* at 145.
[1016] *Id.* at 145-46.
[1017] *Id.* at 147.
[1018] *Id.*
[1019] *Id.* at 147.
[1020] *Id.*

The court thus denied Loftus' motion to dismiss and granted Unum's motion for a preliminary injunction.[1021]

Cases Discussing Summary Judgment

A number of cases have adjudicated DTSA claims at the summary judgment stage. Some of those cases are discussed below.

Kuryakyn Holdings, LLC v. Ciro, LLC

In March 2017, the United States District Court for the Western District of Wisconsin granted a motion for summary judgment finding that plaintiff failed to identify its alleged trade secrets sufficiently under the DTSA so as to survive summary judgment.[1022] Kuryakyn Holdings, LLC ("Kuryakyn") is a motorcycle aftermarket parts design company.[1023] Thomas Rudd, the founder and president of Kuryakyn, resigned after twenty-five years with Kuryakyn and started a competing company: Ciro, LLC ("Ciro").[1024] Ciro poached three of Kuryakyn's main designers.[1025] Kuryakyn subsequently brought suit against the defendants alleging that the individual defendants used Kuryakyn's trade secrets to benefit Ciro.[1026]

[1021] *Id.* at 149.
[1022] *Kuryakyn Holdings, LLC v. Ciro, LLC*, 242 F. Supp. 3d 789 (W.D. Wis. 2017).
[1023] *Id.* at 792.
[1024] *Id.*
[1025] *Id.*
[1026] *Id.* at 792-93.

Kuryakyn claimed the following as its trade secrets: design drawings and other engineering information, techniques for design and manufacture of its products, market research and information on consumer demand, cost structures and pricing strategies, budgets and operating plans including "[i]nformation about Kuryakyn's development of a smartphone app for controlling colored lights applied to motorcycles," contact information for customers, contact information for suppliers, solicitations from potential suppliers seeking to serve as distributors, and ideas for new products.[1027] Defendants contended that none of the information Kuryakyn claimed as a trade secret was subject to the DTSA or UTSA because it was publicly available and easily acquired by others.[1028] The court agreed with the defendants and held that Kuryakyn's claims offered vague, generalized descriptions of its purported trade secrets without demonstrating that any specific piece of information meets the statutory definition of trade secret.[1029] The court acknowledged that Kuryakyn's description about the smartphone app was marginally more specific, but still failed to identify what information it claimed was a trade secret.[1030] The description could have meant anything from the mere knowledge that Kuryakyn was developing an app, to the code it was using.[1031]

The court further found that even if it was determined that Kuryakyn sufficiently identified the alleged trade secrets, it failed to take the next required step which is to

---

[1027] *Id.* at 798.
[1028] *Id.*
[1029] *Id.* at 799.
[1030] *Id.*
[1031] *Id.*

demonstrate that the information is not readily ascertainable.[1032] For example, Kuryakyn failed to rebut defendant's claims that much of the allegedly trade secret information is common knowledge in the industry, that Kuryakyn's designs can be reverse engineered, and that Kuryakyn did not take reasonable measures to protect the confidentiality of the information.[1033]

Accordingly, the court granted Ciro's motion for summary judgment on Kuryakyn's trade secret misappropriation claims.[1034]

Yager v. Vignieri

In October 2017, the United States District Court for the Southern District of New York denied cross motions for summary judgment when Jeffrey Yager d/b/a Yager Esthetics/Estetica ("Yager") sued Italia Vignieri for trade secret appropriation.[1035]

Yager operated a plastic surgery practice in New York City and Vignieri began working for the practice in 2011.[1036] Vignieri's primary responsibility was to assist in marketing efforts.[1037] Vignieri often worked from home and sent work documents from her work address to her personal email address, including documents with patient information.[1038]

[1032] *Id.* at 799-800.
[1033] *Id.*
[1034] *Id.*
[1035] *Yager v. Vignieri,* 16cv9367(DLC), 2017 WL 4574487, at *1 (S.D.N.Y. Oct. 12, 2017).
[1036] *Id.*
[1037] *Id.*
[1038] *Id.*

While still employed by Yager, Vignieri began working with the business TS Skin Clinic Spa.[1039] Yager alleged that Vignieri used trade secrets from Yager's practice in this new business venture.[1040] Importantly, after the enactment of the DTSA, Vignieri twice exported patient emails to her personal account.[1041]

In December 2016, Yager filed suit against Vignieri under the DTSA. In April 2017, Yager added TS Cosmetic Surgery & Skin Clinic Spa as a defendant, alleging that Vignieri misappropriated Yager's trade secrets to create and operate the new business.[1042] Both Yager and Vignieri submitted motions for summary judgment in September 2017.[1043]

Summary judgment is proper when "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law."[1044] The DTSA provides a remedy for trade secrets owners whose information is misappropriated.[1045] Misappropriation includes either acquisition or use/disclosure of trade secrets in certain circumstances.[1046] Therefore, to prevail on a motion for summary judgment, there must be no dispute as to the fact that trade secrets were improperly acquired, used, or disclosed.[1047]

[1039] *Id.*
[1040] *Id.*
[1041] *Id.*
[1042] *Id.*
[1043] *Id.*
[1044] F.R.C.P. 56(a).
[1045] *Yager,* 2017 WL 4574487, at *3.
[1046] *Id.*
[1047] *Id.*

The court reasoned that summary judgment was not appropriate because Yager's motion did not focus on the date of Vignieri's alleged acquisition and it was possible Vignieri had obtained all trade secret information before the DTSA was enacted.[1048] Furthermore, the two occasions after the DTSA's effective date when Vignieri emailed information were insufficient to demonstrate improper means of acquiring the trade secrets.[1049] Because the court found there were still questions of fact regarding Vignieri's motivation in sending these emails, it denied the motions for summary judgment for further fact-finding.[1050]

Openwave Messaging, Inc. v. Open-Xchange, Inc.

More recently, the United States District Court for the Northern District of California elaborated on the sufficiency and admissibility of evidence at the summary judgment stage of a proceeding involving a DTSA claim.[1051]

Openwave Messaging, Inc. ("Openwave") sued Open-Xchange, Inc. ("OX") for targeting and hiring numerous people from Openwave's operations in Italy to operate a similar business in the same city.[1052] Openwave alleged that OX improperly received and used Openwave's trade secrets in the process of hiring its employees.[1053] Simultaneous

---

[1048] *Id.*
[1049] *Id.*
[1050] *Id.*
[1051] *Openwave Messaging, Inc. v. Open-Xchange, Inc.*, No. 16-cv-00253-WHO, 2018 WL 2117424 (N.D. Cal. May 8, 2018).
[1052] *Id.* at *1.
[1053] *Id.*

with this litigation, Openwave sought injunctive relief and seizure of property in a proceeding in Turin, Italy.[1054]

OX filed a motion to dismiss the DTSA claim in this case in June 2017 because of the pending litigation in Italy and OX alleged that Openwave had failed to assert its trade secrets adequately.[1055] After an August 2017 hearing, the court converted the motion to dismiss to a motion for summary judgment.[1056] In its brief in opposition of summary judgment, "Openwave identified scant evidence to support misappropriation of any trade secret, and failed to identify its trade secrets."[1057] Instead, Openwave argued that it had not had the opportunity to conduct sufficient discovery.[1058]

Openwave claimed that OX misappropriated trade secrets including customer lists, product pricing information, customer demand information, customer satisfaction surveys, customer mapping information, customer contract forms, Openwave's email platform stack, and other technical data.[1059] In its motion for summary judgment, OX argued that Openwave could not prove (1) ownership of any misappropriated trade secret, (2) any action of trade secret misappropriation by OX, or (3) any damages suffered by Openwave.[1060]

Although the court held that Openwave had adequately disclosed its purported trade secrets to provide "'reasonable notice of the issues which must be met at the time

---

[1054] *Id.* at *2.
[1055] *Id.*
[1056] *Id.*
[1057] *Id.*
[1058] *Id.*
[1059] *Id.* at *3.
[1060] *Id.*

of trial,'" it failed to meet the burden of proving the information was a protectable trade secret.[1061] In regard to the customer information, the court found that Openwave's trade secret disclosure was not admissible evidence and therefore could not be considered for the purposes of summary judgment because it was not accompanied by any declarations or affidavits.[1062] Therefore, the court granted summary judgment to OX regarding the six trade secrets dealing with customer information.[1063] However, the court found that Openwave had demonstrated that its technology stacks are trade secrets because it submitted a deposition of its Chief Technology Officer ("CTO").[1064] The CTO testified to the technology stacks' contents as well as the value of the confidential information.[1065] Furthermore, Openwave submitted a declaration regarding the measures the company took to maintain this information's secrecy.[1066] The court thus held that Openwave had met its burden regarding the trade secret protection of the technology stacks.[1067]

Nonetheless, the court found that Openwave had not demonstrated misappropriation of these trade secrets by OX.[1068] In support of its position, Openwave alleged that there was evidence in the form of emails from a former Openwave employee, interactions between OX and former Openwave employees, OX's success with former Openwave customers, a USB device containing Openwave information, and OX's work

---

[1061] *Id.* at *4 (quoting *Diodes, Inc. v. Franzen,* 260 Cal. App. 2d 244, 253 (1968)).
[1062] *Id.* at *5.
[1063] *Id.*
[1064] *Id.*
[1065] *Id.*
[1066] *Id.*
[1067] *Id.*
[1068] *Id.* at *6.

with one of Openwave's key contacts.[1069] Openwave submitted a ruling from the Turin, Italy court, copies of sales agreements, and a deposition to demonstrate its position regarding this evidence at the summary judgment stage.[1070] The court found that Openwave had not pointed to any evidence beyond its own allegations and that findings from another court are insufficient for the purposes of determining whether to grant summary judgment.[1071] Additionally, the court noted that Openwave had not identified any improper conduct by OX.[1072] Rather, all evidence of record involved subsidiaries of the parent company and the court found there had been a "total failure of proof by Openwave that OX has or had anything to do with OX [Italy's] hiring of Openwave's former Italian employees."[1073] For these evidentiary reasons, the court granted OX's motion for summary judgment.[1074]

Case Discussing Damages under the DTSA

While the focal point of many trade secrets cases is injunctive relief, many trade secrets cases do proceed to the damages stage. The following DTSA case discusses issues related to damages.

[1069] *Id.*
[1070] *Id.*
[1071] *Id.*
[1072] *Id.*
[1073] *Id.*
[1074] *Id.*

Waymo LLC v. Uber Technologies, Inc.

The court in *Waymo LLC v. Uber Technologies, Inc.* issued a host of interesting decisions in the course of that trade secret litigation. One of those decisions is discussed earlier in this article. The court's January 2018 order addressed a party's duty to preserve claims for damages under the DTSA.[1075] In advance of a pretrial conference, the judge asked Waymo and Uber (1) whether acquisition alone is enough to support an unjust enrichment award under the DTSA; and (2) whether Waymo had preserved an unjust enrichment theory based on acquisition of the trade secrets alone.[1076] The court sought clarification on the parties' stances because it believed that under the DTSA, a claim for damages based on unjust enrichment requires actual use or disclosure of the trade secrets as opposed to only acquisition.[1077] Ultimately, the court held that although acquisition of trade secrets may be sufficient to support an unjust enrichment theory, Waymo did not properly preserve this claim and therefore it was precluded from relying on that theory.[1078]

Under Federal Rule of Civil Procedure 26(a)(1)(A)(iii), parties are required to provide "a computation of each category of damages claimed."[1079] Unless a party properly discloses calculations under this rule, it cannot present evidence on these damages at trial except if the court finds its failure to disclose was substantially justified

---

[1075] *Waymo LLC v. Uber Techs., Inc.,* No. C 17-00939 WHA, 2018 WL 466510, at *1 (N.D. Cal. Jan. 18, 2018).
[1076] *Id.*
[1077] *Id.*
[1078] *Id.*
[1079] *Id.*

or harmless.[1080] The parties agreed that acquisition alone was sufficient to support an award for damages under an unjust enrichment theory.[1081] However, Waymo failed to preserve its damages theory based on acquisition alone in any of the submissions filed with the court.[1082]

Waymo set forth multiple arguments why it should have been able to assert an unjust enrichment claim based on damages alone. Waymo argued that because there was no theory of damages specified and Waymo never explicitly said it *would not* seek recovery based on acquisition alone, the company was free to assert any theory of recovery it wished when the time came.[1083] Additionally, Waymo cited discovery responses to demonstrate that there are improper competitive benefits from acquiring trade secrets even if a competitor never intends to actually use them.[1084] Furthermore, Waymo argued that Uber's knowledge of a negative trade secret conferred a benefit to the company by nature of knowing which technologies to *avoid*, even if it did not actually use the trade secret information.[1085] Waymo also asserted that unjust benefits result from improper acquisition of control over information relating to trade secrets. Ultimately, Waymo presented seven reasons why it should not be precluded from presenting an unjust enrichment theory based on acquisition alone and it emphasized

---

[1080] *Id.*
[1081] *Id.*
[1082] *Id.*
[1083] *Id.*
[1084] *Id.*
[1085] *Id.* at *2.

the blurred lines between acquisition and actual use to explain its failure to explicitly state a theory of damages solely from acquisition.[1086]

The court was unpersuaded and found that Waymo's theories throughout the litigation related only to the actual use or disclosure of trade secret information.[1087] The court found that although acquisition was implied as a prerequisite to using or disclosing the information, Waymo had never given the court or Uber any reason to think it was pursuing damages based on acquisition alone.[1088] Furthermore, the court pointed out Waymo's difficulty in articulating its theory of recovery on acquisition even when specifically asked by the court to do so.[1089] The court sensed that Waymo's discovery had been less fruitful in finding evidence that Uber actually used Waymo's trade secret information and that the company was now attempting to fall back on a less stringent theory of recovery.[1090] The court therefore ordered that the jury instructions preclude a damages award based on acquisition alone.

Conclusion

The DTSA is a timely and positive response to the growing problem of trade secret theft, and it will undoubtedly have a substantial impact on this practice area. While the Computer Fraud and Abuse Act has resulted in many trade secrets disputes

[1086] *Id.* at *2-3.
[1087] *Id.* at *3.
[1088] *Id.*
[1089] *Id.*
[1090] *Id.*

being litigated in federal court, the passage of the DTSA will mean most trade secrets cases are likely to be litigated in federal court as is evident from the cases summarized above. Setting aside the likely impact on where trade secret disputes are litigated, the DTSA will assuredly help companies of all sizes confidently and securely protect their innovations and intellectual property as trade secrets, knowing that adequate remedies are available to effectively redress trade secret theft.

Choice Of Law, Venue And Other Procedural Issues In Restrictive Covenant Litigation

Presented By:

John G. Perry
Womble Bond Dickinson (US) LLP, Atlanta, GA

Covenants Not to Compete in Georgia

How to avoid the pitfalls of non-compete agreements – what you don't know *could* hurt you.

Choice of Law and Forum Selection Issues In Non-Compete Agreements

John G. Perry*
G. William Long III
Womble Bond Dickinson (US),
A Limited Liability Partnership
271 17th St., N.W.
Suite 2400
Atlanta, Georgia 30363
(404) 879-2441
John.Perry@wbd-us.com

Thomas J. Gallo
Barnes & Thornburg LLP
Prominence in Buckhead
3475 Piedmont Road, N.E.
Suite 1700
Atlanta, Georgia 30305
(404) 846-1693
www.btlaw.com

* *My thanks to Bill Long and Tom Gallo of Barnes & Thornburg LLP for their years of work in compiling the vast majority of these materials and their permission to use them in this year's presentation.*

January 10, 2019

TABLE OF CONTENTS

I. CHOICE OF LAW ISSUES IN RESTRICTIVE COVENANT AGREEMENTS

In Georgia, absent a contrary public policy, courts will normally enforce a choice of law clause. See, e.g., Neibert v. Computer Scis. Corp., 621 F. App'x 585, 589 (11th Cir. 2015); Benjamin v. Am. Airlines, Inc., CV 213-150, 2015 WL 8968297, at *3 (S.D. Ga. Dec. 15, 2015); DLJ Mortgage Capital, Inc. v. U.S. Money Source, Inc., 1:06-CV-2484-WSD, 2008 WL 115063, at *2 (N.D. Ga. Jan. 9, 2008), citing Carr v. Kupfer, 250 Ga. 106, 107, 296 S.E.2d 560, 562 (1982); Deep Sea Fin., LLC v. British Marine Luxembourg, S.A., CV 409-022, 2010 WL 3603794, at *3 (S.D. Ga. May 13, 2010); Breland v. McDonald's Corp., 1:09-CV-0523-BBM, 2009 WL 10666356, at *7 n.9 (N.D. Ga. Dec. 31, 2009); Branch Banking & Tr. Co. v. Lichty Bros. Constr., Inc., 488 F. App'x 430, 433 (11th Cir. 2012).

A. Choice of Law Issues in Covenants Pre-Dating Georgia's New Restrictive Covenant Law.

Historically, the State of Georgia has a strict public policy against restraints on trade, which has resulted in "employee restriction" contracts in Georgia being subject to strict scrutiny. Where a non-compete covenant in the employment context creates a restraint on trade, it is against Georgia public policy and therefore unenforceable.[1] Georgia's public policy against restraints on trade has resulted in many non-compete covenants being construed under Georgia law, despite the parties' intention to apply the law of another state. See, e.g., Lowe Elec. Supply

---

[1] This policy has its origin in the Georgia Constitution, Article III, Section VI, Paragraph V(c) which provided:

> The General Assembly shall not have the power to authorize any contract or agreement which may have the effect of or which is intended to have the effect of defeating or lessening competition, or encouraging a monopoly, which are hereby declared to be unlawful and void.

O.C.G.A. § 13-8-2 provided:

> A contract which is against the policy of the law cannot be enforced. Contracts deemed contrary to public policy include * * * Contracts in general restraint of trade.

Co. v. Rexel, Inc., 5:14-CV-335 CAR, 2014 WL 5585857, at *9 (M.D. Ga. Nov. 3, 2014); Lapolla Indus., Inc. v. Hess, 325 Ga. App. 256, 266–67, 750 S.E.2d 467, 476 (2013) (affirming trial court's holding that Texas choice of law and forum selection clauses were unenforceable as violative of Georgia public policy because a Texas court would apply Texas law and under Texas law the clauses, which were clearly unenforceable under Georgia law, would likely be blue-penciled and enforced); Carson v. Obor Holding Co., LLC, 318 Ga. App. 645, 654, 734 S.E.2d 477, 485 (2012) (reversing trial court holding regarding enforceability of Florida forum selection clause, holding Florida choice of law clause unenforceable under Georgia law because the restrictive covenants violated Georgia law, and finding a Florida court would apply Florida law to determine the enforceability of the covenants and covenants would likely be enforceable under Florida law); Becham v. Synthes (U.S.A.), 5:11-CV-73 MTT, 2011 WL 4102816, at *7 (M.D. Ga. Sept. 14, 2011), aff'd sub nom. Becham v. Synthes USA, 482 F. App'x 387 (11th Cir. 2012) (Applying Georgia law over Pennsylvania law); Hix v. Aon Risk Servs. S., Inc., 1:11-CV-3141-RWS, 2011 WL 5870059, at *3 (N.D. Ga. Nov. 22, 2011) (Applying Georgia law over Illinois law); Boone v. Corestaff Support Servs., Inc., 805 F. Supp. 2d 1362, 1370 (N.D. Ga. 2011) (Applying Georgia law over Delaware law); Hulcher Servs., Inc. v. R.J. Corman R.R. Co., LLC., 247 Ga. App. 486, 489, 543 S.E.2d 461, 465 (2000) (Applying Georgia law over Texas law). See also Nasco, Inc. v. Gimbert, 239 Ga. 675, 676, 238 S.E.2d 368, 369 (1977) (Applying Georgia law over Tennessee law); Enron Capital & Trade Res. Corp. v. Pokalsky, 227 Ga. App. 727, 730, 490 S.E.2d 136, 139 (1997) (Applying Georgia law over Texas law); Barnes Group, Inc. v. Harper, 653 F.2d 175, 178 n.4 (5th Cir. 1981), cert. denied, 455 U.S. 921 (1982) (Applying Georgia law over Ohio law); Marketing and Research Counselors, Inc. v. Booth, 601 F. Supp. 615, 616 (N.D. Ga. 1985) (Applying Georgia law over Texas law); Lowe Elec. Supply

Co. v. Rexel, Inc., 5:14-CV-335 CAR, 2014 WL 5585857, at *9 (M.D. Ga. Nov. 3, 2014) (Applying old Georgia law over Florida choice of law provision since covenants void under applicable Georgia law, which does not allow blue penciling, whereas Florida does permit blue penciling and covenants might be enforceable under that law; 2014 agreement between employee and company dealing with compensation not sufficient to bring old 2011 agreement under Georgia's new law); Cold Chain Techs., Inc. v. IGH Holdings, Inc., 1:15-CV-2493-SCJ, 2015 WL 12778346, at *4 (N.D. Ga. Aug. 5, 2015) (Applying old Georgia law over Massachusetts choice of law provision since covenants void under applicable Georgia law, which does not allow blue penciling, whereas Massachusetts does permit blue penciling and covenants might be enforceable under that law; employee's recent move to Georgia sufficient nexus to apply Georgia law).

Because Georgia has not adopted the Restatement (Second) § 187(2), Georgia courts need not determine whether Georgia has a "materially greater interest" in applying Georgia law, as opposed to the law of another state, before invalidating a non-compete provision as against Georgia public policy. Convergys Corp. v. Keener, 276 Ga. 808, 809, 582 S.E.2d 84, 85 (2003). See also CS Lakeview at Gwinnett, Inc. v. Simon Property Group, Inc., 283 Ga. 426, 427–28, 659 S.E.2d 359, 361 (2008) (Georgia Supreme Court reaffirms refusal to adopt Restatement (Second) § 187(2)). A party must only have sufficient contacts with the State of Georgia to justify application of Georgia law. Applying this rule, the Eleventh Circuit in Keener v. Convergys Corporation, applied Georgia law to the non-compete at issue, despite a provision providing that Ohio law would govern. 342 F.3d 1264, 1268 (11th Cir. 2003). In a different context, in American Management Services East, LLC v. Fort Benning Family Communities, LLC, the Georgia Court of Appeals held that the Georgia constitution requires that there be

significant contacts between the claims and the state in order to apply Georgia law. 333 Ga. App. 664, 690–92, 774 S.E.2d 233, 253–54 (2015).

As a practical matter, Georgia's application of its own law, contrary to the laws of other states on public policy grounds could potentially allow employees to move to Georgia and file a preemptive lawsuit solely to avoid their non-compete agreements. It also raises the issue of how broadly Georgia courts may impose injunctive relief. In Keener, for example, the court limited injunctive relief to the State of Georgia. In doing so, while the court found that Georgia's public policy could override the policies of other states, it impliedly recognized that it could not impose its public policy on other states. By contrast, in Hostetler v. Answerthink, Inc., the injunctive relief was not limited to Georgia; however, this case had markedly different facts in that the non-compete agreement was executed in Georgia by a Georgia resident who would be working in Georgia. 267 Ga. App. 325, 330, 599 S.E.2d 271, 276 (2004).

The Eleventh Circuit's decision in Palmer & Cay, Inc. v. March & McLennan Companies, could be read to sanction the preemptive lawsuits mentioned above. 404 F.3d 1297 (11th Cir. 2005). In Palmer & Cay, Meathe was a managing director for Marsh. In January 2003, Meathe left Marsh and became president of Palmer & Cay, an insurance broker which was a competitor of Marsh. Meathe moved to Georgia and filed suit in the Northern District of Georgia seeking to avoid application of his non-compete agreements with Marsh. The non- compete agreements at issue contained choice-of-law provisions providing that New York and Illinois law would apply. The court applied Georgia law and held that the agreements were unenforceable under Georgia law. In fashioning relief, relying on Hostetler, the court ultimately held that while injunctive relief should be limited to Georgia, declaratory relief should not be so limited. Thus, Meathe was able to move to Georgia, file a preemptive lawsuit, and avoid application of his

restrictive covenants. In effect, this decision may be read to allow Georgia's policy of refusing to enforce non-compete agreements which may be enforceable under other state's laws to potentially override the policies of other states with more significant contacts, where the employee moves to Georgia for the purpose of filing suit here. Under a broad reading of Palmer & Cay, an employee working in another state, who signs a non-compete agreement which is enforceable under the laws of that state and which contains a choice-of-law provision providing that the other state's law applies, could potentially avoid the non-compete agreement by moving to Georgia and filing suit.

Importantly, only a final judgment, not temporary injunctive relief, has preclusive effect in other jurisdictions. In Hulcher, 543 S.E.2d 461 (Ga. App. 2001), the plaintiff filed suit in Georgia, seeking a declaration that the non-compete at issue was unenforceable. Thereafter, the defendant filed suit in Texas, and obtained preliminary injunctive relief enforcing the covenant. Id. at 487. After the Georgia court entered a final judgment declaring the covenant unenforceable, the defendant appealed, claiming that the final judgment of the Georgia court should be vacated due to the interlocutory injunction entered by the Texas court. The Georgia Court of Appeals disagreed, holding that "only a final adjudication on the merits precludes [another], separate jurisdiction for making a determination on the merits." A final judgment as to enforceability by a Georgia court precludes re-litigation of these issues in other jurisdictions. Id.; See also Hostetler v. Answerthink, Inc., 267 Ga. App. 325, 329, 599 S.E.2d 271, 275 (2004).

In order to avoid the preemptive lawsuits mentioned above, employers can take some actions, including drafting non-compete agreements to be enforceable under the laws of the State of Georgia. As recently recognized in Smallbizpros, Inc. v. Court, where the other state's law does not contravene the public policy of the State of Georgia, it will be applied. 414 F.Supp.2d

1245, 1249 (M.D. Ga. 2006). The court in Smallbizpros applied Michigan law to a covenant not to compete related to territorial restrictions, finding that under either Michigan or Georgia law, the covenant at issue was enforceable. Accordingly, application of Michigan law did not violate Georgia public policy.

B. Choice of Law Issues Under Georgia's New Restrictive Covenant Law.

In 2009, the Georgia General Assembly passed HB 173 (O.C.G.A. § 13-8-2.1) which significantly changed the law of Georgia regarding restrictive covenants. In order to overcome constitutional challenges to the new law, its effectiveness was contingent upon voter approval of an amendment to Article III, Section VI, Paragraph V(c) of the Georgia Constitution. The constitutional amendment was approved in November 2010. The amendment provides:

> (2) The General Assembly shall have the power to authorize and provide by general law for the judicial enforcement of contracts or agreements restricting or regulating competitive activities between or among:
>
> (A) Employers and employees;
>
> (B) Distributors and manufacturers;
>
> (C) Lessors and lessees;
>
> (D) Partnerships and partners;
>
> (E) Franchisors and franchisees;
>
> (F) Sellers and purchasers of a business or commercial enterprise; or
>
> (G) Two or more employers.
>
> (3) The authority granted to the General Assembly in subparagraph (c)(2) of this paragraph shall include the authority to grant to courts by general law the power to limit the duration, geographic area, and scope of the prohibited activities provided in a contract or agreement restricting or regulating competitive

> activities to render such contract or agreement reasonable under the circumstances for which it was made.

Georgia's strong public policy, as had been set forth in Article III, Section VI, Paragraph V(c) of the Georgia Constitution, against any "any contract or agreement which may have the effect of or which is intended to have the effect of defeating or lessening competition, arguably has been changed by the adoption of the constitutional amendment. Now, the General Assembly has the power to authorize certain contracts or agreement "restricting or regulating competitive activities" and has done so with the adoption of O.C.G.A. §§ 13-8-2.1 *et seq*.

There has been confusion about the effective date of the statute. While the Georgia Constitution was amended, the amendment did not contain an effective date. Therefore, pursuant to Georgia Constitution, Art. X, § 1, ¶ 6, the amendment became effective on January 1, 2011. Yet, the new statute was to become effective on the day following the adoption of the constitutional amendment. Arguably, the new statute was unconstitutional. To cure the perceived defect, the General Assembly passed another bill reenacting the original O.C.G.A. § 13-8-2.1 which became effective on May 11, 2011. *Compare* HB 173, 2009 Ga. Laws 99 § 1 *with* HB 30 Georgia Laws 2011.

In any event, both the 2009 and 2011 codification of O.C.G.A. § 13-8-2.1 *et. seq*. provide that it shall apply to contracts entered into on and after the effective date of the statute and shall not apply in actions determining the enforceability of restrictive covenants entered into before such date. See 2011 Ga. Laws 99, § 5 and 2009 Ga. Laws 231, § 4. In Cox v. Altus Healthcare and Hospice, Inc., in reviewing restrictive covenants entered into in 2008, the Court of Appeals did not apply the new statute because the 2009 statute provides that it "shall not apply in actions determining the enforceability of restrictive covenants entered into before" ratification of the constitutional amendment. 308 Ga. App. 28, 706 S.E.2d 660 (2011). Similarly, in Gordon

Document Products, Inc. v. Service Technologies, Inc., the Court of Appeals' review of restrictive covenants entered into in 2003 was "unaffected" by the new statute. 308 Ga. App. 445, 448, 708 S.E.2d 48, 52 (2011). See also Clark v. Johnson Truck Bodies, LLC, CV411-132, 2012 WL 1014827, at *5 (S.D. Ga. Mar. 23, 2012).

The issue of whether the public policy of Georgia has been changed by the constitutional and legislative amendments and their effect on a choice-of-law analysis arose in Boone v. Corestaff Support Services, Inc., 1:11-CV-1175-RWS, 2011 WL 2358666 (N.D. Ga. June 9, 2011) ("Boone I"). In Boone I, both an Employment Agreement and Non-Compete Agreement entered into in 2008 contained a choice-of-law provision stating that Delaware law would govern. Boone sued his former employer in Georgia upon resigning from his employment and sought injunctive and declaratory relief that the restrictive covenants were unenforceable under Georgia law and the application of Delaware law would violate Georgia public policy. Defendants sought dismissal or transfer of the Georgia action. In its initial opinion, the federal court looked to the new Georgia statute and concluded that it "announced a shift in Georgia's public policy, such that it is not in contravention of Delaware law." It noted that the new statute permitted enforcement of reasonable restrictions, expressed a preference for construing restrictive covenants "in favor or providing reasonable protection to all legitimate business interests established by the person seeking enforcement." O.C.G.A. § 13-8-53(a). In addition, the court highlighted the provision empowering courts to "modify" covenants that would otherwise be unreasonable and unenforceable. Based upon those considerations, the court held that it would enforce the Delaware choice of law provision and dismissed the Georgia action, in favor of an action pending in Delaware, because (among other things) the Delaware court "is

more familiar with that state's substantive law and is in a better position to interpret and apply it."

Upon motion for reconsideration, the court reversed itself in Boone v. Corestaff Support Services, Inc., 805 F. Supp. 2d 1362 (N.D. Ga. 2011) ("Boone II"). In Boone II, the court considered the decision of the Court of Appeals of Georgia in Bunker Hill International, Ltd. v. Nations Builder Insurance Services, Inc. 309, Ga. App. 503, 710 S.E.2d 662 (2011) and concluded that Georgia's public policy in effect at the time the restrictive covenants agreement became effective should be considered in determining whether to enforce a choice of law provision. Finding that Delaware law was violative of Georgia's public policy prior to the effective date of the new statute, the court held that it would apply Georgia law in determining the enforceability of the covenants and determined that it would permit the Georgia action to proceed. Ultimately, the court concluded that the restrictive covenants were unenforceable under Georgia law.

In Becham v. Synthes USA, the Court of Appeals affirmed the trial court's application of Georgia law to restrictive covenants despite a Pennsylvania choice of law provision. 482 F. App'x 387, 393 (11th Cir. 2012). In applying Georgia law, the court reasoned that Georgia's public policy disfavoring restrictive covenants was not changed by either ratification of the constitutional amendment in November 2010 or the effective date of HB173. The court concluded that Georgia's public policy regarding restrictive covenants was changed on May 11, 2011, when HB30 was adopted. Since the restrictive covenants at issue were entered into prior to May 11, 2011, Georgia's old law disfavoring restrictive covenants was applied to defeat the covenants.

II. FORUM SELECTION CLAUSES IN RESTRICTIVE COVENANT AGREEMENTS

In Bremen v. Zapata, the Supreme Court of the United States set forth the factors to be considered in determining whether a forum selection clause is enforceable. 407 U.S. 1 (1972). The Court ruled that such clauses are *prima facie* valid and should be enforced unless the opposing party shows that such enforcement would be unreasonable under the circumstances. Id. at 10. A freely negotiated clause should be upheld absent a compelling reason such as "fraud, undue influence, or overweening bargaining power." Id. at 12. In addition, a forum selection clause should be held unenforceable if enforcement "would contravene a strong public policy of the forum in which the suit it brought, whether declared by statute or judicial decision." Id. at 15. To invalidate such a clause based upon the inconvenience of the chosen forum, the opposing party must show that, for all practical purposes, he would be deprived of his day in court. Id. at 18. In Harry S. Peterson Company, Inc. v. National Union Fire Insurance Company, Georgia adopted the United States Supreme Court's analysis with respect to the enforceability of forum selection clauses. 209 Ga. App. 585, 590, 434 S.E.2d 778, 782 (1993). See also Ramsey v. New Times Moving, Inc., 332 Ga. App. 555, 557–58, 774 S.E.2d 134, 136 (2015) ("forum selection clause in an agreement that is not freely negotiated, or is the product of fraud or undue influence is not *prima facie* enforceable.")

The U.S. Supreme Court in Atlantic Marine Construction Company, Inc. v. United States District Court for the Western District of Texas, reaffirmed that federal courts must enforce forum-selection clauses in all but the most exceptional cases. 571 U.S. 49, 134 S. Ct. 568, 187 L. Ed. 2d 487 (2013). The Supreme Court unanimously held that when parties have agreed to a valid forum selection clause, a district court should ordinarily transfer the case to the specified forum, and that transfer should be denied under extraordinary circumstances unrelated to the

convenience of the parties. See also Atmane Amir v. Pomagalski, 1:14-CV-03261-RWS, 2015 WL 3904570 (N.D. Ga. June 25, 2015).

A. Forum Selection Issues in Covenants Pre-Dating Georgia the New Restrictive Covenant Law.

Contrary to choice of law provisions, Georgia courts have consistently enforced mandatory and exclusive forum selection clauses in employment agreements.[2] Iero v. Mohawk Finishing Products, Inc., 243 Ga. App. 670, 534 S.E.2d 136 (2000). Courts have found that these clauses involve procedural, rather than substantive, rights. Lease Finance Group v. Delphi, Inc., 596 S.E.2d 691 (Ga. App. 2004).

In Iero, where the employee failed to show that enforcement of the forum selection clause was unreasonable under the circumstances of the case, the court enforced the clause. See also Hasty v. St. Jude Medical S.C., Inc., CIV.A. 7:06-CV-102(H, 2007 WL 1428733 (M.D. Ga. May 11, 2007) (Forum selection clause "will rarely be outweighed in considering a motion to transfer"); OFC Capital v. Schidtlein Electrical, Inc., 289 Ga. App. 143, 656 S.E.2d 272 (2008); Rode v. St. Jude Medical, S.C., Inc., 1:06-CV-02448-WSD, 2006 WL 3391382 (N.D. Ga. Nov. 22, 2006) (Rejecting argument that transfers to Minnesota would subject employee to law less favorable than Georgia and violate Georgia public policy.); General Pump & Well, Inc. v. Laibe Supply Corporation, CV607-30, 2007 WL 3238721 (S.D. Ga. Oct. 31, 2007) (Forum selection clause given "nearly conclusive weight" in considering whether to transfer an action.); OFC Capital v. Colonial Distributors, Inc., 648 S.E.2d 140 (Ga. App. 2007) (Stating that a freely negotiated forum selection clause "should be upheld absent a compelling reason such as fraud,

[2] Outside the employment context, Georgia courts enforce forum selection clauses. See, e.g., Houseboat Store, LLC v. Chris Craft Corp., 302 Ga. App. 795, 692 S.E.2d 61 (2010); Alcatraz Media, LLC v. Yahoo! Inc., 290 Ga. App. 882, 660 S.E.2d 797 (2008) (Granting motion to dismiss for lack of personal jurisdiction based upon mandatory forum selection clause); Anthem Leather, Inc. v. Kamino International Transport, Inc., CIV.A.1:06-CV-3130JE, 2008 WL 516289 (N.D. Ga. Feb. 25, 2008).

undue influence, or overweening bargaining power."); Lease Fin. Group v. Delphi, Inc., 596 S.E.2d 116 (Ga. App. 2004) ("[v]enue forum selection clauses are *prima facie* valid and should be enforced unless enforcement is shown by the resisting party to be unreasonable under the circumstances."); Carter's Royal Dispos-All v. Caterpillar Financial Services, 609 S.E.2d 116 (Ga. App. 2004) (To invalidate forum selection clause, opposing party must show that "trial in the chosen forum will be so inconvenient that he will, for all practical purposes, be deprived of his day in court."); SR Business Services, Inc. v. Bryant, 600 S.E.2d 610 (Ga. App. 2004).[3] See also Atlantic Pacific Equipment, Inc. v. Graham, 1:12-CV-3306-TWT, 2013 WL 489064 (N.D. Ga. Feb. 8, 2013) (Employee collaterally estopped from challenging a forum selection clause when its enforceability has been decided earlier by another court.)

Contracts containing restrictive covenants, such as non-competition, non-solicitation and non-disclosure provisions, and forum selection clauses have been analyzed by Georgia courts in the context of the strict public policy against contracts in restraint of trade. In Iero v. Mohawk Finishing Products, Inc., a former employee sued in Georgia for a declaration that non-competition and non-disclosure covenants were unenforceable under Georgia law. 243 Ga. App. 670, 534 S.E.2d 136 (2000). The employment agreement contained a forum selection clause requiring that any action be filed in New York. Iero failed to show that a trial in New York would deprive him of his day in court. He also failed to show that the contract was the product of "manifest disparity" of bargaining power or fraud or overreaching. Iero argued that the forum selection clause should be unenforceable because it would be violative of Georgia public policy against restraints of trade in that a New York court would enforce covenants that would not be

[3] In an action arising under the Georgia statutes governing the business of "debt adjusting," however, the Georgia Court of Appeals recently refused to enforce a forum selection clause. The Court of Appeals considered that a choice of law provision and forum selection clause requiring that any action be filed in Texas and governed by Texas law would violate Georgia's public policy relating to debt adjustment agreements. Moon v. GA-Credit Solutions of America, Inc., 304 Ga. App. 555, 696 S.E.2d 486 (2010).

enforced in Georgia. Iero failed to carry his burden of showing that requiring litigation in New York would result in the enforcement of otherwise unenforceable covenants. The Court of Appeals stated: "Under these circumstances, Iero fails to show that the mere enforcement of a freely negotiated forum selection clause violates Georgia public policy. *Indeed, he does not even address whether the New York court would apply New York law*." 243 Ga. App. at 672, 534 S.E.2d at 538 (Emphasis supplied).

The Iero decision left open the question of how Georgia would treat a forum selection clause if the former employee showed that the foreign jurisdiction's law would apply and would permit the enforcement of an otherwise unenforceable covenant. This question was answered in the very recent decision of Bunker Hill International, Ltd. v. Nationsbuilder Insurance Services, Inc., 309 Ga. App. 503, 710 S.E.2d 662 (2011). In Bunker Hill, the Court of Appeals again addressed the issue of whether a forum selection clause in an agreement containing restrictive covenants was enforceable under Georgia law. The forum selection clause required the parties to litigate "any disputes" regarding the agreement in Illinois.

In concluding that the forum selection clause was unenforceable under Georgia law as violative of Georgia public policy, the Court of Appeals began with the premise that procedural questions are governed by the law of the forum – Georgia. 309 Ga. App. at 506, 710 S.E.2d at 665. Citing Iero v. Mohawk Finishing Products, 243 Ga. App. 670, 534 S.E.2d 136 (2000), the Court then noted that forum selection clauses in agreements containing restrictive covenants are enforced "unless the opposing party show that such enforcement would be unreasonable under the circumstances."

> To invalidate such a clause the opposing party must show that trial in the chosen forum will be so inconvenient that he will, for all practical purposes, be deprived of his day in court. A freely

> negotiated agreement should be upheld absent a compelling reason such as fraud, undue influence, or overweening bargaining power.
>
> 243 Ga. App. at 671, 534 S.E.2d at 136.

In addition, a forum selection clause may be invalid "where the clause 'contravenes a strong public policy of the forum in which the suit is brought, whether declared by statute or judicial decision.'" Iero, 243 Ga. App. at 671, 534 S.E.2d 136. Therefore, the Bunker Hill court concluded a party may defeat a forum selection clause "if he can show that (a) at least one of the covenants violate Georgia public policy and (b) such a covenant would likely be enforced against him" by a court in the selected forum. Bunker Hill, 309 Ga. App. at 507, 710 S.E.2d at 666.

The plaintiff in Bunker Hill demonstrated that if the forum selection clause were enforced, an Illinois court would apply Illinois law to the restrictive covenants and enforce covenants that would otherwise be unenforceable under Georgia law. The Court of Appeals then concluded:

> It follows that the agreement's forum-selection provision is void because its application would likely result in the enforcement by an Illinois court of at least one covenant in violation of Georgia public policy. The trial court therefore erred when it granted NBIS's motion to dismiss this action.
>
> 309 Ga. App. at 508, 710 S.E.2d at 667.

In Crump Insurance Services v. All Risks, Ltd., 315 Ga. App. 490, 727 S.E.2d. 131 (2012), a forum selection clause requiring that any legal action be filed in Maryland was enforced. While the Court of Appeals acknowledged that the restrictive covenants would have been unenforceable under Georgia law, it concluded that the employee had failed to show that a Maryland Court would enforce the covenants. In a special concurrence, Judge Blackwell concluded that the employee had failed to show that a Maryland court would likely apply Maryland law.

Similarly, in Pickvet v. Viking Group, Inc., Judge Duffey analyzed an employment agreement with restrictive covenants that provided that Michigan law governed and that exclusive venue lay in a Michigan court. 1:17-CV-320-WSD, 2017 WL 460895 (N.D. Ga. Feb. 3, 2017). The employee had petitioned for a declaratory judgment in Georgia and the employer moved to transfer the case to Michigan. Although Judge Duffey assumed that Michigan law would violate Georgia's public policy, he then held that the employee had made no sufficient showing that the Michigan court would apply Michigan law. Rather, "To the extent applying Michigan law to the Restrictive Covenants would, as Plaintiff claims, offend Georgia's fundamental policy regarding restrictive covenants, the Court predicts the Western District of Michigan, pursuant to Section 187(2)(b), would apply Georgia law," and he transferred the case to Michigan. This shows the importance of demonstrating not only that the foreign law would violate Georgia policy but also that the foreign court would apply the offending law rather than Georgia law.

B. Forum Selection Issues In Agreements Entered Into After Georgia's New Restrictive Covenant Law.

With respect to agreements with restrictive covenants entered into after the effective date of the constitutional amendment and new statute, it may be significantly more difficult to show that litigation in a foreign forum will likely result in an outcome in violation of Georgia public policy. The United States District Court's discussion of the public policy implications of the new constitutional amendment and restrictive covenant statute in Boone I may be a foreshadowing of future decisions. So might Atlantic Pacific Equipment, Inc. v. Graham, in which the employee unsuccessfully sought to bring a declaratory judgment action in Texas, despite a Georgia choice of law and Georgia forum selection clause in his agreement. 1:12-CV-3306-TWT, 2013 WL 489064 (N.D. Ga. Feb. 8, 2013). The employer brought suit in Georgia

and the employee moved to dismiss. The District Court enforced the Georgia provisions. What is interesting is that the employer was the one seeking to have Georgia law apply, since the agreement was signed under the new Act and Georgia's new law was more favorable to enforcement than was Texas law – something that would never have been the case under Georgia's old law.

C. Consent To Jurisdiction Provisions.

It is important to note the difference not only between a forum selection clause and a choice-of-law provision, but also between a forum selection clause and consent to jurisdiction clause. In Georgia, consent to jurisdiction clauses, like forum selection clauses, are *prima facie* valid and should be enforced unless enforcement is shown by the parties to be unreasonable under the circumstances. Lease Finance Group, 596 S.E.2d at 692. However, Georgia courts have recognized an important distinction between these two types of provisions. While forum selection clauses dictate where a suit must be filed, consent to jurisdiction clauses provide only that the parties have consented to jurisdiction in the event that a suit is filed in a particular forum. See, e.g., PNC Bank v. GVTG, LLC, 592 F. App'x 775 (11th Cir. 2014); Bixy, Inc. v. KBI Holdings, LLC, 2007 WL 3407623 (N.D. Ga.) (Permissive forum selection clause gives plaintiff an absolute right to choose the forum and specifies forums to which a defendant cannot object.); Murray v. The Education Resources Institute, Inc., 612 S.E.2d 23 (Ga. App. 2005) (citing Carbo v. Colonial Pacific Leasing Corp., 592 S.E.2d 445 (Ga. App. 2003)). In other words, a consent to jurisdiction clause does not mandate that suit be brought in a particular court. Rather, it simply provides that the parties have consented to jurisdiction in a certain forum, allowing a suit to be brought in a place where jurisdiction and venue might otherwise not be proper. Murray, 612 S.E.2d 23. First State Bank of Nw. Arkansas v. Georgia 4-S Investments LLLP, 715 F.

Supp. 2d 1301 (N.D. Ga. 2010), aff'd sub nom. First State Bank of Nw. Arkansas v. Georgia 4-S Investments LLP, 418 F. App'x 838 (11th Cir. 2011). In Smyrna Plumbing Co., Inc. v. MDH Builders, Inc., CIVA 107CV126 (AAA), 2008 WL 410365 (S.D. Ga. Feb. 12, 2008), the court construed a permissive forum selection clause choosing Richmond County State Court to have waived defendant's right to remove the action to federal court. In First State Bank, supra, the court held that a consent to jurisdiction clause referring to "courts of the State of Georgia" was ambiguous, but under those circumstances meant that suit was permissible in Georgia State Courts, not federal courts in Georgia.

Covenants Not to Compete in Georgia

How to avoid the pitfalls of non-compete agreements – what you don't know *could* hurt you.

Non-Compete Agreements in Alabama, Florida, South Carolina and Tennessee

John G. Perry*
G. William Long III
Womble Bond Dickinson (US),
A Limited Liability Partnership
271 17th St., N.W.
Suite 2400
Atlanta, Georgia 30363
(404) 879-2441
John.Perry@wbd-us.com

Thomas J. Gallo
Barnes & Thornburg LLP
Prominence in Buckhead
3475 Piedmont Road, N.E.
Suite 1700
Atlanta, Georgia 30305
(404) 846-1693
www.btlaw.com

* *My thanks to Bill Long and Tom Gallo of Barnes & Thornburg LLP for their years of work in compiling the vast majority of these materials and their permission to use them in this year's presentation.*

January 10, 2019

TABLE OF CONTENTS

COVENANTS NOT TO COMPETE IN ALABAMA

In June 2015, the governor of Alabama signed into law an Act that substantially revises statutes governing restrictive covenants in Alabama. The law revises Alabama Code § 8-1-1 et seq. and becomes effective on January 2, 2016. Commentary on the new Act states that it will "apply to actions filed after that date even if the contract at issue was written and entered into prior to January 1, 2016." The Alabama Lawyer, Vol. 76, No. 6, pp. 385, 389 (Nov. 2015).

I. INTRODUCTION

Covenants not to compete are disfavored in Alabama as restraints on trade which tend to "deprive the public of efficient service" and to "impoverish the individual." James S. Kemper & Co. v. Cox and Associates, 434 So.2d 1380 (Ala. 1983); Keystone Automotive Industries, Inc. v. Stevens, 854 So.2d 113 (Ala. Civ. App. 2003); Pinzone v. Papa's Wings, Inc., 72 So.3d 620 (Ala. Civ. App. 2010). However, Alabama also has a public policy of enforcing contracts freely entered into between the parties. See Puckett, Taul & Underwood, Inc. v. Schreiber Corn., 551 So.2d 979, 983 (Ala. 1989). A court examining a covenant not to compete makes the ultimate determination as to whether it is adverse to the public interest by balancing these two policy interests. See, e.g., Diamond Talent, Inc. v. Smith, 653 So.2d 290, 291 (Ala. 1995).

Restrictive covenants in Alabama are governed under Alabama Code § 8-1-1, which states, in part:

> (a) Every contract by which anyone is restrained from exercising a lawful profession, trade, or business of any kind otherwise than provided by this section is to that extent void.
>
> (b) One who sells the good will of a business may agree with the buyer and one who is employed as an agent, servant or employee may agree with his employer to refrain from carrying on or engaging in a similar business and from soliciting old customers of such employer within a specified county, city or part thereof as long as the buyer or any person deriving title to the good will from him, or employer carries on a like business therein.

(Part (c) of the statue refers to partnerships).[1] Both non-competition covenants and nonsolicitation covenants are subject to the statute. In order to be enforceable, a restrictive covenant must fall within one of the exceptions set forth in Ala. Code § 8 -1-1(b). Clark Substations, L.L.C. v. Ware, 838 So.2d 360 (Ala. 2002).

In 2006, the Supreme Court of Alabama held that a non-solicitation/non-hire agreement between employers may be valid as to individual employees, even where no valid employer-employee agreement exists. Ex parte Howell Eng'g & Surveying, Inc., 981 So.2d 413, 422–23 (Ala. 2006). In other words, a non-hire agreement between the corporate employers may validly restrain an individual employee, where the agreement is reasonable and does not prevent the employee from practicing in his or her trade or profession. Id.

II. FACTORS CONSIDERED WHEN DETERMINING ENFORCEABILITY

A party seeking to enforce a covenant not to compete has the burden of showing it is not void under § 8-1-1, which governs contract law. Benchmark Medical Holdings, Inc. v. Rehab Solutions, LLC, 307 F. Supp. 2d 1249 (M.D. Ala. 2004); King v. Head Start Family Hair Salons, Inc., 886 So.2d 769 (Ala. 2004); Ware, 838 So.2d at 363. See also Keystone, 854 So.2d at 115; Construction Materials v. Kirkpatrick Concrete, Inc., 631 So.2d 1006 (Ala. 1994). Alabama courts examine four factors in determining whether a covenant is enforceable:

(a) The employer has a protectable interest;
(b) The restriction is reasonably related to that interest;
(c) The restriction is reasonable in time and place; and
(d) It places no undue hardship on the employee.

---

[1] While parts (b) and (c) of the statute are exceptions to the general prohibitions of restrictive covenants, they do not apply to professionals (i.e. doctors, attorneys, accountants). See Thompson v. Wilk, Reimer & Sweet, 391 So.2d 1016 (Ala. 1980); Friddle v. Raymond, 575 So.2d 1038 (Ala. 1991). The court has considered several factors in determining what constitutes a "professional" including: professional training, skill and experience required to perform certain services, the nature of the services offered and the ability or need to make instant decisions. Benchmark Medical Holdings, Inc. v. Barnes, 328 F. Supp. 2d 1236 (M. D. Ala. 2004).

See Systrends, Inc. v. Group 8760, 959 So.2d 1052, 1480 (Ala. 2006); Benchmark. Medical Holdings, Inc. v. Rehab Solutions, LLC, 307 F. Supp. 2d 1249, 1264 (M. D. Ala. 2004); King, 886 So.2d at 771; Nobles-Hamilton v. Thompson, 883 So.2d 1247, 1249 (Ala. Civ. App. 2003); Clark v. Liberty Nat. Life Ins. Co., 592 So.2d 564 (Ala. 1992); DeVoe v. Cheatham, 413 So.2d 1141, 1142 (Ala. 1982).

The party seeking to enforce the covenant has the burden of showing that the agreement is valid under the circumstances of the case. In Jones v. Wedgeworth Pest Control, Inc., an injunction preventing a pest control employee from competing was reversed where counsel for the parties offered no testimony concerning the enforceability of the covenant. 763 So.2d 261 (Ala. 2000).

In Booth v. Newport Television, LLC, a non-compete agreement was unenforceable against an employee when the acquiring company failed to identify the agreement as an asset to be acquired and assigned. 111 So. 3d 719 (Ala. Civ. App. 2011).

A. Protectable Interest of Employer.

An interest is a legally protectable interest where an employer possesses "a substantial right in its business sufficiently unique" to warrant to type of protection contemplated in a restrictive covenant. Devoe v. Cheatham, 413 So.2d 1141, 1142 (Ala. 1982). An employer has a sufficiently protectable interest in restricting an employee from "appropriating valuable trade information and customer relationships to which he had access during the course of his employment." See James S. Kemper, 434 So.2d at 1384. The employer must have a "substantial right" in its business that is sufficiently unique to warrant protection. Id. at 1384; Keystone, 854 So.2d at 115–16. Such a substantial right exists where an employee has access to confidential information, "secret" lists or has had an opportunity to develop confidential customer

relationships. James S. Kemper, 434 So.2d at 1384. In Thompson, 883 So.2d at 1250, the plaintiff health food store had a protectable interest in limiting competition where the defendant had a "long history" of maintaining relationships with many of its customers. See also Clark, 592 So.2d at 566 (former employee's "close and special relationship" with the policyholders constituted a protectable interest of the employer). In Robertson v. C.P. Allen Construction Co., Inc., the Court of Appeals held the employer had a protectable interest in preserving customer relationships developed by a former salesman even though no confidential information was involved. 50 So. 3d 471 (Ala. Civ. App. 2010).

Future business opportunities may also constitute a protectable interest. Benchmark, 328 F. Supp. 2d at 1260. Even if an employee builds client relationships independently of the employer, where he is able to "nurture, maintain, and further develop" those relationships during his employment, the employer may have a protectable interest in those relationships. Keystone, 854 So.2d at 115–16. However, a "simple labor skill" is not a protectable interest of the employer. Thompson, 2003 Ala. 883 So.2d at 1250; Sheffield v. Stoudenmire, 553 So.2d 125, 127 (Ala. 1989) (Information obtained by former employee of insurance company was not a protectable interest where employee did not develop close relationships with policyholders, and did not take information with him).

B. Reasonable Relation To The Employer's Interest.

Restrictions must be considered as reasonably related to the protectable interest identified by the court. Nationwide Mut. Ins. Co. v. Cornutt, 907 F.2d 1085, 1088 (1990) (Ala.). Where restrictions are "in the line of the former employer's business," they have a reasonable relation to the employer's business. Central Bancshares of the South, Inc. v. Puckett, 584 So.2d 829, 831 (Ala. 1991); Cullman Broadcasting Co. v. Bosley, 373 So.2d 830, 835 (Ala. 1979).

C. Reasonableness of Time and Place.

The reasonableness of time and place is dependent on the nature and extent of the business and the surrounding circumstances. See Parker v. Ebsco Industries, 282 Ala. 98, 209 So.2d 383 (Ala. 1968). Courts examine the type of business involved and the scope of the former employee's work. Booth v. WPMI Television Co., 533 So.2d 209, 211 (Ala. 1988) (Upholding a restriction from sales for one year within a 60 mile radius for a former salesman of a television station). For example, to enforce a non-compete clause in a particular territory, the employer must establish that it continues to engage, in the particular locale, the activity that it seeks to prohibit. Nationwide, 907 F.2d at 1088.

A two-year time limitation has been held reasonable for a former employee of a property and casualty insurance brokerage company. James S. Kemper, 434 So.2d at 1384. With respect to territorial restrictions, a non-compete agreement may properly include Alabama, all of Alabama or more than the State of Alabama, depending on the circumstances. Systrends, 959 So.2d at 1280. See also Central Bancshares, 584 So.2d at 830 (territorial restriction in the entire state of Alabama held to be reasonable); James S. Kemper, 434 So.2d at 1385.

Solicitation of specific customers may be validly substituted for a specific territorial limitation. Digitel Corp. v. Delta Com, Inc., 953 F. Supp. 1486, 1496 (M.D. Ala. 1996); Clark, 592 So.2d at 564.

In King v. Head Start Family Hair Salons, Inc., the Alabama Supreme Court reversed an injunction issued against a former employee of a hair salon which prohibited her from working within a two (2) mile radius of any location of her former employer. 886 So.2d 769 (Ala. 2004). The court found the restriction was unreasonably broad and imposed an undue hardship on the employee, because the, employer had over thirty locations in the relevant area, making it

impossible for the employee to find work as a hairdresser. It remanded with instructions to blue-pencil the agreement to preclude competition within a two mile radius of the location where the former employee worked. Id. Under markedly different circumstances, the court in Benchmark, upheld a restriction within seventy-five miles of any of the plaintiff's currently existing clinics within the state of Alabama, finding that defendant's contacts extended throughout the state, in Georgia and into Chattanooga, Tennessee. 328 F. Supp. 2d at 1266.

D. Undue Hardship on the Employee.

Alabama courts will find an undue hardship on the employee where he is prohibited in engaging in "the only trade he [knows] and by which he [can] support himself." Chavers v. Copy Products Co., 519 So.2d 942, 945 (Ala. 1988); King, 886 So. 2d at 771–72. Undue hardship will generally exist where a restriction:

> Imposes on the employee a greater restraint than is reasonably necessary to secure the business of the employer ...regard being had to the injury which may result to the public from restraining the breach of the covenant, in the loss of the employee's service and skill and the danger of his becoming a charge on the public. Clark, 592 So.2d at 567.

In Chavers, a restriction preventing a copier repairman from working for two years within the entire copier service industry within a geographic area of seventy-five (75) miles of his former employer imposed undue hardship where the employee was not skilled in any other line of work. Id. at 944. See also Calhoun v. Brendle, Inc., 502 So.2d 689, 693–94 (Ala. 1986) (Non-compete unenforceable where enforcement would deprive the employee of his livelihood). But see, Eastis v. Veterans Oil, Inc., 65 So.3d 443 (Ala. Cir. App. 2010) (Non-compete enforceable where former employee had worked in a variety of occupations).

By way of contrast, in Clark, there was no undue hardship on an insurance salesman who was prohibited from soliciting or accepting replacement policies from his former employer's

policyholders. 592 So.2d at 566–67. The employee was not prohibited from selling all insurance, or from soliciting new customers. Id.

III. CONSIDERATION NECESSARY FOR A RESTRICTIVE COVENANT IN ALABAMA

Where an employee signs a covenant not to compete at the beginning of his employment, his employment is sufficient consideration. Clark, 592 So.2d at 567. See also Digitel Corp., 953 F. Supp. at 1495. Even where a non-compete covenant is executed after employment begins, the promise of continued employment and payment received constitutes adequate consideration. Daughtry v. Capital Gas Co., 229 So.2d 480, 483 (Ala. 1969). Employment at will is also adequate consideration for a restrictive covenant. See Affiliated Paper Co. v. Hughes, 667 F. Supp. 1436 (N.D. Ala. 1987).

A covenant that is signed prior to inception of an employee/employer relationship is unenforceable. Pitney Bowes, Inc. v. Berney Office Solutions, 823 So.2d 659 (Ala. 2001). The employer/employee relationship must exist at the time the agreement is executed. Clark, 838 So.2d at 364; Dawson v. Ameritox, Ltd., 571 Fed. Appx. 875 (11th Cir. 2014).

IV. WILL AN ALABAMA COURT "BLUE PENCIL" AN OVERBROAD COVENANT?

Alabama courts have the discretion to "blue pencil" overbroad non-compete covenants. Systrends, 959 So.2d at 1280; Benchmark, 328 F. Supp. 2d at 1264; Thompson, 883 So.2d at 1251; King, 886 So.2d 769. As stated by the Alabama Supreme Court: "A court of equity has the power to enforce a contract against competition although the territory or period stipulated may be unreasonable, by granting an injunction restraining the [employee] from competing for a reasonable time and within a reasonable area." Mason Corp. v. Kennedy, 286 Ala. 639, 244 So.2d 585, 590 (Ala. 1971); Thompson, 883 So.2d 1251 (affirming "blue penciling" of

geographic limitations of agreement); Dobbins v. Getz Exterminators of Ala., Inc., 382 So.2d 1135, 1138 (Ala. Civ. App. 1980) (Affirming modification of territorial limitation in agreement).

V. RELIEF AVAILABLE FOR A BREACH OF A RESTRICTIVE COVENANT

Trial courts in Alabama may issue an injunction for breach of a restrictive covenant. Ormoco Corporation v. Johns, 869 So.2d 1109 (Ala. 2003); Sheffield, 553 So.2d at 125. The party seeking an injunction must show: (1) without an injunction the plaintiff will suffer immediate and irreparable injury; (2) plaintiff has no adequate remedy at law; (3) plaintiff has at least a reasonable chance of success on the merits; and (4) the hardship imposed on the defendant does not unreasonably outweigh the benefit to the plaintiff. Pirtek, USA LLC v. Whitehead, CIV.A. 05-0242-CG-C, 2006 WL 2038651, at *2 (S.D. Ala. Apr. 27, 2006); Ormoco, 869 So.2d at 1113; Seymour v. Buckley, 628 So.2d 554, 557 (Ala. 1993); CraneWorks, Inc. v. RPM Cranes, LLC, 239 So. 3d 561 (Ala. 2017). A rebuttable presumption of irreparable injury exists where an employee allegedly breaches such a covenant. Ormoco, 869 So.2d 1117. The employer must show: (1) that a valid agreement exists; (2) that it has a protectable interest; and (3) that the former employee is actively competing with the former employer in the same geographic area in violation of the agreement. Id. at 1119. The employee may then rebut this presumption.

Damages may also be recoverable. In a breach of contract action in Alabama, the measure of damages is "an amount sufficient to return the plaintiff to the position he would have occupied had the breach not occurred." Systrends, 959 So.2d at 1280; Aldridge v. Dolbeer, 567 So.2d 1267, 1269 (Ala, 1990). See also Clark, 592 So.2d at 567; Buckley v. Seymour, 679 So.2d 220, 225 (Ala. 1996). As with all breach of contract actions, the plaintiff has the burden of proving the amount of damages sustained from a breach of restrictive covenant, and damages

may not be speculative. Clark, 592 So.2d at 567; Systrends, 959 So.2d at 1280. Where there are no substantial damages, nominal damages are recoverable. See James S. Kemper, 435 So.2d at 1385. Nominal damages should be "minimal awards" for technical violations of legal rights or when no actual damages have been proven. Roberson v. C.P. Allen Const. Co., Inc., 50 So.3d 471 (Ala. Civ. App. 2010) (Reversing award of $25,000 nominal damages). The grant or denial of injunctive relief has no bearing on whether a plaintiff can recover damages. See Cullman Broadcasting Co. v. Bosley, 373 So.2d 830, 837 (Ala. 1979).

VI. CHOICE OF LAW

Parties in Alabama are generally free to determine which state's law should apply to their contracts. Where there is no choice made, Alabama follows the Restatement (2d) of Conflicts §§ 187 and 188, which provides that the law of the state with the "most significant relationship" to the transaction will apply. But see Core Laboratories LP v. AMSPEC, 16-0526-CG-N, 2018 WL 2144355 (S.D. Al. May 9, 2018) (holding under doctrine of *lex loci contractus*, Louisiana law would apply in the absence of a New Jersey choice of law provision in a contract formed in Louisiana, so any conflict between New Jersey law and Alabama public policy would not matter, but also finding Alabama did not have a materially greater interest). However, similar to Georgia, where the law which would ordinarily be applicable violates the public policy of Alabama, the parties' choice of law is not given effect. Crown Castle USA, Inc. v. Howell Eng'g & Surveying, Inc., 981 So. 2d 400, 411–12 (Ala. Civ. App. 2005), rev'd on other grounds sub nom. Ex parte Howell Eng'g & Surveying, Inc., 981 So. 2d 413 (Ala. 2006); Benchmark, 307 F. Supp. 2d at 1262. A court will not enforce a covenant in Alabama against an Alabama resident where it is void under Alabama law. Id. See also Cherry Bekaert & Holland v. Brown, 582 So.2d 502, 506 (Ala. 1991); Buckley, 679 So.2d at 220.

In cases where another state's law is chosen to govern the restrictive covenant and is not in conflict with Alabama's public policy, it will be applied. Sylvan Learning, Inc. v. Learning Solutions, Inc., 795 F. Supp. 1284 (S.D. Ala. 2011) (Applying Maryland law); Sylvan Learning, Inc. v. Gulf Coast Educ., Inc., 1:10-CV-450-WKW, 2010 WL 3943643 (M.D. Ala. Oct. 6, 2010); Movie Gallery US, LLC v. Greenshield, 648 F. Supp. 2d 1252 (M.D. Ala. 2009) (applying Montana law in determining that a non-compete agreement was unenforceable due to a lack of consideration); Physiotherapy Assocs., Inc. v. Deloatch, 1:16-cv-02014-ACA, 2018 WL 4409349 (N.D. Ala. Sept. 17, 2018) (applying Pennsylvania law).

In the recent case of Ex parte PT Solutions Holdings, LLC, an Alabama employee signed a restrictive covenant agreement in 2014, which required that any actions be brought in Fulton County Superior Court in Georgia. 225 So. 3d 37 (Ala. 2016). The agreement was to be governed by Georgia law. The employee sued in Alabama for a declaratory judgment that the non-compete covenant was unenforceable under Alabama statutory law because she was a "professional." The employee asked the court to ignore the forum selection clause because, *inter alia*, it violated Alabama's public policy. The Alabama Supreme Court held that the employee would have to show that the forum selection clause itself violated Alabama's public policy. A showing of the unenforceability of the non-compete clause under Alabama law was not sufficient. It is unclear whether the result would have been different had the employee expressly and carefully demonstrated that the Georgia court was likely to enforce the covenant under Georgia's new law.

Even more recently, in DJR Associates, LLC v. Hammonds, the court engaged in an interesting analysis of an employment agreement between an Alabama company and its former employee who had worked for the company in Georgia and, after termination of the

employment, had commenced competing in Georgia. 241 F. Supp. 3d 1208 (N.D. Ala. Mar. 13, 2017). The agreement was formed in Georgia but provided that its restrictive covenants were governed by Alabama law. After a thorough and complex analysis of the laws of both states, the DJR court decided that Georgia law should apply to the noncompete and nonsolicitation covenants, but Alabama law should apply to the nondisclosure covenant. Moreover, even though the court ruled that the noncompete and nonsolicitation covenants were void under the applicable new Georgia law (and apparently declined to reform them), it then said that those covenants could be enforced in Alabama, but not in Georgia, and entered injunctive relief accordingly. This appears to be a one-off decision based on a very specific fact pattern, but it warrants review prior to deciding whether to bring an action in Alabama or Georgia under similar circumstances.

COVENANTS NOT TO COMPETE IN FLORIDA

I. INTRODUCTION

Covenants not to compete in the State of Florida are governed by statute. See F.S.A. § 542.335. The statute applies to all covenants that became effective on or after July 1, 1996. The previous statute, F.S.A. § 542.33, is still effective for all covenants effective prior to July 1, 1996. See Scarbrough v. Liberty National Life Ins. Co., 872 So.2d 283 (Fla. Dist. Ct. App. 2004); North American Products Corp v. Moore, 196 F. Supp. 2d 1217, 1228 (M. D. Fla. 2002) (Enforceability of a covenant not to compete governed by statute in effect at the time the agreement was entered into).

Accordingly, three different sets of rules apply to non-compete covenants in Florida: (1) Contracts effective before June 28, 1990; (2) Contracts effective on or after June 28, 1990 but before July 1, 1996, and; (3) Contracts effective on or after July 1, 1996. American Residential Servs., Inc. v. Event Technical Servs., Inc., 715 So.2d. 1048 (Fla. Dist. Ct. App. 1998); Cooper v. Thomas Craig & Co., LLP, 906 So.2d 378 (Fla. Dist. Ct. App. 2005).

II. FACTORS TO BE CONSIDERED WHEN DETERMINING ENFORCEABILITY

FSA § 542.335(1) provides that covenants restricting competition are valid "so long as such contracts are reasonable in time, area, and line of business." Such contracts must be in writing and signed by the party against whom enforcement is being sought. F.S.A. § 542.335(1)(a). In order for an enforceable covenant to exist, two additional requirements must be met. First, there must be a "legitimate business interest" of the employer which justifies such a covenant. F.S.A. § 542.355(1)(b); Winmark Corp. v. Brenoby Sports, Inc., 32 F. Supp. 1206 (S.D. Fla. 2014); Milner Voice & Data, Inc. v. Tassy, 377 F. Supp. 2d 1209 (S.D. Fla. 2005); Advantage Digital Systems, Inc. v. Knaus, 870 So.2d 111 (Fla. App. 2 2003). Second, the

restraint within the contract must be "reasonably necessary to protect the legitimate business interest or interests justifying the restriction." F.S.A. §542.355(1)(c). [2]

When considering the enforceability of a covenant, a court must hear evidence as to the reasonableness and scope of the covenant at issue. Whitby v. Infinity Radio Inc., 951 So. 2d 890 (Fla. Dist. Ct. App. 2007) (Reversing trial court ruling on enforceability of covenant where court did not hear evidence as to reasonableness and scope)

A. Legitimate Business Interest.

FSA § 542.355(1)(b)(1) - (5) lists five protected business interests under Florida law, but expressly provides that this it is not an exclusive list:

(1) Trade secrets;
(2) Confidential business or professional information (not otherwise a trade secret);
(3) Substantial relationships with prospective or existing customers or clients;
(4) Customer goodwill associated with a certain practice, geographic location or marketing area; and
(5) Specialized training.

The mere desire to avoid competition is not a legitimate business interest. Pirtek USA, LLC v. Wilcox, 606CV566ORL31KRS, 2006 WL 1722346 (M.D. Fla. June 21, 2006). With respect to customer relationships, Florida courts have held that the proper inquiry focuses on the relationship between the employer and its prospective and existing customers, not on the relationship between the employee and customers. Milner Voice & Data, Inc., 377 F. Supp. 2d at 1218.

Where the plaintiff is no longer in business at the time it attempts to enforce the covenant, it has no legitimate business interest to protect. Wolf v. James G. Barrie, P.A., 858

[2] The statute allows enforcement of non-compete covenants by successors or assignees only where the contract expressly authorizes enforcement by an assignee or successor. F.S.A. § 542.335(1)(f)(2); Marx v. Clear Channel Broadcasting, Inc., 887 So.2d 405, 406 (Fla. App. 4 Dist. 2004); DePuy Orthopaedics, Inc. v. Waxman, 95 So.3d 928 (Fla. App. 1st Dist. 2012). However, the contract does not have to include the statutory language in order to be enforceable by the assignee or successor. Patel v. Boers, 68 So.3d 380 (Fla. App. 5 Dist. 2011).

So.2d 1083 (Fla. Dist. Ct. App. 2003). Additionally, where the employer seeks to protect information that is not confidential and is commonly known in the industry, no legitimate business interest exists. Pirtek, 2006 WL 1722346, at *3; Colucci v. Kar Kare Auto. Grp., Inc., 918 So.2d 431 (Fla. Dist. Ct. App. 2006); Anich Industries, Inc. v. Raney, 751 So. 2d 767 (Fla. Dist. Ct. App. 2000) (Where employee did not have a substantial relationship with the customers, was given little training, had no access to trade secrets or confidential information, and customers were commonly known in the industry, there was no legitimate business interest).

However, a legitimate business interest exists where the employee has access to confidential and proprietary business information. Proudfoot Consulting Co. v. Gordon, 576 F.3d 1223 (11th Cir. 2009); AutoNation v. O'Brien, 347 F. Supp. 2d 1299, 1304 (S.D. Fla. 2004). See North American Products, 196 F. Supp. 2d at 1228 (legitimate business interest existed where employee gained knowledge of former employer's customers and their purchasing history, needs and specifications); Balasco v. Gulf Auto Holding, Inc., 707 So.2d. 858, 860 (Fla. Dist. Ct. App. 1998) (Employer had legitimate business interest in "specialized training" where it invested time and money in training sales people in a certain manner); Milner, 377 F. Supp. 2d at 1218 (relationship with customers and specialized training given to employee was legitimate business interest); Estetique, Inc. v. Xpamed LLC, 0:11-CIV-61740, 2011 WL 4102340 (S.D. Fla. Sept. 15, 2011) (Protection of client contact information is a legitimate business interest). In addition, an employer need only show that the former employee, by working with a competitor, "endangers" the confidential information. "It was not decisive whether the employee had ever used the information or intentionally breached the agreement's confidentiality clause." S. Wine & Spirits of Am., Inc. v. Simpkins, 10-21136-CIV, 2011 WL 124631 (S.D. Fla. Jan. 14, 2011).

The statute provides "substantial" relationships with "specific prospective or existing customers" is a legitimate business interest. In The University of Florida v. Sanal, where the plaintiff could not identify any *specific* prospective patients with whom the doctor had interfered, it failed to establish a legitimate business interest. 837 So.2d 512 (Fla. App. 1 Dist. 2003). See also GPS Industries, LLC v. Lewis, 691 F. Supp. 2d 1327 (M.D. Fla. 2010) (Failure to show substantial relationship with customers who were allegedly solicited); Litig. Sols., LLC v. McGonigal, 09-14374-CIV, 2010 WL 111822 (S.D. Fla. Jan. 11, 2010). However, in Advantage Digital Systems, Inc., where the employer proved it had a specific customer base, has a legitimate business interest. 870 So.2d at 114. See also Atomic Tattoos, LLC v. Morgan, 45 So.3d 63 (Fla. Dist. Ct. App. 2010); JonJuan Salon, Inc. v. Acosta, 922 So.2d 1081, 1084 (Fla. Dist. Ct. App. 2006) (Customer relationships were legitimate business interest); Litwinczuk v. Palma Beach Cardiovascular Clinic, 939 So.2d 268 (Fla. Dist. Ct. App. 2006) (Where doctor began practicing a few blocks from clinic and saw 49 of clinic's prior patients, temporary injunction enforcing non-compete was affirmed). However, relationships with vendors of a former employer are not legitimate business interests meriting protection. Concrete Surface Innovations, Inc. v. McCarty, 610CV568ORL28GJK, 2010 WL 1930971 (M.D. Fla. May 13, 2010). According to one Florida court, protection against solicitation of former employer's "referral sources" is a legitimate business interest. Infinity Home Care, LLC v. Amedisys Holdings, LLC, 180 So. 3d 1060 (Fla. Dist. Ct. App. 2015). However, about one month later, another Florida court in Hiles v. Americare Home Therapy, Inc., disagreed and held that "referral sources" of unidentified potential patients are not a protectable interest, acknowledging the conflict between the two cases. 183 So. 3d 449 (Fla. Dist. Ct. App. 2015), decision quashed sub nom. White v. Mederi Caretenders Visiting Servs. of Se. Florida, LLC, 226 So.3d 774 (Fla.

2017). In White, the court discussed at length the diverging approaches of these courts, engaged in statutory construction, and held "that section 542.335, Florida Statutes, is non-exhaustive and does not preclude the protection of referral sources; hence, home health service referrals may be a protected legitimate business interests depending on the context and proof adduced. As a result, we approve the decision in White and quash the decision in Hiles." 226 So.3d 774, 786 (Fla. 2017). The protection of referral sources was again confirmed in Ansaarie v. First Cardiovascular Institute, P.A., 252 So. 3d 287, 291 (Fla. Dist. Ct. App. 2018) (rejecting argument that physician referral sources are not legitimate business interests in light of holding in White).

In order to be protected, information gained by an employee during his or her employment does not have to constitute a "trade secret." It is sufficient that the information is confidential. See F.S.A. §542.335(1)(b)(2); American Residential Servs., Inc., 715 So.2d. at 1049 (holding that employer had a legitimate business interest in "[v]aluable confidential business or professional information that otherwise [did] not qualify as trade secrets.")

B. Reasonably Necessary Restraint.

Under the statute, restraints on competition must be reasonably necessary to protect the employer's legitimate business interests. The statute outlines presumptively reasonable periods of time for non-compete covenants. Each of these presumptions is rebuttable. F.S.A. § 542.335(1)(d).

Where the covenant applies to a former employee, agent or independent contractor (not involving sale of a business), the court presumes reasonableness of a covenant 6 months or less and unreasonableness of a covenant longer than two (2) years. F.S.A. § 542.335(1)(d)(1).

A covenant involving a distributor, dealer or franchise (again not involving sale of a business) will be presumed reasonable if less than one year, and unreasonable if greater than three years. F.S.A. § 542.335(1)(d)(2).

A covenant involving the sale of a business will be presumed reasonable if less than three years, and unreasonable if greater than seven years. F.S.A. § 542.335(1)(d)(3).[3]

In Balasco, examining a covenant under the parameters set up by the statute, the court found a three year restrictive period presumptively invalid. 707 So.2d. at 860. When the employer did not rebut this presumption, the court modified the time restriction to two years, as provided under the statute. Id.

Florida courts have held that a non-compete period may be equitably extended to allow for "what was intended in the bargain." Michele Pommier Models, Inc. v. Michele Pommier Diel, 886 So. 2d 993 (Fla. Dist. Ct. App. 2004). In other words, where an employee violates a valid non-compete agreement, the court may extend the restriction for a period contemplated in the agreement to begin from the date of its holding rather from the termination of employment. The Southern District of Florida recently reaffirmed that the court has discretion to equitably extend the time of the non-compete restrictions as has the Eleventh Circuit in Proudfoot Consulting Co. v. Gordon, 576 F.3d 1223 (11th Cir. 2009). See Sunbelt Rentals, Inc. v. Dirienzo, 487 F. Supp. 2d 1361, 1363 (S.D. Fla. 2007) (Holding that the equitable nature of preliminary injunctions and the Supreme Court of Florida's decision in Capelpouto permit, but do not require, a court to equitably extend a preliminary injunction to run from the time of entry of the preliminary injunction). Courts have reasoned that employers are "entitled" to the agreed

[3] A covenant protecting trade secrets may be longer, and is presumed reasonable if 5 years or less and unreasonable if over 10 years.

upon "competition-free" period. Capelpouto v. Orkin Exterminating Co., 183 So.2d 532, 535 (Fla. 1966). However, where an employer does not file suit until after the expiration of the non-compete agreement, the time period may not be equitably extended. Michele Pommier, 886 So.2d at 995.

In Anakarli Boutique, Inc. v. Ortiz, the court held that where there has been a delay in the entry of a non-compete injunction, the party seeking enforcement is entitled to the enforcement for the full non-compete period set forth in the agreement. 152 So.3d 107 (Fla. App. 4 Dist. 2014). In Anakarli, the former employer had appealed the denial of an injunction and prevailed on appeal, but the time period for enforcement of the non-compete had expired when the action was remanded.

The 1996 statute does not specify parameters for reasonable geographic restrictions, giving trial courts discretion to address whether such restrictions are reasonable. See, e.g. Dyer v. Pioneer Concepts, Inc., 667 So.2d. 961 (Fla. App. 2 Dist. 1996). The court considers whether the restriction is so broad that it is "oppressive" on the employee's ability to support himself. Availability, Inc. v. Riley, 336 So.2d. 668 (Fla. Dist. Ct. App. 1976) (Reversing the lower court's determination that a geographic restriction was too broad; the employee was "otherwise well able to support himself and his family"). In GPS Industries, LLC v. Lewis, the court refused to enforce a "global" restrictive covenant as "patently unreasonable." 691 F. Supp. 2d 1327 (M.D. Fla. 2010). If a geographic restriction is overbroad, or lacking altogether, the court has discretion to determine under the facts of the case what a reasonably limited geographic area would be, and enforce the covenant within that area. Kofoed Public Relations Associates, Inc. v. Mullins, 257 So.2d 603, 605 (Fla. Dist. Ct. App. 1972). See also Orkin Exterminating Co., Inc. v. Girardeau, 301 So.2d. 38 (Fla. Dist. Ct. App. 1974), cert. denied, 317 So.2d. 75 (Fla. 1975)

(Modifying a covenant containing a geographical restriction which included a larger area than the employee's former work area). In Ameripath, Inc. v. Wetherington, the trial court limited the territorial restriction of 100 miles only to the office where the former employee worked rather than all of the employer's offices. 10-60766-CIV, 2011 WL 1303804 (S.D. Fla. Apr. 4, 2011). Lack of a geographic restriction not fatal when the non-compete provision was limited to customers with whom former employees had business related contact. Environmental Services, Inc. v. Carter, 9 So.3d 1258 (Fla. Dist. Ct. App. 2009).

C. Other Factors Considered By Florida Courts Under the 1996 Statute.

A Florida court is not to apply any rules which require it to construe the covenant narrowly against the drafter or against enforcement. F.S.A. § 542.335 (l)(h). Courts are also statutorily required to construe covenants "in favor of providing reasonable protection to all legitimate business interests established by the person seeking enforcement." Id. AutoNation, 347 F. Supp. 2d at 1304. The statute also provides that courts:

(1) Should not consider individual economic hardship that may be caused to the person against whom enforcement is sought.[4]
(2) May consider as a defense, the fact that the person seeking enforcement no longer does business in that area /line of business sought to be protected, only if the discontinuance of any such business is not the result of a violation of the covenant.
(3) Must consider all relevant legal and equitable defenses; and
(4) Must consider the effect of enforcement on the public health, safety and welfare.

See F.S.A. § 542.335(1)(g)(1) - (4).

In TransUnion Risk and Alternative Data Solutions, Inc. v. MacLachlan, the court held that in federal court actions the trial court must consider "individual economic hardship" in applying Rule 65 standards—contrary to F.S.A. § 542.335(1)(g)(1). 625 Fed. Appx. 403 (11th

[4] Compare Availability, Inc., 336 So.2d at 670, which considered the "oppressive" effect on the employee, and his ability to support his family. This case was decided in 1976, under Florida's 1975 non-compete statute.

Cir. 2015). The court further held, however, that the statutory presumption of irreparable injury is not inconsistent with Rule 65.

In Florida Digestive Health Specialists, LLP v. Colina, the trial court was reversed for denying an injunction against a former physician employee after considering the individual economic hardship the injunction would inflict. 202 So.3d 94 (Fla. Dist. Ct. App. 2016).

Florida law considers that "the public has an interest in the enforcement of restrictive covenants." North American Products, 196 F. Supp. 2d at 1232. Therefore, a court may not refuse enforcement of an otherwise enforceable restrictive covenant on the ground that it violates public policy, unless the public policy is specified by the court and the policy requirements substantially outweigh the need to protect the business interests of the person seeking enforcement. F.S.A. § 542.335(1)(1). See North American Products, 196 F. Supp. 2d at 1232 (Florida sharply limits the use of the "contrary to public policy" defense to enforcement to a restrictive covenant.); Leighton v. First Universal Lending Group, Inc., 925 So.2d 462 (Fla. Dist. Ct. App. 2006) (Affirming injunction against former employee, stating: "in determining the enforceability of noncompete clauses, the trial court must consider all applicable legal and equitable defenses.").

Included among Section (g)(3) of the statute is the employer's breach of the contract. The court in Benemerito & Flores, M.D.'s P.A. v. Roche, M.D., affirmed the denial of an injunction against the employee, after considering the fact that the employer had breached the employment contract by reducing the amount of bonus to which she was entitled. 751 So.2d 91 (Fla. Dist. Ct. App. 1999). See also Leighton, 925 So.2d at 464. But see, Reliance Wholesale, Inc. v. Godfrey, 51 So.3d 561 (Fla. Dist. Ct. App. 2010) (Employer must breach a "dependent covenant" in order to provide a defense to former employee); Richland Towers, Inc. v. Dentono,

139 So.3d 318 (Fla. Dist. Ct. App. 2014) (Non-payment of bonus was an independent covenant and did not provide defense).

III. CONSIDERATION NECESSARY FOR A RESTRICTIVE COVENANT IN FLORIDA

Continued employment is sufficient consideration to support a covenant not to compete, even where the employment is at-will. Open Magnetic Imaging, Inc. v. Nieves-Garcia, 826 So.2d 415, 417 (Fla. Dist. Ct. App. 2002); Balasco, 707 So.2d. at 860. See also Tasty Box Lunch Co. v. Kennedy, 121 So.2d. 52, 54 (Fla. Dist. Ct. App. 1960). In Kroner v. Singer Asset Finance Co., L.L.C., a non-compete agreement contained in a Settlement Agreement, under which Singer relinquished its right to pursue certain claims, was held to be adequately supported by consideration. 814 So.2d 454 (Fla. Dist. Ct. App. 2001).

However, where the employment agreement between the parties has expired, and the employee continues to work under an oral agreement, the covenant contained in the original written agreement will likely be unenforceable. Gran v. Prime Mgmt. Group, Inc., 912 So.2d 711 (Fla. Dist. Ct. App. 2005) (Florida law requires written renewal of the employment agreement to enforce covenant.). See Fla. Stat. § 542.335(1)(a) ("A court shall not enforce a restrictive covenant unless it is set forth in writing signed by the person against whom enforcement is sought.").

IV. BURDEN OF PROOF

The party seeking enforcement of a restrictive covenant bears the burden of pleading and proving that the covenant is reasonable. F.S.A. § 542.355(1)(c). Where this burden is met, it shifts to the party opposing enforcement to establish that the contract is overbroad, or otherwise not necessary to protect the employer's interest. Id. See also AutoNation, 347 F. Supp. 2d at

1307 (where employee failed to show covenant was overbroad or not necessary to protect employer's interest, injunction enforcing covenant was affirmed).

V. WILL A FLORIDA COURT "BLUE PENCIL" OR MODIFY AN OVERBROAD COVENANT?

Prior to 1990, Florida courts were required to modify overbroad covenants. See Health Care Financial Enterprises v. Levy, 715 So.2d. 341, 342 (Fla. Dist. Ct. App. 1998); Flammer v. Patton, 245 So.2d. 854 (Fla. 1971). The 1990 amendment removed this requirement, but did not prohibit modification. Levy, 715 So.2d. at 343.

The 1996 statute returned to a requirement of modification. As long as a legitimate business interest exists, if a restraint within a covenant is overbroad, the court must modify it to a restriction necessary to protect an employer's business interest. FSA § 542.335 (1)(c); Open Magnetic Imaging, 826 So.2d at 418 (trial court abused its discretion in denying injunctive relief rather than modifying overly broad geographic restraint). See also Shields v. The Paving Stone Co., Inc., 796 So.2d 1267 (Fla. Dist. Ct. App. 2001) (Modifying an injunction to protect only the interests which were "reasonably necessary"); Sears Termite and Pest Control, Inc. v. Arnold, 745 So.2d 485 (Fla. Dist. Ct. App. 1999) (Limiting the scope of a non-compete agreement to solicitation of the employer's customers and disclosure of pricing information.) Audiology Distribution, LLC v. Simmons, 8:12-CV-02427-JDW, 2014 WL 7672536, at *1 (M.D. Fla. May 27, 2014) (Trial court blue-penciled indefinite confidentiality covenant to provide 6-month limitation.)

VI. PRESUMPTION OF IRREPARABLE INJURY

Prior to 1990, there was a presumption under Florida law of irreparable injury to the employer where a covenant not to compete was violated, and a party seeking enforcement had

only to show a valid covenant and a breach. See, e.g., Capraro v. Lanier Business Prod., Inc., 466 So.2d. 212 (Fla. 1985); King v. Jessup, 698 So.2d. 339, 340 (Fla. Dist. Ct. App.1997).

Under the 1990 statute, there was no judicial presumption of irreparable injury. F.S.A. § 542.33(2)(a); King, 698 So.2d. at 341. A party seeking enforcement of covenants entered into during the effective period of this statute must make a showing of irreparable injury before an injunction will be issued. Id. See also AGS Computer Services, Inc. v. Rodriguez, 592 So.2d. 801 (Fla. Dist. Ct. App. 1992).

Under the current statute, "the violation of an enforceable restrictive covenant creates a presumption of irreparable injury to the person seeking enforcement." F.S.A. § 542.335(1)(j). See Data Payment Sys., Inc. v. Caso, 253 So.3d 53, 58 (Fla. Dist. Ct. 2018) (reversing trial court for failing to apply rebuttable presumption of irreparable injury); Medco Data, LLC v. Bailey, 152 So.3d 105 (Fla. Dist. Ct. App. 2014) (same); AutoNation, 347 F.Supp.2d at 1307 (irreparable injury is presumed and burden shifts to employee to establish absence of such injury); USI Ins. Servs. of Fla., Inc. v. Pettineo, 987 So.2d 763,766 (Fla. Dist. Ct. App. 2008) (Same); I.C. Systems, Inc. v. Oliff, 824 So.2d 286 (Fla. Dist. Ct. App. 2002) (Violation of enforceable covenant creates presumption of irreparable injury); America II Electronics, Inc. v. Smith, 830 So.2d 906 (Fla. Dist. Ct. App. 2002) (Same). The presumption is rebuttable. Pirtek USA, LLC v. Wilcox, 606CV566ORL31KRS, 2006 WL 1722346 (M.D. Fla. June 21, 2006); Colucei, 918 So.2d at 440; JonJuan Salon, Inc. v. Acosta, 922 So.2d 1081 (Fla. Dist. Ct. App. 2006). To the extent that the relief sought by the plaintiff is speculative, the presumption is rebutted. Id. Don King Productions, Inc. v. Chavez, 717 So.2d. 1094, 1095 (Fla. Dist. Ct. App. 1998). The focus of the injunctive relief is on maintaining the employer's longstanding relationships built up over the course of time. Variable Annuity Life Ins. Co. v. Hausinger, 927

So.2d 243 (Fla. Dist. Ct. App. 2006). The fact that the employer does not have contractual relationships with its customers is insufficient to rebut the presumption of irreparable injury. North American Products, 196 F. Supp. 2d at 1230.

The statute also requires the posting of a bond before any injunctions will be issued. A bond should be sent in an amount that reflects the court's determination of the foreseeable damages for a wrongful injunction. Advantage Digital Sys., Inc. v. Digital Imaging Servs., Inc., 870 So. 2d 111, 116 (Fla. Dist. Ct. App. 2003).

VII. RELIEF AVAILABLE FOR BREACH OF A RESTRICTIVE COVENANT

As in other states, the most common remedy for violation of a restrictive covenant is an injunction. Ameripath, Inc. v. Wetherington, 10-60766-CIV, 2010 WL 3470914 (S.D. Fla. Sept. 3, 2010); Medi-Weightloss Franchising USA, LLC v. Sadek, 8:09-CV-2421-T-24MAP, 2010 WL 1837767 (M.D. Fla. Mar. 11, 2010), report and recommendation adopted sub nom. Medi-Weightloss Franchising USA, LLC, 8:09 CV 2421 T 24 MA, 2010 WL 1837764 (M.D. Fla. Apr. 29, 2010); Brannon v. Auto Center Mfg. Co., 393 So.2d. 75 (Fla. Dist. Ct. App. 1981). To obtain an injunction, the plaintiff must show: "(1) the existence of an enforceable contract, including a statutorily-defined 'legitimate business reason' supporting each restrictive covenant; (2) defendants' intentional breach of the restrictive covenants; and (3) that plaintiff has no adequate remedy other than injunctive relief." Milner, 377 F. Supp. 2d at 1214. See also Ameripath, Inc. v. Wetherington, 10-60766-CIV, 2010 WL 3470914 (S.D. Fla. Sept. 3, 2010). Irreparable harm is presumed if plaintiff can show an intentional breach of an enforceable restrictive covenant. Id. A Florida court may issue an injunction prohibiting competition not only by the employee who signed the agreement, but also by his new employer. North American Products, 196 F. Supp. 2d at 1230. See also Temporarily Yours-Temporary Help Services, Inc.

v. Manpower, Inc., 377 So.2d 825, 827 (Fla. Dist. Ct. App.1979) (Injunction properly issued against corporation and the former employee, since the corporation existed for the purpose of aiding and abetting the employee); Smart Pharmacy, Inc. v. Viccari, 213 So. 3d 986 (Fla. Dist. Ct. App. 2016) (Injunction allowed to remain in effect against new employer even after employee had left its employ). Where no legitimate business interest exists, no injunction may be entered. Pirtek, 2006 WL 203865 ; Colucci v. Kar Kare Auto Group, Inc., 918 So.2d 431 (Fla. Dist. Ct. App. 2005). Similarly, an injunction is improper where there is no or insufficient evidence that the employee took any action in violation of the covenant. Coastal Loading, Inc. v. Tile Roof Loading, Inc., 908 So.2d 609 (Fla. Dist. Ct. App. 2005); Commercial Bank v. Hill, 210-CV-126-FTM-29SPC, 2010 WL 2854174 (M.D. Fla. July 21, 2010); Loans of Am. Fl., LLC v. Rapid Auto Loans, LLC, 10-60416-CIV, 2010 WL 2754336 (S.D. Fla. July 12, 2010); Concrete Surface Innovations, Inc. v. McCarty, 610CV568ORL28GJK, 2010 WL 1930971 (M.D. Fla. May 13, 2010).

An injunction may not be broader than the agreement entered into between the parties. Advantage Digital Systems, 870 So.2d at 115. A court is also generally prohibited from extending the term of an expired non-compete covenant through entry of an injunction. Vela v. Kendall, 905 So.2d 1033 (Fla. Dist. Ct. App. 2005) (Reversing injunction which extended term of expired non-compete agreement by two years). But see, Florida Digestive Health Specialists, LLP v. Colina, supra at 97 ("The two-year injunctive period shall commence on the date the order is entered on remand.").

A court may also award damages for a violation of a restrictive covenant, including damages such as lost profits and damages from unfair competition of the employee. Brannon, 393 So.2d. at 76. However, "it is not proper to award damages for the breach and to enforce the

entire contract." Id. at 77. Moreover, the former employer bears the burden of proving both that it sustained a loss and the lost profits were a "direct result" of the former employee's breach of the restrictive covenants. Proudfoot Consulting Co. v. Gordon, 576 F.3d 1223 (11th Cir. 2009).

In calculating net lost profits expenses of salaries paid to corporate officers must be deducted. Karl v. Carefree Lifestyle, Inc., 95 So.3d 289 (Fla. Dist. Ct. App. 2012). The 1996 statute also allows for an award of attorney's fees and costs to the prevailing party in an action for enforcement of a restrictive covenant. F.S.A. § 542-335(1)(k); DeWitte, 890 So.2d at 411; Kohlmeier v. Diversified Drilling Corp., 898 So.2d 994, 995 (Fla. Dist. Ct. App. 2005) (Awarding fees under the statute).

VIII. CHOICE OF LAW

Parties to a contract may agree on what state's law will apply to the governance of the contract, so long as the application of that law is not against the public policy of the State of Florida. Electrostim Med. Servs., Inc. v. Lindsey, 8:11-CV-2467-T-33TBM, 2012 WL 1405707 (M.D. Fla. Mar. 13, 2012), report and recommendation adopted, 8:11-CV-2467-T-33TBM, 2012 WL 1405681 (M.D. Fla. Apr. 23, 2012) (Applying Florida choice of law provision); Godwin Pumps of America, Inc. v. Ramer, 8:11-CV-580-T-24 AEP, 2011 WL 2670191 (M.D. Fla. July 8, 2011) (Applying New Jersey law). Muniz v. GCA Servs. Grp., Inc., 3:05 CV 172 J 33MMH, 2006 WL 2130735 (M.D. Fla. July 28, 2006) (Applying Pennsylvania law to covenant where it did not violate Florida public policy); Snelling & Snelling v. Reynolds, 140 F. Supp. 2d 1314 (M.D. Fla. 2001) (Applying Pennsylvania law to a covenant where it did not violate Florida public policy). See also Maritime Ltd. Partnership v. Greenman Advertising Assocs., 455 So.2d. 1121, 1123 (Fla. Dist. Ct. App. 1984); Rollins, Inc. v. Parker, 755 So.2d 839 (Fla. Dist. Ct. App. 2000) (Enforcing parties' choice of law provision that Georgia law governed non-compete

agreement); Local Access, LLC v. Peerless Network, Inc., 614CV399ORL40TBS, 2016 WL 6990734 (M.D. Fla. Nov. 29, 2016) (applying Illinois law to non-compete covenant in business to business agreement). Where there is no choice of law provision, "the enforceability of [covenants not to compete] in the courts of Florida must be determined by the law of this state." Forrest v. Kornblatt, 328 So.2d. 528, 529 (Fla. Dist. Ct. App. 1976) (Citing Statewide Ins. Co. v. Flaks, 233 So.2d. 400 (Fla. App. 1970)).

A forum selection clause in a non-compete agreement is reasonable and enforceable. Ware Else, Inc. v. Ofstein, 856 So.2d 1079 (Fla. Dist. Ct. App. 2003). However, under the Florida long arm statute, a forum selection clause as a matter of law is not sufficient to confer personal jurisdiction over a non-resident defendant. Rexam Airspray, Inc. v. Arminak, 471 F. Supp. 2d 1292 (S.D. Fla. 2007). The party seeking to establish jurisdiction must separately establish one of the grounds for jurisdiction under the long arm statute.

In Bovie Medical Corp. v. Livneh, the court enforced different forum selection clauses in several agreements and required that certain claims be filed in New York while others were to be filed in Florida. 8:10-CV-1527-T-24EAJ, 2010 WL 4117635 (M.D. Fla. Oct. 19, 2010). A forum selection clause was enforced against non-signatories in East Coast Karate Studios, Inc. v. Lifestyle Martial Arts, LLC, 65 So.3d 1127 (Fla. Dist. Ct. App. 2011). In East Coast, the non-signatories were the former employee's wife and her competing company. The Court of Appeals identified the close relationship between the wife and former employee and the fact that their claims were derivative of the former employee's interest as factors in enforcing the agreement.

COVENANTS NOT TO COMPETE IN SOUTH CAROLINA

I. INTRODUCTION

As in other states, covenants not to compete are generally disfavored in South Carolina as restraints on trade. See, e.g., Moser v. Gosnell, 334 S.C. 425, 513 S.E.2d 123 (S.C. App. 1999); Standard Register Co. v. Kerrigan, 238 S.C. 54, 119 S.E.2d 533 (S.C. 1961). Upon weighing the interests of both the employer and the employee, a South Carolina court will uphold a covenant where it finds that it is necessary to protect the interests of the employer. Rental Uniform Service of Florence, Inc. v. Dudley, 278 S.C. 674, 301 S.E.2d 142 (S.C. 1983).

II. FACTORS CONSIDERED WHEN DETERMINING ENFORCEABILITY

South Carolina courts consider five factors when determining whether a covenant not to compete is valid:

(a) Necessary for the protection of the legitimate interests of the employer;
(b) Reasonably limited in its operation with respect to time and place;
(c) Not unduly harsh and oppressive in curtailing the legitimate efforts of the employee to earn a livelihood;
(d) Reasonable from the standpoint of sound public policy; and
(e) Supported by valuable consideration.

Dove Data Products, Inc. v. Murray, CIV.A. 4-05-CV-72-25, 2006 WL 463588, at *3 (D.S.C. Feb. 23, 2006); Faces Boutique, Ltd. v. Gibbs, 318 S.C. 39, 455 S.E.2d 707 (S.C. App. 1995), Dudley, 301 S.E.2d at 143. Covenants are examined on a case-by-case basis, and are strictly construed against the employer. Faces Boutique, 455 S.E.2d at 709; Carolina Chem. Equip. Co., Inc. v. Muckenfuse, 322 S.C. 289, 471 S.E.2d 721 (S.C. App. 1996).[5] The Supreme Court of South Carolina recently held that a lower level of scrutiny is applied in the case of a sale of business. Palmetto Mortuary Transport, Inc. v. Knight Sys., Inc., 424 S.C. 444, 456 (2018)

[5] Confidentiality and invention assignment agreements are not restraints of trade and should not be treated as non-compete agreements. Milliken & Co. v. Morin, 399 S.C. 23, 731 S.E.2d 288 (2012).

("Non-compete covenants executed in conjunction with the sale of a business should be scrutinized at a more relaxed level than non-compete covenants executed in conjunction with employment contracts.").

A. Supported By Valuable Consideration.

At-will employment provides sufficient consideration for a covenant not to compete in South Carolina. Reidman Corp. v. Jarosh, 289 S.C. 191, 345 S.E.2d 732 (S.C. App. 1986), aff'd, 290 S.C. 252, 349 S.E.2d 404 (S.C. 1986); Small v. Springs Industries, Inc., 292 S.C. 481, 357 S.E.2d 452 (S.C. 1987); Wolf v. Colonial Life and Ace. Ins. Co., 309 S.C. 100, 420 S.E.2d 217, 222 (S.C. App. 1992); Murray, 2006 WL 463588, at *3; Hagemeyer N. Am. Inc. v. Thompson, C/A 2:05-3425, 2006 WL 516733, at *6 (D.S.C. Mar. 1, 2006).

Where a non-compete covenant is entered into after the inception of employment, separate consideration is necessary to make the covenant enforceable. Nucor v. Bell, 482 F. Supp. 2d 714 (D.S.C. 2007) (Citing Poole v. Incentives Unlimited, Inc., 345 S.C. 378, 548 S.E.2d 207 (S.C. 2001)). A "promise" of continued employment is "illusory" because the employer retains the right to discharge her employment at any time. Id.[6]

B. Reasonably Limited With Respect To Time And Place.

(1) Duration.

A covenant that restricts the employee from competing "at any time" will be invalid under most circumstances. See Sermons v. Caine & Estes Ins. Agency, Inc., 275 S.C. 506, 273 S.E.2d 338 (S.C. 1980). However, covenants for a specified reasonable number of years have been upheld. In Kerrigan, the court upheld a covenant with a two-year duration. 119 S.E.2d at 544. See also Reidman Corp., 345 S.E2d at 732 (covenant restricting competition by former

[6] Non-compete agreements also are assignable in the context of a sale of business. Uhlig LLC v. Shirley, 6:08-CV-01208-JMC, 2011 WL 1119548 (D.S.C. Mar. 25, 2011) and Uhlig LLC v. Shirley, 6:08-CV-01208-JMC, 2012 WL 2923242 (D.S.C. July 17, 2012).

insurance agent for two years held enforceable); Dudley, 301 S.E.2d at 142 (three-year time limitation in non-compete of former employee of uniform laundering business was not unreasonable).

(2) Territorial Limitation.

A territorial limitation will generally be invalid under South Carolina law if it covers an area broader than necessary to protect the business of employer. Kerrigan, 119 S.E.2d at 539. A limitation will be reasonable if it limited to the area in which the employee had customer contacts during his employment. Id. By way of example, in Stringer v. Herron, the court found a covenant restricting competition within a fifteen mile radius from the former employer to be too broad for a veterinarian where the former employer's clients lived closer than fifteen miles, and where the restriction extended into additional counties and another state. 309 S.C. 529, 424 S.E.2d 547 (S.C. App. 1992). In Team IA v. Lucus, a nationwide territorial restriction was deemed unenforceable. 395 S.C. 237, 717 S.E.2d 103 (S.C. Ct. App. 2011). But see Palmetto Mortuary Transport, Inc. v. Knight Sys., Inc., 424 S.C. 444, 456 (2018) (holding a 150 mile radius in sale of business context enforceable).

Employers in South Carolina may validly restrict competition with certain customers as a substitute for a geographical limitation. Indus. Packaging Supplies, Inc. v. Martin, CA 6:12-713-HMH, 2012 WL 1067650 (D.S.C. Mar. 29, 2012) (Enforcing non-compete provision limited to persons whom former employee sold products during last 12 months of employment.) Murray, 2006 WL 463588, at *5; Wolf v. Colonial Life and Acc. Ins. Co., 309 S.C. 100, 420 S.E.2d 217, 222 (S.C. App. 1992).[7]

[7] As in Georgia, South Carolina courts are more lenient in the standards used for enforceability for covenants in connection with the sale of a business. See, e.g., South Carolina Finance Corp. of Anderson v. West Side Finance Co., 236 S.C. 109, 113 S.E.2d 329 (S.C. 1960) (covenant for three years and within a radius of twenty-five (25)

C. Protection of Employer's Legitimate Business Interests, Burden On Employee, And Public Policy.

It is impossible to place a numerical limit on what constitutes a "reasonable" time or territorial limitation without considering the type of business involved. This is where the remaining three factors come into play. A covenant will be held unduly harsh and oppressive on an employee where it deprives him of the opportunity to earn a livelihood. Kerrigan, 119 S.E.2d at 540; Murray, 2006 WL 463588, at *5. A court will consider adverse general business considerations, possible deprivation of support for the employee and his family, and necessity that the employee changes "his calling or residence." Id. See also Wolf, 420 S.E.2d at 222 (covenant did not deprive former insurance agent of right to earn a livelihood where he was making more money after leaving the job of the employer); Hagemeyer North America, Inc. v. Thompson, C/A 2:05-3425, 2006 WL 516733, at *5 (D.S.C. Mar. 1, 2006) (Covenant was not unduly oppressive where it did not "shut [defendant] out of the industry.")

A restrictive covenant that seeks to "protect [the employer's] existing business contracts, including the protection of its customers, among other things, from pirating by a former employee," is reasonably necessary to protect the interests of the employer. Wolf, 420 S.E.2d at 221. Courts have recognized that one of the most important assets of a business is its "stock of customers." Murray, 2006 WL 463588, at *3. Employers also have a legitimate interest in protecting existing employees. Id. The court in Hagemeyer, noted that existing business contacts, customer good will, trade secrets and confidential information are all legitimate business interests warranting protection. 2006 WL 516733, at *3.

---

miles held valid). See also Cafe Associates Ltd. v. Germross, 305 S.C. 6, 406 S.E.2d 162 (S.C. 1991) (covenant for five years within a geographic area of five miles held valid.)

South Carolina is similar to Georgia in that covenants which prohibit competition "in any capacity" are overbroad and unreasonable. In Faces Boutique, the court refused to enforce such a covenant. 455 S.E.2d at 709. The court found that a prohibition which prevented the employee from being associated "in any capacity" with a competing business went "far beyond the protection of any legitimate business interest [the employer] may be able to articulate." Id.

With respect to considerations of public policy, South Carolina requires the enforcement of contracts "freely entered into by the parties." Wolfe, 420 S.E.2d at 221. Thus, a court must balance the policy against restraints on trade with that of the enforcement of freely negotiated contracts.

III. WILL A SOUTH CAROLINA COURT "BLUE PENCIL" OR MODIFY AN OVERBROAD COVENANT?

South Carolina courts follow a rule similar to that of old Georgia law and will strike the entire covenant where one area of the covenant is unenforceable. See Faces Boutique, 455 S.E.2d at 709; Eastern Business Forms, Inc. v. Kistler, 258 S.C. 429, 189 S.E.2d 22, 24 (S.C. 1972) (A court "cannot make a new agreement for the parties into which they did not voluntarily enter. We must uphold the covenant as written or not at all, it must stand or fall integrally."). In Poynter Investments, Inc. v. Century Builders of Piedmont, Inc., the South Carolina Supreme Court held that a court cannot rewrite a non-compete agreement to make it enforceable. 387 S.C. 583, 694 S.E.2d 15 (2010). See also Somerset v. Reyner, 233 S.C. 324, 104 S.E.2d 344, 346 (1958) ("If . . . the territorial scope of the restraint is unreasonable . . . no inquiry need to made as to the presence or absence of the other necessary requirements."); Stonhard, Inc. v. Carolina Flooring Specialists, Inc., 621 S.E.2d 352 (S.C. 2005). Fournil v. Turbeville Insurance Agency, Inc., 3:07-3836-JFA, 2009 WL 512261 (D.S.C. Mar. 2, 2009); Team IA v. Lucas, 395 S.C. 237, 717 S.E.2d 103 (S.C. App. 2011). South Carolina Supreme Court recently reiterated the court

will not blue pencil an overbroad geographic limitation. Palmetto Mortuary Transport, Inc. v. Knight Sys., Inc., 424 S.C. 444, 456 (2018).

IV. RELIEF AVAILABLE FOR BREACH OF A RESTRICTIVE COVENANT

Generally, a plaintiff suing for violation of a covenant not to compete will seek injunctive relief to preserve the status quo pending resolution of the case. In determining whether such relief is appropriate, courts have implemented a balancing of equities test, considering: (1) the probability of irreparable injury to the plaintiff; (2) the likely harm to the defendant if enjoined; (3) plaintiff's likelihood of success; and (4) the public interest. Ancora Capital & Mgmt. Grp., LLC. v. Gray, 55 Fed. Appx. 111, 113 (4th Cir. 2003). See also Dove Data Products, Inc. v. Murray, CIV.A. 4-05-CV-72-25, 2006 WL 463588, at *3 (D.S.C. Feb. 23, 2006); MailSource, LLC v. M.A. Bailey & Associates, Inc., 356 S.C. 363, 588 S.E.2d 635 (2003); Almers v. South Carolina Nat'l Bank of Charleston, 265 S.C. 48, 217 S.E.2d 135 (S.C. 1975); Milliken & Co. v. Evans, 7:14-CV-00778-BHH, 2014 WL 8240512 (D.S.C. Oct. 10, 2014), report and recommendation adopted, CIV.A. 7:14-778-BHH, 2015 WL 1280871 (D.S.C. Mar. 20, 2015) (Court refused to grant preliminary injunction where former employer was unable to prove lost sales or customers). Where the balance of the first two factors tips "decidedly in favor" of the plaintiff, it need not show a likelihood of success. Ancora, , 55 Fed. Appx. at 114.

The evidence must show that the injunction is "reasonably necessary to protect the legal rights of the plaintiff pending in the litigation." MailSource, 588 S.E.2d at 638. A court may not, through an injunction, extend the time period for an expired restrictive covenant. Stonhard, Inc. v. Carolina Flooring Specialists, Inc., 621 S.E.2d 352, 354 (S.C. 2005).

Damages may be recoverable for a breach of a covenant not to compete where they can be determined with "reasonable certainty." South Carolina Finance Corp., 113 S.E.2d at 336.

For example, profits are recoverable where they are fairly certain to have been earned. Id. See also Depositions and . . . Inc. v. Campbell, 305 S.C. 173, 406 S.E.2d 390, 391 (Ct. App. 1991).

In Moser v. Gosnell, a liquidated damages clause in a non-compete agreement ancillary to a sale of business was invalidated as a penalty. 334 S.C. 425, 513 S.E.2d 123 (S.C. App. 1999). The Court of Appeals concluded that it was not intended to compensate the parties for actual damages where it could be invoked in case of a "threatened breach," but was intended to provide punishment for a breach. Id. at 126–27. In Foreign Academic & Cultural Exchange Services v. Tripon, the South Carolina Supreme Court concluded that a liquidated damages provision was unenforceable because it was "plainly disproportionate" to any probable actual damage. 394 S.C. 197, 15S.E.2d 331 (S.C. 2011).

V. CHOICE OF LAW

A covenant in South Carolina will not be enforceable if it is invalid under the state where it was to be performed, or if it is contrary to the public policy of South Carolina. Kerrigan, 119 S.E.2d at 542; Stonhard, Inc. v. Carolina Flooring Specialists, Inc., 621 S.E.2d 352 (S.C. 2005). However, where the covenant does not contravene a public policy of the State of South Carolina or where no allegation is made that such a policy violation exists, the court will construe the covenant in accordance with the law of the state chosen by the parties in the agreement. Rental Serv. Corp. v. Nunamaker, 1:06-970-MBS, 2006 WL 1677152 (D.S.C. June 14, 2006) (Construing covenant in accordance with Arizona law where no allegation that enforcement of choice of law provision could violate a strong public policy of the State of South Carolina); Prym Consumer USA, Inc. v. Rhode Island Textile Co., 388 Fed. Appx. 352 (4th Cir. 2010) (Applying Rhode Island law); Team IA v. Lucas, 395 S.C. 237, 717 S.E.2d 103 (S.C. App. 2011) (Applying

South Carolina law); Saint-GoBain Corp. v. Miller, CA 2:14-1662-MBS, 2014 WL 6686787 (D.S.C. Nov. 25, 2014).

COVENANTS NOT TO COMPETE IN TENNESSEE

I. INTRODUCTION

Similar to the previous States examined, covenants not to compete are disfavored in Tennessee because they are deemed to be in restraint of trade. Murfreesburo Medical Clinic, P.A. v. Udom, 166 S.W.3d 674, 678 (Tenn. 2005). Tennessee does not have a statute governing all covenants not to compete. However, Tenn. Code Ann. § 47-25-101, which governs Tennessee's public policy, provides:

> All arrangements, contracts, agreements, trusts, or combinations between persons or corporations with a view to lessen, or which tend to lessen, full and free competition in the importation or sale of articles imported into this state, or in the manufacture or sale of articles of domestic growth or of domestic raw material. . . are declared to be against public policy, unlawful, and void.[8]

The remainder of restrictive covenants in Tennessee are governed under common law principles. These covenants are viewed as restraints on trade and are not favored in Tennessee, but will be enforced where reasonable under the circumstances of the case. Money & Tax Help, Inc. v. Moody, 180 S.W.3d 561, 564 (Tenn. App. 2005); Murfreesboro, 166 S.W.3d at 674; H & R Block E. Tax Servs., Inc. v. Bates, M200102589COAR3CV, 2002 WL 2008765, at *9 (Tenn. Ct. App. Sept. 3, 2002); Central Adjustment Bureau v. Ingram, 678 S.W.2d 28 (Tenn. 1984); Hasty v. Rent-A-Driver, Inc., 671 S.W.2d 471 (Tenn. 1984). Tennessee courts strictly construe covenants in favor of the employee. Vantage Technology, LLC v. Cross, 17 S.W.3d 637, 643 (Tenn. Ct. App. 2000); Brasfield v. Anesthesia Servs., P.C., 03A01-9811-CH-00392, 1999 WL 817507 (Tenn. Ct. App. Oct. 13, 1999). See Murfreesboro Medical Clinic, P.A. v. Udom, 166

[8] Tennessee also has a statute governing covenants not to compete in the medical field, which provides that restrictive covenants prohibiting a doctor's right to practice medicine may be enforced, subject to certain limitations. Tenn. Code Ann. § 63-6-204(e). Such covenants must be restricted to two years and one county. See Murfreesboro Medical Clinic, P.A. v. Udom, 166 S.W.3d 674 (Tenn. 2005) (non-compete agreements restricting doctors unenforceable under public policy, except for limited circumstances set forth in Tenn. Code Ann. § 63-6-204(e)).

S.W.3d 674 (Tenn. 2005). As such, employers must "take responsibility" for ambiguous provisions of the agreement. Int'l Sec. Mgmt. Grp., Inc. v. Sawyer, 3:06CV0456, 2006 WL 1638537, at *14 (M.D. Tenn. June 6, 2006).

II. FACTORS CONSIDERED WHEN DETERMINING ENFORCEABILITY

Tennessee's general rule regarding covenants not to compete is a "Rule of Reasonableness." Sawyer, 2006 WL 1638537, at *12; Borg-Warner Protective Servs. Corp. v. Guardsmark, Inc., 946 F. Supp. 495, 501 n.6 (E.D. Ky. 1996), aff'd, 156 F.3d 1228 (6th Cir. 1998) (Applying Kentucky and Tennessee law). Under this rule, Tennessee courts have considered several factors:

(a) Consideration given for the agreement;
(b) Danger to employer if there is no such agreement;
(c) Economic hardship on employee by the covenant; and
(d) Public interest.

See J.T. Shannon Lumber Co., Inc. v. Barrett, 07-2847-ML/P, 2011 WL 1130530 (W.D. Tenn. Feb. 9, 2011), report and recommendation adopted, 07-2847-JPM TMP, 2011 WL 1113237 (W.D. Tenn. Mar. 24, 2011); Columbus Medical Services, LLC v. Thomas, 308 S.W.3d 368 (Tenn. App. 2009); Sawyer, 2006 WL 1638537, at *7; Udom, 166 S.W.3d at 678; Cross, 17 S.W.3d at 643; Allright Auto Parks, Inc. v. Berry, 409 S.W.2d 361, 363 (Tenn. 1966); S. Fire Analysis, Inc. v. Rambo, M200800056COAR3CV, 2009 WL 161088 (Tenn. Ct. App. Jan. 22, 2009); Amarr Co., Inc. v. Depew, 03A01-9511-CH-00412, 1996 WL 600330 (Tenn. Ct. App. Oct. 16, 1996).

A. Adequate Consideration.

Where a non-compete covenant is part of the employee's original employment agreement, the employment alone is sufficient consideration, even where the employment is at-will. Ramsey v. Mutual Supply Co., 427 S.W.2d 211 (Tenn. 1968). The continued future

employment of an at-will employee has also been considered sufficient consideration to support enforcement of a non-compete agreement. Cummings, Inc. v. Dorgan, 320 S.W.3d 316 (Tenn. Ct. App. 2009); Girtman & Assocs., Inc. v. St. Amour, M2005-00936-COA-R3CV, 2007 WL 1241255 (Tenn. Ct. App. Apr. 27, 2007) (Citing Central Adjustment Covenant v. Ingram, 678, S.W.2d 28, 33 (1984)). Performance by the employer is adequate consideration for a non-compete agreement even where it is entered into after the employee has started work. Even if the promise of employment is illusory, performance can make a binding contract. Ingram, 678 S.W.2d at 35 (citing Hoyt v. Hoyt, 372 S.W.2d 300 (Tenn. 1963). See also Crain v. Kesterson Food Co., Inc., 02A01-9302-CH-00041, 1994 WL 52645 (Tenn. Ct. App. Feb. 16, 1994). Where an employee is discharged in an arbitrary or capricious manner, or with bad faith on the part of the employer, a Tennessee court will be less likely to enforce the non-compete covenant. Id. See Gibsons Suits in Chancery, § 18 (6th ed. 1982).

B. Danger To Employer.

An employer is not permitted to restrain ordinary competition. Medical Education Assistance Corp. v. State of Tennessee, 19 S.W.3d 803, 813 (Tenn. Ct. App. 2000); Hasty, 671 S.W.2d at 471. The employer must show the existence of "special facts over and above ordinary competition" to demonstrate that without the covenant the employee would gain an unfair advantage in competition with the employer. Udom, 166 S.W.3d at 682; Cross, 17 S.W.3d at 643; Davis v. Johnstone Group, Inc., W201501884COAR3CV, 2016 WL 908902 (Tenn. Ct. App. Mar. 9, 2016). The following factors are considered in determining whether the employee would have an unfair advantage:

(1) Whether the employer provided the employee with specialized training;
(2) Whether the employee was given access to trade or business secrets or other confidential information; and

(3) Whether the employee had repeated contacts with the customers such that the customers associated the employer's business with the employee. Id. Medical Education Assistance Corp., 19 S.W.3d at 813; H&R Block, 2002 WL 2008765, at *9.

A danger to the employer exists where it has legitimate business interest that is properly protectable by a non-competition covenant. Moody, 180 S.W.3d at 565; Cross, 17 S.W.3d at 643. Employers have an interest in the "time, effort, and money" spent training its employees. Borg-Warner, 946 F. Supp. at 503. In cases involving employment or staffing agencies, Tennessee recognizes the employer's legitimate business interest in preventing unfair disintermediation – the client hiring the employees directly. Columbus Medical Services, LLC v. Thomas, 308 S.W.3d 368 (Tenn. App. 2009).

General knowledge and skill by the employee is not a protectable interest, even if acquired while the employee was employed. Cross, 17 S.W.3d at 644; B&L Corp. v. Thomas and Thorngren, Inc., 162 S.W.3d 189, 211 (Tenn. Ct. App. 2004). In addition, information that is publicly available and not confidential to the business will not be protected. Depew, 1996 WL 600330, at *4; B&L Corp., 162 S.W.3d at 211 (prices, customer names, contact information and contract renewal dates were not confidential business information and therefore were not a protectable interest of employer); Hinson v. O'Rourke, M201400361COAR3CV, 2015 WL 5033908 (Tenn. Ct. App. Aug. 25, 2015) (Alleged trade secrets "readily available," training "widely available through other sources"). In Cross, the employer had a protectable interest where the employee was given 250 hours of training within his first month of employment, and where he developed close relationships with the employer's customers. 17 S.W.3d at 646. By way of contrast, in H&R Block, the training given by H&R Block to its tax preparers was minimal, and did not provide them with any confidential information, and therefore was not protectable. 2002 WL 2008765, at *9.

Trade secrets are also legitimate, protectable business interests. See Hasty, 671 S.W.2d at 473. Covenants preventing the misuse of customer lists are reasonable. H&R Block, 2002 WL 2008765, at *9. With respect to confidential business information that does not rise to the level of trade secrets, in order to be protectable, it must not be generally available to the public. Baker v. Hooper, 03A01-9707-CV-00280, 1998 WL 608285 (Tenn. Ct. App. Aug. 6, 1998); Cross, 17 S.W3d at 646 (preferences of doctors who were customers of the employer, its pricing information, and identity of customers was found to be confidential and therefore protectable).

The employee's development of strong relationships with the customers of the employer also weighs in favor of the employer having a protectable interest. Present, rather than past or future customers or clients are a protectable interest of an employer. Thompson, Breeding, et al. v. Bowlin, 765 S.W.2d 743, 745 (Tenn. App. 1987). See also Sawyer, 2006 WL 1638537, at *22; Vaughn v. Weems, 01A01-9407-CV-00324, 1994 WL 681158, at *2 (Tenn. Ct. App. Dec. 7, 1994); Moody, 180 S.W.3d at 565; Outfitters Satellite, Inc. v. CIMA, Inc., M2003-02074-COA-R3CV, 2005 WL 309370, at *3 (Tenn. Ct. App. Feb. 8, 2005) (Reasonable to restrict competition with current customers where customers associate employer's business with the employee); Medical Education Assistance Corp., 19 S.W.3d at 814.[9]

C. Hardship on Employee.

The court weighs the employer's protectable interest with the hardship that will be caused to the employee if the covenant is enforced. Columbus Medical Services, LLC v. Thomas, 308 S.W.3d 368 (Tenn. App. 2009); Dabora, Inc. v. Kline, 884 S.W.2d 475, 479 (Tenn. App. 1994). The burden of showing the enforceability of a covenant is on the employer. See, e.g., Berry, 409 S.W.2d at 363. See also Baker, 1998 WL 608285, at *4. Where an employee creates a situation

[9] Outside the employment context, the court in Affinion Benefits Group, Inc. v. Econ-O-Check Corp., 784 F. Supp. 855 (M.D. Tenn. 2011) held that a contract to provide checking services to bank which contained a one year non-compete did not protect a legitimate business interest of the provider, but merely restrained competition.

of hardship by his or her own action, there will be a limitation to the court's protection. Dabora, 884 S.W.2d at 479 (where employee knew employer would not waive her covenant and moved to take a job in competition with employer, court refused to hold hardship on employee outweighed employer's right to be free of unfair competition); Cross, 17 S.W.2d at 646 (hardship on employer outweighed that of employee, where employer would lose investment in customers, while employee would only lose "that which does not belong to him.").

D. Public Interest.

If a "private contract tends to harm the public good, public interest, or public welfare, or to conflict with the constitution, laws or judicial decisions of Tennessee" it will be held to violate public policy. Holt v. Holt, 751 S.W.2d 426, 428 (Tenn. App. 1988). Where the enforcement of a covenant not to compete will tend to do greater harm to the public than the damage not enforcing it will do to the employer, a court will invalidate it. See Columbus Medical Services, LLC v. Thomas, 308 S.W.3d 368 (Tenn. App. 2009); Herbert v. W.G. Bush & Co., 298 S.W2d 747, 752 (Tenn. App. 1956).

In Udom, a doctor left his practice group, and started a competing practice within the territory prohibited by his non-compete agreement. 166 S.W.3d at 677. While the court noted that the public's interest in allowing a patient to choose his or her physician was prominent, that interest was "tempered" by the facts of the case, and affirmed the lower court's decision that the covenants at issue were enforceable.

E. Scope Of The Restrictions.

(1) Territorial Restrictions.

Assuming that there is a protectable interest of the employer, a covenant not to compete in Tennessee must contain time and geographical restrictions that are "no greater than is

necessary to protect the business interests of the employer." Berry, 409 S.W.2d 361. See also Dabora, 884 S.W.2d 475. This is a case by case determination.

Generally, a covenant not to compete that encompasses a territorial area in which the employee performed no services while employed will be unreasonable unless the employee possesses knowledge of the employer's trade secrets. In Berry, the court held that a restriction "in any city" where the employer operated was overbroad where the employee had only worked in three of the forty-six counties in which the employer did business. Berry, 409 S.W.2d at 364; Cross, 17 S.W.3d at 647 (Agreement that restricted competition within 50 miles of any company office or any customer location was too broad and was modified to restrict competition only in customer locations where the employee had performed services).

In Harvey, the court upheld a covenant covering a 100 mile radius of the employer's business. 1995 WL 140746, at *2. The employee was a heavy equipment claims adjuster, and the employer had been making affirmative efforts to become involved in that business. Because the company had made special efforts to market its services in this narrow field within that territory, to allow the employee to compete in that area would "seriously undermine the company's efforts" to become involved in this specific area of expertise. Id.

(2) Use Of A Customer Restriction In Place Of A Territorial Restriction.

In Bowlin, the court enforced a covenant which limited a former employee from either working for or soliciting "clients" of his accounting firm employer. 765 S.W.2d 743 (Tenn. App. 1987). The lack of territorial limitation did not make it overbroad, as he was only prohibited from soliciting specific customers. Id. at 745. The court noted that as the "specificity of limitation regarding the class of persons with whom contact is prohibited increases, the need for limitation . . . in territorial terms decreases." Id. at 746 (citation omitted); Dabora, 884

S.W.2d at 478 (covenant containing nationwide limitation but which was complemented with a restriction from competition with a certain type of publication was reasonable.); Hamilton-Ryker Group, Inc. v. Keymon, W200800936COAR3CV, 2010 WL 323057 (Tenn. Ct. App. Jan. 28, 2010) (Enforcing non-compete without a territorial restriction where employee was prohibited from soliciting customers of former employer); J.T. Shannon Lumber Co., Inc. v. Barrett, 2:07-CV-2847-JPM-CGC, 2010 WL 3069818 (W.D. Tenn. Aug. 4, 2010); J.T. Shannon Lumber Co, Inc. v. Barrett, 07-2847-ML/P, 2011 WL 1130530 (W.D. Tenn. Feb. 9, 2011), report and recommendation adopted, 07-2847-JPM TMP, 2011 WL 1113237 (W.D. Tenn. Mar. 24, 2011).

In contrast, a non-compete clause which prohibited former tax preparers of H&R Block from performing services for former H&R customers, without regard as to where the services were performed, and which had no limitation as to contacts with the individual preparers, was overly broad and unenforceable. H&R Block, 2002 WL 2008765, at *9.

(3) Time Restrictions.

The reasonableness of time limitations is dependent on the circumstances of the case. A five year restriction was enforced against a pediatric cardiologist. Medical Education Assistance Corp., 19 S.W.3d 803 at 815. In Bowlin, a restrictive covenant for a period of three years was valid and enforceable against a former employee of an accounting firm. 765 S.W.2d at 745. See also Cross, 17 S.W.3d at 647 (Three year covenant upheld); Harvey, 1995 WL 140746, at 3 (three year covenant upheld); Powell v. McDonnell Ins., Inc., 02A01-9608-CH-00176, 1997 WL 589232 (Tenn. Ct. App. Sept. 24, 1997) (Two year restriction upheld).

Where an employment agreement expires, but the employee continues to work for the employer, the non-compete agreement period will continue to run and may expire while the employee remains employed. Homebound Medical Care of Southeast Tenn., Inc. v. Hospital

Staffing, Servs. of Tenn., Inc., 03A01-9707-CH-00303, 1998 WL 46516 (Tenn. Ct. App. Feb. 6, 1998); B & L Corp. v. Thomas & Thorngren, Inc., 917 S.W.2d 674 (Tenn. App. 1995). See also Thuy-Tlam v. Tuan Ngoc Bui Le, E200802491COAR3CV, 2009 WL 2047290 (Tenn. Ct. App. July 15, 2009) (Where agreement was silent as to when non-compete began to run, court concluded it began upon execution of the agreement).

(4) Waiver of Non-Compete Agreement.

In the case of Minor v. Farmers Ins. Exchange, the Court of Appeals concluded that, although there was no dispute that the non-compete agreement at issue was reasonable and enforceable, the plaintiff had waived its right to enforce the agreement. M2000-01217-COA-R3CV, 2002 WL 2023130 (Tenn. Ct. App. Sept. 5, 2002). The plaintiff was an agent for a group of several insurance companies in a specific county in Tennessee. He executed an Agent Appointment Agreement containing a non-compete clause which prohibited him from accepting business from any current policyholders. During the period that he acted as an agent for the group of companies, they were fully aware that he also represented other companies, placed business with other companies, and frequently switched his clients to and from the defendant companies with other companies. Id. at *3. In holding that the defendant companies waived their right to enforce the non-compete agreement, the court noted that the defendants were "fully aware of the plaintiff's history as an independent agent, and of his representation of a host of companies at the time he contracted with the defendant[s]." Defendants never objected to these activities. See also Knoxville Rod & Bearing, Inc. v. Bettis Corp. of Knoxville, Inc., 672 S.W.2d 203 (Tenn. App. 1984) (A covenant not to compete may be waived by the clear and unequivocal actions of the party seeking to enforce it).

III. WILL A TENNESSEE COURT MODIFY OR "BLUE PENCIL" AN OVERBROAD COVENANT?

Tennessee permits "judicial modification" of an overbroad covenant not to compete. Ingram, 678 S.W.2d at 35. This is true especially where the covenant itself provides for modification. Id. In Ingram, Tennessee Supreme Court upheld the trial court's modification of a two year restriction to one year. Id. See also Carrigan v. Arthur J. Gallagher Risk Mgmt. Servs., Inc., 870 F. Supp. 2d 542 (M.D. Tenn. 2012) (Modifying territory based upon where plaintiff was licensed, had clients and had conducted marketing activities); J.T. Shannon Lumber Co., Inc. v. Brannon, 07-2847-ML/P, 2011 WL 1130530 (W.D. Tenn. Feb. 9, 2011), report and recommendation adopted, 07-2847-JPM TMP, 2011 WL 1113237 (W.D. Tenn. Mar. 24, 2011); J.T. Shannon Lumber Co., Inc. v. Barrett, 2:07-CV-2847-JPM-CGC, 2010 WL 3069818 (W.D. Tenn. Aug. 4, 2010) (Modifying territory); Thuy-Tlam v. Tuan Ngoc Bui Le, E200802491COAR3CV, 2009 WL 2047290 (Tenn. Ct. App. July 15, 2009) (Modifying territory and duration of restriction); Outfitters Satellite, Inc., 2005 WL 309370, at *4 (Modifying territorial restriction from North America to United States); Moody, 180 S.W.3d at 566 (Modifying covenant prohibiting competition for three years within 50 miles of Knoxville, TN to prohibiting employee from providing services to clients on current customer list for three years); Baker v. Hooper, 50 S.W.3d 463, 469 (Tenn. App. 2001) (Affirming lower court's modification of a six month restriction on competition by nail technicians to a time period of two months); Depew, 1996 W.L. 600330, at *2 (Modifying a 2 year, 150 mile covenant to one year and 100 miles).

A Tennessee Court will not modify a covenant where the evidence supports a finding of bad faith on the part of the employer, or that the covenant is deliberately unreasonable and oppressive. Moody, 180 S.W.3d at 567. This rule protects against employers drafting overly

broad restrictions expecting the worst sanction to be modification by the court to the maximum extent allowed by law. Cross, 17 S.W.3d at 647.

IV. RELIEF AVAILABLE FOR BREACH OF A RESTRICTIVE COVENANT

When faced with a violation of a restrictive covenant, a court will usually issue an injunction. Harvey, 1995 WL 140746. In determining whether injunctive relief is appropriate, the court will consider: (1) the threat of irreparable harm to the plaintiff, (2) the balance between the harm to the plaintiff and any injury to the defendant in granting the injunction; (3) probability of success on the merits; and (4) the public interest. Sawyer, 2006 WL 1638537, at *7. Where the parties are able to agree on specific suns of money that would be an adequate remedy if the defendant breached the non-compete clause, the court may find that the plaintiff has an adequate remedy at law, weighing against injunctive relief. Udom, 166 S.W.3d at 682. However, courts have held that the loss of fair competition that results from a breach of a non-compete covenant is likely to constitute irreparable harm to an employer. Sawyer, 2006 WL 1638537, at *8. The court in Sawyer further noted that companies have a public interest in keeping certain information confidential and in maintaining their clientele. Id. at *8. Tennessee courts will also enforce a tolling provision to enjoin a breaching party after a covenant has expired. Great American Opportunities, Inc. v. Cherry Brothers, LLC, 3:17-cv-01022, 2018 WL 2218959 (M.D. Tn. May 15, 2018) (agreeing to enforce the tolling provision as written, but finding an insufficient showing that the employee violated the covenants to warrant application of the tolling provision).

Damages may also be recoverable. Tennessee measures damages for a breach of contract as those which would place the plaintiff in the same position as it would have been in had the contract been performed. Powell v. McDonnell Ins., Inc., 02A01-9608-CH-00176, 1997 WL

589232 (Tenn. Ct. App. Sept. 24, 1997) (Citing Wilhite v. Brownsville Concrete Co., 798 S.W.2d 772 (Tenn. App. 1990)). See also Baker, 50 S.W.3d at 469. Damages must be able to be determined to a reasonable degree of certainty. Powell, 1997 WL 589232, at *8 (citation omitted); Harvey, 1995 WL 140746, at *5 (where damages for breach of non-competition covenants were uncertain, it was not an error for the trial court to refuse to award them). Liquidated damages are also available under Tennessee law. See Bowlin, 765 S.W.2d at 746.

V. CHOICE OF LAW

Under Tennessee law, "the rights and obligations under a contract are governed by the law of that state with the view to which it is made. . ." Ohio Casualty Ins. Co. v. Travelers Indem. Co., 493 S.W. 2d 465, 467 (Tenn. 1973). A contract is "made" with reference to the law of the place where it was entered into, unless it appears it was entered into in good faith with reference to the law of some other state. Deaton v. Vise, 210 S.W.2d 665, 668 (Tenn. 1948). A Tennessee court will enforce a choice of law provision provided that it is executed in good faith, the jurisdiction chosen bears a connection to the transaction at issue, the basis of choice of a jurisdiction' s law is reasonable, and the choice is not contrary to the policy of the state's whose law would otherwise govern. Id. See also Cross, 17 S.W.2d at 649; American National Property and Casualty Co. v. Campbell Insurance, Inc., 636 F. Supp. 2d 659 (M.D. Tenn. 2009); Am. Nat. Prop. & Cas. Co. v. Campbell Ins., Inc., 3:08-CV-00604, 2011 WL 2550704 (M.D. Tenn. June 27, 2011), order set aside, 3:08-CV-00604, 2011 WL 6259473 (M.D. Tenn. Oct. 14, 2011) (Parties agreed to application of Missouri law); Strategic Equip. & Supply Corp. v. Mobile Fixture & Equip. Co., 3:11-CV-313, 2011 WL 4479196 (E.D. Tenn. Sept. 26, 2011) (Applying Texas Law).

Covenants Not to Compete in Georgia

How to avoid the pitfalls of non-compete agreements – what you don't know *could* hurt you.

Arbitration in the Employment Context

John G. Perry *
G. William Long III
Womble Bond Dickinson (US),
A Limited Liability Partnership
271 17th St., N.W.
Suite 2400
Atlanta, Georgia 30363
(404) 879-2441
John.Perry@wbd-us.com

Thomas J. Gallo
Barnes & Thornburg LLP
Prominence in Buckhead
3475 Piedmont Road, N.E.
Suite 1700
Atlanta, Georgia 30305
(404) 846-1693
www.btlaw.com

* *My thanks to Bill Long and Tom Gallo for their years of work in compiling the vast majority of these materials and their permission to use them in this year's presentation.*

January 10, 2019

TABLE OF CONTENTS

I. ARBITRATION CLAUSES IN EMPLOYMENT CONTRACTS

The Georgia Arbitration Code ("GAC") governs arbitration proceedings in Georgia to the extent they are not preempted by the Federal Arbitration Act. See O.C.G.A. §§ 9-9-1, et. seq. The GAC applies to all disputes in which the parties have agreed in writing to arbitrate, and provides the exclusive means by which such agreements can be enforced. See O.C.G.A. § 9-9-2. It provides a means by which the parties can demand arbitration, procedures to be followed in arbitration, discovery rules, selection of an arbitrator, the effect of an award, and procedures for appealing or vacating an award. Id.

The GAC does not apply to "any contract relating to terms and conditions of employment unless the clause agreeing to arbitrate is initialed by all signatories at the time of the execution of the agreement." O.C.G.A. § 9-9-1(c)(9) (emphasis added). Thus, under Georgia law, unless the parties initial an arbitration clause contained within an employment contract, it is unenforceable. See, e.g., ISS Int'l Serv. Sys. v. Widmer, 589 S.E.2d 820 (Ga. App. 2003); Primerica Financial Services, Inc. v. Wise, 217 Ga. App. 36, 456 S.E.2d 631, 635 (1995); Columbus Anesthesia Group, P.C. v. Kutzner, 218 Ga. App. 51, 459 S.E.2d 422 (1995).

A. Preemption by the Federal Arbitration Act.

Where an arbitration agreement falls within the scope of the Federal Arbitration Act ("FAA"), the federal statute preempts the GAC. Attenborough v. Dillard's Dep't Store, 1:06 CV 0291 TWT, 2006 WL 1663299 (N.D. Ga. June 9, 2006); Columbus Anesthesia Group, 459 S.E.2d at 423. In determining the enforceability of an arbitration provision, the FAA preempts state law to the extent it treats arbitration agreements differently from other contracts. Sanders v. Kave Enterprises, LLC, 3:07-CV-123CDL, 2008 WL 275746, at *3 (M.D. Ga. Jan. 30, 2008), citing Caley v. Gulfstream Aerospace Corp., 428 F.3d 1359 (11th Cir. 2005). In cases where the

FAA preempts Georgia's arbitration code, the FAA governs as to substantive issues. The GAC, however, sets forth the procedural body of law that controls the arbitration process in Georgia courts, i.e. seeking to confirm or vacate an arbitration award. SCSJ Enters, Inc. v. Hansen & Hansen Enters, Inc., 306 Ga. App. 188, 702 S.E.2d 12 (2010); Green Tree Servicing, LLC v. Jones, 333 Ga. App. 184, 775 S.E.2d 714 (2015) ("Georgia is entitled to apply its own procedural rules where those rules do not undermine the FAA objective to enforce private arbitration agreements.").

A contract falls within the scope of the FAA where it "evidenc[es] a transaction involving commerce." 9 U.S.C. § 2. See Caley v. Gulfstream Aero. Corp., 428 F.3d 1359 (11th Cir. 2005); Greenway Capital Corp. v. Schneider, 229 Ga. App. 485, 494 S.E.2d 287 (1997) ("Where there has been no agreement by the parties to be bound by state arbitration law, and where the transaction involved interstate commerce within the meaning of the [FAA], state law is preempted by federal law"); Hydrick v. Management Recruiters International, Inc., 738 F. Supp. 1434 (N.D. Ga. 1990) (where contract involved interstate commerce, FAA governed over state arbitration law).

Federal law will not preempt state law where there is no effect on interstate commerce. In Columbus Anesthesia Group, supra, the court held that the GAC applied to a doctor's employment agreement, where it did not involve interstate commerce because it was for membership in a Georgia corporation and for services to be performed in Georgia. Id. at 424.

Under the FAA, the agreement to arbitrate must be in writing, but it does not have to be executed by the parties. See, e.g., Bruce v. Pharmacentra, LLC, CIV.A.1:07CV3053TWT, 2008 WL 1902090 (N.D. Ga. Apr. 25, 2008); Caley v. Gulfstream Aero. Corp., 428 F.3d 1359, 1368–69 (11th Cir. 2005); Tam Nguyen v. Federated Dep't Stores, Inc., 1:05-CV-0140-JOF, 2005 WL

8155067 (N.D. Ga. July 12, 2005), report and recommendation adopted sub nom. Nguyen v. Federated Dep't Stores, Inc., CIV.A. 105CV0140JOF, 2006 WL 149051 (N.D. Ga. Jan. 19, 2006). In McBride v. Gamestop, Inc., the court held that an employee's continued employment constituted acceptance of the terms of an arbitration agreement of which they had notice. McBride, 1:10-CV-2376-RWS, 2011 WL 578821 (N.D. Ga. Feb. 8, 2011). In Payne v. WBY, Inc., the Court held that posting an arbitration policy in the employees' dressing room was not sufficient to create a binding agreement. 141 F. Supp. 3d 1344 (N.D. Ga. 2015).

Section 1 of the FAA contains a narrow exemption. 9 U.S.C. § 1. Under Section 1, employment contracts of transportation workers are exempt, even where interstate commerce is involved. See Circuit City Stores v. Adams, 121 S.Ct. 1302, 522 U.S. 105 (2001); (construing exemption in Section 1 of the FAA, which states: "[N]othing herein contained shall apply to contracts of employment of seamen, railroad employees, or any other class of workers engaged in foreign or interstate commerce. 9 U.S.C.A. § 1"). See also, Attenborough, 2006 WL 1663299 (FAA applies where employee was not a transportation worker); Hill v. Rent-A-Center, Inc., 398 F.3d 1286 (11th Cir. 2005) (where employee not a transportation worker, arbitration agreement is not exempt from the FAA); Roberson v. Clear Channel Broadcasting, Inc., 144 F.Supp. 2d 1371 (S.D. Fla. 2001).

Parties to a contract also have the ability to agree whether federal or state arbitration law will control the arbitration. In Primerica, 456 S.E.2d at 635, the court held that the GAC did not apply, because the parties had expressly agreed within the contract that the FAA would govern arbitration. See also Anderson v. AIG Life & Ret., 199 F. Supp. 3d 1371 (S.D. Ga. 2016), aff'd sub nom. Anderson v. Am. Gen. Ins., 688 Fed. Appx. 667 (11th Cir. 2017) (enforcing arbitration provision as requested by employer despite the fact that the provision was unilateral in that it

allowed the employer, but not the employee, to elect to carve out equitable actions from the provision. This did not render the provision illusory or otherwise unenforceable).

B. Claims Subject To Arbitration.

The claims that are subject to arbitration depend upon the scope of the parties' agreement. TermNet Merch. Servs. v. Phillips, 277 Ga. 342, 588 S.E.2d 745 (2003) (bifurcating trial of the case, holding that all claims arising from the employment be submitted to binding arbitration as provided in the agreement); Lambert v. Austin, Ind., 544 F3d 1192 (11th Cir. 2008) (holding arbitration provisions covering "workplace disputes" or "arising from or related to employment" applies in termination and post-termination contexts); BellSouth Corp. v. Forsee, 265 Ga. App. 589, 595 S.E.2d 99 (2004) (holding arbitration provision required arbitration of "any dispute, controversy or claim arising out of or relating to" the employment agreement or to "the breach, termination or invalidity" thereof, pursuant to the rules of the American Arbitration Association."). All doubts concerning the scope of arbitrable issues should be resolved in favor of arbitration. Forsee, 595 S.E.2d at 102–03; DBGS, LLC v. Kormanik, 333 Ga. App. 22, 775 S.E.2d 283 (2015). An injunction against arbitration is only warranted where a claim "clearly falls outside of the substantive scope of the agreement." Id. In deciding whether a claim is subject to arbitration, the court should not examine the merits of the claims. Id. If claims not expressly subject to arbitration are presented in the arbitration proceeding, the parties are bound by the arbitration award. Ansley Marine Construction, Inc. v. Swanberg, 290 Ga. App. 388, 660 S.E.2d 6 (2008). In Nitro-Lift Technologies, LLC v. Howard, 133 S. Ct. 500 (2012), the Supreme Court held that a state court cannot determine enforceability of noncompetition covenant when there is an enforceable arbitration agreement; the arbitrator has the power to decide the enforceability of the noncompetition covenant.

In Supply Basket, Inc. v. Global Equipment Company, Inc., the District Court held that when an arbitration agreement incorporates the rules of the American Arbitration Association, the arbitrator – not the court – has authority to determine the enforceability of the arbitration agreement. Supply Basket, Inc., 1:13-CV-3220-RWS, 2013 WL 5729574 (N.D. Ga. Oct. 22, 2013). See also Fatt Katt Enters., Inc. v. Rocksolid Granit (USA), Inc., 1:17-CV-1900-MHC, 2018 WL 482461 (N.D. Ga. Jan. 11, 2018) (holding delegation clause and incorporation of the AAA rules dictated that arbitrator decides whether the arbitration clause applies and the claims are arbitrable); Cellairis Franchise, Inc. v. Duarte, CV 2:15-CV-00101-WCO, 2015 WL 11422299 (N.D. Ga. July 20, 2015) (denying request for preliminary injunction, since arbitration provision provided that the scope of a carve out for judicial determination of equitable claims was itself subject to determination by the arbitrator in the first instance.); Cellairis Franchise, Inc. v. Duarte, 2:15-CV-00101-WCO, 2015 WL 6517487 (N.D. Ga. Oct. 21, 2015) (after arbitrator ruled that plaintiff could pursue injunctive relief in court, court granted preliminary injunction under Georgia's "new" law, although covenants would have been void under old law).

C. Courts Have Authority to Stay Proceedings, Compel Arbitration, Dismiss and Enjoin Competition Pending Arbitration.

Where a valid arbitration clause exists in an employment agreement, pursuant to sections 3 and 4 of the FAA, courts have the authority to stay a pending litigation pending the outcome of the arbitration and compel the parties to arbitrate. 9 U.S.C. §§ 3 and 4 (section 3 mandates that the federal court "stay" proceedings; section 4 authorizes federal court to compel arbitration in its district).

If the venue of the arbitration is outside the district of the trial court, the court may stay the judicial proceedings even if it cannot compel arbitration in a foreign venue. See, e.g., Sanders v. Kane Enterprises, LLC, 3:07-CV-123CDL, 2008 WL 275746 (M.D. Ga. Jan. 30,

2008) ("The FAA permits a court to grant a motion to stay even if it does not have authority to compel arbitration."); Haluska v. RAF Financial Corp., 875 F. Supp. 825 (N.D. Ga. 1994).

In determining whether to stay proceedings and compel arbitration or dismiss, the courts determine whether: "(1) there is a valid written agreement to arbitrate; (2) the issue [sought to be arbitrated] is arbitrable under the agreement; and (3) the party asserting the claims has failed or refused to arbitrate the claims." Young v. Quixtar, Inc., 1:07-CV-02310-WSD, 2008 WL 269516 (N.D. Ga. Jan. 29, 2008), quoting Lomax v. Woodmen of the World Life Insurance Society, 228 F. Supp. 2d 1360 (N.D. Ga. 2002).

Federal courts in Georgia routinely stay proceedings and compel parties to arbitrate disputes. See, e.g., Fatt Katt Enters., Inc. v. Rocksolid Granit (USA), Inc., 1:17-CV-1900-MHC, 2018 WL 482461 (N.D. Ga. Jan. 11, 2018); Supply Basket, Inc. v. Glob. Equip. Co., Inc., 1:13-CV-3220-RWS, 2014 WL 2515345 (N.D. Ga. June 4, 2014); Wedemeyer v. Gulfstream Aerospace Corp., 739 S.E.2d 241 (Ga. App. 2013) (Trial court properly exercised its "gatekeeper role" in determining that claims of a former employee were covered by the arbitration agreement and properly granted the employer's motion to compel arbitration.); Slawienski v. Nephron Pharm. Corp., 1:10-CV-0460-JEC, 2010 WL 5186622 (N.D. Ga. Dec. 9, 2010) (Stay); Alexander v. Nissan, 4:10-CV-270, 2011 WL 1557852 (S.D. Ga. Apr. 25, 2011) (Stay); Zekri v. Macy's Retail Holdings, Inc., 1:10-CV-1740-MHS, 2010 WL 4660013 (N.D. Ga. Nov. 4, 2010) (Stay and compelling arbitration); Fitzgerald v. Asbury Auto. Atlanta, LLC, CIVA 107CV-2080-TWT, 2008 WL 544744 (N.D. Ga. Feb. 26, 2008); Young v. Quitar, Inc., 1:07-CV-02310-WSD, 2008 WL 269516 (N.D. Ga. Jan. 29, 2008); Smith v. First Equity Card Corp., 4:08-CV-08(CDL), 2008 WL 4541012 (M.D. Ga. Oct. 9, 2008); Jones v. Titlemax of Georgia, Inc., CIV.A. 105CV1154TWT, 2006 WL 562189 (N.D. Ga. Mar. 7, 2006); Johnson v. Macy's South,

LLC, 1:07-CV-1256-WSD, 2007 WL 2904126 (N.D. Ga. Sept. 27, 2007). In Jones v. Titlemax of Georgia, Inc., although court held that all of plaintiffs' claims were subject to arbitration, it stayed the litigation, rather than dismiss it, in the event that the arbitrator concluded that any of plaintiffs' claims belong in court. Courts also dismiss actions subject to enforceable arbitration agreements. CIV.A. 105CV1154TWT, 2006 WL 562189 (N.D. Ga. Mar. 7, 2006)2006 WL 562189 (N.D. Ga.). See, e.g., Odeion v. Avesis, Inc., 327 Ga. App. 443, 759 S.E.2d 638 (2014); Shubert v. Scope Products, Inc., 2:10-CV-00101-RWS, 2011 WL 3204677 (N.D. Ga. July 27, 2011). But see, Beverly Enterprises, Inc. v. CYR, 608 Fed. App. 924 (11th Cir. 2015) (Reversing trial court's order to compel arbitration where the designated arbitration forum was no longer conducting consumer arbitrations).

Georgia courts also have the authority to grant a temporary injunction restricting competition while arbitration is pending, so long as the non-compete agreement is enforceable. In Forsee, the trial court originally granted an *ex parte* TRO enjoining Forsee from accepting employment with Sprint pending arbitration. 595 S.E.2d at 100. After conducting an emergency hearing, the court issued an order finding the noncompetition covenant in Forsee's employment agreement to be unenforceable under Georgia law and dissolved the part of the TRO that related to it. BellSouth appealed, arguing that the court erroneously made a determination on the issue of enforceability, which should have been left to the arbitrator. The Georgia Court of Appeals affirmed, holding that the severability clause in the contract allowed the trial court to modify the TRO and to remove the issue of enforceability from the arbitrator's decision.

In Global Link Logistics, Inc. v. Briles, the Court of Appeals affirmed the decision of the trial court determining that restrictive covenants were unenforceable and entered a temporary restraining order barring their enforcement. 296 Ga. App. 175, 674 S.E.2d 52 (2009). The trial

court then ordered the parties to arbitrate all remaining claims. On appeal, the court concluded that there was no contractual provision or legal rule that barred the employee from seeking injunctive relief barring enforcement of the restrictive covenants prior to arbitration.

In Merrill Lynch, Pierce, Fenner, & Smith v. Schwartz, the court granted an injunction pending the outcome of arbitration before the National Association of Securities Dealers (NASD). 991 F. Supp. 1480, 1482 (M.D. Ga. 1998). After finding the covenant not to compete valid, the court reasoned that even a few days of solicitation can cause irreparable harm in this case, and an injunction was warranted. Id. at 1482.

D. Review of Arbitrator's Award.

Under Georgia law, judicial review of an arbitrator's award is very narrow. Berger v. Welsh, 326 Ga. App. 290, 756 S.E.2d 545 (2014); Malice v. Coloplast Corp., 629 S.E.2d 95 (Ga. App. 2006) ("Judicial review of an arbitration awards is among the narrowest known to the law"). Courts are not permitted to inquire into the merits of the case or consider the sufficiency of the evidence. Payton v. Jackson, 326 Ga. App. 319, 756 S.E.2d 555 (2014); Lanier Worldwide, Inc. v. BridgeCenters at Park Meadows, LCC, 633 S.E.2d 49 (Ga. App. 2006). Arbitrators are permitted to make an award on broad principles of fairness and equity and need not state the basis to support their award. With respect to modification of an arbitration award, the scope of a trial court's review is governed by statutory grounds. Id. A trial court is bound to confirm an arbitration award unless one of the statutory grounds for vacating an award is found to exist. Bilbo v. Five Star Athlete Mgmt., Inc., 334 Ga. App. 208, 778 S.E.2d 834 (2015).

The FAA provides four grounds upon which a court may vacate an arbitrator's award. Section 10(a) of the FAA provides:

> In any of the following cases the United States court in and for the district wherein the award was made may make an order vacating the award upon the application of any party to the arbitration –
>
> (1) Where the award was procured by corruption, fraud, or undue means.
>
> (2) Where there was evident partiality or corruption in the arbitrators, or either of them.
>
> (3) Where the arbitrators were guilty of misconduct in refusing to postpone the hearing, upon sufficient cause shown, or in refusing to hear evidence pertinent and material to the controversy; or of any other misbehavior by which the right of any party have been prejudiced.
>
> (4) Where the arbitrators exceeded their powers, or so imperfectly executed them that a mutual, final, and definite award upon the subject matter submitted was not made.
>
> (5) Where an award is vacated and the time within which the agreement required the award to be made has not expired the court may, in its discretion, direct a rehearing by the arbitrators.

O.C.G.A. § 9-9-13 sets forth the grounds under Georgia law for vacating an award. As compared to the FAA, Georgia has recognized three additional bases on which an award may be vacated: (1) if the award is arbitrary and capricious; (2) if it is contrary to public policy; or (3) if it is made in manifest disregard of law. Malice, 629 S.E.2d at 98. A decision is only in "manifest disregard" of the law if the arbitrator deliberately ignored the law. An error in interpretation of the law will not constitute manifest disregard. Id. In Malice, the employee challenged the arbitrator's decision that he had violated his non-compete agreement, arguing that it was in manifest disregard of the law. The court upheld the award, finding that the employee was merely asserting that the arbitrator erred in interpreting the law. The court agreed with the arbitrator's finding that the covenants at issue were enforceable and that the employee violated them. See Berger v. Welsh, supra.

In Brookfield Country Club, Inc. v. St. James Brookfield, Inc., the Georgia Supreme Court held parties to an arbitration agreement cannot expand or modify by contract the statutory grounds for vacating of an award. 287 Ga. 408, 696 S.E.2d 663 (2010). In Atlanta Flooring Design Centers, Inc. v. R.G. William Construction, Inc., the Georgia Court of Appeals held that a contractual provision waiving the right to challenge an arbitration award is void and unenforceable and contrary to Georgia public policy. 333 Ga. App. 528, 773 S.E.2d 868 (2015).

Under both Georgia and federal law, it is important to comply with procedural requirements regarding modification of the arbitration award and objections to confirmation. See, e.g., Bilbo v. Five Star Athlete Mgmt., Inc., 334 Ga. App. 208, 778 S.E.2d 834 (2015) (under Georgia act, a request to modify the award – in that case, to include an award of attorney's fees – must be made within 90 days of receipt of the award or it is waived); Careminders Home Care, Inc. v. Kianka, 666 Fed. Appx. 832 (11th Cir. 2016) (under the federal act, "This Court has long held that the failure of a party to move to vacate an arbitral award within the three-month limitations period prescribed by section 12 of the FAA bars it from raising the alleged invalidity of the award as a defense in opposition to a motion brought under section 9 of the USAA to confirm the award." Id. at *2 (internal quotes and citations omitted).

Covenants Not to Compete in Georgia

How to avoid the pitfalls of non-compete agreements – what you don't know *could* hurt you.

Breach of Fiduciary Duty in the Employment Context

John G. Perry*
G. William Long III
Womble Bond Dickinson (US),
A Limited Liability Partnership
271 17th St., N.W.
Suite 2400
Atlanta, Georgia 30363
(404) 879-2441
John.Perry@wbd-us.com

Thomas J. Gallo
Barnes & Thornburg LLP
Prominence in Buckhead
3475 Piedmont Road, N.E.
Suite 1700
Atlanta, Georgia 30305
(404) 846-1693
www.btlaw.com

* *My thanks to Bill Long and Tom Gallo of Barnes & Thornburg LLP for their years of work in compiling the vast majority of these materials and their permission to use them in this year's presentation.*

January 10, 2019

BREACH OF FIDUCIARY DUTY

The Georgia Supreme Court has held that fiduciary duties are owed where a confidential relationship exists between the parties. Atlanta Market Center Management Co. v. McLane, 269 Ga. 604, 606, 503 S.E.2d 278, 281 (1998). O.C.G.A. § 23-2-58 delineates that a "confidential relationship" arises under Georgia law:

> . . . whether arising from nature, created by law, or resulting from contracts, where one party is so situated as to exercise a controlling authority over the will, conduct, and interest of another or where, from a similar relationship of mutual confidence, the law requires the utmost good faith, such as the relationship between partners, principal and agent, etc.

See also Megel v. Donaldson, 288 Ga. App. 510 (2007).

A failure to act in the best interests of the employer while still employed may give rise to a claim for breach of fiduciary duty or the duty of loyalty.[1] In Impreglon, Inc. v. Newco Enterprises, Inc., the trial court entered summary judgment against Jarrell, former President and CEO of Impreglon, finding that while employed by Impreglon, Jarrell solicited Impreglon's customers. 508 F. Supp. 2d 1222 (N.D. Ga. 2007). The court held Jarrell liable for breach of fiduciary duty after holding corporate officers and directors owe a fiduciary relationship to the corporation and its shareholders, and finding Jarrell's activities went beyond "merely making plans to enter a competing business." In Professional Energy Management v. Necaise, the plaintiff's former employer stated a claim for breach of fiduciary duty where the employee, while still employed, solicited existing and prospective clients to contract with his rival business. 300 Ga. App. 223, 684 S.E.2d 374 (2009). The Court of Appeals further held that the breach of

[1] A cause of action for breach of loyalty must be based upon a fiduciary duty owed by the employee and must "rise and fall with any claim for breach of fiduciary duty." See Vernon Library Supplies, Inc. v. Ard, 249 Ga. App. 853, 550 S.E.2d 108 (2001).

fiduciary duty claim was not preempted by the Georgia Trade Secrets Act, O.C.G.A. § 10-1-767, et. seq.

Employees are free to compete (absent a contractual obligation) after the end of employment; actions taken by them cannot be in breach of these duties (if they were ever owed).[2] Where an agency relationship is created between two parties, it will be deemed confidential. In the employment context, although an employee may act on behalf of his employer at certain times, it does not necessarily mean that an agency relationship has been created. Atlanta Market, 503 S.E.2d at 281; Cochran v. Murrah, 235 Ga. 304, 219 S.E.2d 421 (1975). In order for an employee to be deemed an agent of his employer, he must be "vested with authority, real or ostensible, to create obligations on behalf of [the employer], bringing third parties into contractual relations with [the employer]." Atlanta Market, 503 S.E.2d at 281; Hilb, Royal & Hamilton Co. v. Holley, 295 Ga. 54, 670 S.E.2d 874 (2008); Sitton v. Print Direction, Inc., 312 Ga. App. 365, 718 S.E.2d 532 (2011) (evidence that employee had authority to solicit business on employer's behalf and to bind employer for certain obligations authorized finding of fiduciary duty); Wright v. Apartment Inv. And Management Co., 315 Ga. App. 587, 726 S.E.2d 779 (2012) (evidence that employee had authority to solicit and review bids and make recommendations and authority to approve changes in scope of work, contract documents, scheduling and costs authorized a finding of fiduciary duty).

[2] This is distinguished from the duties owed to a corporation by directors and officers. Officers and directors are required to act with "utmost good faith and loyalty and in the best interests of the corporation." Brewer v. Insight Technology, Inc., 301 Ga. App. 694, 689 S.E.2d 330 (Ga. App. 2009); Hilb, Royal & Hamilton Company v. Holley, 295 Ga. App. 54, 670 S.E.2d 874 (2008). These duties have also been described as requiring officers and directors to "discharge their duties in good faith with the care of an ordinary prudent person in similar positions." Sewell v. Cancel, 331 Ga. App. 687, 691, 771 S.E.2d 388 (2015). They are also prohibited, even after separation from the company, from appropriating business or corporate opportunities existing at the time of resignation. O.C.G.A. § 14-2-153. If an opportunity falls within the "scope and ability of [the corporation's] business and that [the corporation] had both an interest and an expectancy in [the business] growing out of its prior relationship." McCrary, 273 S.E.2d at 116; B.S.T. AG Sols., Inc. v. PWB AG Consulting, LLC, 1:15-CV-88 LJA, 2015 WL 4067569 (M.D. Ga. July 2, 2015).

Corporate officers and directors occupy a fiduciary relationship to the corporation and its shareholders and are held to the standard of "utmost good faith and loyalty." Lubin v. Skow, 382 Fed. Appx. 866 (11th Cir. 2010); Quinn v. Cardiovascular Physicians, P.C., 254 Ga. 216, 326 S.E.2d 460 (1985); Wachovia Insurance Services, Inc. v. Fallon, 299 Ga. App. 440, 682 S.E.2d 657 (2009); Thunderbolt Harbor Phase II Condominium Association, Inc. v. Ryan, 326 Ga. App. 580, 757 S.E.2d 189 (2014) (Sole officer and director of a homeowner's association owed fiduciary duty). A managing member of a limited liability company owes a fiduciary duty to its fellow members. Denim N. Am. Holdings, LLC v. Swift Textiles, LLC, 816 F. Supp. 2d 1308 (M.D. Ga. 2011)[3].

The Supreme Court of Georgia has held that the duty owed by an agent who is neither an officer nor a director of the principal is one of loyalty and good faith, and such an agent "may not make a profit for himself out of the relationship or out of the knowledge obtained from the relationship, to the injury of the principal." Koch v. Cochran, 251 Ga. 559, 307 S.E.2d 918, 919 (1983). See also Harrison v. Harrison, 214 Ga. 393, 105 S.E.2d 214, 218 (1958); Instrument Repair Service, Inc. v. Gunby, 238 Ga. App. 138, 518 S.E.2d 164 (1999); Nilan's Alley, Inc. v. Ginsburg, 208 Ga. App. 145, 430 S.E.2d 368 (1993); Hanson Staple Co. v. Eckelberry, 297 Ga. App. 356, 677 S.E.2d 321 (2009). In Gunby, the court affirmed summary judgment in favor of the defendants where "the evidence was undisputed that [the defendants] did not unlawfully profit at the expense of [the plaintiff] during any agency relationship." 518 S.E.2d at 164.

In Atlanta Market, the Atlanta Market Center ("AMC") employed McLane as a leasing director. She was an at-will employee. McLane was required to obtain approval before she could

[3] O.C.G.A. §14-11-305(1) provides: "In managing the business or affairs of a limited liability company [, a] member or manager shall act in a manner he or she believes in good faith to be in the interests of the limited liability company[.]" A member of an limited liability company in which management is vested in a manager, and who is not a manager, owes no duties to the company or the other members solely by reason acting in the capacity as a member, however. Id.

enter into any leases on AMC's behalf. Following the termination of her employment, McLane brought suit against AMC, alleging that it had breached its fiduciary duties to her by failing to pay her certain commissions. The Court of Appeals held that AMC had a fiduciary duty toward McLane, implicitly finding that an agency relationship existed between them. The Georgia Supreme Court reversed, holding that because there was no evidence that McLane had any authority to obligate AMC by entering into contracts on its behalf there was no agency relationship created between them. Id. at 281. Since she failed to establish that she was AMC's agent, there could be no breach of any fiduciary duty. Id.

Where employees have no authority to bind their employer while employed, or to hire or fire other employees, there is no agency relationship and, therefore, no fiduciary duties are owed. Physician Specialists In Anesthesia, P.C. v. Wildmon, 238 Ga. App. 730, 521 S.E.2d 358 (1999). Physician Specialists In Anesthesia ("Physician Specialists") was in the business of anesthesia and pain management. Pain Management was a corporation that was operated and controlled by Physician Specialists. Id. at 359. Duddles was employed at Pain Management, and Wildmon was employed at Physician Specialists, both as Assistant Practice Administrators, and both as at-will employees. Id. Following the termination of their employment, Physician Specialists brought suit against both defendants, alleging that they had breached their fiduciary duties and their duty of loyalty to it by providing confidential information to its competitors. The trial court granted summary judgment for the defendants.

In affirming the grant of summary judgment, the Court of Appeals found that neither employee had authority to: (1) enter into contracts on behalf of either company; (2) hire or fire personnel of either company; or (3) sign checks or make payments on behalf of either company. Id. The Court concluded that because neither defendant could "create obligations on behalf of

Physician Specialists or bring third parties into contractual relations with it," they were not agents of either company, and therefore owed it no fiduciary duties. Id. See also Lou Robustelli Marketing, Services, Inc. v. Robustelli, 286 Ga. App. 816, 650 S.E.2d 326 (2007) (holding employee performing clerical work not liable for breach of fiduciary duty because employee was neither an officer or director nor an agent and she lacked authority to deal with third parties on behalf of employer); White v. Shamrock Bldg Systems, Inc., 294 Ga. App. 340, 669 S.E.2d 168 (2008) (reversing summary judgment in favor of employee and finding evidence sufficient to present jury question as to existence of fiduciary duty, breach by soliciting employer's customers while employed and aiding and abetting by newly formed corporation); Scott v. State, 810 S.E.2d 613, 616, 344 Ga. App. 412, 416 (2018) (finding no fiduciary duty where employee "did not have authority to act for [employer] beyond weighing the metals and assigning to the weight a dollar amount that had been previously fixed by [the employer]. He could not negotiate with the customers, independently determine how much the metals were worth, or obligate [employer] to the customer for anything beyond what [employer] had determined it would pay to each customer.").

In Gordon Document Products, Inc. v. Service Technologies, Inc., the Court of Appeals held that an employee's authority to bind the employer must relate to type of transaction being complained of. 708 S.E.2d 48 (Ga. App. 2011). In Gordon, the former employee was accused of improperly soliciting his co-workers. While the former employee may have had the authority to bind the company with respect to customer contracts, he had no authority to bind the company on employment matters. The Court of Appeals concluded, therefore, that he could not be liable for breach of fiduciary duty in soliciting his co-workers. See also HCC Insurance Holdings, Inc. v. Flowers, 237 F. Supp. 3d 1341 (N.D. Ga. 2017) (holding in-term solicitation of co-workers to

leave and go work with a competitor can be a breach of fiduciary duty if the solicitor is an officer or employee with power to bind the company on employment matters, uses his/her position to induce the co-worker to leave, and initiated the conversations. Otherwise, probably not a breach). Compare, Burson v. Milton Hall Surgical Associates, LLC, 806 S.E.2d 239 (Ga. App. 2017) (employee cannot solicit customers or otherwise engage in direct competition while still employed).

Georgia courts have recognized that even where an employee is not an agent of the employer, a confidential relationship may nonetheless arise due to the specific facts of the situation. Although an employer/employee relationship generally does not create a confidential relationship as a matter of law, under certain facts, such a relationship may be created. Bedsole v. Action Outdoor Advertising JV, LLC, 325 Ga. App. 194, 750 S.E.2d 445 (2013); Cochran v. Murrah, 235 Ga. 304, 219 S.E.2d at 421, 423–24 (1975). See also Atlanta Market, 503 S.E.2d at 281. However, "the mere circumstance that two people have come to repose a certain amount of trust, and confidence in each other as a result of business dealings is not, in and of itself, sufficient to find the existence of a confidential relationship." Parello v. Maio, 268 Ga. 852, 494 S.E.2d 331 (1998). In Parello, the court refused to hold that a confidential relationship existed between the owner of a barbershop, and the lessee of a chair in his shop, despite the fact that they had a business relationship for a prolonged period of time, and that the defendant was primarily responsible for the day-to-day operations of the business. Id. at 333. The court noted that there was no evidence that the plaintiff exercised a controlling influence over the will of the defendant with respect to the transaction at issue. Id.

In Irons v. CSX Transportation, Irons was an employee at CSX who was injured on the job. 224 Ga. App. 586, 481 S.E.2d 575 (1997). Following his injury, a representative of CSX

spoke to Irons with regard to a possible claim against a third party. Irons alleged that the claims representative made misrepresentations to him regarding his rights against the third party, in breach of his fiduciary duty. Id. at 576. He claimed that the actions of the representative created a confidential relationship between him and CSX, giving rise to such a duty. The court rejected this argument, holding that no confidential relationship existed, as there were no facts to show any controlling influence over Irons or that there was any interaction between the representative and Irons from "positions of mutual confidence so that Irons should have believed anything other than that their relationship was an arms-length—and even adversarial—one." Id. at 577. The court granted summary judgment to CSX. Id. See also Gale v. Hayes Microcomputer Products, Inc., 192 Ga. App. 30, 383 S.E.2d 590 (1989) (no confidential relationship existed between plaintiff and defendant; relationship was merely one of employee to employer).

Assuming an employee owes duties to the employer, Georgia law is clear that he can make plans to compete while employed, so long as he does not do so on the employer's time or using the employer's resources. Well-established Georgia law holds that an employee "breaches no fiduciary duty to the employer simply by making plans to enter a competing business while he is still employed." Lou Robustelli Mktg. Servs. v. Robustelli, 286 Ga. App. 816, 650 S.E.2d 326 (2007); Hanson Staple Co. v. Eckelberry, 297 Ga. App. 356, 677 S.E.2d 321 (2009); Nilan's Alley, 430 S.E.2d at 369; E.D. Lacey Mills, Inc. v. Keith, 183 Ga. App. 357, 359 S.E.2d 148, 155 (1987); Vernon Library Supplies, Inc., 550 S.E.2d at 111. "Before the end of employment, he can properly purchase a rival business and upon termination of employment immediately compete." Id. at 362. An employee agent, however, may not solicit customers for a competing business or otherwise engage in direct competition while still employed. See Sitton v. Print Direction, Inc., 312 Ga. App. 365, 718 S.E.2d 532 (2011) (Employee had authority "to bind PDI

for certain obligations, which authorized the trial court to find that Sitton, as PDI's agent, owed a fiduciary duty to his employer, PDI."); Wachovia Insurance Services, Inc. v. Fallon, 299 Ga. App. 440, 682 S.E.2d 657 (2009); Hilb, Royal & Hamilton Company v. Holley, 295 Ga. App. 54, 670 S.E.2d 874 (Ga. App. 2008) (Affirming jury verdict against employee who had been appointed as a client contact at a competitor, created an e-mail account and telephone number of competitor and printed conference invitations listing him as competitor of employer); Impreglon, Inc. v. Newco Enterprises, Inc., 508 F. Supp. 2d 1222 (N.D. Ga. 2007). In addition, an employee may breach her duty of loyalty by deleting client contact information or destroying client files prior to departing her former employer. Fine v. Commc'n Trends, Inc., 305 Ga. App. 298, 699 S.E.2d 623 (2010). An employee may breach his fiduciary duty to his former employer by using the employer's resources to establish a new competing business. S. Parts & Eng'g Co., LLC v. Air Compressor Servs., LLC, 1:13-CV-2231-TWT, 2014 WL 667958 (N.D. Ga. Feb. 20, 2014).

In cases where an agent breached his fiduciary duty to an employer, the agent forfeits his right to compensation during the period of time in which the agent fails to act in a fiduciary manner. O.C.G.A. § 10-6-31. See, e.g., KEG Technologies v. Laimer, 436 F. Supp. 2d 1364, 1378 (2006); E.H. Crump Co. of Ga. v. Millar, 194 Ga. App. 687, 391 S.E.2d 775 (1990); Vinson v. E.W. Buschman Co., 172 Ga. App. 306, 323 S.E.2d 204 (1984). In a case where an agent sought unsuccessfully to solicit business for his personal benefit while still employed, the employer nevertheless has a claim to seek to recover compensation it paid to its agent during the time of the breach. Helms & Greene, LLC v. Willis, 333 Ga. App. 396, 773 S.E.2d 491 (2015).

Georgia courts also recognize a claim for aiding and abetting a breach of fiduciary duty. See Kahn v. Britt, 330 Ga. App. 377, 389, 765 S.E.2d 446 (2014); Wright v. Apartment Inv. And Management Co., 315 Ga. App. 587, 726 S.E.2d 779 (2012); Insight Tech., Inc. v. FreightCheck,

LLC, 280 Ga. App. 19, 633, S.E.2d 373 (2006); NCI Group, Inc. v. Cannon Services, Inc., 2009 WL 2411145 (N.D. Ga.). A claim for aiding and abetting breach of fiduciary duty requires:

> (1) through improper action or wrongful conduct and without privilege, the defendant acted to procure a breach of the primary wrongdoer's fiduciary duty to the plaintiff; (2) with knowledge that the primary wrongdoer owed the plaintiff a fiduciary duty, the defendant acted purposely and with malice and the intent to injure; (3) the defendant's wrongful conduct procured a breach of the primary wrongdoer's fiduciary duty; and (4) the defendant's tortuous conduct proximately caused damage to the plaintiff.
>
> NCI, 2009 WL 2411145.

Accord, Post-Confirmation Comm. for Small Loans, Inc. v. Martin, 1:13-CV-195 (WLS), 2016 WL 1274124 (M.D. Ga. Mar. 31, 2016).

Covenants Not to Compete in Georgia

How to avoid the pitfalls of non-compete agreements – what you don't know *could* hurt you.

Tortious Interference with Business Relations in the Employment Context

John G. Perry*
G. William Long III
Womble Bond Dickinson (US),
A Limited Liability Partnership
271 17th St., N.W.
Suite 2400
Atlanta, Georgia 30363
(404) 879-2441
John.Perry@wbd-us.com

Thomas J. Gallo
Barnes & Thornburg LLP
Prominence in Buckhead
3475 Piedmont Road, N.E.
Suite 1700
Atlanta, Georgia 30305
(404) 846-1693
www.btlaw.com

* *My thanks to Bill Long and Tom Gallo of Barnes & Thornburg LLP for their years of work in compiling the vast majority of these materials and their permission to use them in this year's presentation.*

January 10, 2019

TABLE OF CONTENTS

I. INTRODUCTION

Georgia courts have long recognized a cause of action for tortious interference with business or contractual relations in the employment context. See Nager v. Lad 'N Dad Slacks, 148 Ga. App. 401, 251 S.E.2d 330 (1978); Rome Industries, Inc. v. Jonsson, 202 Ga. App. 682, 415 S.E.2d 651 (1992); McDaniel v. Green, 156 Ga. App. 549, 275 S.E.2d 124, 126 (1980) ("The intentional and non-privileged interference by a third party with existing contractual rights and relations constitutes a tort for which an action shall lie."). The claim has its basis in the principle that each individual has the right to pursue a legitimate occupation and conduct business in accordance with his own plan, so long as he does not interfere with the rights of others. Perry & Co. v. New South Ins. Brokers, Inc., 182 Ga. App. 84, 354 S.E.2d 852 (1987).

Tortious interference also has a statutory basis in O.C.G.A. §51-12-30, which states, in part:

> [A] person who maliciously procures an injury to be done to another, whether an actionable wrong or a breach of contract, is a joint wrongdoer and may be subject to an action either alone or jointly with the person who actually committed the injury.

II. GENERAL ELEMENTS OF A CLAIM OF TORTIOUS INTERFERENCE

Claims for tortious interference with contractual relations and business relations have the same elements under Georgia law. The plaintiff must show that the defendant:

(1) Acted improperly and without privilege;

(2) Acted purposely and with malice and with the intent to injure;

(3) Induced a third party or parties not to continue a business relationship with the plaintiff; and

(4) The plaintiff suffered financial injury as a result.

U.S. Capital Funding VI, Ltd. v. Patterson Bankshares, Inc., 137 F. Supp. 3d 1340 (S.D. Ga. 2015); Earthcam, Inc. v. OxBlue Corporation, 49 F. Supp. 3d 1210 (N.D. Ga. 2014), aff'd, 703 Fed. Appx. 803 (11th Cir. 2017); White v. Shamrock Bldg. Systems, Inc., 294 Ga. App. 340, 669 S.E.2d 168 (2008) (holding tortious interference involves proof of same elements as aiding and abetting breach of fiduciary duty); Kirkland v. Tamplin, 285 Ga. App. 241, 645 S.E.2d 653 (2007); Coloplast Corp. v. Am. Breast Care, L.P., 209 Fed. Appx. 945 (11th Cir. 2006); Ferrellgas Partners, Inc. v. Barrow, 4:03-CV-107 (WDO), 2006 WL 372602 (M.D. Ga. Feb. 16, 2006); Bacon v. Volvo Services Center, Inc., 266 Ga. App. 543, 597 S.E.2d 440 (2004); Sumter Regional Hospital, Inc. v. Healthworks, Inc., 264 Ga. App. 78, 589 S.E.2d 666 (2003); Camp v. Eichelkraut, 246 Ga. App. 275, 539 S.E.2d 588 (2000); Watkins & Watkins, P.C. v. Colbert, 237 Ga. App. 775, 516 S.E.2d 347 (1999).[1]

A. Improper Means.

To prove improper means, the plaintiff must show that the defendant used "predatory tactics such as physical violence, fraud or misrepresentation, defamation, use of confidential information, abusive civil suits and unwarranted criminal prosecutions." Ferrellgas, 2006 WL at *13; Abassi v. Bhalodwala, 149 F. Supp. 3d 1372 (M.D. Ga. 2015); General Productions, LLC v. I.A.T.S.E. Local 479, 981 F. Supp. 2d 1357 (N.D. Ga. 2013) (Union had contractual right to interact with plaintiff's employees; actions "justified" or "privileged"); Matthew Focht Enterprises, Inc. v. LePore, 1:12-CV-04479-WSD, 2013 WL 4806938 (N.D. Ga. Sept. 9, 2013); American Bldgs. Co. v. Pascoe Bldg. Systems, 260 Ga. 346, 392 S.E.2d 860 (1990); Gowen Oil

[1] A claim for tortious interference relating to claims for misappropriation of trade secrets may be superseded by The Georgia Trade Secrets Act, O.C.G.A. § 10-1-767. See Diamond Power International, Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); Agilysys, Inc. v. Hall, 258 F.Supp.3d 1331(N.D. Ga. 2017). However, in Professional Energy Management, Inc. v. Necaise, the Court of Appeals held that a tortious interference claim against a third party soliciting plaintiff's customers was not preempted by the GTSA. 300 Ga. App. 223, 684 S.E.2d 374 (Ga. App. 2010).

Co., Inc. v. Greenberg Traurig, LLP, 453 Fed. Appx. 897 (11th Cir. 2011). See also Advanced Testin Technologies, Inc. v. CDI Corporation, 660 F.. App'. 889 (11th Cir. 2016) (applying Georgia law). Inducing a former employee to disclose a competitor's confidential information would support a claim for tortious interference. Fine v. Communication Trends, Inc., 305 Ga. App. 298, 699 S.E.2d 623 (2010). Where a party exercises its rights under a contract, there can be no liability for tortious interference with that contractual relationship. Nobel Lodging, Inc. v. Holiday Hospitality Franchising, Inc., 249 Ga. App. 497, 548 S.E.2d 481 (2001).

Evidence of improper means must be conclusive, and not based upon speculation. Where the court must infer wrongful conduct, the claim will fail. Watkins, 516 S.E.2d at 347; Coloplast, 209 Fed. Appx. At 946 (No evidence of improper interference with employment contracts); Barnwell v. Barnett & Co., 222 Ga. App. 694, 476 S.E.2d 1 (1996) (No evidence of wrongful conduct); Camp, 539 S.E.2d at 593 (same); Palombi v. Frito-Lay, Inc., 241 Ga. App. 154, 526 S.E.2d 375 (1999) (same); Fine, 305 Ga. App. at 309, 699 S.E.2d at 633 (No evidence that employer asked employee to use former employer's customers' billing histories to project future revenue).

B. What Constitutes Malice?

For purposes of a tortious interference claim, "malicious" means "any unauthorized interference" or "interference without legal justification or excuse." Batayias v. Kerr-McGee Corp., 267 Ga. App. 848, 601 S.E.2d 174 (2004). "The act is malicious when the thing done is with the knowledge of the plaintiff's rights, and with the intent to interfere therewith." Architectural Mfg. Co. v. Airotec, Inc., 119 Ga. App. 245, 166 S.E.2d 744, 747 (1969). See also White v. Shamrock Bldg. Systems, Inc., 294 Ga. App. 340, 669 S.E.2d 168 (2008) (No improper action or wrongful conduct by defendant); Cumberland Center Assoc. v. Southeast Mgmt. and

Leasing Corp., 228 Ga. App. 571, 492 S.E.2d 546 (1997), disapproved of on other grounds by Atlanta Market Center Management Co., 503 S.E.2d 278.

Personal ill will is not necessary to create malice. Valdez v. Power Industry Consulting, Inc., 215 Ga. App. 444, 451 S.E.2d 87, 91 (1994) (citing Arford v. Blalock, 199 Ga. App. 434, 405 S.E.2d 698 (1991), aff'd, 262 Ga. 95, 414 S.E.2d 1 (1992)). Subjective good faith is also not sufficient to constitute a defense to the malice element of a claim of tortious interference. Id. at 90. See also Lake Tightsqueeze v. Chrysler First Financial Serv. Corp., 210 Ga. App. 178, 435 S.E.2d 486, 489 (1993).

C. Contractual or Business Relationship.

In order to prove tortious interference with contractual or business relations, a contractual or business relation must exist between the plaintiff and a third party. In All Star, Inc. v. Fellows, 297 Ga. App. 142, 676 S.E.2d 808 (2009), the Court of Appeals affirmed a directed verdict against the plaintiff who failed to prove that it had a business relationship with a third party that defendants allegedly interfered with. The alleged interference must be with a third party; a party cannot tortiously interfere with its own business relationship. H&R Block Eastern Enterprises, Inc. v. Morris, 606 F.3d 1285 (11th Cir. 2010).

D. Financial Injury.

Plaintiff bears the burden of proving that defendant's alleged tortious conduct caused a third party to discontinue or fail to enter into a contractual relationship. Without some evidence that customers or potential customers decided to forego their business relationships due to tortious acts by the defendant, the tortious interference claim fails. B&F System, Inc. v. LeBlanc, 7:07-CV-192 HL, 2011 WL 4103576, at *13 (M.D. Ga. Sept. 14, 2011), on reconsideration in part, 7:07-CV-192 HL, 2011 WL 5117712 (M.D. Ga. Oct. 25, 2011), and aff'd

in part, 519 Fed. Appx. 537 (11th Cir. 2013); T.V.D.B. Sarl v. Kapla USA, 4:12-CV-230, 2013 WL 6623186 (S.D. Ga. Dec. 16, 2013); Seki v. Groupon, Inc., 333 Ga. App. 319, 775 S.E.2d 776 (2015).

III. TORTIOUS INTERFERENCE WITH EMPLOYEE RELATIONS

A. Claims by Employer.

An employer may bring a claim against a former employee or a third party, including the former employee's new employer, for improperly inducing an employee to terminate his or her relationship. See Rome Industries, 415 S.E.2d at 652; Witty v. McNeal Agency, 239 Ga. App. 554, 521 S.E.2d 619 (1999); Ferrellgas Partners, Inc. v. Barrow, 4:03-CV-107 (WDO), 2006 WL 372602, at *13 (M.D. Ga. Feb. 16, 2006).

Employers may also bring a claim against a third party for breach of a former employee's restrictive covenants. Bijou Salon & Spa, LLC v. Kensington Enters., Inc., 283 Ga. App. 857, 843 S.E.2d 531 (2007) (Party may be subject to injunctive relief where there is evidence that it maliciously induced former employee to breach restrictive covenant). However, where the non-compete and/or non-solicitation agreements at issue are unenforceable, no claim for tortious interference of these agreements exists. Thus, an employee's new employer should always examine the enforceability of any restrictive covenants its employees may have with their former employers. Becham v. Synthes (U.S.A.), 5:11-CV-73 MTT, 2011 WL 4102816 (M.D. Ga. Sept. 14, 2011), aff'd on other grounds sub nom. Becham v. Synthes USA, 482 Fed. Appx. 387 (11th Cir. 2012); MAU, Inc. v. Human Techs., Inc., 274 Ga. App. 891, 619 S.E.2d 394 (2005); Atlanta Market Center Management Co. v. McLane Real Estate Investment Management, Inc., 269 Ga. 604, 503 S.E.2d 278, 282 (1998); Lake Tightsqueeze v. Chrysler First Financial Serv., 210 Ga. App. 178, 435 S.E.2d 486 (1993) (Tortious interference must be based on existing

contractual rights); Kitfield v. Henderson, Black & Greene, 231 Ga. App. 130, 498 S.E.2d 537, 541 (1998). Accord, HCC Insurance Holdings, Inc. v. Flowers, 237 F. Supp. 3d 1341 (N.D. Ga. 2017) (no tortious interference with contract claim where non-disclosure covenant void for lack of a time limit under old Georgia law).

Courts have also found that a claim for tortious interference may exist without an actual breach of a contract. It is sufficient that a third party interferes with a contract such that performance of the contract is more difficult or more expensive. Each party to a contract has a property interest in that contract and a right to expect performance of the contract free from interference. Id. (citing Perry & Co. v. New South Ins., 182 Ga. App. 84, 354 S.E.2d 852 (1987)). This concept has its basis in O.C.G.A. § 51-9-1, which states:

> The right of enjoyment of private property being an absolute right of every citizen, every act of another which unlawfully interferes with such enjoyment is a tort for which action shall lie.

Thus, a party may be liable for tortious interference where it induces a breach of a particular duty, such as a fiduciary duty. In Insight Tech., Inc. v. FreightCheck, LLC, the court held that a freight factoring company's allegations that its competitors aided and abetted the company's president's breach of his fiduciary duty stated a viable claim for tortious interference. 633 S.E.2d 373 (Ga. App. 2006). See also White v. Shamrock Bldg. Systems, Inc., 294 Ga. App. 340, 669 S.E.2d 168 (2008) (Failure to prove defendant's aiding and abetting breach of fiduciary duty claim also results in dismissal of tortious interference claim); McDaniel, 275 S.E.2d at 126; Rome Industries, 415 S.E.2d at 652.

B. The "Competition" Privilege.

Georgia courts have recognized that actions taken in furtherance of legitimate competition may be privileged. American Bldgs. Co., 392 S.E.2d at 862. The privilege "guards

against the imposition of undue restraints on the pursuit of employment opportunities in the marketplace." Gresham & Associates, Inc. v. Strianese, 265 Ga. App. 559, 595 S.E.2d 82 (2004). For example, a former employee with no valid contractual restrictions on employee piracy is permitted to properly solicit other employees of the employer so long as the solicitation is not done while he is still employed. Bacon, 597 S.E.2d at 444.

The privilege has its basis in the Restatement of Torts §768 and exists where:

(1) The relation concerns a matter involved in the competition between the actor and the competitor;
(2) The actor does not intend to create or continue an illegal restraint of competition; and
(3) The actor's purpose is a least, in part, to advance its interests in competition with the other.

The privilege is lost when an illegal restraint of trade is established or wrongful means are used to solicit employees. Id.; American Bldgs. Co., 392 S.E.2d at 862; Orkin Exterminating Co. v. Martin Co., 240 Ga. 662, 242 S.E.2d 135 (1978). A defendant's actions are "wrongful" where he makes material misrepresentations about the plaintiff employer or its financial condition; or where he engages in a plan to damage the employer's ability to function. Orkin, 242 S.E.2d at 138–39; American Bldgs. Co., 392 S.E.2d at 862.

In Orkin, Martin Company (Martin) was a holding company that acquired and operated small pest control companies. Martin's executives solicited several Orkin employees. Id. at 137. None of the employees who left Orkin were induced to do so by any false statements. Id. The court held that the defendant's actions were privileged in the absence of evidence that any Martin employee had engaged in a plan or scheme to steal employees from Orkin. Id. at 138–39. Similarly, in Gresham, the court applied the privilege where the defendant solicited and hired four of Gresham's employees, nearly its entire wholesale property department. Although Gresham demonstrated that the loss of these employees harmed its business, the evidence

showed that it had other employees who were capable of servicing and producing the business that the lost employees had produced. Id. at 563. There was no evidence that the solicitation "destroyed or substantially injured Gresham's ability to function as an effective competitor." Id.; See also American Bldgs. Co., 392 S.E.2d at 862 (applying the privilege where seven employees left plaintiff, but testified that they left because they were dissatisfied with their work and that defendant made no disparaging or false statements about plaintiff). By way of contrast, in Nager v. Lad 'N Dad Slacks, the court found issues of fact existed as to whether it was fair competition where the defendant solicited a substantial portion of plaintiff's sales force, solicited solely from the plaintiff and used confidential information in connection with the solicitations. 148 Ga. App. 401, 251 S.E.2d 330 (1978). See also Airotec, Inc., 166 S.E.2d at 745–46 (finding questions of fact as to liability existed where practically entire sales force persuaded to leave and solicitations included misrepresentations of financial stability of plaintiff and use of confidential information. Court viewed it as "planned campaign" of recruiting).

C. Claims by Employee.

An employee may bring a claim alleging that a third party wrongfully interfered with his employment. Howerton v. Harbin Clinic, LLC, 333 Ga. App. 191, 776 S.E.2d 288 (2015) (Surgeon employed by independent medical clinic subject to tortious interference claim by surgical nurse employed by hospital); Saye v. Deloitte & Touche, LLP, 295 Ga. App. 128, 670 S.E.2d 818 (2008) (Factual issues exist regarding auditor's statements to employer which resulted in termination of controller's employment; conditional privilege applied to auditor's statements); Batayias v. Kerr-McGee Corporation, 267 Ga. App. 848, 601 S.E.2d 174 (2004). Such a claim applies both where the employee has an employment agreement and where he is an employee-at-will. Palmer v. Stewart Cty. Sch. Dist., 4:04-CV-21 (CDL), 2005 WL 1676701

(M.D. Ga. June 17, 2005); Ott v. Gandy, 66 Ga. App. 684, 19 S.E.2d 180 (1942). The plaintiff must still show wrongful conduct by the third party or the claim fails. Batayias, 601 S.E.2d at 176. Simply "divulging truthful information" and expressing "critical personal opinions" about a co-worker is not a wrongful or unlawful act. Williams v. Cobb County Farm Bureau, Inc., 312 Ga. App. 350, 718 S.E.2d 540 (2012); Rose v. Zurowski, 236 Ga. App. 157, 511 S.E.2d 265 (1999).

Where an employee is terminated by a supervisor who does not have absolute authority to fire that employee, that supervisor may be held liable for tortious interference with the employee's employment, even where the employment is at-will. Palmer v. Stewart Cty. Sch. Dist., 4:04-CV-21 (CDL), 2005 WL 1676701, at *15 (M.D. Ga. June 17, 2005) (denying summary judgment, finding that employee, who did not have authority to discharge the plaintiff without permission from his superiors, may be liable for such discharge.). See also Troy v. Interfinancial, Inc., 171 Ga. App. 763, 320 S.E.2d 872 (1984).

IV. TORTIOUS INTERFERENCE WITH CUSTOMER RELATIONS

As shown above, unless an employee has executed a valid non-compete or non-solicit covenant, he is permitted to solicit customers of his former employer on behalf of a new employer, so long as improper means are not used.[2] His actions will be privileged. Cont'l Mar. Servs. v. Mar. Bureau, Inc., 275 Ga. App. 533, 621 S.E.2d 775 (2005) (holding absent a contractual restriction, there is no bar to former employee contacting customers of his former employer); Bacon, 597 S.E.2d at 444; Tom's Amusement Co. v. Total Vending Svcs., 243 Ga. App. 294, 298, 533 S.E.2d 413 (1990). In order to succeed on a tortious interference claim, a plaintiff must show improper action by the defendant, and that it lost customers due to the

[2] Solicitation of employer's customers or prospective customers while still employed gives rise to claims for breach of fiduciary duty and tortious interference. See White v. Shamrock Bldg. Systems, Inc., 294 Ga. App. 340, 669 S.E.2d 168 (2008).

defendant's improper actions. Bacon, 597 S.E.2d at 444. Absent evidence that customers left due to the defendant's actions, the claim fails. Cont'l Mar. Servs., 621 S.E.2d at 779; Pendley Quality Trailer Supply, Inc. v. B&F Plastics, Inc., 260 Ga. App. 125, 578 S.E.2d 915, 918–19 (2003) (holding claim for tortious interference with customer relations failed where plaintiff obtained no testimony from any of the allegedly lost customers about their reasons for leaving, and jury would have had to speculate as to why customers left).

V. THE STRANGER DOCTRINE

In order to be liable for tortious interference, a defendant must be a "stranger" to the contract and to the business relationship giving rise to the contract. MAU, Inc. v. Human Techs., Inc., 619 S.E.2d 394 (Ga. App. 2005). Under Georgia law, a defendant is not a "stranger" as a matter of law when:

> 1) the defendant is an essential entity to the purported injured relations; 2) the allegedly injured relations are inextricably a part of or dependent upon the defendant's contractual or business relations; 3) the defendant would benefit economically from the alleged injured relations; or 4) both the defendant and the plaintiff are parties to a comprehensive interwoven set of contracts or relations.
>
> Brilliant Alternatives, Inc. v. Feed Mgmt. Sys., Inc., 1:09-CV-2348-RWS, 2011 WL 723336, at *3 (N.D. Ga. Feb. 22, 2011(quoting, Britt/Paulk Agency, Inc.., v. Vandroff Ins. Agency, Inc., 952 F. Supp. 1575, 1584 (N.D. Ga. 1996)).

Proof that the defendant was not a stranger to the business relationship at issue is fatal to a claim for tortious interference. New York Life Ins. Co. v. Grant, 57 F. Supp. 3d 1401 (M.D. Ga. 2014); Hart Care, LLC v. Frederica Acres, Inc., 5:13-CV-109 CAR, 2013 WL 6494594 (M.D. Ga. Dec. 10, 2013) (Lessor not a stranger to lessee/sublessee relationship); Mabra v. SF, Inc., 316 Ga. App. 62, 728 S.E.2d 737 (2012) (Defendant with direct economic interest in business relationship not a stranger); Med. Ctr., Inc. v. Humana Military Healthcare Servs., Inc.,

4:10-CV-124 CDL, 2012 WL 3295640 (M.D. Ga. Aug. 10, 2012); Patterson v. Citi Mortgage, Inc., 1:11-CV-0339-CC, 2012 WL 4468750 (N.D. Ga. Sept. 26, 2012), aff'd in part, 820 F.3d 1273 (11th Cir. 2016); Life Alarm Systems, Inc. v. Valued Relationships, Inc., CV 109-117, 2011 WL 1167174 (S.D. Ga. Mar. 28, 2011); Kingdom Ins. Grp., LLC v. Cutler & Associates, Inc., 7:10-CV-85 HL, 2011 WL 2144791 (M.D. Ga. May 31, 2011) (Defendants that were financing plaintiff's operations and received compensation as a result of insurance sales by plaintiff's agents were not strangers); ACS Construction Equipment USA, Inc. v. City Commercial Real Estate, Inc., 303 Ga. App. 309, 693 S.E.2d 559 (2010); OnBrand Media v. Codex Consulting, Inc., 301 Ga. App. 141, 687 S.E.2d 168 (2009); Perry Golf Course Development, Inc. v. Housing Authority of Atlanta, 299 Ga. App. 387, 670 S.E.2d 171 (2008) (AHA party to contractual relationship to redevelop Perry Homes and not a stranger to the relationship); Med S. Health Plans, LLC v. Life of S. Ins. Co., 4:07-CV-134(CDL), 2008 WL 2119915 (M.D. Ga. May 19, 2008) (Sales agent of plaintiff not stranger to contracts between plaintiff and its sub-agents); ULQ, LLC v. Meder, 293 Ga. App. 176, 666 S.E.2d 713 (2008) (Minority owner of LLC not a stranger to business and contractual relationships between LLC and its customers); Harrick v. NCAA, 454 F. Supp. 2d 1255 (N.D. Ga. 2006) (NCAA is not a stranger to employment contracts between coaches and university in intercollegiate basketball); Sam v. Reich, 1:03-CV-3178-JOF, 2006 WL 319259 (N.D. Ga. Feb. 9, 2006), aff'd, 225 Fed. Appx. 840 (11th Cir. 2007); Kollman v. International Brotherhood of Electrical Workers, 369 F.3d 1209 (11th Cir. 2004); Strahley, 510 S.E.2d at 821; Lake Tightsqueeze, 435 S.E.2d at 489 ("All parties to an interwoven contractual arrangement are not liable for tortious interference with any of the contracts or business relationships."); Nobel Lodging, 548 S.E.2d at 485. See also Iraola & CIA v. Kimberly-Clark Corp., 325 F.3d 1274, 1283–84 (11th Cir. 2003); Mulligan

v. Brunswick Memorial Hospital Auth., 264 Ga. App. 39, 589 S.E.2d 851 (2003) (Basing affirmation of summary judgment on the "stranger" doctrine); Voyles v. Sasser, 221 Ga. App. 305, 472 S.E.2d 80, 82 (1996) (Claim fails where defendant was "no stranger" to business relations at issue). However, a defendant's failure to raise the stranger doctrine as a defense to a tortious interference claim will result in a waiver. GT Software, Inc. v. WebMethods, Inc., 465 Fed. Appx. 844 (11th Cir. 2012).

Where a defendant has a financial interest *in one of the parties* to the contract *or within* the contract, he is not a stranger to the contract or business relationship, even if he is not a contractual signatory. Hammer Corp. v. Wade, 628 S.E.2d 638 (Ga. App. 2006). See also BMC-The Benchmark Mgmt. Co. v. Ceebraid-Signal Corp., 292 F. App'x 784 (11th Cir. 2008) (Lenders or equity investors not strangers); Wachovia Ins. Servs. v. Paddison, 406CV083, 2006 WL 8435384 (S.D. Ga. Oct. 30, 2006). In other words, to qualify as a non-stranger, a defendant must have a legitimate economic interest in either the contract or a party to the contract. Tidikis v. Network for Med. Communs. & Research, LLC, 274 Ga. App. 807, 619 S.E.2d 481 (2005) (No claim for tortious interference with employment agreement lies against majority shareholder of the employee's former employer).

An intended third-party beneficiary of a contract is not a stranger and, therefore, cannot be sued for tortious interference. Boller v. Robert W. Woodruff Arts Center, 311 Ga. App. 693, 698, 716 S.E.2d 713 (2011). However, an unintended third-party beneficiary may be a stranger and subject to suit. If the unintended third-party beneficiary has a "direct economic interest" in, or benefit from the contract, it will not be considered a stranger. See, e.g., Howerton v. Hubrin Clinic, LLC, 333 Ga. App. 191, 776 S.E.2d 288 (2015); Disaster Svcs. v. ERC Partnership, 228

Ga. App. 739, 492 S.E.2d 526 (1997); Jefferson-Pilot Communications v. Phoenix City Broadcasting of Atlanta, 205 Ga. App. 57, 421 S.E.2d 295 (1992).

The stranger doctrine precludes an employee from filing suit against his employer for tortious interference with his employment. Walker v. General Motors, Corp., 152 Ga. App. 526, 263 S.E.2d 266 (Ga. App. 1979); McElroy v. Wilson, 143 Ga. App. 893, 240 S.E.2d 155, 157 (Ga. App. 1977), cert denied, 435 U.S. 931 (1978). An employee's supervisor is also not a "stranger" to an employment contract and cannot be sued for tortious interference. See, e.g., Weigand v. City of Perry, 5:05-CV-392 (HL), 2008 WL 350975 (M.D. Ga. Feb. 7, 2008); Palombi v. Frito-Lay, Inc., 241 Ga. App. 154, 526 S.E.2d 375 (1999); Atlanta Market Management Co., 503 S.E.2d 278 (1998). Additionally, in an employment-at-will situation, one who has the authority to terminate an employee cannot be held liable for having improper motives in the discharge or termination of the employee. McElroy, 240 S.E.2d at 157. See also Moore v. Barge, 210 Ga. App. 552, 436 S.E.2d 746, 748 (1993) (citations omitted) (Where president had "absolute right" to terminate employee, he cannot be liable for tortious interference). But see, Brathwaite v. Fulton-DeKalb Hosp. Authority, 729 S.E.2d 625 (Ga. App. 2012) (Manager could be liable for tortious interference with subordinate's employment for actions taken while manager was not employed); Howerton v. Harbin Clinic, LLC, 333 Ga. App. 191, 776 S.E.2d 288 (2015) (Surgeon employed by independent medical clinic subject to tortious interference claim by surgical nurse employed by hospital).

However, Georgia courts have recognized that with respect to employment contracts, "the category of non-strangers who are privileged and therefore immune from a tortious interference claim is quite limited." Howerton, supra. An employee is not a stranger to the business relationship between his employer and the customers he personally served while

employed. Tom's Amusement Co., Inc. v. Total Vending Services, Inc., 243 Ga. App. 294, 533 S.E.2d 413 (2000). See also Physician Specialists in Anesthesia, P.C. v. MacNeill, 246 Ga. App. 398, 539 S.E.2d 216 (2000) (Doctors not liable for tortious interference with their former employer's business relations with their own patients); Mulligan v. Brunswick Memorial Hospital Auth., 264 Ga. App. 39, 589 S.E.2d 851 (2003); Parks v. Multimedia Techs., Inc., 239 Ga. App. 282, 520 S.E.2d 517 (1999). Accord, Feldman v. American Dawn, Inc., 849 F.3d 1333 (11th Cir. 2017) (applying Georgia law).

VI. DAMAGES RECOVERABLE FOR A CLAIM OF TORTIOUS INTERFERENCE

To be recoverable, damages must be proximately caused by the tortious act. If a plaintiff cannot "show that damage to his rights or obligations under a contract proximately resulted from the third party's interference, the claim for tortious interference fails as a matter of law." Canter v. Willowrun Condo. Assn., 179 Ga. App. 257, 259, 345 S.E.2d 924 (1986). See, e.g., Duke Galish, LLC v. Manton, 291 Ga. App. 827, 662 S.E.2d 880 (2008); Smith v. Morris, Manning & Martin, LLP, 293 Ga. App. 153, 666 S.E.2d 683 (2008) (Law firm's alleged actions did not proximately cause damage); Trilink Saw Chain, LLC v. Blount, Inc., 583 F. Supp. 1293 (N.D. Ga. 2008) (Failure to prove business relationships were "reasonably likely to develop;" claim for interference with business relationship cannot be based on speculation).

A successful plaintiff in a claim for tortious interference may recover both actual and punitive damages. In Arford, 405 S.E.2d at 700, the plaintiff recovered $200,000 in actual damages and $1 million in punitive damages for tortious interference where the evidence supported the jury's verdict that the defendant intentionally took wrongful action to "freeze out" the plaintiff from his business partnership. Id. at 705.

State Bar of Georgia
INSTITUTE OF CONTINUING LEGAL EDUCATION

STATE BAR SERIES

Litigation And ADR Strategies In Restrictive Covenant Disputes

Presented By:

Gary S. Freed
Freed Howard LLC, Atlanta, GA

Litigation & ADR Strategies in Restrictive Covenant Disputes

Gary S. Freed
F. Beau Howard
Nick B. Corser
FREED HOWARD LLC
101 Marietta Street NW
Suite 3600
Atlanta, Georgia 30303
gary@freedhoward.com
beau@freedhoward.com
nick@freedhoward.com
(470) 839-9300
(470) 839-9301 (fax)

Table of Contents

Whether you represent a former employer or a former employee in a dispute over the enforceability of a restrictive covenant, do these things at the beginning of the engagement to reach the best possible result for your client.

I. Be a Sponge/Just the Facts

Spend time with your client to get the whole story. Litigating restrictive covenants is about more than legal enforceability. Where injunctive or declaratory relief is sought, the Court must also make an equitable decision. To best frame the law, facts, and equities, you must know the whole story. Ask your client to draft a timeline of events and a cast of characters. Once you have your client's story, learn the other side's version. Meetings, phone conferences and even mediation can provide free discovery to help you judge how to pursue the matter.

A. Reasonableness of the Covenants

The reasonableness of a covenant will generally be determined by examining its scope, duration and geographic scope. To determine whether the covenants are reasonable, learn as much as you can about the employer's business and about the competitive landscape.

- What were the employee's responsibilities, assigned duties, and area of expertise?
- Where did the employee work? Where does the employer do business?
- When did the employer, or the employee, develop products, services, customer bases, etc.?
- To what extent did the employee have contact with the employer's customers? With which customers was the employee in contact?

B. Trade Secrets/Confidential Information

Determine whether the former employee had access to or possesses sensitive, proprietary, trade-secret, or confidential information.

C. Key Documents

Gather and review the key documents from your client, e.g., contracts, e-mails, correspondence, memoranda, employee manuals, audio recordings, et cetera.

II. Counsel, Don't Advocate

It is important that you give the client your opinion as to the enforceability of the restrictive covenants at issue, but your efforts should not stop there. There will be plenty of time to advocate a position once you are in court. At the early stage, counsel your client. Regardless of the strength or weakness of the covenants, you should explain to your client the temporal, financial, and opportunity costs associated with litigating the restrictive covenants. This is not to say that your advice should necessarily counsel against litigation. Just don't let the tail wag the dog.

A. Is it Worth the Trouble?

David Porter said, "Litigation is the basic legal right which guarantees every corporation its decade in court." Regardless of whether you are representing the employer or the employee, or whether you are defending a suit or have been asked to file suit, you need to determine whether litigation is worth the cost.

1. If you are representing the employer:

- Does the employee's direct competition with the company pose a real threat?
- Are there other similarly situated employees such that letting this employee get away with violating the restrictive covenants will indicate acquiescence on the part of the employer?

2. If you are representing the employee:

- Is the competitive opportunity worth litigating with the former employer?
- Can the employee afford not to work during the restricted period? Put another way, can the employee afford not to litigate the enforceability of the covenants?
- Is there a tolling provision in the contract that is enforceable, and would it lengthen the period when a restriction is in effect? Does your client want to risk having both the challenged covenant and the tolling provision enforced against her?

3. Will My Customers Hate Me?

What effect will litigation have on future business for the employer or the employee? To prove that customers have been approached (or not), or that competitive activities have been undertaken (or not), it will often be necessary to secure the cooperation of the customers over whom the parties are fighting. Their testimony is often necessary to prove the existence or non-existence of the competition or solicitation. Yet, many customers would rather do business elsewhere than become embroiled in this type of dispute. Thus, the opportunity costs of involving customers in these disputes must be carefully considered.

4. Will the Contract be Blue Penciled?

If working under the new law or with a contract ancillary to the sale of a business, consider the effect that blue-penciling could have on the agreement. Will your client's resources be better used by efforts on your part to strike an agreement with opposing counsel to blue-pencil the agreement without seeking the assistance of the courts?

III. Which Laws Will Apply?

Different laws will govern the enforceability of your restrictive covenant depending upon when it was executed, and when the litigation is or was initiated. Further, the availability of a federal trade secret claim could affect whether you file your case in federal or state court. The court that hears the case will affect the procedural rules and substantive laws that apply.

A. Applicable Georgia Law?

1. Before November 2, 2010

Agreements executed prior to November 2, 2010 (the date of the general election ratifying the Constitutional amendment enabling the new law) are interpreted under the old case law.

2. After May 11, 2012

Agreements executed after May 11, 2012 (the effective date of O.C.G.A. § 13-8-50, *et seq*.) will be interpreted under the new code sections. Note that

the new code sections only permit post-employment[1] non-compete agreements for certain categories of employees – *e.g.*, salespeople; executives; managers; employees with significant input into hiring, firing, promotions, demotions, and lateral moves; and "key employees." O.C.G.A. § 13-8-53(a)(3).

3. Between November 2, 2010 and May 11, 2011

There is conflicting authority concerning which law applies to agreements executed between November 2, 2010 and May 11, 2011.

i. Georgia Court of Appeals

The Georgia Court of Appeals has stated that HB 173 (the 2009 law which is essentially identical to the current O.C.G.A. § 13-8-50, *et seq*.) applies to agreements executed during the "gap" period. *See Cox v. Altus Healthcare & Hospice, Inc*., 303 Ga. App. 28, 30, 706 S.E. 2d 660, 663-64 (Jan. 24, 2011) (new law "[n]ow effective as a result of the ratification of an amendment to the Constitution of Georgia in the general election of November 2, 2010"); *Bunker Hill Int'l, Ltd. v. Nationsbuilder Ins. Servs.*, 309 Ga. App. 503, 505 n.1 (May 5, 2011) ("the November 2010 ratification of an amendment to the Constitution of Georgia adopt[ed] O.C.G.A. § 13-8-2.1(a) into law.").

ii. The Eleventh Circuit

Without acknowledging either *Cox* or *Bunker Hill*, the Eleventh Circuit reached the opposite conclusion in *Becham v. Synthes USA*, 482 Fed. Appx 387, 2012 WL 1994604 (11th Cir. June 4, 2012) (HB 173 unconstitutional and HB 30 not effective until May 11, 2011).

iii. Georgia Supreme Court

The Georgia Supreme Court has not resolved this issue, which leaves Georgia state courts bound by the *Cox* and *Bunker Hill* decisions for now.

[1] All employees, regardless of their job duties, can be restricted from competing ***during*** their employment with the employer. O.C.G.A. § 13-8-53.

4. Federal Law – Defend Trade Secrets Act ("DTSA")

In May of 2016, President Obama signed the DTSA into law. It creates a private, civil cause of action for trade-secret misappropriation "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." Defend Trade Secrets Act of 2016, PL 114-153, May 11, 2016,130 Stat 376, § 2. The DTSA creates subject matter jurisdiction for trade secret misappropriation claims. In so doing, the DTSA gives many restrictive covenant plaintiffs access to federal courts and their uniform procedures, rules, and body of law. It also provides access to a high-level judiciary and a wide range of remedies, including injunctions, compensatory damages, punitive damages where the misappropriate was willful and malicious, attorneys' fees where there is bad faith, enhanced criminal penalties for organizations, the ability to direct federal officials to seize property containing a misappropriated trade secret, and the ability to condition the future use of the trade secret on the payment of a reasonable royalty. *Id*. §§ 2(b)(2), 2(b)3.

The DTSA does not preempt state laws. *Id*. § 2(f).

No federal court in Georgia has reported a decision in a DTSA case yet, but cases are ongoing in district courts in other jurisdictions. *See e.g. Henry Schein, Inc. v. Cook*, 2016 WL 3212457 (N.D. CA. 2016) (The court issued a temporary restraining order where a DTSA plaintiff would suffer irreparable harm and immediate damage absent the order, the order would serve the public interest, and the balance of the hardships was in the plaintiff's favor); *Phyllis Schlafly Revocable Trust v. Cori*, 2016 WL 6611133 (E.D. MI. 2016) (Denying a Motion for a Temporary Restraining Order where the plaintiffs failed to show a likelihood of success on their claims or a threat of immediate and irreparable harm).

IV. Actions & Reactions

Once you have gathered all the information readily available, you can formulate a plan.

A. Damage Control

The initial step is triage; that is, addressing the most serious and time sensitive issues first. Are there trade secrets (including but not limited to customer lists) in the hands of the former employee? Do these materials need to be returned

immediately? Are there particular customers who need to be informed, or actions that need to be prevented?

B. Getting the Word Out

Separation of key employees from a company can often be a confusing time for customers, who have long associated the employees' faces with the company. If done properly, efforts to clear up this confusion can assist in solidifying client bases and creating a smooth transition. This can be accomplished through phone calls, face-to-face visits with key customers, mass mailings or e-mailings, or even press releases. However, if executed poorly, these efforts to "spread the word" can lead to claims for defamation and/or tortious interference with business relationships. Thus, counsel must be cognizant of the tenor and substance of these communications. Clients will often be angry and emotional at the early "crisis stage" of the dispute and should not be left to their own devices in this regard.

C. Settlement Discussions

Early in the case is often a good time to reach out to the other side to see if a resolution can be reached or, at least, whether the issues can be narrowed. However, if suit has not been filed, you might consider whether it is wise to focus your energies on getting the first crack at filing suit and choosing the forum in which to litigate, and then entertaining settlement discussions.

V. Litigation Options

A. Forum Selection

The forum in which a case is litigated can have an enormous impact on its outcome. Thus, the following considerations are very important.

1. Contractual Provisions

Does the contract containing the covenants at issue have a forum selection clause (generally upheld in the restrictive covenant setting) or a choice of law provision (often deemed unenforceable in the Georgia restrictive covenant context)?

2. Presiding Judges

While you have little to say over the judge ultimately assigned to your case, a call down to the courthouse to determine who is presiding may reveal the

judge likely to be assigned to an emergency injunction hearing should you be anticipating that route.

3. Superior Court vs. Federal Court vs. Both

If you are the plaintiff, you will want to determine whether there is federal court jurisdiction for your claim. DTSA? Diversity? Copyright? Trademark? Patent infringement? If you can file in federal court, you will next want to determine whether you would rather be in state or federal court. Federal court is typically a more expensive forum in which to litigate, in no small part because of the many mandatory filings that must be prepared early in the case. Federal courts also are typically much stricter regarding adherence to rules and procedures. Federal courts generally have a very high quality of judiciary, such that if you believe your case requires the application of complex law and facts, you are perhaps more likely to receive a well-reasoned opinion from the federal courts.

The newly enacted DTSA makes it easier to file in federal court if the defendant appears to have taken confidential information or trade secrets to his new business or employer. However, the law is still developing.

Because the DTSA does not preempt state laws (18 U.S.C. § 1836(f)), plaintiffs appear to have the following options:

- sue in federal court and invoke the Court's supplemental jurisdiction to hear state claims;
- file all claims in state court; or
- file parallel actions with state claims in state court and federal claims in federal court.

4. Other Options

i. Mediation or Arbitration.

ii. Fulton County Business Court

iii. Appointment of a Special Master

A Special Master may be able to save costs in several ways and can help determine at the outset whether a covenant has been breached.

For example, discovery battles may be avoided simply by submitting confidential customers lists to the Special Master to determine whether the parties' lists overlap with each other.

B. Injunctive or Declaratory Relief in Georgia

Many factors can assist in deciding whether to assert a claim for injunctive relief, declaratory judgment or both. For example:

1. When to Seek an Injunction

Is there great potential for immediate irreparable harm? If a former employee is actively competing and negatively impacting the business of her former employer, injunctive relief is likely appropriate. Injunctive relief includes temporary restraining orders ("TRO") and injunctions, whether interlocutory or permanent. By seeking a temporary restraining order, you can typically get a hearing within a few days of filing suit.

2. When to Seek Declaratory Relief

Alternatively, if a former employee merely seeks to compete, without fear of liability for breaching her restrictive covenants, she may be well served by seeking a declaratory judgment. O.C.G.A. § 9-4-5 authorizes a trial court to conduct a final hearing on a prayer for declaratory judgment as soon as 21 days after service of the action.

3. Are your facts stronger than your law, or vice versa?

i. If the facts work in your favor, then an injunctive hearing, where evidence and testimony of witnesses can be introduced, may aid your cause.

ii. Alternatively, if the law is strongly on your side, but your facts are less than desirable, you may be better off pursuing a declaratory judgment action, where the questions before the court will be largely legal ones, and the facts typically introduced by more sanitized, verified pleadings and affidavits.

4. Race to the Courthouse

"The race to the courthouse" must also be considered. Under *Hosteller v. Answerthink, Inc.*, 267 Ga. App. 325, 330, 599 S.E.2d 271, 276 (2004), an injunction issued in Georgia has effect only within this state, whereas a declaratory judgment rendered in Georgia is entitled to full faith and credit nationwide. Thus, it may be prudent to ask for both injunctive and declaratory relief to ensure issue and claim preclusion around the country.

Note: An actual claim or controversy must exist before seeking relief. *See e.g.*, *Mitchell v. W.S. Badcock Corp.*, 230 Ga. App. 352, 355, 496 S.E.2d 502, 505 (1998) (summary judgment vacated as erroneous advisory declaratory judgment where the court improperly ruled on the outcome of future litigation over the covenant); *see also Jones v. Solomon*, 207 Ga. App. 592, 593-94, 428 S.E.2d 637, 639-40 (1993) (anticipatory repudiation not found where employee questioned validity of covenant and failed to give employer adequate assurances that employee intended to comply with the covenant).

C. Injunctions and TROs

1. Injunctions

No Adequate Remedy at Law

Equitable remedies, like injunctions, are only available to restrain improper acts for which no adequate remedy is provided at law. O.C.G.A. § 9-5-1. Because an injunction is an equitable remedy, Georgia superior courts have jurisdiction. *See* Ga. Const. 1983, Art. VI, § IV, ¶ 1; *See also Mar-Pak Michigan, Inc. v. Pointer*, 226 Ga. 189, 173 S.E.d2d 206 (1970); *Brown v. Johnson*, 251 Ga. 436, 436 (Ga. 1983) ("Generally, the superior courts of this state have the power, in proper cases, to issue process in the nature of … injunctions, and hence the need to resort to the appellate courts will be extremely rare.").

Injunctions Must be Specific

O.C.G.A. § 9-11-65(d) requires that all restraining orders "be specific in terms," "describe in reasonable detail, and not by reference to the complaint or other document, the act or acts sought to be restrained," and be binding only on "the parties to the action, their officers, agents, servants, employees and attorneys, and upon those persons in active participation with [the

enjoined party] who received[d] notice of the order by personal service or otherwise."

Posting Bond

The court may also require that the party moving for a TRO or injunction provide security, in an amount to be determined by the court, for the potential damage to the enjoined party from the injunction. O.C.G.A. § 9-11-65(c) recognizes the right to recover actual damages resulting from a wrongful restraint. *Moody v. Harris*, 170 Ga. App. 254, 256 (Ga. Ct. App. 1984). Petitions for injunctive relief require supporting proof, which can be accomplished by a verified affidavit. O.C.G.A. § 9-10-110.

Interlocutory Injunctions

An interlocutory injunction issues before the final adjudication of the matter and is designed to preserve the status quo and balance the conveniences of the parties pending final adjudication. *Grossi Consulting, LLC v. Sterling Currency Group, LLC*, 290 Ga. 386, 388 (2012); *Holton v. Physician Oncology Servs., LP*, 292 Ga. 864, 866 (2013); *CRE Venture 2011-1, LLC v. First Citizens Bank of Georgia*, 326 Ga. App. 133 (2014). A permanent injunction is intended to remain in force for an extended period after final adjudication of a matter on its merits. *See e.g. Jacobs v. Chatham County*, 295 Ga. App. 74 (2008).

Permanent Injunction

To obtain a permanent injunction, the moving party must show that it is suffering or would suffer from a continuous, harmful wrong. *Robinson v. Landings Ass'n, Inc.*, 264 Ga. 24, 440 S.E.2d 198 (1994); *Am. Med. Sec., Inc. v. Parker*, 279 Ga. 201, 204, 612 S.E.2d 261 (2005). Evidence of past infractions and a reasonable apprehension of future infractions may compel a court to issue a permanent injunction. *Ellis* v. *Georgia Kraft Co.*, 219 Ga. 335, 336-337, 133 S.E.2d 350, 352 (1963).

Notice Required

Both an interlocutory injunction and a permanent injunction require notice to the adverse party. *See* O.C.G.A. § 9-11-65(a). A court may choose to expedite the trial on the merits of the case so that the hearing on the interlocutory injunction is combined with the trial on the merits. *Id*. If the

trial on the merits is not consolidated with the hearing on the interlocutory injunction, the evidence submitted at the hearing on the injunction becomes part of the record and does not need to be repeated at trial. *Id*.

Appeals

"When an appeal is taken from an interlocutory or final judgment granting, dissolving, or denying an injunction, the court in its discretion may suspend, modify, restore or grant an injunction during the pendency of the appeal upon such terms as to bond or otherwise as it considers proper for the security of the rights of the adverse party." O.C.G.A. § 9-11-62(c). If a court does affirmatively alter an injunction during the pendency of an appeal, the injunction remains in place. *See id*.

Keep in mind that injunctions and TROs are available under the DTSA for trade secret misappropriation claims. DTSA § 2.

2. TROs

Ex Parte TRO

The main difference between a TRO and an injunction, whether interlocutory or permanent, is that a TRO occasionally does not require notice to the party seeking to be restrained.

Short Duration

It is only valid for 30 days at most in state court. O.C.G.A. § 9-11-65. Injunctions require notice. *Id*.

The court may fix the date that the TRO expires, but the court cannot issue a TRO for more than 30 days without the enjoined party's consent. O.C.G.A. § 9-11-65(b). Where a TRO is granted without notice, a hearing on an interlocutory injunction, to take the place of the TRO, shall occur as soon as possible. *Id*. If the party moving for the TRO does not apply for an interlocutory injunction by the date of the hearing, the court "shall" dissolve the TRO. *Id*. The enjoined party may move to dissolve or modify the TRO with two days' notice to the opposing patty, unless the court approves a shorter notice period. *Id*. The Court shall hold a hearing on the motion to dissolve or modify a TRO as soon as possible. *Id*. A TRO may be extended one time only. OCGA § 9-5-9.

In federal court, a TRO should expire after 14 days if the party seeking the injunction does not proceed to a preliminary injunction hearing. FED. R. CIV. P. 65. The Court may extend the TRO for an additional 14 days on a finding of good cause or for a longer period with the consent of the adverse party. FED. R. CIV. P. 65(b)(2). However, one court in the Northern District of Georgia has been willing to indefinitely extend a TRO without a preliminary injunction hearing, at least where the moving party claims to have been denied the opportunity to collect evidence through discovery as a result of the disappearance of the adverse party. *See* Order (Aug. 9, 2018) [Doc. 61], *Solvay Specialty Polymers USA, Inc. v. Dr. Zhenguo (Leo) Liu*, Civ. Act. No. 1:18-cv-2120-ELR, United States District Court, Northern District of Georgia, Atlanta Division. Other federal courts have been willing to extend TROs past 28 days without first holding preliminary injunction hearings when the moving party needed discovery to complete the record, the adverse party was intentionally delaying the hearing, or the court found good cause to preserve the status quo but court not schedule a timely hearing because of other pending litigation. *See Saint Consulting Grp., Inc. v. Payne*, No. 8:10-cv-01089-T-24-AEP, 2010 WL 2804860, at *1-2 (S.D. Fla. July 15, 2010); and *Trefelner ex rel. Trefelner v. Burrell Sch. Dist.*, 655 F. Supp. 2d 581, 598-99 (W.D. Pa. 2009).

Sworn Proof Needed

O.C.G.A. § 9-11-65(b) provides that a "temporary restraining order may be granted without written or oral notice to the adverse party or his attorney only if: (a) It clearly appears from specific facts shown by affidavit or by the verified complaint that immediate and irreparable injury, loss, or damage will result to the applicant before the adverse party or his attorney can be heard in opposition; and (b) The applicant's attorney certifies to the court, in writing, the efforts, if any, which have been made to give the notice and the reasons supporting the party's claim that notice should not be required."

TROs should be accompanied by a verified application or supporting affidavits to satisfy the evidentiary burdens of O.C.G.A. § 9-10-110. See *Harvard v. Walton*, 243 Ga. 860, 861, 257 S.E.2d 280, 281 (Ga. 1979) (decided under former code section); *Nunn Better Enterprises, Inc., v. Marietta Lanes, Inc.*, 230 Ga. 230, 196 S.E.2d 404 (1973).

Legal Requirements

To obtain a TRO, the plaintiff must: (a) demonstrate a substantia1 likelihood of success on the merits of the claim, (b) that the injury to the movant must outweigh the harm to the respondent, and (c) that the public interest will not be disserved by the grant of the injunction.

Appeals

The granting or dissolving of a TRO is not immediately appealable. See *Shelton v. Peppers*, 237 Ga. 101, 227 S.E.2d 29 (1976*); see also Clements v. Kushinka*, 233 Ga. 273, 210 S.E.2d 804 (1974).

3. Ex-Parte Seizure of Property Under the DTSA

The DTSA allows a plaintiff to ask the Court for an *ex parte* seizure of property. *Ex parte* seizures may only be granted in "extraordinary circumstances," 18 U.S.C. § 1836(b)(2)(A)(i), and the request must include "specific facts" justifying the seizure, *id.* § 1836(b)(2)(A)(ii), and "describe with reasonable particularity the matter to be seized," id. § 1836(b)(2)(A)(ii)(VI). As part of the showing, the party applying for the *ex parte* seizure must demonstrate that an injunction against disclosure or use of the trade secret would be insufficient because "the party to which the order would be issued would evade, avoid or otherwise not comply with such an order." *Id.* § 1836(b)(2)(A)(ii)(I).

4. Picking Causes of Action

Whether bringing or defending an action to challenge the enforceability of restrictive covenants, the enforceability of the covenants is rarely the only issue between the parties. It is, therefore, important to examine what other claims your client may have to assert. Those claims commonly associated with restrictive covenant litigation are:

- Computer Fraud and Abuse Act (18 U.S.C. § 1030)
- Computer Theft, Trespass and Invasion of Privacy Statute (O.C.G.A. § 16-9-93)
- Georgia Trade Secrets Act (O.C.G.A. § 10-1-760, *et seq.*)
- Tortious Interference with Business Relations
- Misappropriation of Trade Secrets

- Defamation
- Breach of Fiduciary Duty
- ADEA
- ADA
- Title VII – discrimination claims
- Wages
- Deceptive Trade Practices Act
- RICO
- Conspiracy
- Malicious Prosecution/Abuse of Process
- Promissory Estoppel (oral contracts)

5. Inevitable Disclosure/Inevitable Use

What if you do not have an enforceable restrictive covenant? Can your client prevent an executive or other employee with trade secret information from joining a competitor, or conversely, can your client be so enjoined in the absence of a valid non-compete? Georgia's appellate courts have not yet explicitly ruled on whether the doctrine of "inevitable disclosure" is viable in our state, although a few other jurisdictions have. *See*, *e.g.*, *PepsiCo. v. Redmond*, 54 F.3d 1262, 1270 (7th Cir. 1995); *Novell Inc. v. Timpanogos Res. Group Inc.*, 46 U.S.P.Q. 2d 1197, 1216-17 (D. Utah Jan. 30, 1998).

In 2003, in a much-publicized Fulton County case, *Bellsouth Corp. v. Forsee*, 2003 WL 25436590 (Ga. Super. Ct.), Judge Stephanie Manis kept in place for 30 days an ex-parte TRO restraining a high-level executive at Bellsouth from accepting a similar position at Sprint based on a non-disclosure provision in an employment agreement while simultaneously dissolving the portion of the TRO based on an unenforceable non-compete. Although Bellsouth's claim was based at least in part on inevitable disclosure, neither Judge Manis nor the subsequent Court of Appeals

opinion, *Bellsouth Corp. v. Forsee*, 265 Ga. App. 589, 595 S.E.2d 99, (2004), squarely addressed the viability of the inevitable disclosure claim.

The Georgia Supreme Court has, however, unequivocally held that Georgia Trade Secrets Act gives courts authority to fashion injunctive relief to prevent "actual or threatened misappropriation [of trade secrets.]" O.C.G.A. § 10-1-762(a). In *Essex Group v. Southwire Co.*, 269 Ga. 553, 558, 501 S.E.2d 501, 505 (1998), the Georgia Supreme Court held that courts had the authority, under the Trade Secrets Act, to enjoin a former employee with trade secret information from at least working in certain segments of a competitor's business where he could use the former employer's trade secrets to the benefit of the competitor.

The Georgia Supreme Court against addressed the viability of an inevitable disclosure claim in 2013 in *Holton v. Physician Oncology Services, LP*, 292 Ga. 864, 870 (2013). In *Holton*, the Georgia Supreme Court held that the inevitable disclosure doctrine is not an independent claim under which a trial court may enjoin an employee from working for an employer or disclosing trade secrets. However, the Georgia Supreme Court declined to address whether the inevitable disclosure doctrine may be applied to support a claim for the threatened misappropriation of trade secrets. Importantly, the Georgia Supreme Court did not overturn or even limit its previous holding in *Essex*.

6. Timing

Georgia provides expedited discovery and rulings when warranted and a motion should be made requesting the same when time is of the essence. See *e.g.* O.C.G.A. §§ 9-1 l-30(b)(3) ("court may, for cause shown, enlarge or shorten the time for taking the deposition"); O.C.G.A. 9-11-34(b)(2) (response to request for document production may be shortened by court); Ga. Unif. Super. Ct. R. 6.7 (motions in emergencies).

VI. Working with Experts

Expert witnesses can assist and facilitate the presentation of your case.

A. Computer Experts

Often computer forensics experts can assist in determining whether an employee deleted information, accessed information, etc., from a company's system, or

alternatively, whether the information was shielded adequately from the public domain. E-mail retrieval is important.

B. Industry Experts

Often, a factual question will arise as to whether the activities in which a former employee is now engaging are "competitive" with the business of the former employer. Industry experts can assist in educating the Court to your client's perspective on these issues.

C. Public Relations Experts

Public relations experts can help your client put a proper spin on developments and help move toward a marketable strategy.

D. Auditors

Auditors can help demonstrate expenses going in and out and may help in calculating damages.

E. Accountants

Accountants can assist in determining the economic harm to the client and whether it can be reasonably ascertained.

VII. Effective Advocacy

A. Pigs Get Fat and Hogs Get Slaughtered

In litigating restrictive covenants, it is important to remember that the trial court has wide discretion in whether to grant an injunction. Even if the judge rules erroneously, an appeal is likely to take a substantial portion of the length of time that the former employee was purportedly restricted from competing. The issues may well be moot by the time an appellate decision is rendered. It is therefore important to appeal to the discretion of the court. Be reasonable. If you push too hard as either employee or employer, you may lose credibility or sympathy with the judge.

B. KISS (Keep It Simple, Stupid)

Georgia law as it existed prior to the enactment of O.C.G.A. § 13-8-50 *et seq.* on restrictive covenants is far from straightforward. For every case that stands for a

proposition of law on an issue, there is typically another that infers nearly the opposite. Many judges are unfamiliar with the law in this area. The easier you can make the case for your judge (and her law clerk), the better your chances. Consider preparing a hearing notebook containing the following:

- The relevant agreement (with the covenants highlighted);
- Correspondence;
- A timeline;
- Pleadings (whether in the instant action or those of an action pending in another forum);
- Cases (again, highlighted) which support your position;
- Other documents.

During your argument, you can refer the judge to those portions of the notebook which support your arguments and it will be easy for the judge to follow along.

If you are working under the new law in Georgia, be prepared to educate the judge on the nuances of reasonableness. Depending on your client's case, be prepared to distinguish the new law from old case law or to show the court how the new law favorably compares with how courts have already decided cases.

If you are bringing a suit under the DTSA, be prepared to argue unsettled law.

VIII. **Damages**

A. **Measure of Damages**

The measure of damages for violation of a restrictive covenant is all damages incident to the violation, including the benefits, advantages, or profits gained by the defendant and, in the case of stolen trade secrets, the value of the secret to the Defendant. *Robert B. Vance & Assocs. v. Baronet Corp.*, 487 F.Supp. 790, 800 (N.D. Ga. 1979); *Williamson v. Palmer*, 199 Ga. App. 35, 36, 404 S.E.2d 131, 133 (1991).

B. Difficulty Calculating

However, the Georgia Supreme Court has repeatedly held that damages for violations of a restrictive covenant are often difficult, if not impossible, to calculate. See *Rash v. Toccoa Clinic Medical Associates*, 253 Ga. 322, 326, 320 S.E.2d 170 (1984); *Physician Specialists in Anesthesia, P.C. v. Macneill*, 246 Ga. App. 398, 539 S.E.2d 216 (2000). See also *Proudfoot Consulting Co. v. Gordon*, 576 F.3d 1223 (11th Cir. Fla. 2009).

The Northern District of Georgia has held that in some instances, such as where a stockbroker changes brokerage houses, monetary damages can be precisely calculated because every sale of stock is recorded. *Morgan Stanley DW, Inc. v. Frisby*, 163 F.Supp.2d 1371, 1376 (N.D. Ga. 2001). In *Morgan Stanley*, the court stated that the damages were awardable under a breach of contract theory, and the measure of damages would be plaintiff's lost profits, which the competing broker earned. *Id*. *Morgan Stanley* also cites *Merrill Lynch, Pierce, Fenner & Smith v. Bennert*, 980 F.Supp. 73, 75 (D. Me. 1997) for the proposition that damages could also be calculated by examining "past history of the earning on accounts and expert testimony." *Id*.

However, the Georgia Supreme Court has noted, at least twice, the difficulty of proving damages for violation of a restrictive covenant. In *Rash*, 253 Ga. at 327, a doctor left a partnership to form a competing medical clinic. *Id*. The Court held that "[d]amages would be difficult to calculate, and even the awarding of same would not properly vindicate the plaintiff's rights." *Id*. Similarly, in *Poe & Brown of Ga., Inc. v. Gill*, 268 Ga. 749, 750, 492 S.E.2d 864, 865 (1997), where a salesperson left an insurance company, the court held that "it would be difficult, if not impossible, to quantify the damages stemming from the loss of a customer."

C. Lost Profits

In *Annis v. Tomberlin & Shelnutt Associates, Inc.*, 195 Ga. App. 27, 32,392 S.E.2d 717, 722-23 (1990), the court awarded lost profits for breach of a restrictive covenant, arguing that a "party who has been injured by a breach of a contract can recover profits that would have resulted from performance when their amount and the fact that they have been prevented by the breach of the [party] can be proved with reasonable certainty." The jury's award was upheld because it was based on the employer's estimate, which he made with "reasonable certainty." *Id*.

D. Set-Off

If damages can be proven, they can almost certainly be set off from monies due for the sale of a business. In *Annis*, just because the restrictive covenants were ancillary to the sale of a business, the jury was authorized "to find in favor of [employer's] claim of failure of consideration and/or that defendants were entitled to a set-off of the balance owed." 195 Ga. App. at 30.

E. Punitive Damages

Punitive damages are not recoverable unless there are allegations of fraud, conversion, or proof of fraudulent inducement to breach. *Williamson*, 199 Ga. App. at 36-37.

F. Liquidated Damages

A liquidated damage clause will be enforceable so long as (1) the breach of the restrictive covenant caused an injury that is difficult or impossible to estimate with accuracy, (2) the intent of the parties was to provide for damages and not a penalty; and (3) the amount is a reasonable pre-estimate of the probable loss. *Allied Informatics v. Yeruva*, 251 Ga. App. 404, 405, 554 S.E.2d 550, 552 (2001) (finding no evidence that the stipulated sums in the contract bore any relation to the actual damages that could be incurred from a breach); *See also Capricorn Sys. V. Pednekar*, 248 Ga. App. 424, 427, 546 S.E.2d 554 (2001) ($50,000 liquidated damage provision unenforceable and arbitrary because amount bore no rational relationship to actual or potential damages).

G. DTSA Damages

Section 2 of the DTSA allows for the following:

- Compensatory damages;
- Punitive damages no greater than two times compensatory damages where the misappropriation was willful and malicious'
- Attorneys' fees where there is bad faith.

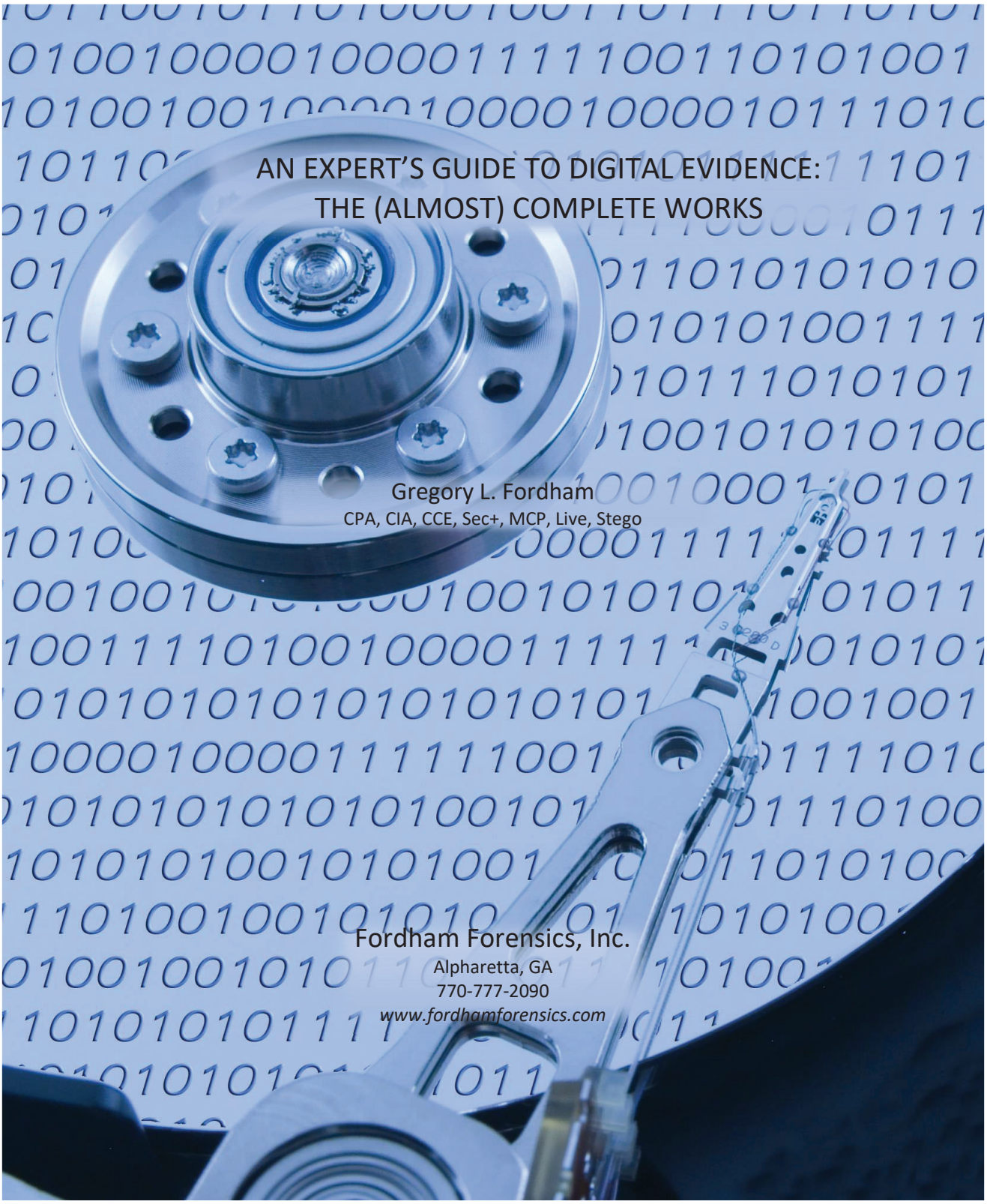
State Bar of Georgia
INSTITUTE OF CONTINUING LEGAL EDUCATION

STATE BAR SERIES

Forensic Investigations And E-Discovery In Restrictive Covenant Litigation

Presented By:

Gregory L. Fordham
Fordham Forensics, Inc., Alpharetta, GA



AN EXPERT'S GUIDE TO DIGITAL EVIDENCE: THE (ALMOST) COMPLETE WORKS

Gregory L. Fordham
CPA, CIA, CCE, Sec+, MCP, Live, Stego

Fordham Forensics, Inc.
Alpharetta, GA
770-777-2090
www.fordhamforensics.com

TABLE OF CONTENTS

Preface

There have been many articles and books written about computer forensics. Typically, they are written by experts for experts or experts for enthusiasts or other subject matter buffs. Often, they are written for the crime scene investigator or the computer security specialist.

While these may be the people with considerable interest in the subject, the interest in the subject has also spread to other areas. One area where the interest has gown is the legal profession, in general, and in litigation matters more specifically. The primary interest of that group is the collection of digital evidence and not so much on device operations or security. In addition, there is considerable interest in how to optimize cost, schedule, and quality of the entire litigation lifecycle in order to accomplish the primary constraint which is to secure the just, speedy, and inexpensive determination of every action and proceeding.

The litigation world has some significant differences from other areas where the interest in computer forensics has blossomed. Perhaps the key difference is that litigation is not just about answers. It is about process as well. As a result, in the context of litigation, there can be a lot more to the subject of computer forensics than just the collection and analysis of the artifacts themselves. After all, there are both rules of procedure and rules of evidence which directly impact what, when, and how digital evidence will be considered. Thus, there is a significant challenge in how to harmoniously integrate digital data analysis with legal processes while optimizing cost, schedule, and quality.

To complicate matters further, the overall effort in any litigation is being led and managed by people like lawyers and judges who are less informed about the technical issues of digital data even though, like most people today, they are frequent users of digital tools and may feel quite comfortable with them. For many of these professionals, computer forensics is like turning cards where a queen always beats a jack. The game is actually more complicated than that, however. A pair of twos can beat a queen but five aces is a sign of even bigger problems as is a marked deck or a deck with more or less than fifty-two cards. There simply are a lot of ways to cheat and the magic of computers and digital data has made cheating even easier.

The digital age has also made things more complicated. In its early years the subject was focused on a more narrow understanding of computerized devices and their data. Today, the category of computerized devices covers many things never before considered. Furthermore, the subject has also expanded to include data not even in the custody of the individual but in the custody of “service” providers that could range from pay to play service providers like ISPs, SaaS providers and cloud based data storage providers to social and entertainment providers like Facebook, Instagram, and Twitter.

Even the concept of a computer has undergone a revolution. No longer is it a mainframe, or server, or desktop or laptop but something even more personal and ubiquitous—the cellphone.

Related subjects like privacy, security, and performance keep changing as well. These changes influence the underlying technology such that what was once common can go from not just uncommon but to completely unavailable. Thus, the processes needed to analyze digital data keeps changing. The expectations keep changing too. Thus, the complexity issue just continues to grow and expand.

Moore's Law that data density will double about every 18 months is a well known rule developed by Intel co-founder Gordon Moore in 1965. It was based on his observation that the number of transistors per inch on integrated circuits had doubled every year. It has been applied and correlates well with many aspects of the tech revolution.

If applied to the subject of computer forensics the fundamentals of Moore's Law means that the subject will change very fast and perhaps at a pace the legal profession could find hard to match. After all, even though the 2006 changes to the FRCP are widely perceived as the acceptance of digital evidence in the legal profession the reality is that by 2006 digital evidence already had quite a history. In fact, the case of *Bills v Kennecott Corp*., not only used the term ESI 20 years before the 2006 changes to the federal rules it also stated that, "It is now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure. . . ."[1] Similarly, in the case of *Anti-Monopoly Inc. v Hasbro*, it was stated more than a decade prior to the 2006 changes that the discovery of computerized data was now black letter law.[2] Clearly the legal revolution can be much slower than the digital one.

I have been writing and teaching about computer forensics and e-discovery for over 15 years. I finally decided to bring all that work together in a single resource. In the process, I'm trying to accomplish three goals with what I have put together.

First, the subjects I address are a number of computer forensic and e-discovery concepts and techniques that tend to provide real bang for the buck in litigation situations. In addition, I want to explain those concepts and techniques in enough detail to be useful while not getting so deep in the details that it becomes meaningless noise. For example, if I were going to explain how to drive a car I would likely describe certain operational aspects about starting, stopping, steering and control. I might even provide some useful information about how to refuel and do simple maintenance like how to change a tire or replenish the oil. Other subjects like gear ratios and cylinder compression are very important details about what actually makes the vehicle run but those kinds of details would likely be useless information for my target audience.

Second, I want to provide an approach for using computer forensics in legal situations with adequate attention to rules of evidence. There are a lot of practitioners in the technology field. It is not uncommon for them to perceive what they think is a better, cheaper and faster way of doing things. The problem for them is their new approach typically omits the much needed "process". This involves digital data and not paper documents. Digital data can be a better a truth detector but it is easy to get ambushed as well. The "process" is an essential element intended to detect the ambush and avoid the trap. There is a saying in the technology

[1] 108 F.R.D. 459, 461 (D. Utah 1985)
[2] Not Reported in F.Supp., 1995 WL 649934 (S.D.N.Y.)

field about “Garbage-in. Garbage-out.” The “process” is simply the means devised to winnow out the garbage.

Finally, I want to blend the technical details with a process compatible and cognizant of the rules of procedure. For decades the legal profession has relied on a discovery process built around an exchange of documents and the manual review of those documents. With the digital age this methodology is simply not practical, nor is it necessary. The computer created this problem and the computer can solve it as well, although the solution will never be fully automated. It will always require some design and management by human controllers.

CHAPTER 1

Introduction

Computer forensics is the application of specialized knowledge to solve legal problems involving digital evidence. The problems range from collection and preservation of digital data, to the analysis of the data, reporting of the findings and then admission of the data as evidence at summary judgment and trial.

E-discovery is not the same as computer forensics. E-discovery is simply the disclosure of digital evidence in a legal proceeding. Thus, e-discovery is focused solely on the disclosure of the data and not its analysis. Indeed, once the data is disclosed, e-discovery is arguably concluded. There can be some overlap between e-discovery and computer forensics, since collection and preservation of digital data is part of the disclosure problem as well

It is well known that more than 98 percent of today's data is stored in electronic form. As a result, there is hardly a dispute or litigation that could not involve computerized devices or their data, which is otherwise known as Electronically Stored Information (ESI).

The dispute may not involve a lot of data but it likely will involve some kind of computerized device or data even if it is a single text message, e-mail, voice mail, transaction record, web search, document, etc. As a result, there is hardly any case that is not a candidate for e-discovery or computer forensics.

Despite the widespread presence of ESI, does every case actually require it? For example, consider a payment dispute for services or products. One might think that the simple production of the contract and proof of non-payment is all that would be required. Nevertheless, it is amazing how such a seemingly simple case could transform into something requiring ESI.

For example, when the contract was breached by the failure to make payment the issue of liability may be settled but the other elements involving causation and quantum, could still be unresolved particularly if the contract's performance is not yet complete. Consequently, proof elements could quickly expand into complex damages issues like mitigation, which could involve the production and analysis of extensive ESI.

As it turns out this kind of scenario is all too common. When the case becomes more complex than initially expected, it is not surprising that the collection of ESI is often inadequate, which potentially exposes the responsible collector to sanctions.

An adequate collection is not the only the only challenge posed by ESI. Indeed, there are many. First, ESI is more complex than its paper counterpart. Thus, it contains much more evidential matter than does its paper counterpart, which tends to make it much more useful, as well. Unfortunately, the increased complexity of this evidential matter also often has many forms which frequently change as devices and applications provide ever increasing functionality. The fact that ESI takes many different forms and is constantly changing also increases the

diversity of expertise needed to analyze and evaluate it and actually make it useful as relevant evidence.

Second, ESI is easily changed and altered. This could be by accident or it could be on purpose. Either situation can substantially alter the evidence and have significant consequences for how the case proceeds and ultimately concludes.

Third, sometimes when ESI is altered it is not just a change to its content. Rather, it could be something more subtle that simply disguises its existence in order to prevent its detection and subsequent analysis. Although there are some very sophisticated techniques for doing this, many are also very simple; yet, very effective still.

Finally, working with ESI can be like being buried alive in the treasure room of the pharaoh. Its volume can simply be overwhelming, particularly if only manual mining techniques are used. Thus, one's success with cyber litigation is highly correlated to one's proficiency with automated search and analysis techniques.

The following sections examine these vary issues. The examination begins with preservation and then moves to analysis and validation of the devices, media and their data. Next, search techniques essential to economically and effectively finding the key evidence is examined. Finally, the rules for getting evidence admitted are examined, at least those with the most likely relevance to ESI.

CHAPTER 2

ESI Preservation - Don't Lose Before You Begin

Introduction

Preservation of ESI is not only the first thing one should do when contemplating litigation, it is the most important one, too. That may seem counter intuitive considering all the other important things that come later but it is true. After all, the remaining steps are impotent without persuasive evidence, which could be missed without an effective identification of ESI followed by its proper preservation.

Ensuring that a litigation has sufficient ammunition and that all of the significant relevant evidence has been collected is not the only reason that ESI preservation is important. In fact, there are several others as well. First, an ineffective ESI preservation can not only hamstring a case, it also exposes it to spoliation sanctions and the cost of spoliation motion practice.

When ESI is not preserved timely it is not hard for it to become damaged and its usefulness diminished. Simply not deleting anything is not enough, since simply continuing to use a computer alters the data it contains. Thus, pr0mptly preserving ESI is very important.

When it comes to sanctions, preservation issues account for a large portion of sanctions awards. In one study, preservation issues accounted for almost sixty percent of the sanctions awards involving ESI.[3]

Remarkably, spoliation sanctions are not simply a defendant's problem. In that same study, nearly 40 percent of preservation related sanctions awards were against Plaintiffs.[4]

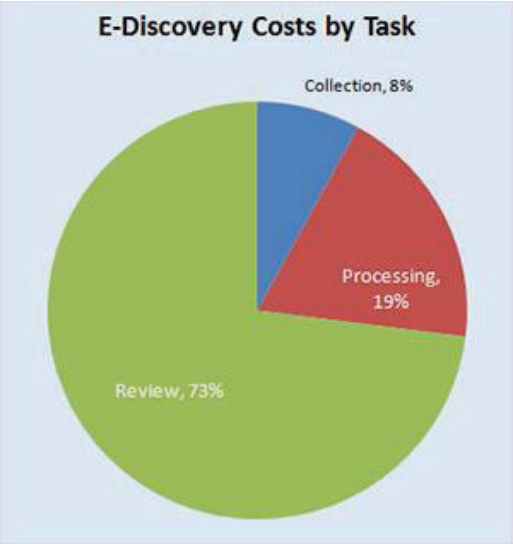
A third reason preservation of ESI is so important involves getting it admitted at trial. Evidence must meet certain criteria before it can be admitted. One of those is authenticity.

[3] *Sanctions for E-Discovery: By the Numbers,* Dan Willoughby, Rose Jones and Gregory Antine, Duke Law Journal, November 15, 2010. Of the 401 decisions from 1981 to 2009 that were reviewed, 230 actually resulted in sanction awards of one kind or another. That is a 57 percent success rate. Of the 230 awards, 136 of them involved preservation issues, which is 59.13 percent of the sanction awards.

[4] Ibid, 53 of the 136 preservation related sanction awards involved plaintiffs

With regard to ESI there are many things that can compromise its authenticity. Some of those things can happen prior to collection and some of them can happen after its collection. A timely and proper preservation is essential to satisfying the authenticity requirement.

Remarkably, many do not appreciate the importance of the preservation phase or understand the special procedures required. As a result, they shortcut the effort in ways that only compromise their case as a result of degraded evidence or even totally missed evidence. Typically, they make these mistakes in the name of economy or budget constraints if not out of sheer ignorance. The concerns about the cost of preservation and its perceived budget busting consequences tend to be ill-conceived, however.



In 2012 the results of a study by the Rand Corp was released that examined the cost of e-discovery. This study is commonly called the Rand Report.[5] According to this report, the preservation and collection phase of e-discovery accounts for only about 8 percent of total discovery costs. It should be noted that e-discovery costs examined in this report covered only the production of ESI from collection through review and did not consider other aspects of the litigation like depositions, motion practice or the trial itself. Thus, in the overall scheme of discovery in particular and litigation in general the costs of preservation and collection are minimal.

Despite its insignificance when compared to the overall discovery effort, the failure to properly preserve digital evidence for litigation can have colossal consequences for the reasons discussed previously. The following sections examine the preservation problem and provide suggested answers for solving it efficiently and effectively.

Common Preservation Mistakes

It is always a big question about what and when to preserve ESI. The simple answer is that potentially relevant evidence should be preserved and it should be preserved when litigation is reasonably anticipated. Unfortunately, there is no bright line standard for determining the question of when. What is likely clear, however, is that waiting until after the case has been filed when earlier notice existed is too late.

[5] Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery, Nicholoas M. Pace, and Laura Zakaras, Rand Corp, (2012), The study examined the costs of 57 litigation matters involving "traditional lawsuits and regulatory investigations". The focus of the study was the cost of producing ESI in discovery across the spectrum of collection, processing and review. Thus, other aspects of the litigation lifecycle like motion practice, depositions and trial itself were not considered.

When deciding what might be potentially relevant evidence there is no need to preserve every copy of potentially relevant evidence, rather, preserving one copy is sufficient. Of course, the problem can often be that while there are many similarities between two data sources there can also be important differences.

Another problem encountered when trying to answer the question about what to preserve is that the issue of relevancy may not be fully developed. A common example is that while the Plaintiff may know what is relevant to its case prior to any filing, it typically is not clear what will be relevant to the Defendant until much later. As illustrated above, the issue for the Defendant may not be limited to the question of liability but could include the Plaintiff's duty to mitigate damages.

As a result, the answer about what to preserve may not be the particular documents but the media on which they are stored. After all, if the media is preserved then everything will have been preserved that could be needed no matter in what direction the case ultimately turns.

Failure to Adequately Identify ESI for Preservation

Preservation failures can start early when ESI is overlooked and not even targeted for preservation. The cause for those failures tend to be either poor identification of key individuals or poor identification of systems and devices.

ESI identification is an important first step in the preservation process. The objectives and targets of a preservation order are often generally stated. Thus, converting those general objectives into the specific devices that should be preserved can be challenging for the less experienced.

There are several complexities to identification. The first is identifying all of the devices subject to preservation when they may reach far beyond a particular target's personal computer. Indeed, the focus can expand to many devices and resources that are not immediately obvious to a person's personal computer such as:

- network resources such as storage devices like
- file servers with personal share and/or departmental share data,
- e-mail, and
- data and document management applications;
- employee's home resources when working from home like
- personal computers,
- attached storage devices, and even
- network storage devices;
- cloud based resources like
- data backups, or
- e-mail;
- disaster recovery and data retention resources for any of the above like,
- backup tapes,
- cloud based resources, and
- disk-to-disk backups;
- many other personal devices such as

- phones,
- tablets, and
- removable storage devices like
  - flash drives, and
  - external hard drives;
- Retirement and replacement policies of
- storage media like
  - backup tapes
  - hard drives,
- Computer devices like
  - Cell phones,
  - Personal computers
  - Network resources like servers;
- Assignment history of
- storage media like
  - backup tapes, and/or
  - Hard drives,
- Computer devices like
  - Cell phones,
  - Personal computers
  - Network resources like servers.

In some cases not all of the resources need to be preserved. It is possible that one resource could provide better coverage than others. Thus, properly identifying which items should be preserved requires knowledge and skills about the systems in order to identify all that should be considered as well as the ability to eliminate some in favor of the best source.

While identifying the ESI sources for preservation is important, another critical factor is selecting the correct preservation method and conducting the preservation in the least disruptive manner. It is often useful to also consider these factors during the identification process.

Before discussing the various preservation techniques that should be used in particular situations and why they should be used it is probably good to have an understanding of the many common preservation mistakes that can fatally wound a litigation before it even gets started.

Continuing to Use a Device After a Duty to Preserve

Continuing to use a device destroys potentially relevant evidence even though the user has not deleted any data. Whether computer users are actually using their devices or just letting them run but not using them there are things happening that can destroy potentially relevant evidence.

When using an application those applications are typically creating temporary files with which the user is actually interacting. The creation of these temporary files can overwrite previously deleted data that could have been relevant evidence. Also, when using applications the data they manage, like documents or spreadsheets, can be changed. Even if the content is not being changed there is application metadata that could be changed by the application which

the user is not even aware. In addition, there is other system metadata like date stamps, registry hives, as well as application and system logs that could be changed.

Even when not using the device its own operating system is constantly performing tasks designed to optimize its own performance. These operations are also destroying potentially relevant evidence. Typically, these are not just a single operation but a battery of operations that have been designed to periodically perform "house cleaning" as a means to optimize performance. In a Windows system for example, after ten minutes of inactivity the system will run processes that will reorganize applications and even frequently used data files to make them more easily accessible. In the process of this optimization previously deleted data can be overwritten and made unrecoverable. In addition, at predefined intervals the system will optimize not only recently used applications but the entire storage media contents. This process, too, can overwrite previously deleted data and make it unrecoverable.

The damage that can be done by continuing to use a device after a duty to preserve is not limited to a destruction of previously deleted items. Indeed, as the system continues to run it will be assessing various active data, typically system metadata but can also include application data as well, and determining whether its established life span is over. If so, even this active data can be purged and deleted where it now become susceptible to being overwritten by the processes described above. On a Windows system, this kind of activity can result in things like Volume Shadow Copy archives being purged as well as other file activity artifacts like link files, jump lists and browser history records to name a few.

Interestingly, some of the system data that is being purged is the very kind of data that could be essential to demonstrate that the device was operating properly. System event logs which, for example, could verify that the system clock is set properly and that important and frequently used date stamps are accurate, are the kind of logs whose records are being purged once their life horizon is reached. Thus, the consequence of continuing to use a device after a duty to preserve is not just a problem with losing important evidence but losing the very data that would be essential to establishing that the data is authentic and is what it purports to be.

Clearly there is a lot of destruction that is happening. It is also quite unpredictable as to whose case it will help or hurt. In other words, it might not just be data owner's case that suffers the consequences. Indeed, it could very well be the opposing party whose data is destroyed or is unable to authenticate whatever interpretation is given to the data by the data owner.

Examining a Device in an Unprotected State

All too often clients and counsel have questions about a computing device. If they are not sure that they actually have something to be concerned about, they might decide to conduct their own analysis before launching a formal analysis. If they are not performing their examination in a protected state then they are subjecting the device to the same kind of damage described in the previous section.

Proper forensic practice is to make a copy of the device or its media. This copy is typically a special copy that captures the data in a way that protects it from future alteration. All subsequent analyses are performed using this special copy of the data in its protective container.

When a device is examined without taking these special collection procedures or at least employing techniques that prevent alteration of the data on the original device the result is the same as continuing to use a device after the duty preserve. Thus, considerable potential evidence can be destroyed.

Even if the device is not damaged by the examination, collecting its data in an unprotected state can still add complexity to the case. If items of interest are discovered there will always be the question about whether the data was put on the storage media by the person performing the examination.

Collection Without Proper Protection Measures

Forensic collection methods are designed to collect their data in a manner that will prevent it from being destroyed or altered. This is typically achieved by collecting the data using any number of different collection methods. In addition, the data collected is typically stored in a way that protects it from future alteration. In other words, either during the collection or after the collection it is placed in a protective container that protects it from accidental alteration through normal usage methods.

Windows is an especially invasive operating system. Collecting a device running the Windows operating system or even a device attached to a Windows operating system can cause many of the data changes described previously. Consequently, devices running Windows are typically collected by using other operating systems or by removing the storage media and attaching it to some kind of write blocking device that will prevent the data from being altered by the collection system. The same is true for any kind of attached storage devices like flash drives or external hard drives.

These kinds of protection measures are not available for things like social media and other cloud based storage systems, since the examiner will not have access to the physical systems. Thus, these kinds of measures are only available when the examiner has access to the physical device.

Many kinds of collection measures copy the data and place it into a protective wrapper that will protect the data from accidental alteration. This is what is commonly meant by the term image, although if the collection is simply a data collection like from social media or cloud based accounts, it is not a physical image or mirror image or bit-for-bit copy or any other term normally associated with a physical image.

Collecting the data without using proper protection measures exposes the data to all of the damages described previously and exposes whatever artifacts are found to later questions about its authenticity.

Inferior Collection Method

There are all kinds of methods that people might want to try and use to collect potentially relevant evidence from devices, media, and storage accounts. For example, some people might simply collect screen shots of certain data displays as a means to collect potentially relevant evidence. Others might try some kind of selective data backup of active files or folders.

Even if these approaches do not destroy or alter any potentially relevant evidence, they can still fall short of a preservation obligation, particularly if it is later determined that they omitted other elements of potentially relevant evidence.

In e-discovery it has become popular to perform the preservation by using a targeted data approach. In other words, the entire media is not captured. Rather, the media is inspected and files of interest are selected for preservation and moved to other media. Supposedly the targeted data approach has grown in popularity for perceived economy reasons. In other words, it is believe that targeted data is more economical than FGI.

The targeted data approach has several shortcomings. First, it takes time to inspect the media, search its contents and decide what should be preserved. This process can often be more time consuming and expensive than just preserving the media using FGI methods.

Second, targeted data collection could involve methods that are not forensically sound and even alter aspects about the data like important system date stamps or application metadata.

Third, at the time when the targeted data approach is performed the issues in the case may not be fully developed. Consequently, documents or other data elements that could become significant later will not have been collected. It is possible that when the importance of those documents or data elements is realized that they do not exist or their contents or other forensically relevant attributes have been changed. This problem will exist even when automated methods have been developed that solve the earlier problems with a targeted collection.

Fourth, should documents harvested in targeted data collection become evidence at trial or at other stages of the case, their authentication will be necessary. In the case of loose files, the authentication of those documents will be impaired if the media from which they were harvested cannot be inspected and determined to be reliable. Typically this is done by examining certain system files and logs that can reveal computer usage and betray that data has been manipulated or all together eliminated. In the case of larger data collections like from complete e-mail post offices or application database there could be other ways to authenticate the data without depending on the original media.

Preservation Verification Failures

A final kind of preservation failure involves the failure to verify the preservation. This usually happens in three different ways that are discussed in the following sections.

Failure to Verify Successful Preservation

The first kind of verification failure is a failure to confirm that the data collected matches the original data source. In all cases of forensic grade images and copies the method of verification is done by comparing the hash values of the original data source to the hash value of the imaged data. The two hashes should match.

While forensic grade images and copies are always preferred, there are times, such as with data copies from cloud based accounts, that the collector will need to devise some method of verification. This could be a count of files and folders and visual verification that the copy matches the original source. Then after collecting the data the collector should preserve the collected data in some kind of protective wrapper. In essence the collector will be performing some kind forensic data copy. At that point a hash verification can be performed of the data collected and the data preserved in the protective wrapper.

Failure to Review Preservation Logs and Confirm Successful Collection

The second king of verification failure involves the failure to review the logs that were created during the collection to determine whether there were any unexpected issues. There could be any number of problems that were encountered during the collection. They could include things like the hashes did not match or that certain media storage areas like sectors in the case of a physical imaging could not be read or that particular files could not be read or copied.

When physical images are being created it is quite possible that certain sectors could not be read for a variety of reasons. They include things like the sector is going bad and either it cannot be read or whatever is read does not pass other integrity checks.

While failures with some sectors can be expected, particularly with older media, read failures with a lot of sectors can signal problems with the imaging process itself or that the device has substantial damage. In either case, a large number of read errors should cause the collector to investigate the cause for an explanation and assessment whether any changes to the process should be tried.

Interestingly, the hashes could match even if there are read errors. The hash match simply means that the collection process has simply written to the copy media whatever it read from the original source media. If the process is unable to read sectors then it will typically write zeros for those sectors to the copy media. Thus, it has written whatever it was it read.

Failure to Review Collected Data and Confirm Suitable Condition

The final preservation verification failure is the failure to view the final product and make sure that the data is viewable. These days it is fairly common for storage media to be encrypted. While in some cases an encrypted drive will manifest itself with a large number of read problems, that is not always the case. In some cases, it is possible for the image to verify, have no read problems and still be encrypted and unreadable. If it is unreadable then it cannot be analyzed.

A detailed examination is not required in order to confirm that the image is in a suitable condition. All that is required is to mount the image and visually inspect the file system and make sure that files and folders are viewable at a few different levels.

Failure to Identify Important ESI Data Sources

There is an old saying in the technology world about "Garbage in. Garbage out." The same rule applies to litigation whenever ESI is involved. Consequently, it is simply foolish to commit resources and proceed with discovery if there are significant omissions in the population, or perhaps worse something even less accidental, that if known would have altered the direction of discovery and the allocation of resources. After all, if one is looking for a needle in a haystack, one at least wants to have the right haystack and have some comfort that the needle is still there; otherwise, it is a lot of wasted effort.

Similarly, if one has limited ammunition, one shoots only at verified targets and not blindly into the darkness. Using the home building analogy once again, it is better to wait and purchase the building materials once the construction plans are known; otherwise, it could just be a waste of resources.

Before committing resources to process and review documents it only makes sense to validate that the media from which they come is worthy of that commitment. After all, there will likely be many different data sources but are they all worthy of consideration? Are some likely to be more worthy than others? Would the worthiness of certain storage media change if it was known that it did not cover the period of interest, the custodian of interest during the period of interest, or if it showed signs of deliberate manipulation? Even if all of the media are valid, would some media still have a higher probability of producing relevant evidence than others and would decisions about the allocation of resources and their timing be different if that information was known?

While counsel typically does not like to "investigate" its client, validating that the population of preserved devices is something that both sides should want to have performed, at least on the opposition's preservation. There are several areas of interest when validating the population of preserved devices and data.

- Whether there have been any other storages devices like external hard drives or flash drives that were attached to bootable devices like personal computers but not preserved that could have relevant evidence?
- Whether bootable devices are the original device for the period in question or was there another hard drive or an earlier hard drive that has not been preserved?
- Whether there are other network attached devices that could have been used to store data and whose contents need to be included in the preserved and potentially producible data?
- Whether the attached storage devices that have been preserved were attached to any other bootable devices other than those that have been preserved?
- What files have been used from bootable devices and are those files on storage devices or media not covered in any of the above?

Although the parties could agree for the examination of their electronic media for these purposes by an independent expert or by their own experts it is also possible to answer these questions without having to examine the devices themselves. Instead, there are certain system files on the bootable devices that could be produced as part of discovery and those files could be examined to answer the questions about what devices have been attached and whether the bootable device's media appears legitimate.

The particular files that one would want to examine depend on the type of bootable device. In other words, is it Windows or is it Apple, for example. For Windows systems the files

of interest for confirming storage media and attached devices are generally several Registry hives. For Apple machines is it several Property List (PLIST) files. Even after identifying the type of bootable device there could still be differences between the operating system versions on those devices that could affect the particular files that will be of interest.

Answering the first two questions above is easily accomplished by requesting the same system files on bootable media. The other questions above could also be answers but there are different files and it is not as simple as a "look" at a few files on bootable devices. Nonetheless, the information is easily obtainable with file system and file pointer kinds of analyses. Consequently, it still is something that the parties would likely want to confirm before "wasting" valuable resources on incomplete, or potentially worse, questionable data.

In a multi-stage discovery plan the parties could defer confirming devices in the lower priority strata until it actually looks like they will be examined. Assuming the first stages are related to more important and likely productive targets, validating the population of preserved media for those strata should be done early.

With respect to other network attached storage there are a couple of different places where one could look in order to make that determination. The "look" is a little more involved than just a couple of files, however.

Once again, both sides have an interest in validating that the population of potentially producible documents is complete. Hence, both sides should want to embrace this effort and include the correct process in their discovery plan and protocols.

Why Letting Clients Self-Preserve Can be a Bad Idea

Clients often have technology staff in-house that help with the administration of their computer systems. Nevertheless, client personnel are not a good source for forensic expertise and there are several reasons that this is true.

First, they are not normally involved in forensic processes. Rather they support the organization in the execution of its mission, which is not litigation or forensic services. The difference is often like the difference between the infantry and the special forces. Both may be able to fire a rifle but the ways in which they use them are entirely different. Even the rifles themselves are different because a forensic expert will likely have different tools to examine media and its contents than a client's in-house technical support staff.

A second drawback to using client personnel is that there will be "combat". Litigation is not just using a weapon to fire at paper targets. Further down the line there will actually be contact with the enemy, so to speak. Unless the client personnel have done that kind of thing before, they are likely a less attractive choice than someone that is combat experienced.

Third, a lot of what happens in even the early stages of the collection and analysis process is to prepare for the "combat" that will happen later. Thus, considering less capable client personnel could be like bringing a knife to a gunfight.

Fourth, in a recent Pokemon survey of IT security professionals less than 8 percent would recommend using an outside consultant to assist with the analysis of a data breach; but, more

than 50 percent of those same respondents claimed that their staffs lacked the tools or the training to determine the cause of the breach. These survey results are highly relevant to the selection of a forensic expert particularly when one considers that client IT personnel are more closely aligned to the breach issue than to providing litigation support services. Thus, if they are not well prepared for something more closely aligned with their actual job function, how well will they perform on something that is not aligned to their job function?

Finally, there have been a number of spectacular cases involving spoliation and sanctions involving ESI preservation by client personnel. The lesson that gets learned over and over is that whenever client personnel are involved in the preservation process warning bells should go off and special attention should be given to depose and review exactly what they have done. In the end, therefore, using client personnel may cause more problems than they solve and raise costs accordingly.

Selecting and Using Experts for Identification & Preservation

In the preservation phase there are two areas where the forensic expert can be essential. Those areas are identification of potentially relevant ESI that should be preserved and then actually conducting the preservation effort.

When identifying potentially relevant ESI for preservation the forensic expert can provide several valuable functions. The first is identifying the sources of ESI. Properly identifying ESI is not necessarily as simple as asking the client where their data resides. The client and its technology personnel are likely inexperienced in litigation matters and may think quite narrowly. Their limitations may involve the actual devices as well as the extent of the data that they contain.

The expert should be seasoned in litigation requirements and know to how to develop a conceptual model of the client's systems that not only includes formal system components like servers, personal computers and phones but informal components like flash drives, external hard drives and home computer devices. There could still be other formal system elements worthy of consideration such as backup system, communication systems and document management systems.

A computer expert should know how to define the population and then peal each layer in order to identify those elements likely to contain potentially relevant ESI warranting preservation. As the expert learns about the target's system, he is likely better able to identify that when one type of system or usage occurs then another is likely to exist as well.

While the final decision belongs to the litigator, the expert can present the litigator with intelligent options. For example, if there is detailed backup history then a separate preservation of a server or a least a forensic preservation may not be necessary. Similarly, if the key personnel only used their assigned equipment and never logged into a server as an operator then the server is not likely to contain the kinds of forensic artifacts that could be obtained only from a forensic imaging of a server. So, again there is no need for that kind of expenditure and effort.

The expert may also know to inquire about retirement and replacement policies at the target and history of equipment used by key personnel in particular. He would also know to

inquire about device usage policies and be able to confirm representations when conducting his inquiry or at the time of actual preservation.

Another reason for using the expert for the identification process is that as he learns the system he can determine the best methods for performing the actual preservation. This latter phase can include both the timing of the preservation and the best method of preservation while considering how to reduce disruption and overall costs.

During the identification process the expert can likely also provide feedback to the client and litigator about estimated costs and timing so that reasoned decisions can be made. In the end, the expert is well positioned to testify about the process and justify the reasonableness of the approaches taken. After all, the preservation standards are for potentially relevant evidence and it is not a standard of perfection.

So, there are a lot of benefits to using an expert for both the identification and actual preservation of ESI during the preservation phase. When selecting an expert for this process, the litigator should consider what experience the expert has had in this kind of effort. Specifically, exactly how skilled is he in conducting the preservation phase. It could be that his vast experience is comprised mostly of analysis and testimony based on media that was captured by others and supplied to him. So, it could be that his preservation experience is rather limited both in terms of the identification, the actual requirements for identification, and even in conducting the actual preservation for the various types of equipment that could be encountered.

So, if he is being used in the identification phase, one obvious consideration is whether he has served in that capacity before. An equally important factor could be whether he has had to defend any preservation that he has performed in the past or attack any preservations performed by others or whether, once again, his work has been limited to the actual analysis and findings phase.

If he is being considered for the actual preservation phase, then the things to consider are whether the expert is experienced in preserving the types of devices that need to be preserved? Personal computers can have different preservation approaches than enterprise servers. Phones can have still different approaches. Also, there can be different approaches for Microsoft based systems than Apple based systems. If the interest is e-mail servers, document management systems or other application databases there could still be other approaches to the preservation problem.

If the expert has participated in the identification phase then the device population should be fairly well understood and determining his experience and capability should also be rather straightforward.

When it comes to preservation another factor to consider is that the reality is often different than the plan. The differences often involve the number of devices, types of devices and size of devices. So, the last thing to consider about the expert's relevant preservation experience is his ability to improvise and adapt when field conditions differ from the plan.

Understanding the Preservation Tools and Techniques for Different Situations

There are a variety of preservation tools that create forensic images. Forensic images are different from the images created by a client's technology personnel in that forensic images capture the entire media. Thus, they capture the active data, the deleted data and they even capture areas of the drive where user data would never be stored. The images typically created by normal technology personnel focus on the active data only.

While the forensic tools are often capable of collecting some smaller segment of a storage media, like the active data, those kinds of images are generally specifically identified as logical images, for example, or some other restrictive container name.

Timing is not the only issue. There are many others which are often technological and driven by the different types of devices and media on which evidential data is found.

With respect to personal devices there are personal computers which are different from cellphones. In addition, there are tablets and removable storage devices like flash drives or external hard drives. In the right circumstances even entertainment devices like Ipods and gaming devices could be of interest.

All kinds of business devices can also be included like network servers, storage appliances, and backup systems. Even unexpected devices like printers, security systems, routers and even switches that contain network traffic logs could be of interest.

The internet has also introduced challenges for collection and preservation that include cloud based email systems, websites, social media sites and data storage. In some cases, like a website, collection and preservation can include collecting what is only publicly available even when the collector is not the site owner and cannot access the actual data storage areas.

When the target of collection is not "loose files" but documents or data within another system container, the approach can still differ yet again. An e-mail post office or document management system or application database could warrant more targeted and specialized collection methods.

Even within the different types of devices there can still be differences in collection and preservation methods. For example the approaches that one might use for Windows based systems could be different than for Apple style devices just to mention two examples.

The kinds of tools that an expert will need can vary based on the type of equipment being imaged. The differences tend to be the interface that the storage devices use to transfer their data. For example, internal hard drives use one kind of interface while external devices like flash drives tend to use a different interface. So, the expert needs to have the kind of equipment capable of handling these different interfaces.

The expert is also expected to preserve the data without altering the original evidence. Typically the only concern for alteration is system metadata. It is unlikely that any preservation or collection method would change the data contained within the files themselves

unless they are opened and viewed during the collection and preservation process. The act of opening and viewing the data could alter application metadata that is internal to the data file.

In any event, the protection of the original evidence is done with write blockers that prevent the collection system from altering the original media but in some cases the imaging method itself may be capable of collecting the data without altering anything even without a write blocker.

Additional considerations to the preservation mechanics themselves involve verification and redundancy. The verification confirms that after the imaging is completed that the image the original media. Calculating the verification typically means reading the data twice—once when the image was created and then again after creation.

When creating images it is best to create redundant copies. It is not likely that the device on which the image resides will fail but it does happen. In that event, it is best to have a second copy of the image.

While the approach and technology used by an expert for preservation is one thing to consider, another is the preservation capacity that the expert could deploy. It is not unusual for preservations to involve many devices and their media. In addition, the preservation window is typically narrow. So, the expert needs to have adequate capacity to get the job done within the time constraints.

Forensic Grade Imaging (FGI)

Forensic Grade Imaging (FGI) is the best method for preserving most ESI and evidential media. FGI is different from other forms of imaging such as those frequently used by IT professionals to deploy systems within an organization. There are two fundamental ways in which FGI is different.

First, FGI captures the contents of the entire storage media. This includes the active data, the deleted data, storage areas that may never have been used and even storage areas that are not normally accessible to users.

The second difference is that FGI captures its data in a protected mode that is designed and intended not to alter any of the data contained on the storage media. The protection is achieved by using different write protection mechanisms that while permitting the media to be read prohibits any data from being written back to the media. There are many different types of write protection mechanisms. Some are hardware related and use specific devices that prohibit alterations to the original media. Some are software related and work much the same as the hardware devices from a software standpoint or they alter the methods by which the media is mounted for acquisition as a means of preventing alteration to the media contents.

FGI should usually be used to preserve personal computers and attached storage devices like flash drives and external hard drives. FGI may also be suitable for preserving other devices like network servers and network storage devices, although if network servers and storage devices have a sufficient historical backup history then that history is usually more robust than any current period forensic grade imaging. Also, if the network server or storage device is larger than a few terabytes it may not be practical to preserve their data with FGI. Finally,

network servers likely have multiple drives that have been RAIDed and configured to work as if they are a single device. While the individual drives can be imaged and then reassembled virtually, it is usually best to image their storage area “live” while the machine is running.

Imaging cellphones is very different than imaging computer hard drives. FGI may not be possible with all cell phones ether because cell phones are not as standardized as computer hard drives. Instead, phones are very proprietary to that manufacturer and model. As a result, there are simply too many types of cell phones for forensic tool makers to learn their proprietary technology and then develop a device level imaging technique. In addition, they are changing about every 6 months. Currently, there are more than 7,000 different cell phone models and it is just too much for the forensic tools to keep pace.

As a result, it is more common to preserve cell phones using a logical rather than a physical methodology. The logical method relies on interfaces and access points published by the manufacturer that will not allow full access to the device even though it will often allow full access to its active data. A typical example is that currently there is no way to image e-mail on an Apple iPhone 5 or 6.

Cloud based accounts like web mail or document storage applications are also not conducive to FGI, since access to the storage media is typically not available. Usually at best all that one has is the means to download or copy the data from the cloud based storage to a local storage system.

Devices using full disk encryption can often be imaged but the data cannot be used until it is decrypted. In some cases, full disk encryption can even prevent a successful acquisition using FGI without proper credentials and the ability to decrypt the data on the storage media. In those cases, the imaged data will simply be zeros as if the media were empty or its sectors could not be read.

Some forensic tool manufacturers have incorporated the more commonly used encryption methods in their software such that even an image of an encrypted drive can be read but the examiner will still have to have proper access credentials. It is often safer to treat encrypted devices similar to network servers and image their storage areas “live” while the machine is running.

Monitoring and Validating an Expert's Preservation Work

It is not enough for an attorney to prepare a litigation hold instruction, issue it to the client and then do nothing else. Rather, an attorney must be actively engaged to ensure that his instructions are followed or at least carried out. It may not be necessary that his instructions include details about performing the preservation but his oversight and management should ensure that the job gets done.

When overseeing the work of vendors and experts during the preservation process, there are several things that attorneys can do to properly supervise and manage the collection process. The first of these is the data map that would have been created during the identification phase of the preservation process. This data map would show the universe of storage devices as well as those identified for collection and preservation.

Second, is to communicate frequently about the scope of the preservation effort and how things have progressed. While small case preservations can be handled in a single day or maybe two, more complex cases can take awhile and involve multiple locations. Also, the actual imaging and preservation effort can vary dramatically from the initial identification and preservation plan. Clients often forget about a device's history or what might be available for preservation. Thus, it is quite common that once the process really begins that actually field conditions could vary. For all of these reasons the attorney should want or expect regular communications and updates from his vendor or expert performing preservation.

A third thing that can be done is to accumulate and review the vendor's or expert's chain of custody and evidence records. These records should both memorialize what items have been preserved and identify them to particular custodians.

The fourth thing that can be done is to accumulate and review the vendor's or expert's FGI logs. Typically, FGI tools create logs that memorialize the imaging process. Some of the typical data elements are the:

- imaging date and time;
- imaging tool,
- imaged device manufacturer, model and serial number;
- imaged device storage capacity;
- number of image segments;
- whether any errors or bad sectors were encountered, and
- original and image hash values that confirm the image exactly matches the original data.

Remarkably, this kind of data can be instrumental in confirming that things have been done well and that there are no problems or, on the other hand, alerting the attorney that there are problems. For example, hashes that don't match indicate that the copy does not match the original. If there are no original and image hashes that would signal that the image has not even been verified.

Bad sectors reveal that original data has not been read and captured in the image. There could be many reasons for there to be bad sectors. If the number of bad sectors is few then it likely only signals a storage device with physical problems. When the numbers are larger and particularly if they very material it could signal physical defects to the device that might be something other than natural wear and tear. It could also signal an encryption area on the drive that may need to be decrypted prior to having a successful collection. Remarkably, the hashes could match even if there are bad sectors. In short, there is no limit to what problems could arise.

Handling Preservation Failures

Preservation problems can arise from a variety of causes. Typically it is from inadequate instructions about what and when to preserve or it is completely overlooked media. Fortunately the standard for measuring adequate preservation and collection is not one of perfection. When failures occur there are steps that can be taken to alleviate the consequences. The first is forensic recovery and analysis. The second is defending against a claim of spoliation.

Using Forensic Analysis to Mitigate the Consequence of Overlooked Media

Although time passage is a critical factor in the proper preservation of ESI, if something has been overlooked it might not be too late. The device may well have relevant evidence readily available. If, on the other hand, it appears void of anything significant then the issue becomes did it ever have anything of interest. Of course, even if it has something of interest the question can be did it have more.

If only a few months have passed then the answers to these questions about what is not still available on previously overlooked media might still be available through forensic analysis. If it has been longer than a few months then forensic analysis has a low probability of being effective.

The kinds of information that might be helpful is likely not what one would think. While recovery of deleted files may be possible what will likely be more comforting is did any files of interest ever exist on the media in the first place.

If the newly found device is a bootable device then are typically many kinds of examinations that can be performed that will reveal what had been on the media even if the documents themselves are no longer there. Thus, to mitigate an overlooked device the best that one might hope is confirmation that there are no significant documents missing.

If the newly found device is not a bootable device, like a flash drive, then the types of analyses that may be performed are more limited. Typically, the review will be limited to file system data that can show what files had existed on the device and when they were last there. With bootable devices that have their contents turnover frequently, the file system can be incomplete but with less volatile media like flash drives the file system data is likely more persistent.

Thus, when previously overlooked devices and media are located the best course could well be to forensically examine it. Specifically, the following processes could be useful.

- Collect and preserve
- Forensically analyze
    - File system analysis
    - File activity analysis
    - Link Files
    - Browser history
    - Recycler activity
    - E-mail parsing & recovery

Even when the device or media cannot be located for examination, there may be other artifacts about that device or media that are located on other devices or media that can help to

assess the significance of what is missing. For example, several things could be determined from the device to which it was attached that could help assess its significance like the timeframe of the attachment. If the attachment is determined to have been a single event then both the timing and single event could help minimize the significance of the attachment. If these dates were correlated to other events that could also shed additional light onto the significance of the attachment.

Dealing with a Spoliation Claim

If there has been a preservation failure and it cannot be adequately resolved with forensic examination of the overlooked media, a claim from the opposing side about spoliation could be next. While the study on e-discovery sanctions discussed previously reveals both a high success rate of sanctions awards and a high frequency of preservation related sanctions, there are actually many different kinds of sanctions that can be imposed. Not every error results in mortal wounds like an adverse inference or a default judgment. Indeed, there are actually many types of sanctions and they should be properly matched to the kind of offense.

The different types of sanctions span the gamut and include the following:

- More time,
- More discovery,
- Monetary or cost shifting,
- Fines,
- Special jury instructions (Adverse inference),
- Preclusion of evidence, and
- Default judgment.

Typically sanctions like special instructions, preclusion of the evidence or default judgment require a showing of bad faith or gross negligence and some kind of prejudice. It can be a heavy burden for those advancing such theories. Consequently, if the omission is singular as compared to something much more widespread and conceivably obvious, it can be a tough fight to carry for those claiming the more extreme sanctions. Even if the omission is a more significant volume, if the prospect for prejudice is not clear then such a claim can also fail.

For those advancing such arguments, it can be hard to prevail if the documents have been totally destroyed and no longer available. The next best proof could be the use of system metadata that verifies the prior existence of the documents and perhaps by their names the relevance of them to the case will be obvious.

Summary

The preservation and collection phase of discovery accounts for only about 8 percent of total discovery costs. Thus, in the overall scheme of discovery the costs of preservation and collection are minimal. Amazingly, there is often pre-occupation in finding the most economic solution for this effort as a cost saving measure.

Despite its seemingly minimal contribution to the cost curve, the preservation and

collection phase is likely the most important step in the litigation lifecycle. Indeed, a failure to preserve and collect evidence properly can mortally wound the case before it even has made much progress.

While it can be difficult to quantify the consequences of a flawed preservation and collection, there are several reasons that it is so important. First, simply continuing to use a computer or digital device and its storage media can destroy evidence. Thus, even when not deleting anything a party can be spoliating evidence and exposing itself to considerable risk from sanctions if not just the cost of defending motions against them.

Second, a proper preservation should focus on preserving and collecting the media, although there can be exceptions for large mass storage devices like network file servers. Preservation can be done most effectively if the amount of analysis trying to find what might be producible evidence is limited. Analysis can take more time than preserving the media itself. In addition, it could be hard if not impossible to predict what might be the full scope of relevant evidence at the preservation phase of the case.

Third, computer evidence is subject to the same foundation requirements as paper evidence. This includes the confirmation that the computer itself is working properly and that the data has not been altered and is what it purports to be. The best manner in which to make this determination is often done by examining various system files. The collection of these necessary files is routinely part of a forensic grade imaging while not typically part of lesser preservation and collection methods like a targeted collection.

Clearly, there is much technical expertise required to both preserve and collect evidence properly and in the most efficient and effective manner. In the event that something is overlooked this same expertise will be essential in examining the data source once it is located and determining if there has actually been a significant omission.

Clearly, faulty preservation or the failure to preserve properly is a huge risk from a sanctions perspective. The consequence is not limited to the sanction itself. Indeed, the process of adjudicating the sanctions motion can be very expensive but even that may not be the most costly.

Perhaps the most costly consequence of inadequate preservation can be the injury done to the entire litigation effort. Clearly if one has not done a good preservation effort then they cannot have a good harvest of relevant evidence. If evidence is the foundation of every case, how strong a case can one have if it does not have a strong foundation? How much effort will be wasted trying to make something happen that has been crippled by inadequate preservation?

To borrow from a sports analogy, it is not only easy to fumble the ball in a poorly executed preservation, it is also easy to force a turnover. If the statistics of fumbles and turnovers during the collection process seem small when compared to the total number of kickoffs, that may just mean that coaches are not letting, or are not recruiting, players that know how to strip the ball and recover the fumble for a turnover. In the meantime, continuing to play the game without a proper preservation is like continuing to play without the full team on the field.

CHAPTER 3

File System Analysis – Taking Inventory

Introduction

File system analysis is a means for quickly learning what is on a storage media and assessing its potential significance for further evaluation. Knowing what is on a storage media can support other kinds of analysis such as what is active or deleted, when it was added or deleted, how often it was changed, etc. These kinds of analysis can largely be done at a summary level using the file system.

Electronic storage media can be analogized to a library. The library has the card catalog that tells visitors what books are in the library as well as certain attributes about those books like name, publisher, publishing date, pages, subject area and where the books are located on the shelves. The file system provides similar functionality for a storage media. It tells users what files are on the media, the general nature of the file based on extension, the location of those files and certain attributes such as certain date stamps. In addition, to the active (non-deleted) files on the media, the file system may also contain references to previously deleted files.

File system analysis is a good first step in learning what treasures exist on a particular media. Thus, this step should apply to all digital storage devices like desktops and laptops, cellphones, tablets, flash drives, external hard drives, etc. As the first cut at data analysis it is a fairly straight forward process that simply catalogs the contents of a file system in order to learn what the storage device or media actually contains and prepare for subsequent analysis.

Setting aside the actual analysis of the data, if there is a complexity to file system analysis it is that there are many different types of filing systems. The Hierarchical File System (HFS) used by Apple computers is different from File Allocation Table (FAT) and the New Technology Filing System (NTFS) used on Microsoft systems. Similarly, the EXT2 and EXT3 filing systems used by the Linux operating system and found on many Network Attached Storage (NAS) devices is different from both Microsoft and Apple systems. As a result, just being able to read the filing system requires the use of tools that know how to interpret a device's filing system.

Preparing and Processing File System Data

Prior to doing any actual analysis of the data it has to be prepared for review. Preparing the data for review includes several facets. The first is simply reading the data contained in the file system and presenting it in a form or system where it can be easily reviewed and analyzed. The second is performing various tests about the files and folders and presenting their results for consideration with the cataloged results.

Naturally, each of these two facets has many components. The following sections identify the key data elements that should be cataloged as well as the supplemental tests that should be performed in order to effectively review the results and reach conclusions.

File System Attributes

There are a variety of different filing systems. Each system contains certain data that helps to manage the data on the storage media. The following is not an exhaustive list of file system attributes but only some of the most common attributes that facilitate analysis of digital media storage systems. These attributes are grouped into date stamps and other attributes.

Date Stamps

Date stamps are found in every file system, although the wealth of date stamp information can be different for different file systems. Some file systems have more date stamps than others and those dates may or may not have time stamp information as well.

When something happens is often quite significant when examining a fact pattern. As a result, date stamps tend to be one of the most important and interesting attributes found in a file system.

Typically file systems will have some combination of four different date stamps. Those are the last written or modified date, the create date, the last accessed date and the record date. In addition, there can be issues about interpreting date stamp values. All of these are discussed in the sections that follow.

Last Written or Modified Date

The last written or modified date, also known as the last write date, typically includes a time stamp as well. These values capture the date and time when the file was last saved.

Whether the date stamp is known as the last written or the last modified date often depends on the file system and the tool being used to interpret the file system. A primary cause for the confusion is that in NTFS file systems there are essentially two different last write dates. One applies to the files while the other applies the file system record itself. As a result, users of file system information just need to be less focused on the date stamp name and more focused on the function that the data stamp provides within the file system.

Interestingly, when the file was last saved may not equate to when it was last modified. Whether a “save” process will be initiated is controlled by the application with which it is managed. In some applications, issuing a save command will literally save the file even if it has not been changed. The file system will update the last written date when the “save” process is run.

Newer versions of Office applications like Excel and Word have more intelligence and will only save the file if changes have been made to it. If no changes have been made then no save process is actually run even though the user requested that the file be “saved”.

For many file systems the last written date is the only date stamp that is available. There simply are no other date stamps captured by the device’s file system. Phones, for example, tend only to have a last written date stamp. Phones are not the only systems with this limitation, however. Older versions of Unix file systems are also limited to this single date stamp. There are likely others but the most common file systems in use today, like those on Microsoft and Apple computers, have several others.

Regardless of the file system, the last write date tends to follow the file as it is copied from device to device. Thus, if a file is copied from an employer’s computer system to a flash drive taken by a departing employee, the last write date of the file will be the same on the flash drive as it was on the former employer’s computer system before being copied.

The fact that the last write date does follow the file from storage device to storage device makes this date stamp a useful indicator of whether a file has been changed after it was taken or at least if it was opened, viewed and a save command issued from its managing application.

Created Date

The created date is often a misleading date stamp. On a Windows based system it identifies the date and time that the file was created on the drive. Thus, the create date may not correspond to the date when the file was actually created. If the file was not actually created on the media but was copied from some other media then its actual creation date and time could be much earlier.

On an Apple system, however, the create date tends to follow the file from media to media. Thus, on an Apple system the create date tends to reflect the actual creation date.

The difference in create date behavior between Windows and Apple systems can become blurred when files are moved between the two systems. When this happens the create date can take on entirely different meanings depending on which system the file originated and how many times it has been moved between them.

Last Accessed Date

The last access date is also a feature found on later versions of FAT16 and FAT32 which was used on earlier versions of Windows like Windows 95 and 98. These days the FAT file system is typically found only on flash drives and the last accessed date only captures the date. Thus, there is not time stamp component of the last accessed date on a FAT file system.

On other file systems like the NTFS used on Windows systems of today and the HFS systems used on Apple systems the last access date has both a date and time stamp.

The exact behavior of the last access date stamp can depend on the operating system of the computer to which the storage media is being used. In older Windows systems like 98 the date was typically changed when the file was opened and viewed. On Windows XP system it was much more sensitive. Even simply highlighting a file could update the date stamp.

Starting with Windows Vista and beyond, the last access date stamp was made very insensitive in order to eliminate update operations and let the system run faster. As a result, the last accessed date became less forensically significant since fewer activities effected its value.

Although the last access date has been desensitized, it is possible to make the date stamp resume its more sensitive behavior by setting the System registry hive's NTFSDisableLastAccessUpdate registry key to zero. From a security perspective and for the protection of trade secret data, it is recommended that this configuration be implemented.

On Apple systems the last access date behave more like it did for Windows 98 where the date stamp was updated when the file was opened and viewed.

Record Date

In NTFS file systems there is also a date stamp for when the file system record was changed. In other words, it reflects the date of changes made to the metadata for the file system record.

Since this date stamps pertains to the metadata of the file system record it does not pertain to the file itself; nonetheless, it can reveal very interesting facets about the life of a file. For example, when a file is deleted the metadata related to the file's active or deleted status will be changed. This action can then cause a change to the record's metadata which updates the record date. Similarly, if a defragmenter is run and changes the location of a file this can also cause a change to the record's metadata which updates the record date.

Date Stamp Storage Formats

Interpreting a date stamp is not limited to just understanding behaviors of the create, modified or last accessed stamps. There can be other issues as well such as why is there no time stamp or why are all of the time stamps set to the same time. Another set of questions could be why do all of the date values have a year of 1980 or 1601?

The answer to these questions often starts in understanding how dates are stored and exactly what data is stored. Specifically, if the stamp is captured in a single 64 bit value there is one explanation but if it is captured in one or two 16 bit values there is another.

The date stamps from FAT file systems, which are typically found these days on flash drives, are usually two 16 bit values. One 16 bit value is the date while the other is the time.

When the date is a 16 bit value, the date element is actually a bit mapped value with the first 7 bits being an integer value for the number of years since January 1, 1980. The next 4 bits identify the numeric value for the month and the last 5 bits identify the numeric value of the day. Thus, the date stamp is not actually the date but the number of years since the starting value of January 1, 1980 and then adding the correct month and day.

When the time is a 16 bit value, a similar bit mapped process is followed. The first five bits are the hour. The next six bits are the minutes. The final five bits are the seconds but in 2 second increments. Thus, the time stamp is only approximate within a tolerance of 2 seconds.

While the create and last write dates on a flash drive using a FAT file system have date and time stamps, the last accessed date on a flash drive using a FAT file system does not. For the create and last write dates the FAT system is using the two 16 bit values but for the last accessed date it is using only a single 16 bit value. Thus, only the date is being captured for the last accessed date.

In some presentations of the last accessed date, such as in a spreadsheet, a time stamp for the last accessed date may be presented of around midnight. This is caused by the application interpreting the non-existent time stamp as a zero value or 12 midnight. If the last accessed date time stamp has some other time early in the morning like 4 or 5, then the

application is applying time zone values to the zero timestamp information and calculating from what is essentially Greenwich Mean Time.

A 64 bit date stamp has a starting value of January 1, 1601 and is the number of 100 nano second increments since that date. Thus, even with a 64 bit date stamp, the date and time is not the actual value but a calculation based on the number of nanosecond increments from the starting date of January 1, 1601.

Other Attributes

In addition to the dates described above, the file system, like the card catalog, captures many other attributes about the files and folders residing on the storage media. Some of these other attributes are actual values like the file name and location, while others are bit mapped semaphores, like archive, indicating whether the condition exists.

Name

Like the card catalog captures the title of the book, the filing system captures the name of the file or folder. Depending on the file system the file name can be presented in different ways.

In FAT file systems the file name is limited to only 8 characters, although if it is a version that supports long file names there will also be other segments where the longer file name is stored in addition to the shorter 8 character name. In NTFS file systems the file name can be much longer, 255 characters.

For both FAT and NTFS there are limitations that can be used for the file name characters. Certain special characters are not permitted.

Active or Deleted

Whether a file is active or deleted is memorialized differently on different file systems. For FAT file systems a deleted file is indicated by a special character in the first position of the file name. As a result, deleted file recovery from FAT file systems can have a misleading first character in the file name of a deleted file. If the FAT file system is one that supports long file names and a long file name was actually used, then the recovery tool may be able to reset the first character of the filename to its correct value by reading the first character of the long file name information.

On an NTFS file system there is a separate field in the file record that designates whether the file is active or deleted. As a result, deleted file names from NTFS file systems are usually the actual file name unless something like a file wiper has overwritten the file name as part of its data protection process.

Location

The location provided in the file system is not the same as the path. In the file system, the file location identifies the cluster where the file resides.

On a FAT file system the file name record only has the starting cluster location. If the file is larger than a single cluster the remaining clusters being used to store the file are recorded in the File Allocation Table itself. Thus, locating a file requires knowing the starting cluster number as well as all other storage locations that are contained in the File Allocation Table.

On an NTFS file system, the entire file locations are stored as part of the file record. The record is not a list of all the clusters individually but a record of all of the contiguous cluster ranges, which are called extents. In other words if a file was stored in clusters 5, 6, 7, and 10, the extents captured in the file system would be 5-7, 10.

While the absolute location of a file may not be very user friendly, there are often times when knowing this information can be very useful during forensic analysis. For example, if a file is deleted and overwritten but its prior absolute location is known then the file system information can be used to learn what file actually occupies that location currently. Other attributes about the overwriting file such as date stamp information could provide further insight into what happened to the deleted file and when it was overwritten.

Size

The size of a file is typically stated in bytes. Both FAT and NTFS file systems regularly contain this information.

When the size of a file is not stated in actual bytes but in some other unit of measure such as kilobytes, or megabytes or gigabytes, one often has to indicate whether the unit is a decimal or binary presentation. In a decimal presentation, 1,000 bytes is a kilobyte. In binary terms, however, a kilobyte is actually 1,024 bytes and not 1,000 bytes. Thus, a binary kilobyte is actually larger than a decimal kilobyte.

From a strictly technical perspective the binary presentation is the most accurate. The Windows property presentation, for example, is stated in binary. Thus, for both accuracy and clarity purposes it is important to specify whether any size representation is a decimal or binary presentation.

Archive

The archive indicator on Windows systems and is typically part of a bit mapped semaphore. The archive attribute can provide information about whether a file has been changed since its last backup. When a file is backed up, the archive bit is reset to zero. When the file is changed, the archive bit is set to 1 and signals the backup system that it has changed.

The archive bit only comes into play for backups when performing incremental or differential backups. Both of these backup schemes only capture files that have changed since their last backup.

The condition of the archive bit does not typically have much significance when examining personal computers like workstations and laptops, since those devices are not typically being backed up, although that practice may have changed with the frequent use of cloud based backup tools. The condition of the archive bit can have more significance when examining network resources like servers, since those devices are typically being backup up.

The condition of the archive bit can signal whether a particular file has been used since it was last backed up, which is often an important consideration for trade secret cases. Naturally, it would be highly significant to find a misappropriated document on the server of a new employer. Their defense could well be that the file is not being used. The state of the archive bit could be used to confirm that assertion.

Determine Other Content Attributes

When examining computer storage media not all of the important attributes are contained in the file system. Indeed, there are many other attributes that can provide additional helpful information. Many of these attributes are calculated values and are later used to facilitate analysis of the media and its contents. In fact, most forensic analysis suites provide for these capabilities and memorialize their results in the same presentation provided with the basic file system information. The following sections discuss additional data attributes that should be part of every examination.

File Signatures

Generally, people identify a file type by its extension. This is not the only indicator of a file type nor is it very reliable, since there are many different file types that also happened to have the same extension.

In addition to being identified by their extensions, many types of files have a certain combination of bytes in the first few bytes of the file. These first few bytes are often called the header or the signature. As an example, the following signatures are found in the first few bytes of the indicated file types.

SIGNATURE	FILE TYPE
PK	Zip file
ÿWPC	Word Perfect
MZ	Executable program file
ÐÏ	Microsoft Office file

Many software applications do not rely on file extensions in order to recognize a file for use with that application. Instead, the software applications rely on the file headers. One such example is Microsoft Outlook. Outlook does rely on the file extension. Rather it looks to the file header as the indicator of what to do with the file.

The process of determining file signatures examines these first few bytes in every file and identifies the actual file type based on its signature. Signature analysis, therefore, provides a means to determine file types on their file headers instead of their file extensions which can be easily changed.

File Hash Values

Hashes are frequently used in computer forensics and e-discovery applications. They are essentially a one way algorithm that computes a unique value for a data stream.

The data stream could be anything but for forensic and e-discovery purposes the most common data streams are individual files ad entire hard drives or storage media. like the contents of a file or the contents of an entire hard drive. The most popular hashes for forensic and e-discovery purposes are the MD5 (Message Digest 5) and SHA-256 (Secure Hash Algorithm 256).

The MD5 is a 128 bit calculation while the SHA-256 is a 256 bit calculation. Essentially the 128 versus 256 involves the number bits used in the calculation which also affects the statistical probabilities of two different data streams producing the same calculated output. In the case of the MD5 hash, the 128 bit calculation means that the odds are less than 1 in 3.4 times 10 raised to the 38^{th} power (3.4×10^{38}) or the number 34 followed by 37 zeros.

SHA-256 hash is similar but with less chance that two documents with different hash values are identical or that two documents with identical hash values are different. Thus, the SHA-256 would be 1 in 3.4 times 10 raised to the 76^{th} power or the number 34 followed by 74 zeros.

Other forensic sciences like DNA analysis deal with probabilities in the millions or billions. By comparison, the MD5 hash uses probabilities in the trillions of trillions of trillions. The SHA-256 would be even significantly larger.

A hash calculation is quite sensitive. Changing a single bit in the data stream, such as a file, would change the hash value. Similarly, changing the order of the data stream would also change the hash value.

The hash value is not affected by a change in file name, since the file name is not part of the file itself but resides in the filing system. Thus, if the file name was changed as a means to hide its nature, the hash value would remain unchanged.

Once a hash value is calculated, the value can be used for comparison purposes. The decisions derived from those comparisons are essentially binary. In other words, it can be used to identify similar or dissimilar files, since files with the same hash value are identical while those with dissimilar hash values are not identical with certain statistical probabilities.

Identify Encrypted Files

Encrypted files provide several problems for digital evidence. The most obvious issue occurs when the entire file is encrypted and cannot be accessed. This means that it cannot be reviewed to determine relevance. It also means that even keyword searching would not work until the file has been decrypted and its contents made available to searching.

Files having complete encryption protection are not always the most troublesome, however. The most troublesome can be files that are partially encrypted and thus partially protected. In such cases, parts of the file could be searched and examined while other parts, perhaps the parts containing the sensitive information, are not. Furthermore, the existence of these protected portions may not even be obvious. For example, a spreadsheet could have certain tabs made invisible and then access to those tabs protected so that they cannot be accessed or even known to exist. Since parts of the file were available for examination while other parts were not and since the parts not available for examination were not known to exists, this kind of encrypted file can easily pass through a review process.

What is needed is a means to detect encrypted files, including those that might only have partial encryption. A common method of detecting encrypted files is an entropy test. An entropy test measures the amount of chaos in a document. If a document has been encrypted and its contents scrambled then it will have a high chaos score.

Fully encrypted files tend to fail signature analysis where the file extension does not match the file header. Thus, when examining files identified as encrypted as a result of their entropy results, files that also fail signature analysis are likely fully encrypted and viewable at all. By contrast, files that are identified as encrypted but have matching signature and file extensions are likely only partially encrypted.

File Path Location

While the file system may know a file's location by its cluster number, such a method is not very informative from a practical point of view. For users it makes sense to describe a file's location by its file path. This information should be included with the additional file system attributes developed.

Decode Recycler Data

Everyone should be familiar with the Windows Recycle Bin. When files are deleted the default behavior is for files to be placed in the Recycle Bin and remain there until the Recycle Bin is emptied.

The Recycle Bin is the only place where the actual delete date is captured. In FAT file systems all that is known from the standard create, modified and accessed dates is the last date when the file was still "alive". Thus, any inference about the actual deleted date is that it was on or after the most recent create, modified or accessed date unless the actual delete date can be determined from Recycle Bin artifacts.

For Windows versions XP and earlier, there is a log file named INFO or INFO2 that contains the information about a deleted file such as its original location and its deletion date.

The INFO and INFO2 files are the only place where a file's actual deletion date is typically recorded. For that reason, locating and reviewing the INFO and INFO2 files have significant interest for spoliation analyses.

Since system file deletions do not travel through the Recycle Bin its contents are limited to those files having been deleted by a user. When the Recycle Bin is emptied and the computer shut down, the INFO file is also deleted. Evil doers may at this point rest comfortably in thinking that their misdeeds will go undetected. If so, what they do not realize is that like other deleted files, the INFO or INFO2 files can be recovered as long as the file has not been overwritten. The recovery procedure requires searching for the file's signature in free space as well as matching its contents to the known layout of the INFO and INFO2 file's record format.

In Windows systems Vista and later the Recycle Bin was redesigned and deleted files are documented by two files. The first is a $Rxxxxxx file that is the original file with its name changed to a 6 character alphanumeric name prefixed with the characters $R.

The second is a $Ixxxxxx file that has the same 6 alphanumeric file name as its matching $R file but the prefix is set to $I. While the $R file is the deleted file itself, the $I file is a pointer file that documents the original path location and name of the deleted along with the actual deletion date.

If a $R file's matching $I file still exists in the recycle bin then the original name of the deleted file as well as its original location can be determined. If there is not a matching $I file then the original name and location of the deleted file cannot be known.

It is possible for $I files to exist in the recycle bin without a corresponding $R file. In this case, the original name and location of a deleted file can be known even though the actual deleted file may no longer exist.

Recover File System Remnants

Examining the currently active file system may not provide a complete picture for how a storage media has been used. In fact, the contents of the currently active file system might only contain what someone has intended it to show. Thus, recovering remnants from earlier versions of the file system can provide valuable information about the names and location of files that had existed on a storage media along with their various file system attributes like date stamps that were described previously.

There are many different reasons why remnants from a prior file system can exist. On a FAT file system, for example, file system structures like folders could have been deleted and are no longer part of the active file system. Finding these deleted folders allows one to learn both that these folders had existed and what files they had contained.

If an entire storage media was reformatted an entirely new file system is created and the media will appear empty until new files are copied to it. Nonetheless, to the extent that the old file system has not been overwritten, one can search for remnants of the earlier file system and learn much about its structure as well as the contents of that structure and the various attributes like data stamps of those contents.

There are actually quite a number of situations where more sophisticated data hiding efforts can be revealed by a search and recovery of file system remnants. For example, if an earlier backup of a storage media is restored to that media in an effort to make it appear as if the media had been unchanged or make it appear that the media was in fact something entirely different.

Another situation that can be revealed by the recovery of file system remnants is the defragmentation of a hard drive. In the case of an NTFS file system, the defragmentation process optimizes the file system itself as well as all of its contents. The process of defragmentation moves the position of the file system, which can leave prior versions still recoverable from their old location in freespace.

Many file systems have distinct characteristics that can be used to locate earlier versions of their contents that might exist in freespace. The characteristics are not the same for all file systems, however.

For FAT file systems the distinctive characteristic is the folder signature of DOT followed by 31 zero characters and then a double DOT DOT. Once found, the folder structure provides the list of file contents for that folder in a 32 byte record format.

For NTFS file systems the distinctive characteristic is the FILE0 header. The NTFS file system, unlike the FAT file system, is actually comprised of a series individual files. Each file or folder within the system is represented and described by fixed length records that are actually individual files. The FILE0 header is a file signature similar to what was discussed previously in the section on file signature analysis.

While the individual nodes (folders) of the FAT file system have a specific structure, the FAT system, as a whole, is very unstructured. As a result, its remnants can exist anywhere across the storage media.

Expand Compound Files and Folders

It is important to learn as much as possible about every file on a storage media. The storage media could contain numerous compound files and folders. If so, it is important to expand these files and folders in order to learn what they contain.

Compound files are ones that may contain several documents within them. The classic examples are compressed archives like zip file and e-mail containers. In addition, there are compound system folders like the system volume information that also need to be expanded such that their contents can be subject to analysis.

Compressed Archives

Compressed archives are compound documents like zip files. To gain a complete inventory of the storage media's contents it is essential that these be opened and the contents cataloged.

A lot of forensic tools provide features that will locate these kinds of files and then open them automatically and reveal their contents as well as whatever other data is available such as any date stamps. In some cases the compound documents will be nested, which means that within the compound file is another compound file. In such cases whatever automated tool is used must have the intelligence that there are other compound files that need to be opened and cataloged and then proceed to do so. Another significant requirement is having a means to catalog and preserve the parent child relationship to these documents.

Email Containers

Email containers are another kind of compound file. In fact, e-mail containers can be some of the most complex kinds of compound files that could be encountered. The complexity comes from their structure that includes messages and attachments. The attachments can then have other compound files like compressed archives. If the compressed archives are nested that adds another level of complexity to the issue.

Similar to compressed archives discussed above, the parent child relationship of the container, to the message, to the attachment and then even any nested contents of the attachments needs to be cataloged and memorialized.

Parse System Volume Information

The subject of Volume Shadow Copy and the system volume information is discussed in more detail in the chapter on Device Systems analysis. This section explains what data from the System Volume Information and Volume Shadow Copy should be included as part of file system analysis.

The system volume folder is a protected Windows system folder containing certain system archival data. In older Windows systems it contained restore points having only the system state information. These restore points allowed rollback of the system to an earlier version of a working state in the event that some kind of hardware or software installation or a system update rendered the computer nonfunctional. Since Windows Vista, the system volume information has also included the Volume Shadow Copy (VSC).

The VSC is an improved system protection and recovery scheme. The VSC can include all kinds of files other than system state information. The archived files could even include documents like those created and used by the user. In other words, no longer were just system state files being copied and archived but even other kinds of data files like spreadsheets and word processing documents. Even e-mail containers Outlook PST files could also be copied and archived for future recovery.

While the archival and recovery feature of the Windows VSC was enabled by default in Windows Vista, it was not enabled by default in Windows 7 and 8 or 10. What this often means is that documents stored inside the user's profile will be archived in the VSC while documents stored outside the user's profile will not be archived in the VSC. Since a lot of computer users store their documents in the My Documents folder in their profile, there is a good chance that

earlier versions of a file, even deleted files, have been captured in the VSC and are available for recovery, at least for some period of time.

The amount of data captured in the VSC is limited by size constraints set by the user that determines the amount of disk space allocated to this function. As the size limitations are reached older archives to the VSC are rolled off and the new ones added. Whether these earlier versions of a document will be captured in the VSC is not always predictable. Nonetheless the VSC can be quite fruitful when deletion and data hiding techniques have been employed by a computer user to cover what they have done.

While the VSC contents are easily accessible from a functioning system, they are not so easily accessible from a forensic image or just a static hard drive. As a result, some amount of gymnastics or tools specially designed to access this data is necessary. Parsing the VSC so that its contents are included with the other file system data can provide a wealth of information, however.

For the protection of trade secret information, it is recommended that this feature always be enabled system wide and that the minimum reserved space be increased to between 10 and 20 percent of the available storage capacity. Access to the protected area should be restricted to system administrators as well.

Performing the Analysis

After the file system data has been cataloged and placed in a form suitable for analysis, the next step would be to actually perform the analysis. The following sections describe several of the analyses that can be performed to gain insights about a storage media's contetns.

Analysis of File System Date Stamp Patterns

After examining the file system for its individual contents and reviewing it for file names, other types of trend analyses can reveal interesting patterns that had gone undetected and whether data hiding techniques have been employed. Several of these analyses are discussed in the sections that follow.

Gaps in Produced Materials

It is always useful to know that the devices and data examined covers the period of interest. Examining time line distributions of file system date stamps are another way to examine the produced data for completeness.

Examining date stamps like the create date can help to verify that the storage media was actually being used to store files since the start of the time period of interest. It can also be used to determine how recently new files were added to the storage media and that it was in use recently.

Other date stamps like the last write dates can help to confirm that files were being changed and that work was being done on this piece of media during the period of interest.

Reviewers will want to examine both files and e-mail containers to do this kind of analysis. An e-mail container like a PST could have been brought forward from another machine. Thus, the e-mail would appear to cover the period while file activity will not.

With former employees at a new employer, they may be assigned a temporary machine with which to work prior to receiving their permanent machine. This type of analysis would reveal that there could be an earlier machine. It could also reveal that they have moved to a new machine if the data activity does not align to the period of interest.

Distributions of Deleted Files and Folders

A common, although unsophisticated, data hiding technique is the deletion of files. This kind of activity is common just prior to an employee's departure.

The deletion may be for benign reasons such as the deletion of personal information or it may be for more nefarious reasons such as to destroy evidence of actual intentions, departure planning, disruption of former employer operations after departure or even to destroy evidence of what was taken. As a result, file deletion activity just prior to an employee's departure can not only reveal patterns in activity but demonstrate intent as well. Such evidence of intent could be useful when moving for spoliation sanctions or for discovery and production orders.

Examination of file deletion activity is not simply an examination of all deleted files. There should be a distinction between files deleted by the system versus those deleted by actual user activity. After all, the operating system is constantly performing housekeeping functions and deleting various system files and related content on an almost daily basis. Even other software applications could be performing updates and then deleting the files used to perform the updates or the previous version of files that were updated.

An examination of file deletion activity is likely to reveal that files have been periodically deleted. The fact that deletions have occurred may not be that noteworthy. What will likely be noteworthy is the nature of the particular files that were deleted or the unusual magnitude of the deletions just prior to departure.

With a FAT file system it is not as obvious whether creation activity is overwriting previously deleted files. With an NTFS file system, however, there is a unique, sequential record number assigned to each file system record. Thus, by examining the file system record number one can tell whether the new file creations were additions to the file system or if they are located in records previously held by other files.

Distributions of Created Files and Folders

Remarkably the distribution of created files can be just as alarming as the distribution of deleted files. The act of copying on large numbers of new files file just prior to departure can mask file deletion activity in two respects.

First, when the new files are copied on they can overwrite the actual files that were deleted. Thus, the copying of new files can serve the same purpose of a file wiper and make deleted file unrecoverable without leaving the telltale signs of a file wiper such as remnants of installed software or unusual file name or date stamp artifacts.

Second, when the new files are copied on they populate the file system and will first overwrite instances of deleted files prior to adding new file system records. Thus, the act of copying on new file can not only overwrite the contents of previously deleted file but can also obscure that the deleted file ever existed.

In short, large quantities of files with identical create dates should raise flags about why the files were suddenly copied onto a device. Was this something actually necessary for some activity? Or was done to deceive?

Identification of Unusual Date Stamp Patterns

In previous sections the meaning of the various date stamps and how to interpret them was explained. What can be very interesting is when unusual date stamp patterns are found. For example, consider the case where a last accessed date stamp predates the file's create date stamp. Such an occurrence is inconsistent with date stamp behavior on Windows systems. Thus, such an occurrence could signal system clock manipulation.

Loose files in the file system are not the only place where unusual date stamps could be noticed. Another is in e-mail where a comparison of received dates predates sent dates. There could also be reply chains that contain out of sequence date stamps.

Detecting File wiping

Wiping and shredding programs are applications designed to protect private information contained in deleted computer files by overwriting the contents of those deleted files with other data thereby making the overwritten data unrecoverable. Since people have come to realize that deleting a file does not delete the data, evil doers have turned to wiping and shredding programs to truly delete data.

The legitimate purpose of these programs is to protect private data and not to perpetrate a clandestine sinister act. Consequently, wiping programs tend to leave traces of their use and existence even though they may leave no traces of the original data. These traces of their use and existence are numerous and range from entries in the registry, log files, indicators in the file system such as place holders and constant date values, as well as patterns in the characters used to overwrite the wiped and shredded data.

As a result of the signs left behind by wiping programs, detecting their use can be easily accomplished by reviewing file system information like file names and date stamps and looking for the telltale signs.

Analysis of File Security Identifiers (SIDs)

A Security Identifier, commonly known as a SID, is the identifier of a user, group or other security entity on a Windows NT level operating system like any Windows server level product or Windows XP and higher with domain network capability.

A Security ID (SID) is a number associated with a domain and a user in the domain or to an individual computer and user if that computer is not part of a domain. Computers that are part of a domain are typically business networks. Computers that are not part of a domain have SIDs that are unique to that computer only. These are typically personal or home computers.

The SID is intelligently coded and has essentially three parts. The first part of the SIDs, S-1-5-21, identifies it as a user ID of an NT level Windows installation. The next 30 characters comprised of 3 segments containing 10 numbers identifies the domain or the computer.

The last segment of a SID identifies the individual user on that domain or computer. User segments with fewer than 4 characters are built-in system users like the Administrator account, the Guest account, etc. User segments with 4 or more characters, 1000 and above, are non-system level user accounts. In other words, they correlate to actual users that have been given access credentials to the machine or network.

A SID is associated with many different computer activities and data artifacts as well as permissions. When a SID is associated with data artifacts it identifies the owner of those artifacts and what may be done with them. Similar when a SID is identified with processes it identifies the initiator of the actions while limiting those actions to those for which the initiator has permissions.

SIDs can be found in various two different file system artifacts. First they identify the owner of files and folders within a NTFS file system. Second, they identify the owner of a recycler.

Since a SID is unique to both a Domain and a user or a machine and a user, SIDs can provide some useful information about a storage device and its contents, particularly attached devices like external hard drives having an NTFS file system. First, when files are copied to the external hard drive they will have the SID of the user that copied them to the external hard drive. If the SID matches the SID of the user on a work machine then the SID provides confirmation that the files with that SID were copied to the external hard drive while it was attached to the work computer.

Second, when a list of all SIDs existing in a NTFS file system are identified one can determine the different data source from which all of the files were obtained. If there are multiple SIDs then that is evidence that the external hard drive has been attached to and files copied to it from many different machines.

Third, every time an external hard drive is attached to a different Windows based computer, a new recycle bin will be created on the external hard drive and it will be given assigned the SID for the Domain and UserID or computer and UserID of the person logged into the machine to which the external drive was attached. Thus, even if there have not been any

files copied to the external hard drive from the attached computer, the recycle bin will memorialize that the external hard drive has been attached to a different machine. In addition, the recycle bin will be assigned create dates when it was first attached and modified dates for the last time it was used.

A common question about removable devices like external hard drives is whether they have been attached to any other machines after they were used by a departed employee to misappropriate sensitive information. This question can be answered by examining the SIDs of the attached device.

Unfortunately, this analysis is usually only reliable with external hard drives. This kind of analysis is not reliable for flash drives which typically use FAT file systems and are known not to reliably create recycle bins. Thus, a flash drive without this kind of information is does not provide confirmation that it has not been attached to other devices.

Confirm Signatures to File Extensions

Earlier in file system analysis when determining other content attributes, file signatures were determined. These should now be compared against the file extensions and instances where the signature does not match the extension should be reviewed.

It is a common data hiding technique to change a file's extension as a means to hide its significance. Someone taking a trade secret may well want to disguise its existence by changing its signature to something more benign. In the process they may also change the file name and its location in an effort to hide it even better.

Many of the forensic tools provide this comparison at the time they calculate they file signatures. They then flag any files whose signatures and file extensions don't match.

If a file has been deleted and overwritten, it is certainly possible that its signature will not match its extension. After all, something else entirely is occupying that location now.

Summary

Electronic storage media can be analogized to a library. The library has the card catalog that tells visitors what books are in the library as well as certain attributes about those books like name, publisher, publishing date, pages, subject area and where the books are located on the shelves. The file system provides similar functionality for a storage media. It tells users what files are on the media, the general nature of the file based on extension, the location of those files and certain attributes such as certain date stamps. In addition, to the active (non-deleted) files on the media, the file system may also contain references to previously deleted files.

File system analysis is a good first step in learning what treasures exist on a particular media. Thus, this step should apply to all digital storage devices like desktops and laptops, cellphones, tablets, flash drives, external hard drives, etc. As the first cut at data analysis it is a

fairly straight forward process that simply catalogs the contents of a file system in order to learn what the storage device or media actually contains and prepare for subsequent analysis.

Setting aside the actual analysis of the data, if there is a complexity to file system analysis it is that there are many different types of filing systems. The Hierarchical File System (HFS) used by Apple computers is different from File Allocation Table (FAT) and the New Technology Filing System (NTFS) used on Microsoft systems. Similarly, the EXT2 and EXT3 filing systems used by the Linux operating system and found on many Network Attached Storage (NAS) devices is different from both Microsoft and Apple systems. As a result, just being able to read the filing system requires the use of tools that know how to interpret a device's filing system.

After the inventory is taken, so to speak, there are numerous elementary analyses that can be performed that both help authenticate the evidence as well as identify the potentially relevant evidence.

CHAPTER 4

Device System Analysis – Looking Under the Hood

- Introduction
  - Windows Systems
    - Recycle Bin
    - Registry Analysis
      - System Registry Hive
        - Computer Name
        - Clear Page File at Shutdown
        - Last Successful Shut Down
        - Time Zone Information
        - Product Type
        - Network Interface Cards
        - Last Access Date Stamp Sensitivity
        - USB Storage Devices
        - Portable Device Enumerator Service
        - Mounted Devices
        - Device Classes
        - IDE [Integrated Device Electronics]
      - Software Registry Hive
        - Current version
        - Profile List
        - Portable Devices
        - Volume Info Cache
        - Last Logon
      - Security Registry Hive
        - Local Machine Security Identifier (SID)
      - Security Accounts Manager (SAM)
      - NTUser Hive
        - Most Recently Used (MRU) Lists
        - User Assist Key
        - Mount Points
      - UsrClass Hive
        - Shellbags
    - Event Logs
      - System event log
      - Application Event log
      - Security Event log
    - Prefetch Files
    - Link files and Jump Lists
    - Shadow Copy

Introduction

Device system analysis focuses on the programs that control its hardware and software. The device could be virtually any kind of computing device that actually functions. Thus, it is more than a storage device. It does simply stores data like external hard drives or flash drives but is the device that performs the functions. Thus, it would contain some kind of central processing unit (CPU). I

The device system is commonly referred to as the Operating System (O/S). Thus, device system analysis is actually an examination of the O/S and its operations, configurations and changes there to. Device system analysis examines artifacts in the O/S that reveals its settings and changes thereto. In the process, device system analysis reveals things about device configurations for hardware and software and how those configurations have been changed.

The manner in which device systems analysis is performed can vary according to the type of device it is. Essentially, a Windows system is different from an Apple system which is different from a Linux system or a cellphone.

Windows Systems

Windows systems are managed by the Windows O/S as its name indicates. The exact behavior of the O/S can differ from the various O/S systems. Windows 98 is different from XP is different from Windows 7 is different from Windows 10, although there are some similarities between them too.

When examining a Windows system there are some fairly standard places where valuable information can be found. Those places are the Recycle Bin, the Registry, Event logs, Prefetch files, and System Volume Information. All of those are discussed in the sections that follow.

Recycle Bin

The Recycle Bin has been around for quite a while. It has undergone several changes over the years. The primary difference occurred when security features were added to the file system. Prior to that with versions like Windows 98 that used the FAT file system it was known as Recycled. With the adoption of the NTFS file system and its improved security features it became known as Recycler in Windows 2000, XP and NT and $Recycle.bin with Windows Vista and later.

The Recycle Bin is the place where deleted files go to first after they are deleted, unless the shift key is pressed simultaneously with the delete key. In that case, deleted files bypass the recycle bin altogether.

Deleted files in the recycle bin can be recovered. It is only after the recycle bin is cleared or the file is so called “double deleted” that it is truly deleted.

When files are deleted and placed in the recycle bin their names are changed. In the earlier recycle bine versions, the name was changed to something intelligently coded that was comprised of the characters “D”, the drive letter of the drive from which it was deleted and then a sequential identifier followed by the file’s actual file extension. As an example, a deleted text file could be renamed to something like DC38.txt if it was deleted from the “C” drive and was the 38th file deleted. In the later versions, Windows Vista and later, the original file is renamed with a prefix of $R followed by 6 seemingly random characters.

In addition to the renamed deleted files, Windows memorializes the original name of the deleted file, its size, storage location, and the deletion date. Interestingly, this is the only place where Windows actually records a deleted file’s deletion date and time, although depending on the particular version of Windows and the file system being used the deletion date can be approximated with varying degrees of precision.

The way in which Windows memorializes the deleted file information like the original file name and deletion date changed over time with the various versions of Windows. Prior to Windows Vista it was captured in a file named the “INFO2” file as a text string. Each row of the file was a separate deleted file record. The file would continue to collect records until the Recycle bin was emptied and the machine rebooted. Under those circumstances the INFO2 file would be deleted and restarted a new with the next system boot.

Although the INFO2 was deleted, it could be recovered, like any deleted files, and the record of prior file deletions learned. With the older versions of Windows it was common practice to search freespace and recover the deleted INFO2 files in order to learn the deleted file history.

Since Windows Vista, a different method of memorializing the deleted file name, its recovery path and deletion date was devised. This information was moved from a single file like the INFO2 file and put into individual $I files. Thus, each $R file had a matching $I file whose name contained the same 6 character string as the $R. Both files, the $R and $I files, retain the extension of the original deleted file.

In addition to information about any deleted files, the Recycle bin provides another useful bit information. First, it can confirm that a device has been inserted into a Windows device,

since a recycler will be created if it does not already exist. Every windows storage device will have a recycle bin except for flash drives.

Second the type of windows device can be determined since there is a difference for Recyclers and Recycle Bin. Of course, recognizing this difference is becoming less and less important, since the likelihood of encountering a machine that old still in use is remote.

Registry Analysis

The Windows Registry is a collection of hierarchical database files, otherwise known as hives, that contain information used by Windows to manage the complete system. This management information spans the gamut from hardware interfaces and communications from anything like mice and keyboards to Network Interface Cards (NIC) and data storage devices like hard drives.

As indicated above, the Registry is a collection of database files at both the system and individual user levels. The system level files include hives like the system, software, security and Security Accounts Manager (SAM) just to mention four. There are other system wide registry hives as well but the ones listed above are the most significant registry hives.

As to the user level registry hives, there are principally two. One is the NTUser.DAT and the other is the UsrClass.DAT These user level hives contain user specific information like application preferences and recently used files just to mention a couple of things.

There are a lot of different ways that the Registry hives can be accessed and their data reviewed. Windows itself provides some crude functionality for examining and editing them. Most of the forensic software suites like EnCase, FTK and X-Ways provide a means to review their data in a more friendly manner than Windows provides. In addition, there are also some third party tools that provide the information and present it in both a more intuitive and more friendly manner. Most of the example provided below were obtained using Harlan Carvey's RegRipper tool.

The following sections discuss each of these registry hives and identify the more useful things to consider.

System Registry Hive

The System Hive contains system information and settings about installed hardware and useful date stamps like their install dates and date of last usage. The full notation of the system hive is written as HKEY_LOCAL_MACHINE\SYSTEM\. The individual keys or the paths to the keys and their values then follow the basic root information.

Computer Name

The System name is in the ComputerName key. This is the name given to the particular device and the name by which it would appear on the network.

```
ComputerName    = MY-PC
TCP/IP Hostname = MY-PC
```

Clear Page File at Shutdown

ClearPageFileAtShutdown key maybe set to False but if it is set to True then page file is cleared which could help protect the system since lots of data can be carved from the page file

```
PagingFiles = ?:\pagefile.sys
ClearPageFileAtShutdown = 0
PagingFiles = ?:\pagefile.sys
```

Last Successful Shut Down

The when the system was last successfully shutdown is contained in the Shutdown subkey within the Windows key in the Control Set 1/enum branch of the system hive.

```
ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
LastWrite Time Thu Dec  4 20:24:52 2017 (UTC)
  ShutdownTime = Thu Dec  4 20:24:52 2017 (UTC)
```

Time Zone Information

The Time Zone Information key reveals the time zone to which the system was set. This information is used to know how convert date information, like file system dates, for display.

```
ControlSet001\Control\TimeZoneInformation
LastWrite Time Mon Nov  3 13:33:14 2014 (UTC)
  DaylightName   -> @tzres.dll,-111
  StandardName   -> @tzres.dll,-112
  Bias          -> 300 (5 hours)
  ActiveTimeBias -> 300 (5 hours)
  TimeZoneKeyName-> Eastern Standard Time
```

Product Type

Product Type key reveals the type of system being used.

```
ControlSet001\Control\ProductOptions
LastWrite = Thu May 30 12:50:31 2013

Ref: http://support.microsoft.com/kb/152078
     http://support.microsoft.com/kb/181412

ProductType  = WinNT
Ref: http://technet.microsoft.com/en-us/library/cc782360%28WS.10%29.aspx
WinNT indicates a workstation.
ServerNT indicates a standalone server.
LanmanNT indicates a domain controller (pri/backup).

ProductSuite = Terminal Server
Ref: http://technet.microsoft.com/en-us/library/cc784364%28WS.10%29.aspx
```

Network Interface Cards

The NIC (Network Interface Card) key contains information about the various network adapters and their settings being used by the system.

```
Network key
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}

ControlSet001\Services\Tcpip\Parameters\Interfaces
LastWrite time Thu Jun 19 12:37:35 2014 (UTC)

Interface {40C8A8AD-0AB6-4998-9F0A-82AF6327628F}
Name: Local Area Connection
Control\Network key LastWrite time Tue Oct  9 15:26:27 2012 (UTC)
Services\Tcpip key LastWrite time Wed Jun 18 18:48:25 2014 (UTC)
        IPAddress      = 192.168.1.89
        SubnetMask     = 255.255.255.0
        DefaultGateway = 11.1.1.1
```

Last Access Date Stamp Sensitivity

The file system last access date stamp has been made less sensitive since Windows Vista. Considerable forensic value was lost when the sensitivity of this date stamp was disabled. It was disabled then to improve the performance of the Vista system. Since Windows 7 the performance issues have been solved such that the reduction in performance of having the last access date enabled is not that severe.

Interestingly the sensitivity of the last access date is controlled through a registry setting. In all Windows systems since Vista the sensitivity of the last access date has been disabled by default. Users can enable the last access date sensitivity by setting this registry key value to "0".

Since the last access date can provide useful information and the performance issues have been resolve it is a good idea for users to enable this feature.

```
NtfsDisableLastAccessUpdate
ControlSet001\Control\FileSystem
NtfsDisableLastAccessUpdate = 1
```

USB Storage Devices

The USBStor key contains information about USB storage devices. This key contains considerable information about USB Storage devices such as the Manufacturer, model, and serial number just to mention a few. USBStor key lists all of the USB Storage devices like flash drives and external hard drives. Other USB devices like mice and keyboards are in the USB key

```
USBStor
ControlSet001\Enum\USBStor

Disk&Ven_&Prod_USB_Flash_Memory&Rev_PMAP [Sat Nov  1 22:08:02 2014]
  S/N: 6C626DBED999ED91D000992F&0 [Thu Dec  4 14:21:21 2014]
  Device Parameters LastWrite: [Sat Nov  1 22:08:02 2014]
  LogConf LastWrite         : [Sat Nov  1 22:08:02 2014]
  Properties LastWrite      : [Sat Nov  1 22:08:02 2014]
    FriendlyName    : USB Flash Memory USB Device
    InstallDate     : Tue Apr  1 12:33:53 2014 UTC
    FirstInstallDate: Tue Apr  1 12:33:53 2014 UTC
```

Portable Device Enumerator Service

WpdBusEnum subkey provides additional information about USB devices that is not contained in the USBStor key. The additional information includes the drive letter or volume name.

```
wpdbusenum v.20141111
(System) Get WpdBusEnumRoot subkey info

DISK&VEN_&PROD_USB_FLASH_MEMORY&REV_PMAP (6C626DBED999ED91D000992F&0)
  LastWrite: Thu Dec  4 14:21:34 2017
  DeviceDesc: USB Flash Memory
  Friendly: MY-TD-2
  Mfg:
  Device Parameters LastWrite: [Thu Dec  4 15:01:21 2017]
  LogConf LastWrite         : [Sat Nov  1 22:08:02 2017]
  Properties LastWrite      : [Sat Nov  1 22:08:02 2017]
  InstallDate     : Tue Apr  1 12:33:58 2014 UTC
  FirstInstallDate: Tue Apr  1 12:33:58 2014 UTC
```

Mounted Devices

The MountedDevices key contains information about all the various storage devices that have been attached. The information contained about each device is less detailed than what one might find in other keys specifically related to the type of device such as the USBSTOR key.

```
MountedDevices
LastWrite time = Wed Nov 12 18:29:57 2017Z

\??\Volume{35c31198-122e-11e2-8a1d-806e6f6e6963}
  Drive Signature =  05 6a 6c 2d
\??\Volume{35c31199-122e-11e2-8a1d-806e6f6e6963}
  Drive Signature =  05 6a 6c 2d
\DosDevices\C:
  Drive Signature =  05 6a 6c 2d
#{f8f72da7-1223-11e2-800d-7845c41a4228}
  Drive Signature =  05 6a 6c 2d

Device:
_??_USBSTOR#Disk&Ven_Generic&Prod_STORAGE_DEVICE&Rev_9451#000000009451&0#{53f563
07-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{78536807-098f-11e3-b1be-7845c41a4228}

Device:
_??_USBSTOR#Disk&Ven_Verbatim&Prod_STORE_N_GO&Rev_5.00#07000795130796040033&0#{5
3f56307-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{4bc30405-45ef-11e2-8cc7-7845c41a4228}
  \DosDevices\N:

Device: _??_USBSTOR#Disk&Ven_Generic-&Prod_MS#MS-
Pro&Rev_1.00#20021111153705700&3#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{da3a5278-396a-11e2-be85-806e6f6e6963}
  \DosDevices\J:

Volume                                          Disk Sig    Offset
-------                                         --------    --------
#{f8f72da7-1223-11e2-800d-7845c41a4228}         05 6a 6c 2d 0
\??\Volume{3326b8f6-b5ad-11e3-b1e8-7845c41a4228} 44 fd fe 06 0
\??\Volume{35c31198-122e-11e2-8a1d-806e6f6e6963} 05 6a 6c 2d 0
\??\Volume{35c31199-122e-11e2-8a1d-806e6f6e6963} 05 6a 6c 2d 0
```

Device Classes

Device Classes is another way that Windows tracks hardware devices. The DeviceClasses key contains information about a storage device like a flash drive and a date stamp, which could be the last time the storage device was attached to the system. This is just another key whose information about USB device should be collected and evaluated.

```
DevClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Device   : VID_04A9&PID_3227
LastWrite: Fri Nov 30 14:52:00 2012 UTC

Device   : VID_05AC&PID_1297
LastWrite: Mon Jan  7 20:53:56 2013 UTC

Device   : VID_1004&PID_61F1&MI_03
LastWrite: Wed Jul 30 17:21:38 2014 UTC

DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Thu Dec  4 20:02:32 2014 (UTC)
  Disk&Ven_Seagate&Prod_Backup+_Desk&Rev_050B,NA5KPDK6&0
Thu Dec  4 20:02:31 2014 (UTC)
  Disk&Ven_Generic-&Prod_Compact_Flash&Rev_1.00,20021111153705700&0
  Disk&Ven_Generic-&Prod_MS,MS-Pro&Rev_1.00
  Disk&Ven_Generic-&Prod_SD,MMC&Rev_1.00
  Disk&Ven_Generic-&Prod_SM,xD-Picture&Rev_1.00
Thu Dec  4 14:21:34 2014 (UTC)
  Disk&Ven_Verbatim&Prod_STORE_N_GO&Rev_5.00,07000795130796040033&0
```

IDE [Integrated Device Electronics]

Integrated Device Electronics is another category of devices tracked by windows. The IDE key, which is located at ControlSet001\Enum\IDE, lists the various IDE kinds of storage devices. Frequently, system's internal hard drive is memorialized in the IDE key. Thus, it is a useful place to look in order to learn how many hard drives have been used as well as any that might have influenced the system's internal hard drive such as the original device should the particular Windows installation have come from some kind of deployment image.

```
IDE
ControlSet001\Enum\IDE
LastWrite Time Sat Nov  1 22:08:02 2014 (UTC)

CdRomTSSTcorp_DVD+-RW_SH-216BB_____D100____ [Sat Nov  1 22:08:02 2014]
5&1d34d422&0&1.0.0 [Thu Dec  4 20:02:20 2014 (UTC)]
FriendlyName : TSSTcorp DVD+-RW SH-216BB ATA Device


DiskSAMSUNG_SP1614C_____SW100-34 [Sat Nov  1 22:08:02 2014]
5&2fd5bc68&0&0.0.0 [Thu Dec  4 20:02:20 2014 (UTC)]
FriendlyName : SAMSUNG SP1614C ATA Device


DiskST250DM000-1BD141_____KC45____ [Sat Nov  1 22:08:02 2014]
5&2fee84c7&0&0.0.0 [Thu Dec  4 20:02:20 2014 (UTC)]
FriendlyName : ST250DM000-1BD141 ATA Device
```

Software Registry Hive

The Software hive contains information about installed software and software interactions.

Current version

The current version key identifies the installed version of the Windows operating system as well as the date of the installation.

```
Microsoft\Windows NT\CurrentVersion
LastWrite Time Thu Oct 16 14:17:46 2014 (UTC)

  CurrentVersion : 6.1
  CurrentBuild : 7601
  RegisteredOwner : ACME, Inc.
  CurrentBuildNumber : 7601
  CSDBuildNumber : 1130
  CurrentBuildDW  : 21431
  SoftwareType : System
  InstallationType : Client
  CurrentBuildId  : 3460570
  RegisteredOrganization : Microsoft
  SystemRoot : C:\Windows
  PathName : C:\Windows
  SystemType  : 3133370657
  EditionID : Professional
  CSDVersion : Service Pack 1
  CurrentType : Multiprocessor Free
  ProductName : Windows 7 Professional
  ProductId : 00472-OEM-8882534-00524
  BuildLab : 7601.win7sp1_gdr.140706-1506
  InstallDate : Mon Oct 29 18:52:43 2012 (UTC)
```

Profile List

The profile list contains a list of user accounts on the particular device. It is not a list of user accounts across the network but only those local to the machine. It can provide a useful cross check against which user accounts actually appear in the file system

```
Microsoft\Windows NT\CurrentVersion\ProfileList
LastWrite Time Mon Oct 29 18:52:44 2012 (UTC)

Path     : %systemroot%\system32\config\systemprofile
SID      : S-1-5-18
LastWrite : Tue Jul 14 04:53:25 2009 (UTC)

Path     : C:\Windows\ServiceProfiles\LocalService
SID      : S-1-5-19
LastWrite : Thu Feb 10 16:26:22 2011 (UTC)

Path     : C:\Windows\ServiceProfiles\NetworkService
SID      : S-1-5-20
LastWrite : Thu Feb 10 16:26:22 2011 (UTC)

Path     : C:\Users\MY-PC
SID      : S-1-5-21-4188851126-227768422-451217940-1000
LastWrite : Thu Dec  4 19:33:52 2014 (UTC)
LoadTime  : Thu Jan  1 00:00:00 1970 (UTC)
```

Portable Devices

The software registry hive also tracks portable devices. Thus, it provides another place to look to gather useful usage data about portable devices, including storage devices like flash drives. Less portable devices like external hard drives do not appear in this key, however.

```
Microsoft\Windows Portable Devices\Devices
LastWrite Time Wed Oct 22 15:52:15 2014 (UTC)

Device    : DISK&VEN_&PROD_USB_FLASH_MEMORY&REV_PMAP
LastWrite : Tue Apr  1 12:33:58 2014 (UTC)
SN        : 6C626DBED999ED91D000992F&0
Drive     : MY-TD-2

Device    : DISK&VEN_CAMERA&PROD_PEN_DISK&REV_
LastWrite : Thu Jun 12 21:25:19 2014 (UTC)
SN        : USB_DEVICE&0
Drive     : K:\

Device    : DISK&VEN_CASIO&PROD_QV_DIGITAL&REV_
LastWrite : Wed Oct 22 15:52:15 2014 (UTC)
SN        : 0000000000000000&0
Drive     : K:\
```

Volume Info Cache

The Volume Info Cache lists the volume names for the various attached fixed disk storage devices. While it can include attached storage devices like external hard drives it does not include attached storage devices like flash drives.

```
Microsoft\Windows Search\VolumeInfoCache

C: - LastWrite: Tue Oct  9 14:40:26 2012
DriveType: Fixed
VolumeLabel: OS

F: - LastWrite: Wed Nov 28 14:51:29 2012
DriveType: Fixed
VolumeLabel: Main Files

K: - LastWrite: Mon Oct 28 19:45:01 2013
DriveType: Fixed
VolumeLabel: MY Backup Drive

M: - LastWrite: Thu Mar 27 12:58:18 2014
DriveType: Fixed
VolumeLabel: My Passport

R: - LastWrite: Tue Oct  9 15:25:57 2012
DriveType: Fixed
VolumeLabel: RECOVERY
```

Last Logon

The last logon key captures the date and time of the last successful logon to the system. It does not identify the user of the last logon, however.

```
Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Thu Dec  4 20:24:38 2017 (UTC)
```

Security Registry Hive

The Security hive is another of the registry hives containing system wide information. It is not as robust as either the system or software registry hives which contain considerable diverse information. By contrast the security hive is much more narrowly focused. As a result, its contents are not as voluminous.

Local Machine Security Identifier (SID)

On NT class machines, there is a fairly unique security identifier (SID) assigned to the Domain or the individual machine. These identifiers can be used in numerous situations to specifically identify the device. For example, when an external hard drive is attached to the device, a Recycle Bin will be created for the user, as described above, if one does not already exist. The user's Recycle Bin account on the external hard drive will contain the SID of the machine or domain to which it was attached. Thus, if examining an external hard drive, for example, one way to determine whether it has been attached to other machines is to check the Recycle Bin accounts on that external hard drive.

```
Policy\PolAcDmS
LastWrite Time Tue Oct  9 16:27:34 2012 (UTC)
Machine SID: S-1-5-21-4188851126-227768422-451217940
```

Security Accounts Manager (SAM)

The Security Accounts Manager (SAM) contains security information about the local and group user accounts on the device. Each user is identified with a number. Values of less than 1,000 are system level accounts while those of 1,000 or higher are individual accounts.

```
Username       : Administrator [500]
Full Name      :
User Comment   : Built-in account for administering the computer/domain
Account Type   : Default Admin User
Account Created : Mon Oct 29 18:52:10 2012 Z
Name           :
Last Login Date : Tue Oct  9 15:16:23 2012 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 Z
Pwd Fail Date   : Wed Mar 27 17:16:24 2013 Z
Login Count     : 11
  --> Password does not expire
  --> Account Disabled
  --> Normal user account


Username    : MY-PC [1000]
Full Name      : Claude Reins
User Comment   :
Account Type   : Default Admin User
Account Created : Mon Oct 29 18:52:32 2012 Z
Name           :
Password Hint   : Invisible Man
Last Login Date : Thu Dec  4 18:19:29 2014 Z
Pwd Reset Date  : Wed Nov 28 14:55:14 2012 Z
Pwd Fail Date   : Tue Oct 28 12:29:50 2014 Z
Login Count     : 947
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

NTUser Hive

The NTUser hive is one of the user specific registry hives. As a result, there is a version of the NTUser hive in each user profile on the local device.

Since it is a user specific registry hive the kinds of information that it contains is relevant to a particular user such as their system or application preferences as well as recent system or application activity.

Most Recently Used (MRU) Lists

Windows tracks a user's most recent activity as a means to facilitate a user's return to their last work. That information is stored in the NTUser hive by application. Thus, each application will appear in the NTUser hive along with a list of the user's last files accessed.

The extent of the past activity can be substantial like the last 50 or 100 files accessed. This can be useful information to confirm that a user has actually accessed a particular file. Unfortunately, the only date stamp for the activity is with the most recent access. Thus the other accesses may be known to have occurred the exact date and time is for the other accesses is unknown.

(Illustrating only PDF documents accessed. Each application would have similar lists)

Most recent PDF opened: Thu Dec 4 15:57:47 2014 (UTC)
Key name,file name,sDate,uFileSize,uPageCount
c1,/F/...Acme_Inc/...Acme_ISO/Company Standard/A - Management/A0100 - Policy Control/A0104 - Company Organization/Acme_Organichart_2014.pdf ,20141204105747-05'00' ,806314,1
c2,/F/...Acme_Inc/...Acme_ISO/Company Standard/A - Management/A0100 - Policy Control/A0104 - Company Organization/A0104 - Old_documents/A0104 - Company Organization.pdf ,20141203092250-05'00' ,81653,3
c3,/F/...Acme_Inc/...Acme_ISO/Company Standard/A - Management/A0100 - Policy Control/A0104 - Company Organization/A0104 - Old_documents/A0104(01) - Acme Organichart-old_c.pdf ,20141203091220-05'00' ,12925,1
c4,/F/...Acme_Inc/...Acme_ISO/Company Standard/A - Management/A0100 - Policy Control/A0104 - Company Organization/A0104 - Old_documents/A0104(01) - Acme Organichart-old_b.pdf ,20141203091212-05'00' ,10259,1
c5,/F/...Acme_Inc/...Acme_ISO/Company Standard/A - Management/A0100 - Policy Control/A0104 - Company Organization/A0104(01) - Company Organization-a.pdf ,20141203090222-05'00' ,99225,1

User Assist Key

The User Assist Key provides information about software usage and its last access date. This is a useful key to review to understand application usage and whether any applications of interest were run, such as changing the system clock or data cleaners.

```
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Mon Oct 29 18:55:46 2012 (UTC)

  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\PrivacyEraser Computing\Free Internet
Eraser\InternetEraser.exe (1)
Thu Dec  4 16:52:09 2017 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Pardon 3\Pardon.exe (1)
Thu Dec  4 14:45:26 2017 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office 15\Root\Office15\EXCEL.EXE (1)
Thu Dec  4 14:44:52 2017 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office 15\Root\Office15\WINWORD.EXE (5)
Thu Dec  4 13:36:03 2017 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office12\OUTLOOK.EXE (1)
```

Mount Points

The Mount Points key is another place where storage device information can be found. The storage devices can be local or they can be remote, such as a network storage device.

Since the information is in a user specific registry key, this set of data is able to link a particular user with their last access date of a storage device.

```
     MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Wed Oct 22 15:52:32 2014 (UTC)

Remote Drives:
Fri Nov  8 18:27:25 2013 (UTC)
  ##11.1.1.98#qa
  ##11.1.1.98#QC Lab
  ##11.1.1.98#QC Lab Test
Wed Dec 12 13:44:06 2012 (UTC)
  ##Acmeserver1#files
Tue Dec 11 18:43:18 2012 (UTC)
  ##11.1.1.15#Acme_usa
Thu Nov 29 19:06:14 2012 (UTC)
  ##Acmeserver#Acme_usa
Mon Oct 29 19:30:02 2012 (UTC)
  ##11.1.1.16#Acme_usa
Mon Oct 29 19:28:20 2012 (UTC)
  ##11.1.1.15#files

Volumes:
Thu Dec  4 17:06:20 2014 (UTC)
  {33b6b7ef-445d-11e2-bfc9-7845c41a4228}
Thu Dec  4 17:06:16 2014 (UTC)
  {4bc30405-45ef-11e2-8cc7-7845c41a4228}
Thu Dec  4 15:01:18 2014 (UTC)
  {431d0f22-b998-11e3-b1f5-7845c41a4228}
Thu Nov 20 13:38:00 2014 (UTC)
  {35c3119c-122e-11e2-8a1d-806e6f6e6963}
Wed Oct 22 15:52:32 2014 (UTC)
  {d1f1e4b8-5930-11e4-b5c2-7845c41a4228}
```

UsrClass Hive

The last of the individual registry hives is the UsrClass hive. The UsrClass hive contains a lot of other user specific data essential to Windows Explorer operation such as the association of file extensions to certain file types so that when a user ciicks on a file displayed in Windows Explorer that the desired application is opened and the file viewed. There are other similar types of Windows Explorer data, however.

Shellbags

One of the more significant features contained in the UsrClass registry hive is the information related to Windows Shellbags. Shellbags store display information along with certain file system data such as date stamps about folders previously traversed through Windows Explorer. With this information Windows knows how to more quickly display the folder data when browsing a folder in Windows Explorer, since it is not necessary for the system to perform a complete read of the various attributes prior to display.

The information stored not only applies to folders on the local storage device but folder information on any storage device ever browsed by the user through Windows explorer. This would include flash drives, external hard drives and even network drives.

While there is no file information contained in the Shellbags data, there is folder information. Thus, this can be useful when trying to understand what data might reside on some device that is not available for examination.

Also the data in the Shellbags is persistent and remain even after the folder was deleted from the storage device. Thus, a reconciliation of the Shellbags data against the actual device, if it is available for examination can be very useful in spoliation analyses.

Event Logs

Event logs memorialize certain system activity. Their contents do not recognize all activities but only certain kinds of activities that are considered useful in the analysis of device activity and resolving problem issues. There are thousands of different kinds of events, though.

There are a number of different kinds of event logs. The most prominent ones are the system, application and security logs. Each of these logs capture a number of different attributes such as:

- a record number;
- the date and time;
- the kind of event being captured such as error, information, etc.;
- the user triggering the event, which can include the system or an application;
- an event ID number which can be used to learn the nature of the event;
- the source;
- category; and
- machine name.

The event IDs are not always consistent across all versions of Windows. Thus, when reviewing log events the particular version of the Windows that was running at the time is essential in getting the correct description of what the event ID indicates.

The log history is not historically complete. Rather, it typically spans only a period of the device history. The period that is covered depends on the amount of space allocated for storing the various event log data. The amount of data reserved for storing history is predetermined for each log. Once the allocated space is consumed older records are rolled off in order to make room for newer entries. This limitation, therefore, is one of the reasons that timely preservation can be important particularly when there are questions about device functionality prior to triggering a duty to preserve.

Analysis of the event logs is one thing that would be useful in the assessment of whether a device was functioning properly. There are several different kinds of analysis of the event logs that could reveal whether the device was manipulated to disguise that certain things had been done and whether it is even a counterfeit.

System event log

As its name implies, the system event log captures data about different system related events. These would be somewhat general and could include things like network connections, system services starting and stopping, application updates, and other components. For example, the failure of a driver or other system component to load during startup is recorded in the system log.

Application Event log

The Application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. Program developers decide which events to log.

Security Event log

The Security log contains events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files or other objects. Administrators can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

Prefetch Files

Prefetch files are created during the process of “prefetching”. The process of prefetching was developed as a means to speed Windows performance during bootup and for the start-up of various software applications. The idea is that certain data for those processes is stored for re-use, which then speeds the initiation of the process.

From an evidentiary perspective, the usefulness of prefetch files is to confirm that certain programs have been run, identify on what dates they were run and how many times they have been run.

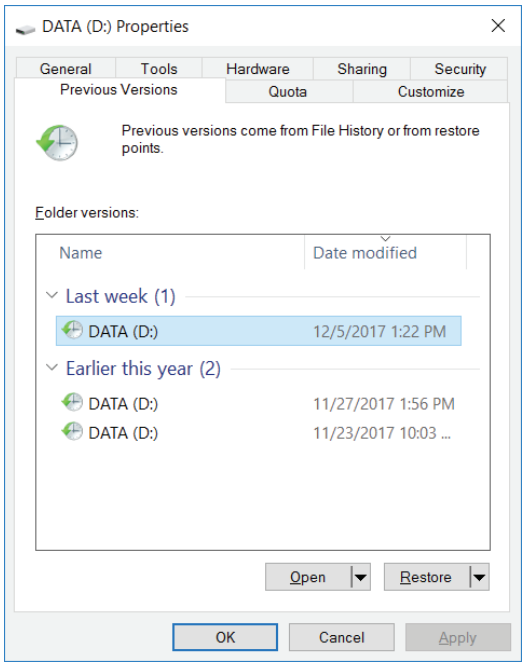
Link files and Jump Lists

Link files and jump list information is created whenever a file is opened and viewed after clicking on the file in Windows Explorer. While these are an artifact created by the Windows Operating System, they are valuable artifacts for the analysis of actual file usage and activity. As a result, they are discussed in more detail in the section on file activity analysis.

Shadow Copy

The Shadow Copy is a feature added to the Windows Operating System in Windows Vista. It essentially provides an archival feature that permits users to recover prior versions of files or even deleted versions of files. It also is the current repository of restore point data that permits recovery of a system to a previously functioning condition.

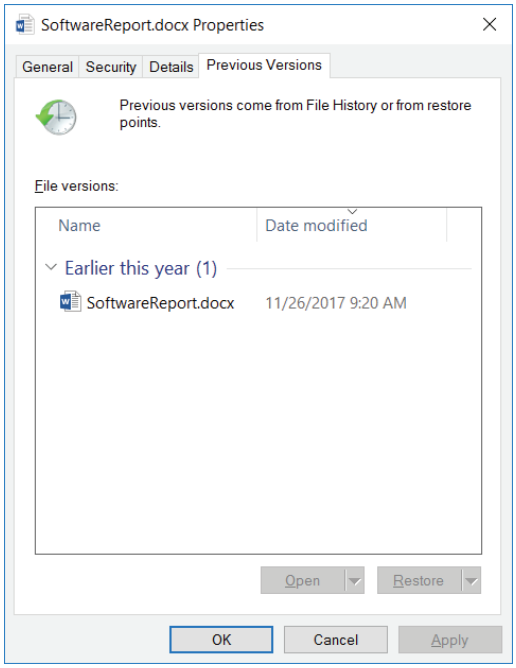
For users, the Shadow copy data is available from two different directions. One is globally from the storage media itself. In that case, all versions of the available Shadow copy archives are displayed and available for selection.



The available prior versions are available by highlighting the storage media, right clicking and then selecting the properties option. The properties option displays the above dialog box

which contains a tab for previous versions. This is the way that a user would go to recover deleted files.

If there is an active file and a previous version is desired, the user can right click on the existing instance of the document within Windows Explorer and once again pick options. When the document properties dialog box is displayed, the user can select the Previous Versions tab to see what prior versions exist and recover them.



Not all file versions are retained and they are not retained indefinitely. The amount of information retained by Shadow copy is constrained by its size. By default it has a size equal to 4 to 10 percent of the volume size. As the size fills, some Shadow Copy data will be purged to make room for new data. The data is at least highly compressed. As a result, the amount of data that will be retained may not be easily calculated based on actual file sizes.

Shadow copy was enable by default on Windows Vista systems. It is not enabled by default on Windows 7 and later system. Rather, it has to be enabled, at least for the functionality related to the deleted or previous versions of files.

Shadow copy is one of the features discussed in the chapter on File System analysis as a means to better understand what data is available on the storage media.

Validating the Evidence

As indicated in several of the preceding sections, the benefit to examining device system information is to review and evaluate device functionality, including whether the device is functioning properly. This can be done through a variety of examinations that are described below.

Actual Device for Period of Interest

When examining a hard drive it is always good to know that it actually covers the period of interest. There simply are a lot of things that could have happened to a hard drive from a machine of interest. Some of them are quite innocent while others indicate that something more nefarious is at hand.

There simply are a number of different things that could have happened to the drive that needs to be included in the calculus for the drive examination. For example, the hard drive could have been upgraded. If the upgrade happened between the examination and the period of interest, then whatever analysis is being done could be fruitless. If it has been upgraded, then the very evidence being sought could be on the prior drive that needs to be located and examined.

If the hard drive has not been upgraded but yet the current hard drive being examined is new and not the original, then clearly something else is going on. This could be the first indication that the entire contents of the drive should be questioned for authenticity. More specifically, the question that would arise is this a drive that was even used, albeit for short period of time, or is this drive a complete counterfeit?

Validating the period covered by examining the data it contains. If the file system analysis contains date stamps across the period of interest then the period of interest would seem to be covered.

There is always the possibility that the file system information is a false positive for the various reasons described above. If a hard drive is a bootable device then there is more that can be done to test its authenticity than just checking the file system data.

In order to validate a bootable hard drive one looks in three places. The first is the System hive of the Windows registry. The specific keys would be the IDE and SCSI keys. These keys will list the various hard drives that have been installed internally and captured in the System registry hive. Hard drives that had been attached externally like by way of a USB connection would appear in the USB key and are discussed later.

If the installation of the system on this computer was accomplished by way of a deployment image[6], then the registry hive could list both the current drive as well as the drive

[6] A deployment image is essentially a standard baseline configuration for the computers in an organization. The deployment image is developed by the organization on a live system and then when new machines are deployed the standard image is restored to the new machine, which populates it with the standard Operating System, software applications and data. Once restored the new target drive is

from which the image was restored. On the other hand, if the current drive itself was imaged by the employee before they left then the drive used to capture the imaged copy would be listed. This would be the case only if the imaged drive was an internal drive such as on a workstation where the copy drive could be attached internally while the imaging was progression.

The second place one should look is the SetupAPI.log file for Windows systems prior to Vista and SetupAPIDev.log file for systems after XP. This file memorializes the first use of any hardware used with the system. The data captured is not just the first installation date but the Manufacturer, Model number and Serial Number of the hardware device.

One can use this information to confirm that the drive being examined is one that was installed and when it was installed. One can then use the knowledge of the first installation date to confirm that the period of interest is reflected in this hard drive.

The third place is the Software hive of the Windows registry. The specific keys would be the CurrentVersion and WinVer keys. These keys reveal the version of Windows that is installed as well as the installation and the registered owner.

When conducting the examination one needs to have all three pieces come together. An anomaly with any of the three pieces can cause problems in terms of a wrong conclusion or indicate a problem with the data as a whole. Thus, if any anomaly is detected they should be run to ground and reconciled.

Genuine Device (Not counterfeit)

Assuming that the device has useful data and the registry confirms the hard drive as an original drive for the period of interest, there can still be concerns about a storage media's authenticity. If the media is a bootable drive, there is still another place that can be consulted to confirm its authenticity. That place is the System event logs.

On a Windows system there are a number of operating system log files that record various operations of interest. Although there are many different types of operating system event log files, the primary log files are the System, Security and Application log files.

All of these event logs contain records related to different system operations. There are thousands of different activities that can be reflected in these logs. Those activities can be things like power ups, logons, logoff, accesses, updates, etc. In a single day, each log cold capture more than a hundred events memorializing things that have happened during system operation.

Although the number of events that are potentially recordable by the operating system are large, they are still a finite number and do not include every conceivable event that occurs. For example, a user pressing a key on the keyboard is an event but it is not one that is recorded in

booted, which then populates the registry with the new drive's data like manufacturer and model number. In the meantime, the data regarding the hard drive of the deployment image was copied over when the image data was restored. As a result, the newly deployed hard drive will have both the data of the new hard drive as well as the data of the standard image hard drive.

the event logs. Nonetheless, there are thousands of activities that can be reflected in the event logs.

The event logs have a fixed size. Once they reach their fixed size, old records are rolled off as new records are added. In the end, it is not likely that the logs will have a complete history of computer activity.

One of the things that makes these logs useful, though, is that each entry is assigned a sequential record number. Furthermore, this record number never resets. Rather, it continues to increment until a new operating system is installed. Thus, by examining the largest record number, one can confirm that the age of this installation matches the computer amount of log activity reflected in the event logs.

It is quite possible for someone to completely fabricate a hard drive and make it appear to cover the period of interest. They can simply turn back the system clock and perform a system installation. Then they can periodically increment the clock forward while copying on files and feigning other types of user activity. In such a case, the maximum event log record number will not reflect a sufficiently large record number for the period covered.

Thus, even if the other attributes like file activity dates, installation dates and even user activity seemed to cover the period of interest, the maximum event log record will not be sufficiently large.

System Clock is Reliable

The date and timing of events is always an important aspect in the analysis of any fact pattern. As a result, ensuring that the computer system clock is accurate and is reliable is important.

There are several ways that an inaccurate system clock can manifest itself. The first could be in unusual date stamp patterns appearing in the analysis of file system activity. Those are discussed further in a subsequent section below.

In cases where the consequence of an inaccurate clock may not be so obvious there are several places one could check to test the clock's accuracy. For Windows systems prior to Windows 7, the first place is user assist key in the NTUser registry hive with a "TimeDate.cpl" reference. For Windows systems of Windows 7 or later the entry would appear in a jump list under the CLSID GUID E2E7934B-DCE5-43C4-9576-7FE4F75E7480.

There could also be indications of clock manipulation in a prefetch file. In the RUNDLL32 prefetch there will be a reference to "TimeDate.cpl" if the system clock has been changed through the Control Panel. Access of the TimeDate.cpl could also appear in the Windows Security Event log.

All of the above examples provide a means of detecting system clock manipulation through the Control Panel. The clock could also be changed through BIOS on boot up. In this case, there would not be any indication in the Control Panel.

Whether or not the Control Panel was used, another way to detect system clock manipulation is by consulting the event logs. In this case, however, one is not looking for access to the TimeClock.cpl. Rather, one is testing the chronology of the time stamps in the event log.

Since each event log record is sequentially numbered and each record has a date stamp, simply order the event log records by their sequential record number. Then test for instances where the date stamps are out of sequence. Such a finding not only confirms a time clock manipulation it also identifies the particular time periods that should be questioned.

When checking the event logs, particularly the System event log, event ID number 34, which indicates that the system clock is off by more than 54,000 seconds or about 15 hours. As it turns out, the system will not adjust the system clock automatically if it determines that the clock is off by more than 54,000 seconds.

Identifying Attached Storage Devices

Whether or not any other storage devices have been attached to a Windows system is always of interest. The primary interest is whether or not removable devices like flash drives have been used to take sensitive information. A secondary interest is whether other hard drives have been attached internally verses externally using a USB connection and whether information has been copied to that other hard drive.

Whether other storage devices have been attached can be determined through the examination of various registry hives. Registry hive are a kind of database that Windows uses to store important information that it will need for system operation.

The principle registry hives are the System and Software registry hives. Amazingly the data about attached devices is not recorded in a single place in these databases. Rather there are actually several different places that capture information about attached devices and that should be consulted such as Mounted Devices, USB Stor, Device Classes, Device Properties, and EMD Mangement to name a few.

In addition to the System and Software registry hives, the NTUser registry hive for each user profile on the computer will also store information about attached devices in the MountPoints2 key. Not only is this information additive to the information contained in the System and Registry hives it also can attribute particular device usage to a particular user at a particular time.

A final source of information about attached devices is contained in the Windows.DriverFrameworks event log. The information captured in this log is not as informative about the specifics of a particular attached device. Rather, the information captured here is more about each of the dates and times at which the device was attached.

While one can determine the first and last dates of a device attachment in the System and Software registry hives, the Windows.Driverframeworks event log captures the timing of each attachment instance, at least for as long as the data exists in this event log.

Apple Systems

Apple systems are very different from Windows systems. Their file systems, which are discussed in more detail in the chapter on recovering deleted files, are different and tend not to leave as many artifacts as Windows systems. The Apple systems themselves are similarly less robust with artifacts than Windows systems. A few of the more useful artifacts for Apple systems are the system log file, kernel log file and the FSEvent log file.

System log

The system log captures numerous activities that can be useful to assessing the system configuration and performance. Unlike Windows systems where the logged events are retained in a single repository, an Apple system log is limited to each session. A new log is created when the system is booted again. The prior log is archived but kept in the same folder as the original log. The older log files are compressed in Bzip2 format. So, they can be uncompressed and reviewed.

Along with other activities the system log is one source where USB device activity can be found. These entries can be found by searching for USBMC keyword identifiers. The information about USB devices is more limited than in other logs like the Kernel log.

Kernel Log

The kernel log is another source of USB device activity. It contains a fuller picture of an attached USB device.

Once again the instances of USB devices can be found by searching for the keyword USBMC.

FSEvent logs

FSEvent (File System Event) logs are another useful source of device activity on an Apple machine. As with other logs, like the system log, there can be numerous FSEvent logs.

FSEvent logs can contain many different kinds of useful facts about Apple system utilization. As with the system log and the Kernel log, the FSEvent log can contain information about attached storage devices. It will also capture mounting information about those devices.

Some of the other information includes documents, downloads, and desktop activity within a user profile. Still other useful information is website connections and I-cloud syncing activity.

Summary

Device system analysis is another useful and important source of device usage. This information can be useful in understanding whether the device was performing as intended and whether any other devices were attached which could also contain could relevant evidential data.

CHAPTER 5

File Activity Analysis – How Has It Been Used

Introduction

File activity analysis looks beyond the contents of a storage media and examines what data was actually used. By looking at what was actually used one gets both an idea of what was actually being done as well as what files exists on a particular storage media.

Since the results of file activity analysis also capture information about the device on which the file was stored, these tests can be used to identify particular media of interests, provide information about the contents of the media and reveal data hiding efforts when the data no longer exists on the media but its prior existence is confirmed by these tests.

Since this data is created during file usage, the data is only captured if the file is actually opened viewed. It does not know and it cannot tell anything about a file's existence if the file is never opened and closed. Thus, this analysis cannot provide a comprehensive list of files on a media. Rather, just a list of those that have been opened and viewed.

Because these tests reveal what files have been opened and closed, they provide a good means to confirm whether particular files are being used or not used. Of course there are some practical limits, since the data sources for these tests have short lives. So, the further back in time the analysis goes the probabilities increase that the data could be incomplete.

The information of file activity is contained in two different artifacts. One is link files and jump lists. The other is browser history.

Typically, it is not a matter of choosing which one to perform. The two provide different information and provide different activity horizons. While they all have about the same active life spans of about 25 days, Link files and Jump lists have shorter horizons than does browser history. The maximum activity horizon of a link file or jump list is about 6 months while the activity horizon of browser history is more typically 8 to 12 months, although several years is possible.

If all one is seeking is information about file access activity on a Windows system then browser history is likely more informative than link files and jump lists simply because of its increased data volume. If one is seeking to know more about the devices from which the files were accessed then link files and jump lists are far more informative than browser history. Thus, it can be a trade-off as to the particular needs of the case as to which one is more useful.

While both link files, jump lists and browser history identify similar information about file activity the two tests are often complimentary to some extent. In other words, even for the same period of time there can be file activity identified in link files and jump lists that do not appear in browser history and vice versa.

Preparing and Processing the Data

As with any kind of analysis the data must first be processed and prepared for analysis. The data principally used for file activity analysis are link files, jump list and browser history. These are individual artifacts that have short lives. Thus, the preparation part of the analysis effort includes an examination of freespace to locate earlier instances of these data source in order to develop as many data points as possible. Once all of the available data points are collected, their contents are parsed because the data that will actually form the basis for the analysis is the metadata contained within these artifacts.

The following sections describe for each data category the nature of the data and how it is used for the analysis.

Link files & Jump Lists

Link files and JMP lists are created by the Windows system when files are opened and viewed. They are essentially file pointers. They are not the data files themselves but are pointers to the files that were opened and manipulated by the machine user.

Link files, jump lists and browser history are created by the Windows operating system and reside on bootable drives—drives having the operating system. Thus, they are not found devices like flash drives or external hard drives used solely for data storage purposes.

Although link files, jump lists and browser history are only found bootable drives, they will reflect files opened from any storage media. Thus, they will reflect files opened from the local internal hard drive as well as flash drives, external hard drives and even network drives.

Link files are a long time feature of Windows systems while jump lists are a more recent addition. Specifically, the feature was added with Windows 7.

While both link files and jump lists are structured similarly and capture similar information, there are differences between them both in terms of their locations and their interpretation. Each is discussed in the sections that follow.

Link files

Link files have a file extension of LNK and are typically stored in the recents folder of the user's profile, although for applications like Microsoft Office they are stored in a separate system folder within the user's profile.

Link files are shortcuts pointing to the location of a file. Link files are useful in a forensic investigation to determine what files have been opened and viewed as well as might have existed on other media. The existence of a link file without the corresponding data file is also an indicator that files have been deleted. If an evil doer had been successful in wiping an important document and removing all traces from the filing system, the link file could still provide evidence that the file had existed at the preservation was performed.

When examining link files the data of interest is typically their internal metadata. The internal metadata contains the file name and full path of the file to which it points. In other words, if a document existed on an external storage device, such as a thumb drive, then the full path within the link file will indicate the logical device letter and the full path and name of the target file.

In addition to the full path and file name, link files also contain the date and time stamps for the file that it references at the time it was last opened. Thus, one can learn much about a file it does not even possess by examining the metadata of the link file related to that file. In other words, from the create date captured in the link file metadata one can learn the date on which the file was placed on its storage media. From the last write date one can learn the date on which the file was last changed, which could be important if that date is after the date when the file was placed on the storage media.

Other pieces of information captured in the link file metadata are the volume label and volume serial number of the storage media on which the data file resided. Both of these pieces of information can help to specifically identify a particular storage device containing the data files of interest.

There are in fact, many data attributes captured in the metadata of a link file. Another useful attribute is an indicator if the storage media is a removable media like a flash drive or a fixed disk like a hard drive.

The actual date when the file was opened and viewed is determined from the last write date of the link file itself. When the file is opened the metadata contained in the link file is updated for the most recent data related to the data file to which it points. Thus, the last write date for the link file itself is the date when the file was last opened and viewed.

When a document is first opened, the link file's create and last write dates will be the same. If the data file is later opened again, the link file's last write date will be changed to that date. At that time the link file's create and last write date will be different.

Link files have relatively short lives of about 25 days since the data file was last opened and viewed. Thus, the information one can learn about file activity can have a relatively short horizon. One might be able to realize something beyond this limitation from two data sources.

First, once the link file is deleted it is recoverable like any other file. A significant drawback, however, is that most link files are so small that they are "persistent", which means that they are actually stored within the file system and not out in the data storage area with other data files. Those that are persistent can be quickly overwritten as new file references are added to the file system.

Second, link files are typically part of the system state information captured in restore points. As a result, it is possible that link file information could exist for several months within the restore point archives. The amount of link file history that can be found in a restore point can depend on many factors that include the operating system version, the size of the drive and the amount of space reserved for restore point activity.

Jump Lists

Starting with Windows 7 the link file concept was augmented for a new but similar artifact known as Jump lists. Jump lists are, essentially, an updated version of the link file concept.

The Jump list is more of a data record than an actual file and the storage location for Jump lists is different than for link files. Jump lists are stored in special subfolders to the Recents folder within a protected folder of the Users profile.

Despite their differences, jump lists contain much of the same information as link files. Thus, jump lists provide much of the same valuable information as link files and they can help provide a more complete picture of file activity, particularly the device on which the file was stored.

Browser history

Browser History Analysis is an excellent test to gain a basic understanding about how a device is being used from a file activity as well as an internet activity perspective. Of course, the device has to be a bootable device or at least one that will contain activity logs. Consequently, it is not the kind of test that is useful for storage devices like flash drives or external hard drives but is excellent for a bootable device and based on the results uncovered can be the basis on which to direct additional analyses.

The Browser History Analysis scans the storage device to find both active and deleted activity logs for various web browsers. While Windows Internet Explorer has been the leading browser and an integral part of the Windows Operating System, it is by no means the only browser. Indeed, there is Mozilla Firefox, Google Chrome (which has gathered considerable market share), Apple Safari and others.

Under standard settings, a user's browser history contains only about the last 25 days of activity. As new activity is incurred the older activity is rolled off and replaced with the most recent activity. By scanning freespace the process finds earlier remnants of the activity logs in order to examine those as well. As a result of searching free space, it is common to find about 8 to 12 months worth of activity log history, although it is often possible to find browser activity going much further back like from 2 and 3 years prior.

Files Opened and Viewed

The Windows Internet Explorer is unique among web browsers in that it also captures a user's file activity as well as its web browsing activity. It is not a function of whether one uses Windows Internet Explorer or some other browser, since the file activity is actually coming from the use of Windows Explorer that users typically use to navigate around their storage devices and then open files. What happens is that Microsoft has just linked this kind of activity with its web activity and store both sets of data in the same data cache—the internet browser cache.

The file activity captured in the browser history is similar to the data captured in the link file and jump list data. There are some differences, though.

First, the file activity captured in the browser cache is not as detailed as the data captured in link files and jump lists. While link files and jump lists capture a lot of other details about the device from which the file was accessed, the browser cache data simply captures information about the date, the user and file path.

Despite its limited data elements the browser history data has some benefits over link files and jump lists. The primary benefit is that browser history data can typically be found that covers a longer period of time than does link files and jump list. It is not uncommon to find browser cache data spanning over a year while link files and jump list data tends to be much shorter.

Web Sites Visited and Pages Viewed

Browser history analysis can identify web sites visited by a user that could be important like cloud based storage systems, the use of web based e-mail, improper activities and even unproductive time while on the job such as on-line shopping.

Learning the websites visited by a computer user is not the only benefit to Browser history analysis. While most browser logs like Google Chrome and Apple Safari capture only a user's web activity, Microsoft Internet Explorer also captures file activity as a result of users opening files through Windows Explorer. It makes no difference whether the files actually reside on the local system or on any attached storage device like flash drives and external hard drives and

even network devices like file servers. Whatever files are opened and viewed are memorialized in the Windows browser cache records.

When the file activity of the Browser History analysis is compared to file system analysis, data hiding and spoliation can become obvious when files no longer reflected in the file system had been recently accessed as evidenced by their appearance in the Browser History report.

There is more information in the logs than just references to the files and websites accessed. The logs can also include other internet based activity such as instant messaging that is sometimes also part of the browser record. In other cases the messaging and other social media content is captured in separate databases that are resident on the storage media but could go unnoticed were it not for its appearance in the Browser history analysis. Since the contents of instant messaging and the other social media databases required decoding and/or decryption, there are different tools that are used for social media and instant messaging.

Analyzing the Data

Once the data is prepared, it is ready for analysis. The following sections provide some examples of the various analyses that can be performed with file activity data.

Reconcile File Activity to File System Data

References to deleted files are not always present in the file system, since those entries can be overwritten as new files are moved onto the storage device. By comparing the results of file activity analysis to file system analysis, it is possible to identify instances of deleted files that no longer appear in the file system.

File references from file activity analysis that do not appear in file system analysis tends to be very concerning, particularly when the results of file activity analysis are filtered to recent activity. In that case, files that appear in file activity analysis that do not appear in file system analysis tends to be intentional file deletions.

Identify Files Accessed from Attached Devices

File activity analysis can provide insight into the contents of storage devices that were not produced, at least if file were accessed from those devices by the system under analysis. Thus, a key analysis of file activity analysis is to compare and contrast the list of files being accessed from attached storage devices with the results of device system analyses where attached devices are identified along with their initial install and attachment dates.

While the file activity recovered in browser history analysis identifies only the file accessed and the drive letter of the attached device from which it is being accessed, link files and jump lists provide more detail about the device from which the files are being accessed. This additional device information can be used to pinpoint which attached device is of interest.

Review Web Sites Accessed

The browser history includes the web sites being accessed. This kind of information can be used to determine whether cloud based storage systems are being used to transfer data. They can also provide insight into how a person uses their computer system.

Compare and Contrast with Registry MRU Lists

The MRU [most recently used] list of documents being accessed are not all matched with date stamps as described in the chapter on device system analysis. When file activity data is matched to these lists the missing date information can sometimes be determined the way a complete picture is revealed after placing all the pieces to a puzzle.

Summary

File activity analysis provides three types of useful information. The first type is how a computing device is being used. It has to be a computing device and one with an operating system, however. This is not the kind of analysis that would be done on an attached storage device like a flash drive or external hard drive unless those devices contained backups of file activity artifacts.

The second type of useful evidence is information about the contents of a device that was not produced or available for examination but the device to which it was attached is available for analysis.

The final type of useful information is a kind of spoliation indicator. The prior existence of files that had been improperly deleted or removed could be betrayed by file activity analysis when that analysis is compared against file system information.

CHAPTER 6

Database Analysis

Introduction

Computerized database applications like accounting systems were among the first uses of computerized technology. Since those early days database applications have simply grown in size, complexity and the types of applications in which they are used. While business management systems like accounting, manufacturing, and personnel are still very common, computerized database systems have become common in many other data management fields too such as medical records, most public records like property and tax records, social media applications and even cellphone applications like text messaging and other cellphone applications.

In today's world there simply is very little that is not captured in a database. Although initially one might shrink when confronted with the prospect of analyzing a database, quite the opposite should occur. Indeed, for the fraud examiner an encounter with a database should be considered a windfall for several reasons.

First, the data is very portable. Thus, it can be easily harvested and taken elsewhere to examine and analyze. Furthermore, in most cases the application software is not needed nor should it be wanted.

Second, despite that there are many different database manufacturers, most of the market is controlled by only a few players. Perhaps even more significant is that even among the various database manufacturers their products are built to industry standards. This standardization enables the investigator to use a single skillset to access any standards compliant database system.

Third, they enable an examiner to use computer power to sift and sort through various transactions rather than trudge through tedious transactions manually. In fact, they enable the examiner to forego sampling and audit 100 percent of the data.

Fourth, there are many third-party tools that enable examiners to apply many different analytical techniques such as graphing, frequency distributions, statistical analysis and trend analysis in order to spot situations warranting more in-depth examination.

In the sections that follow all of these advantages are explored through a review of the database technology, auditing scenarios and review of practical limitations.

Dealing with Databases

Databases can be a wealth of information and they are being used in more and more applications. For example, even things like web browsers and text message systems are using more advanced database technology than the technology of just simple text files with either delimited or fixed length record structures.

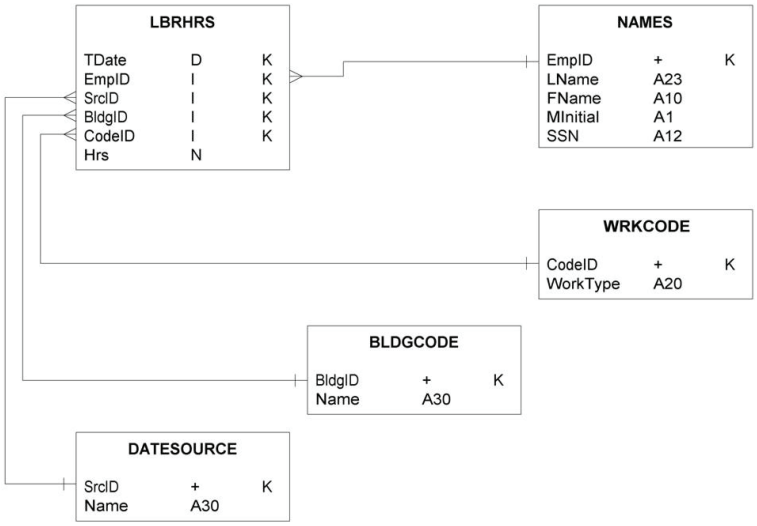
The good news is that encountering a database or database application need not be an impediment to data analysis. The following sections explain why database situations should not be a detriment to data analysis as well as explain approaches that can be used for dealing with them.

The Emergence of Databases

In the early days of computer systems databases were hierarchical, since they reflected the real life models that they emulated. Drawing packages have a hierarchy. Customer and contact lists have a hierarchy. Contracts have a hierarchy. Organizational structures have a hierarchy.

As the use of computers expanded, however, so did the need to match one hierarchy, like customers, to another hierarchy, like contracts. In this respect, the hierarchical structure proved to be a limiting factor. Often times integration of the organization required that the data on one branch of a hierarchy combine with the data on another branch of the same hierarchical tree or even on a different hierarchical tree altogether. For example, engineering data needed to be combined with marketing data and sales forecasts in order to produce a production plan for the factory floor. When engineering was a separate tree from marketing which was also separate from manufacturing it was difficult to automate the integration of these activities.

By the late sixties work was underway to resolve the limitation of the hierarchical data model. By 1968 researchers at IBM had developed the relational database model. Relational databases are so named because they are comprised of multiple data tables that can be related to each other to produce a desired result.



In the above illustration the LbrHrs table contains labor timesheet entries. When the contents of the LbrHrs table are related to the Names table, WrkCode table, BldgCode table and the DataSource table a complete picture is obtained about who was performing the work, the type of work that was being performed, where it was being performed and how the data was entered (timesheet, clock card, wand, etc.). This information could then also be combined with wage rate information to produce payroll or combined with billing information to produce invoices.

There Is a Difference Between the Front End and the Back End

Typically, people still think of computer applications as some kind of monolithic entity. Just as a car is a multitude of different parts built by different manufacturers and then brought together as a final assembly so are computerized applications. Also like cars that can be split into several major assemblies such as engine, transmission, frame, etc. computer applications can be split into major components as well.

As a result, computer applications in today's world can be split into at least two parts; the front end and the back end. Simplistically stated, the front end is that part that interacts with the user while the back end is that part that manages the data.

The significance here is that even though there might be a million accounting systems on the market, those million front ends are probably built on no more than about 100 different back

ends. Even more significant is that the vast majority of today's market is controlled by a small number of those 100 database systems. This concentration of database back ends makes it easier for the auditor to acquire the expertise necessary to penetrate the auditee's electronic data repository.

There are Standards

In addition to the concentration of database back ends, there are other facets to database systems that even further facilitate the auditor's penetration of the auditee's electronic data repository. The most significant of these is standardization.

Relational databases were developed in the late 1960s to overcome the inefficiencies in the hierarchical data model and solve the needs of business applications. Once the solution was determined to be the relational database model there still needed to be a way to retrieve the data in usable form. Researchers at IBM pioneered relational database technology and the relational language initially known as Structured English Query Language (SEQueL). The language was repeatedly revised, improved and renamed to SEQUEL-XRM, SEQUEL2 and finally shortened to SQL, properly pronounced "ess-que-ell" but commonly pronounced "sequel".

By the late 1970s IBM had successfully demonstrated the capability of its relational technology and was developing a commercial product based on its SQL language when other vendors entered the relational database field. By the mid 1980s numerous companies had launched SQL database products and SQL was becoming a de facto standard on everything from micros to mainframes.

At about the same time, however, SQL became an official standard, too. In 1982 the American National Standards Institute (ANSI) began development of a relational language standard. The standard was ultimately ratified in 1986 and commonly referred to as SQL/86. In 1987 the standard was also accepted internationally by the International Organization for Standardization (ISO). The original SQL standard was later expanded and also ratified by both the ANSI and ISO committees in late 1992 and is commonly referred to as SQL/92. Even today work continues on further enhancement of the standard. Numerous features and capabilities continue to be added.

Initially the SQL standard was designed for stand-alone interactive use. Over the years, however, facilities were added to allow invocation of SQL operations from application programs written in other languages. Hence, the front-end versus back-end capability discussed above.

For the auditor there is real significance to all this SQL history. First, since the standard was initially designed for stand-alone interactive use, every SQL based relational database system should provide a console capability or at least some capability for accessing and manipulating its contents that is separate and apart from whatever front-end application might be using it. Thus, neither knowledge nor use of the auditee's application software is necessary in order to access their data.

Second, the broad acceptance of the SQL standard means that with only a few minor syntactical differences auditors can extract electronic data from virtually any system simply by

providing a few standard commands. For example, if one's desire is to take all the data in one of the auditee's data tables that desire can be realized by executing the following command.

SELECT * FROM [*table name*]

The returned result set can then be copied to disk or tape and taken by the auditor. The command can then be repeated for every table in the auditee's database so that the auditor has a complete copy of all of the auditee's data.

The next logical question is how does one know from what tables to request data. The answer is that the console, from which the above command is issued, can also be used to identify all of the tables in the auditee's database. Depending on the system the various tables and their names may be simply viewed or returned as a list in response to a command. The auditor will need to research the particular database management system to learn how this information can be obtained.

Of course, identification of the data tables is not all that can be learned. The structures of the tables can also be learned. Again, the particular procedures will vary from system to system but the information is easily learned from the manuals that accompany each system.

If there are concerns that the contents of data tables may have far more information than is of interest, then the above command can be modified for a selection criteria as shown below.

SELECT * FROM [table name] WHERE [condition1 (... and conditionN)]

So for the auditor this means that regardless of the million front ends being used or the hundred back ends being used the same instructions can be used to obtain the desired electronic data from practically any relational database system anywhere in the world today.

Stay in Your Own Backyard

Many auditors have previously tried acquiring their auditee's electronic data. Typically, they have failed for one of two reasons. First, they were not able to exploit the data once they had it. In other words, they did not know how to analyze it or what kind of analysis should be done. That problem is discussed later in the sections on Database Analysis and Auditing the Data.

The second reason that they failed was they did not request that the data be delivered in a usable form. If they simply requested the data in its native format then they would need their own copy of the backend database engine in order to analyze it. Sometimes those systems can require a fairly sizeable investment.

The solution to this latter problem is to go with what you know and play in your own backyard. This is easily accomplished by requesting the data in a particular, yet standard, format. That way the auditor can take the data and use it in whatever system he might want to use to examine the data.

ASCII [American Standard Code for Information Interchange] format, either fixed length or delimited, is the most widely accepted data format. Every database system should be able to

save its data in ASCII format and any system used by the auditor for analyzing the data should be able to import data in this format.

Other than ASCII, many systems are designed to download data into a number of other popular data formats. Some of the other popular database formats are dBase, Microsoft Access, Corel Paradox or any of the popular spreadsheet programs like Lotus 1-2-3 or Microsoft Excel.

Of course, getting the data and using it can still be two different things. For example, just because the data is produced in a spreadsheet format like Microsoft Excel does not mean that it can be analyzed in a spreadsheet for several reasons.

First, there are frequently constraints regarding how many rows a spreadsheet can contain even though there are no constraints about how many rows can be exported to a file in Excel format. If the data application is of any kind of significant volume then it will likely contains more data than can be examined in something like Excel.

Second, in order for relational data to be analyzed in a meaningful way, the analysis tool must be able to relate the data in one table to the data in other tables. This kind of functionality is not easily accomplished in something like Excel. So, the auditor should be sure that his analysis tools can work with relational data. Something like Excel spreadsheets are designed to work with de-normalized data.

As a result of the above two common problems when performing the analysis of relational database data, the auditor should stay in his own backyard. What that means is that the auditor should request his data in a format that can be examined by his analysis system. Also, whatever analysis system he used should be capable of managing relational data.

Be Sure Not to Pack

A number of database systems are something like hard drives–deleting a record does not actually delete the record. Instead, deleting a record tags the record for deletion but the actual deletion does not occur until the database has been “packed”. When those types of databases are being used the auditor should consider getting those records tagged for deletion before the table has been packed.

In these types of databases the records tagged for deletion can be recovered anytime before the database table is packed. Auditors can identify which records had been tagged for deletion if they ask that the opponent’s database records be provided two different ways. First, ask for the extract from unrecovered database tables and then obtain the same extraction from the recovered database tables. The difference between the two data sets would be the records marked for deletion but not yet packed.

No Limits

Remember that there is typically more data in the electronic data than is visible in the paper version or will even appear through the user interface. For example, there could be system

generated input dates, record tags, and various audit trail information. So, it is a mistake for the auditor to try and list the individual data elements to be delivered. Instead, the auditor should ask for all the data fields (columns) within a table and all the records (rows) within a table matching the relevant case criteria.

When dealing with relational databases, which most databases used in business applications are relational, remember that they are not comprised of one data table but rather numerous data tables that can be related to one another in order to produce an outcome. When the tables are combined, "related", they produce the complete transaction cycle. So, be sure to ask for all the tables including any lookup and data validation tables.

It is also best to ask for the tables in normalized form. With respect to relational databases, "normal" is a term of art.[7] Relational database tables are "normalized" as part of their design process to optimize a number of different attributes; space minimization, speed maximization, facilitate analysis and facilitate maintainability. By asking for normalized tables the auditor is asking that the data be provided in the same optimum configuration as was designed for its use. This should facilitate the auditor's subsequent analysis and also prevent the auditee from combining or denormalizing tables.

Mark the Trail

Relational database systems, particularly when they model complex business processes, can be complex themselves. The auditor's analysis of these complex models can be expedited if the trail is well marked. There are three types of documentation that the auditor will ideally want to acquire in order to mark the trail.

Since the audit data is produced by the auditee, the first piece of documentation that the auditor will want is their production procedures. He can get these by asking for the SQL scripts used to prepare the data downloads. Of particular interest is whether the auditee specifically identified the particular fields to be extracted or whether they used the "*" character, which is the SQL equivalent of all fields. If the auditee specifically identified the fields to be produced they could be hiding important data elements.

Also, the auditor is interested in any selection criteria that the auditee may have used in its SQL scripts to limit the result set. These limitations will be obvious in the "WHERE" or "HAVING" sections of the SQL script, as well as, the "FROM" section, if other than full table joins were used.

The second thing that the auditor will want the auditee to produce are the database table schemas also known as dataset descriptions. These descriptions identify all of the fields and their attributes in each table provided. The auditor can use these to confirm receipt of all data fields and to document how the data is actually arranged when he starts the analysis.

The schemas may also identify the significance of any codes that have been used as

[7] Fleming, Candace C. and Von Halle, Barbara. Handbook of Relational Database Design. Addison-Wesley Publishing Co. Reading. 1989., "Normalization is a body of theory addressing analysis and decomposition of data structures into a new set of data structures exhibiting more desirable properties. Specifically, normalization increases the certainty of achieving an optimal logical data model."

semaphores. For example, in a payroll system the difference between regular hours and overtime hours may be designated by a particular code. If the universe of such codes is large the database designer will likely have chosen to use another table to identify the significance of these codes. If it is small, however, they may be documented in the schemas themselves.

The final type of documentation that the auditor should obtain is any data diagrams that illustrate the relationships of the tables, as well as, any other database documentation. The preceding example of a relational database design is the type of additional database diagrams that the auditor should try to acquire.

If the auditor is not able to obtain any of the above documentation, his excursion into the electronic data of the auditee's databases is not foiled. An experienced database designer can still re-engineer the design and make the data useful, particularly if the data has been delivered in normalized form. After all, the experienced hacker does not need the password to a computer. It just takes him a little longer to gain access without it.

Validating the Production

More than likely everyone's database data will be very different. Not only in content but in structure as well. Just because two companies use the same accounting software does not mean that their financial data or their accounting system will be similar. So, it is impossible to devise any standardized analysis for databases other than some tests to determine that the data delivery was complete and reliable.

As mentioned earlier, one of the things that the auditor can do to confirm a complete database delivery is to analyze the SQL scripts to determine how the data was selected and whether the selection criteria are compliant with the production request. Next the auditor can examine the schema and confirm that the data delivered matches the schemas.

Next by examining the database structure the auditor can check for widows and orphans, unmatched foreign keys, fields with null values and key fields and table indexes. The existence of widows and orphans means that the produced data contains records that cannot be related to anything else. This could be a sign that there was an error in the logic of the selection criteria or that otherwise responsive data has been omitted.

Unmatched foreign keys mean that there are table fields that are used to relate records in one table to the records in another table. The fact that there are unmatched foreign keys means that either an entire table was not delivered or that selected records have not been delivered that otherwise would have met the criteria to deliver a database in normalized form.

Null values are fields in the database records with no value. Null fields are different than fields with zero value. Zero means zero. Null means nothing. The twelve rules for database design devised by E.F. Codd, one of the developers of the relational database model, include a rule that database fields should not be populated with null values. Although this rule is not strictly followed by many database designers, null values can cause problems for relational databases.

When the auditor finds tables with null values he must determine whether these are another

signal that something is amiss with the data produced or whether it was simply the result of a designer who did not follow the rules. If the null values occur on a foreign key field then there certainly is a problem. Also, if the null values occur in important system fields such as userids, transaction dates, etc. then that is another signal that a problem is likely present with the data delivery. If it just happens to occur in a field for a cell phone number then perhaps there simply is no cell phone number to be captured.

Next the study of index and key values can reveal whether records have been omitted and whether they were contemporaneously entered or entered in a later time period. For example, suppose that a particular record in a database table had a field for transaction date. On the surface the date matches other records having similar dates for that particular transaction event. A study of the key fields and table indexes might reveal that those values are inconsistent with a transaction having a date equal to the one in that particular record. While this might not signal an omission of data it would signal that the auditee has falsely entered transactions into their database system such as medical tests performed after the fact, in the case of a medical malpractice issue.

Some other methods that can be employed to test the veracity of the database production is to compare the data structure of the database to data elements on system input forms and output reports. If data is being captured or produced that does not appear in the database production then that is certainly something that should be subsequently investigated.

Auditing the Data

Once the auditor has either accessed the auditee's data or obtained the data for analysis elsewhere and validated its purported content, he can begin examining it. There are no hard and fast rules for how the examination should be performed but there are a number of different types of examinations that can be done.

Metrics

The first kind of examination is likely of a statistical nature. The purpose of this examination is kind of a follow-on to the earlier examinations that the auditor may have performed to validate the content of the data. For example, the auditor may want to determine table record counts; average, minimum and maximum field values.

Distributions

The distributions could be of data records over periods of time or types of records by code, or whatever. Essentially, these can help the auditor to identify trends, understand usage, and identify areas requiring additional examination.

Comparison and Compliance

Comparison and compliance is where the real auditing will occur. It is also where the power of database auditing will distinguish itself from the more traditional manual techniques. Under manual auditing techniques the auditor will likely employ sampling methods to evaluate the population of auditable transactions. Then based on the sample results, the auditor will project the results on the entire population.

This is one area where database auditing will be extremely different. Under database auditing the auditor can actually audit 100 percent of the population. As a result, an absolute result will be known and the results are not subject to projection onto the population based on confidence limits.

There are two ways that compliance auditing can be organized. First, if it is just a matter of error rates, then queries can be created to select those records containing the condition of interest. Out-of-sequence transactions could be such a situation. In that case, it could be a matter of testing various date stamps to other fixed values like self-incrementing key values to find instances of out-of-sequence transactions. Another could be to compare current transaction records to history or archival records of changed records to find instances of potential targets.

Often times, however, quantifying the impact is more complicated than what can be gleaned from simple queries. Indeed, determining that a problem exists could require many levels of complex calculations before the result could ever be compared to a claimed value and its legitimacy confirmed or rejected.

Thus, in this second situation it will likely be necessary to build an audit model. This can either be another database table or tables that links to the auditee's data and contains audited values on which to base a final calculation or additional fields can be added to the auditee's database tables in which to store audited values on which to base a final calculation. Either way can yield the same result, The particular technique will likely be decided by the performance desired by the auditor from his audit model.

Typically, these kinds of things are iterative. So, if the auditee's data model is large and complex, the auditor may choose to develop a separate audit table that can be more quickly queried over and over than could the auditee's data.

Limitations

Although database analysis can be very effective and is much more powerful than traditional auditing, the success that one will experience is limited to the auditor's computer skills and automated system skills. In order to use this technique the auditor must be familiar with SQL at a minimum. Knowledge of this language will allow the auditor to query the data and perform the necessary analysis. The effectiveness of the auditor will be increased if he also understands other languages that can be used to create a working model and audit tool. Knowledge of these other tools helps in the following ways.

First, an auditor's queries will be run time and time again. As the audit progresses and knowledge of the auditee's data is learned, the auditor will likely need to revisit queries previously run in order to determine whether they contained previously unrecognized findings. Thus,

embedding these queries in some kind of working interface not only memorializes the analysis and its findings, it provides a means to return to previous analysis exactly as it had been performed.

Second, the automated model also makes it easier to apply multiple auditors to the project. With a working model, therefore, even auditors unskilled in programming languages but having subject matter knowledge can be brought to bear in the analysis.

The other limiting factor of database analysis is the knowledge required of automated systems. By having this requisite knowledge the auditor can quickly assess which systems will likely have the data of interest. For example, in an accounting system the general ledger will likely not have details about vendor transactions while such information will likely be contained in the accounts payable and purchasing subsystems of the accounting system.

Similarly, access to a manufacturer's drawings (the images themselves) may not provide anything useful to the auditor. After realizing that the contents of this information are likely contained in a configuration management system used to control drawing development, then taking revision data along with bills of material and other part level data can be very helpful in evaluating production and manufacturing efforts.

This need for system knowledge can extend beyond just knowing where the data is located. It also involves understanding how one branch of the tree or a branch in a different tree can be matched to the branches of interest. Imagine how billings for manufactured product can be traced back through the various transaction lifecycles; billing to inventory, inventory to manufacturing, manufacturing to raw materials input and labor conversion, and finally back to order entry and forecasts.

So, while database are common and analyzing their contents through computerized tools is very powerful, an auditor's success in utilizing this tool is very limited to his own skill with databases and knowledge of computerized systems

Summary

With computers controlling virtually every aspect of business today, most business data available is computerized. Furthermore, the data collected by these systems is likely collected and stored in database systems.

Using database technology to conduct audits is nothing that should be ignored. In fact, an auditee who collects its data in databases is a blessing for the auditor. Not only can the auditor use computer technology to audit every transaction, he can also perform far more powerful analyses than otherwise available that can help to identify areas needing special focus.

Although the potential benefits of database auditing are immense, there is a limitation. It requires more skill than just confirming voucher or tracing transactions by hand. Rather, it takes expertise in the database language SQL. In addition, it helps to know other computer programming languages in order to more quickly and capably construct and audit model. Finally,

knowledge of various software systems can help the auditor to accurately identify the likely repository of the data of interest.

CHAPTER 7
Metadata Analysis

Introduction

There has become an increased interest in metadata. According to Wikipedia, metadata (Greek meta "after", “about”, “beyond” and Latin data "information") are data that describe other data. Generally, a set of metadata describes a single set of data, called a resource. Meta is a common English prefix, used to indicate a concept which is an abstraction from another concept, used to analyze the latter. For example, "metaphysics" refers to things beyond physics, and "meta language" refers to a type of language or system which describes language. Metadata are of special interest in various fields of computer science and are used in features such as database, information warehousing, imaging, computer files systems, etc.

Practitioners have learned that there are many things about system use and document management that can be gleaned from the metadata. In the case of *Williams v Sprint/United Management Company* it was held that metadata is discoverable.[8]

[8] *Williams, et al. v Sprint/United Management Company*, 230 F.R.D. 640, 62 Fed.R.Serv.3d 1052, 96 Fair Empl.Prac.Cas. (BNA) 1775, “When party is ordered to disclose electronic documents as they are maintained in ordinary course of business, i.e. as “active file” or in “native format,” producing party should produce electronic documents with their metadata intact, unless that party timely objects to production of

There are two principle types of metadata. There is system metadata and application metadata. Application metadata can then be further divided between embedded metadata and substantive metadata.

System metadata is data that is automatically generated by a computer system. For example, System Metadata often includes file system information such as date and time stamps, file path (location on the media), attributes such as read-only or other system generated information such as pointers, and activity or operation logs.

Application metadata is unique to a particular file type and is generally created and used by the application creating the file types. Application metadata is divided between embedded metadata and substantive metadata.

Embedded metadata includes other data embedded in the document by the system or software application such as author or creator, organization, and various date stamps. Substantive metadata is data that reflects the substantive changes made to the document by the user. For example, it may include the text of actual changes to a document.

While no generalization is universally applicable, system metadata and embedded metadata is less likely to involve include information that could be privileged or confidential. Substantive metadata, on the other hand, could include privileged or confidential information. The well known feature of Microsoft Office track changes is one example of substantive metadata. Similarly comments in excel spreadsheets are another example of substantive metadata.

The following sections examine more closely examples of system and application metadata and explain how they could be useful in identifying sensitive data in covenant related litigation.

System Metadata

System metadata is data created by the computer system. It includes things like file system metadata, file usage metadata, and operations metadata. All of these have been discussed in the prior sections on File system Analysis, file activity analysis and device system analysis. They will not be discussed again and the balance of this section examines application metadata.

Application Metadata

In addition to metadata created by the system, individual applications create their own metadata and store it internal to the data files that the create and manage. Application metadata is of two types, embedded metadata and substantive metadata. Each is discussed in the sections that follow.

---

metadata, parties agree that metadata should not be produced, or producing party requests protective order."

Embedded Metadata

In addition to the filing system, the files themselves can contain metadata, commonly called embedded metadata. This data can be used to validate the author, user, last written, created and accessed date stamps.

Author

Many programs capture the document's author name. Frequently, this is automatically filled by the application based on a value entered at the time of installation of the software or the installation of the operating system or when the user authenticated and logged on to the system.

User

Many times the name of the user of a data file is also captured. This value too is often automatically filled based on values entered at the time the application was installed, the operating system was installed or when the user authenticated and logged on to the system.

Date Stamps

In addition to the file system time and date stamps, the host file can often include a number of its own date and time stamps for file creation and modification.

Organization

Another form of application metadata often found is the organization name that created the document. This too can be helpful in spotting information belonging to a previous employer.

E-mail

While many are familiar with the benefits of e-mail, what they may not realize is that e-mail is frequently a collection of metadata elements. Even the message itself is but one metadata element in a large collection of elements.

Consequently, there are many metadata elements that are contained in e-mails that can be useful in the right circumstances. For example, there are create and modified attributes that can betray that a message has been altered after its sending or receipt. There can be conversation topics that identify the message subject without all of the extraneous other attributes like replay and forward.

Perhaps one of the more significant metadata attributes of an e-mail are its message header that includes IP addresses of the servers it passes along its journey through the internet

as well as the time stamps of when it passed through them. This data can be useful in authenticating e-mail messages.

E-mail messages are often used as evidence in litigation matters. It has also become well known that e-mail can be easily spoofed. Fortunately, e-mail contains a lot more data than the actual message and this additional data can be used to authenticate key elements of an e-mail such as its sender, recipient and the date sent as well as whether the message or its attachments have been changed.

Depending on the e-mail system there could be other helpful metadata as well about the attachments and their creation and changed dates. Examining this information can confirm that the message has not subsequently been changed after it arrived at its destination.

Images

Images can also contain useful metadata that can help to authenticate the image based on metadata elements designed to address key questions like:

- Who is involved with this image? (who took it, who owns it, who's in it?)
- What is interesting about this image?
- Where is this image from?
- When was this image created or modified?

Image metadata is also fairly uniform since there is an industry working group, the Metadata Working Group, that has developed open source standards on this subject. The working group is led by Adobe, Apple, Canon, Microsoft, Nokia and Sony.

The type of metadata contained in a photograph is known as Exchangeable Image File Format (EXIF) data.

Extensible Metadata Platform (XMP)

The Extensible Metadata Platform (XMP) is a media management standard initially developed by Adobe. It is now an ISO Standard and a foundational element in many other metadata standards.

There are many ideas surrounding the benefits of XMP that span cross platform and cross application interoperability, identification, as well as ownership issues such as asset relationships. It is the asset relationship aspect of XMP that provides much of the authentication assistance.

Most documents today are complex documents that have both evolved over time as well as incorporated many data elements. The asset relationship aspect of XMP provides a means to track the history of these changes and, in essence, provide a document pedigree or sorts. The pedigree then provides a means to authenticate a document including its ancestry.

Other Metadata

The above discussions on metadata are but a few. Almost all ESI has some metadata, although it is often kept secret and known only to the manufacturers. There are few widespread metadata standards, although they are developing. Once these attributes are known, they can easily be used for authenticating aspects of the evidence.

Limitations

The drawback of embedded metadata is that it can carry over from document to document. In other words, if someone took an existing document and changed it into something else the new document might retain the name of the original organization and creator. So, when examining metadata properties, users should be cognizant of these limitations.

Substantive Metadata

The form of application metadata is substantive metadata. This kind of metadata is more than attributes of the document and instead includes basic information within the document.

The most well known example of substantive metadata is document text retained through track changes in a Word document for example.

Summary

Metadata in general and application metadata in particular can have significant evidential value. Perhaps that is the because metadata is typically internal to the document. While in some cases it may be accessible to a user, it is not clearly obvious to the user. As a result, it is less likely that a user would think to change the metadata. Thus, application metadata can be quite a truth detector.

In the cases where application metadata is not accessible such as the header information in an e-mail, the metadata has even greater usefulness in authenticating a message.

CHAPTER 8

Recovering Deleted Data

Introduction

The ability to recover deleted data is an important and highly useful skill for the analysis of computerized media. The need to recover deleted data is not simply to recover documents that someone deleted for nefarious reasons. Indeed, there are many things that are routinely being deleted by system processes about which the system user is completely unaware. In the previous section on file activity analysis it was explained that many of the various system artefacts that are examined come from freespace because they have short lives and the system automatically deletes them once their life spans are over as part of routine housecleaning that is designed to maintain optimum system performance. As a result, freespace contains a wealth of information that can shed considerable light on how a device or storage media has been used.

As indicated previously, electronic storage media can be analogized to a library. The library has the card catalog that tells visitors what books are in the library as well as certain attributes about those books like name, publisher, publishing date, pages, subject area and where the books are located on the shelves. Like the library has the card catalog, the electronic storage media has the file system.

Like the card catalog tells library visitors what books are in the library, the file system tells users what files are on the media. Like the card catalog tells something about the kind of book, the file system reveals something about the file based on the file's extension. Like the card catalog can reveal other things about the book like its publication date, the number of pages and location in the stacks, the file system contains certain date stamp attributes of the file as well as its size in bytes and position on the media.

Whether the file system will contain information about deleted files depends on the file system. Not all file systems provide this kind of information, though. In essence, some file systems are just lazier than others. Some will actually delete the file system record of a deleted file, while others simply mark the file as deleted in the file system record. Those that actually delete the file system record do the equivalent of removing the card from the card catalog. Those that simply mark the entry for the file in the file system as deleted but actually leave the record, is like leaving the card in the card catalog and then simply marking it as a book no longer carried.

For those that do not delete the file system record but simply mark the file system record as a file that was deleted there ae two different things that could happen to those entries. For some file systems the file system record marked as deleted remains as an almost permanent record, depending on where in the file system hierarchy the deleted file record resides. For other types of file systems the deleted record remains until something new is saved to the media and the file system record overwritten.

Regardless of how the file system handles its entries for deleted files, the files themselves are typically not deleted even. Rather, when files are deleted either only their entries within the file system are deleted or their entries in the file system are marked as being deleted. In either case, the files themselves remain on the media until actually overwritten by something else subsequently saved to the media. In other words, the book remains on the shelves until it is physically replaced.

The recovery of deleted files is often considered part of the producing party's inaccessible data. In recent times, however, there simply is no reason not to make at least some effort to recover deleted files. After all, there are now plenty of automated systems that use either the filing system or data carving techniques to recover deleted files. Since these efforts are now totally automated the burden and cost of this effort is minimal and would seem unlikely that they qualify as "overly burdensome".

There are two principle techniques for recovering deleted files. One involves using the file system, itself. The other involves using file header signatures. Each of these are discussed in the sections that follow.

Using File System Data to Recover Deleted Files

Just as a library uses the card catalog to track what books it has on its shelves, a computerized storage device uses a filing system.

In other words, if a book were deleted in the library it would only be noted in the card catalog until a new book is actually stored in its location. Thus, using the filing system or the card catalog is one way to recover deleted files. This technique is further discussed in the following sections.

Physically, computer disks are comprised of concentric circles known as tracks. The difference between a floppy disk and a hard disk is that hard disks are a collection of disks referred to as platters. Each platter has two surfaces. The collection of tracks across several

platters is called a cylinder. The concentric circles of a disk are then divided into pie shaped sections known as sectors and each sector is typically 512 bytes.

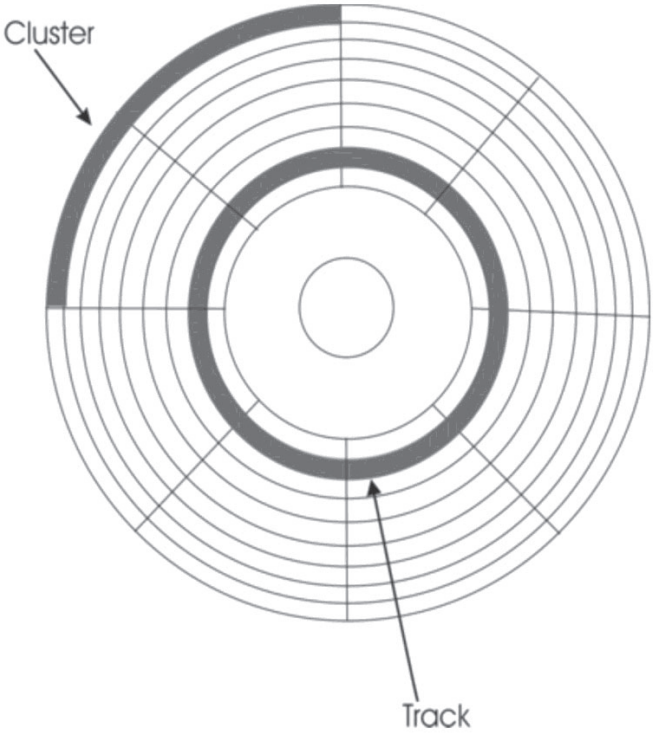


Figure 1 Computer Disk Tracks, Sectors and Clusters

Sectors are then organized into collections. Those collections are known as blocks that are often called clusters. The number of sectors that comprise a cluster is a function of the operating system being used and the size of the hard drive. If the drive is large but the operating system can only reference a few locations on the drive then each cluster must contain a large number of sectors. On the other hand, if the operating system can reference a lot of locations on the drive then the number of sectors in a cluster can be small.

The computer user is totally unaware that the disk is organized into sectors and clusters. Instead the user thinks only in terms of files. From a technical standpoint a file is an abstraction mechanism so that the user does not have to know how the data is physically stored.

Since the operating system is actually referencing clusters, when a file is saved it is saved to cluster(s). If the file is larger than one cluster then it is saved to as many clusters as necessary to hold the data. If the file is smaller than one cluster then the entire cluster is still reserved for that file, since a cluster can be associated with only one file. So, if the cluster is larger than the file or if the last remnant of a file is smaller than the last cluster used to store the file, the remaining space in the cluster is left unused and is referred to as file slack. The entire

process can be analogized to seating in a restaurant. If a party of three is seated at a table for four the fourth chair remains unused.

Since the operating system is actually referencing clusters, when a file is saved it is saved to cluster(s). If the file is larger than one cluster then it is saved to as many clusters as necessary to hold the data. If the file is smaller than one cluster then the entire cluster is still reserved for that file, since a cluster can be associated with only one file. So, if the cluster is larger than the file or if the last remnant of a file is smaller than the last cluster used to store the file, the remaining space in the cluster is left unused. The entire process can be analogized to seating in a restaurant. If a party of three is seated at a table for four the fourth chair remains unused.

The unused remnant has a technical name, slack space. Furthermore, there are some interesting side effects with slack space. More specifically, if the cluster being used to save the current file was used previously to save another file and the previous file occupied a larger portion of the cluster than is being occupied by the current file then the slack area will still contain the data from the previous file.

The location provided in the file system is not the same as the path. In the file system, the file location identifies the cluster where the file resides.

On a FAT file system the file name record only has the starting cluster location. If the file is larger than a single cluster the remaining clusters being used to store the file are recorded in the File Allocation Table itself. Thus, locating a file requires knowing the starting cluster number as well as all other storage locations that are contained in the File Allocation Table.

On an NTFS file system, the entire file locations are stored as part of the file record. The record is not a list of all the clusters individually but a record of all of the contiguous cluster ranges, which are called extents. In other words if a file was stored in clusters 5, 6, 7, and 10, the extents captured in the file system would be 5-7, 10.

While the absolute location of a file may not be very user friendly, there are often times when knowing this information can be very useful during forensic analysis. For example, if a file is deleted and overwritten but its prior absolute location is known then the file system information can be used to learn what file actually occupies that location currently. Other attributes about the overwriting file such as date stamp information could provide further insight into what happened to the deleted file and when it was overwritten.

If references to a previously active file still exist in the file system then there are techniques for recovering those deleted files, if four conditions exist. Those conditions are:

I The size of the file is known,

II The starting location of the file is known,

III The file is stored in contiguous clusters or the specific clusters in which the file is stored is known if it is not stored in contiguous clusters, and

IV The deleted file has not been overwritten in whole or part by some other file.

While Windows based file systems may contain the above four pieces of information, Apple based file systems do not. Thus, while file systems can be used to recover data on Windows based systems, they are not useful on Apple based systems and other file recovery techniques must be used.

The particular file system being used on a Windows based system determines the method that will be employed for the recovery of deleted files. The two principle file systems found on Windows based systems is the File Allocation Table (FAT) and the New Technology File System (NTFS).

The FAT file system is the one most frequently found on bootable hard drives for older systems like Windows 98 and earlier. It is also frequently used on flash drives. For FAT file systems it is simply assumed that the various segments of a larger file will be stored contiguously. Since this is often not the case recovering a workable file from these storage media using a FAT file system is never assured. If there is some encouraging factor it is that more and more intelligence was added to each version of Windows such that it became less likely that files would be fragmented and not stored contiguously but even there is no guarantee.

With the NTFS file system the actual storage locations are part of the data contained within the file system record. Thus, with NTFS system it is more likely that deleted files can be recovered unless they have been completely or partially overwritten by some other file.

File Allocation Table (FAT) File Systems

The FAT file system was developed in the late 970s when storage systems for personal computers were floppy disks whose sizes were stated in kilobytes as compared to gigabytes today. It is known as a linked list file structure.

In the linked list method every cluster is mapped in a data table called the File Allocation Table (FAT). Every entry in the FAT represents a cluster on the drive and each entry tells something about the condition of the data in that cluster. For example, it identifies whether the cluster contains data and whether that data is simply one cluster in the chain of clusters comprising the file or whether it is the last cluster in the chain. The following table identifies the meaning of the various FAT codes used by Microsoft in each of their FAT implementations.

MEANING	FAT12	FAT16	FAT32
Available for allocation	0h	0h	0h
Never used	1h	1h	1h
Reserved	FF0-FF6h	FFF0-FFF6h	FFFFFFF0-FFFFFFF6h
Bad cluster	FF7h	FFF7h	FFFFFFF7h
Last cluster in file	FF8-FFFh	FFF8-FFFFh	FFFFFFF8-FFFFFFFFh
Next cluster in file	xxxh	xxxxh	xxxxxxxxh

"h" indicates hexadecimal notation

In addition to the table there are directories. The directory contains various information about the file residing in the directory including the starting cluster number. To find all the clusters containing the file the operating system uses the starting cluster number listed in the directory record for the file. It then finds that starting cluster number in the FAT table. The cluster number in the FAT table identifies the next cluster number or whether the terminates in that cluster. If the FAT table references another cluster and not the end of the file the process goes to the referenced cluster number in the FAT table and continues until it goes through all of the referenced cluster numbers and finds an end of file marker.

In the example shown in the following figure, the operating system finds the files starting cluster number in the directory, cluster 9. It then goes to the FAT entry for cluster 9 and finds the number of cluster 16. It then goes to the FAT entry for cluster 16 and finds the number for cluster 1. It continues in this fashion until it discovers an entry in the FAT table containing the end of file marker at which time it has identified all the clusters containing that file; 9, 16,1,10 and 25. With that information the operating system can go to the disk and retrieve the data in those clusters.

The linked list provides several advantages over the earlier file management methods. First, files do not have to be saved in contiguous Clusters, although they frequently are.

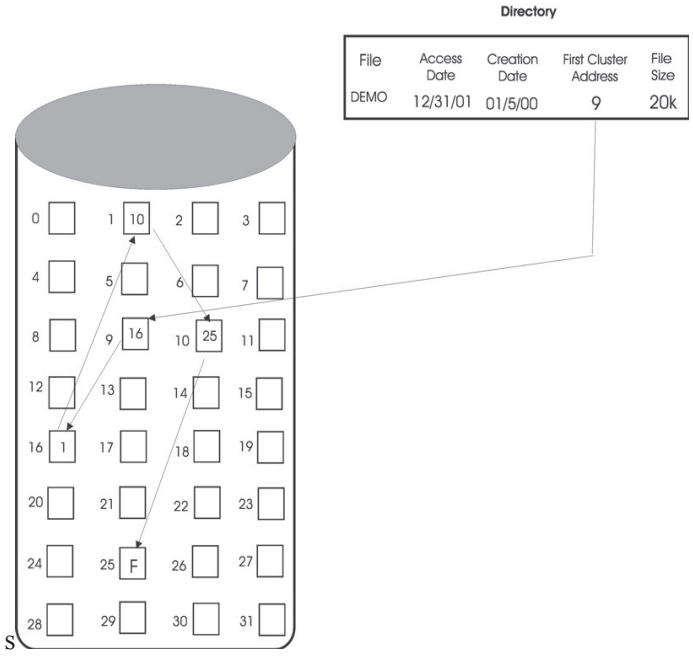


Figure 2 Linked List File Management

As a result, disk space utilization can be much higher. Second, the linked list can be used to track both used and free space clusters. Some of the earlier methods, even with linked lists designs, relied on bit mapped memory lists. As disk drives grew in size this method had to be abandoned, however.

File Directories

The FAT table is only one component of the file management system. Another component is the directory. As mentioned earlier, the directory contains the file name and its starting cluster number; but, it also contains additional data.

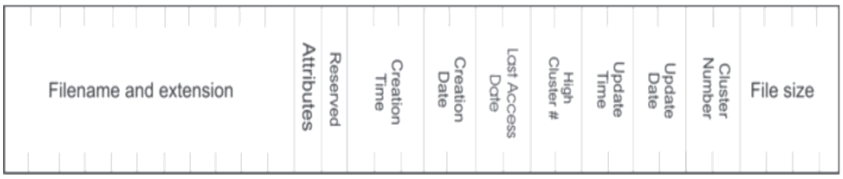


Figure 3 Windows Directory Contents for Windows 98 and Later

In FAT 32 schemes the directory entry is 32 bytes long. The contents of the directory entry contains all of the information shown in the following diagram.

For short file names, the filename and extension is eleven bytes long. For long file names the same 32 byte directory record is used; however, many directory entries are used.

The first byte of the filename can provide some special information. If the first character is E5h then the file has been deleted from the directory and the values of its cluster chain in the FAT changed to 0. If the first character is 2Eh then this is either the “dot” directory entry or the “dot-dot” directory entry. The determination can be made based on the cluster number. If the cluster number points to the directory itself then it is the “dot” entry. If the cluster number points to the parent directory then it is the “dot-dot” entry. In the case of long file names the first character of the file name is intelligently coded as a sequence identifier. The way the operating system knows whether long or short file names are being used depends on the value of the Attributes byte.

So, with long file names the file name is actually comprised of numerous 32 byte directory entries. While the first 32 byte record follows the short file name format each subsequent record can use most of the 32byte record length to retain the additional characters. After all, there is no need to keep repeating the file’s various time and date stamps or file size.

The attributes element is a single byte that is bit mapped. In other words, each bit has a significant meaning. Five of the eight bits are used to identify whether the file is Read-Only, a System file, a Hidden file, a Disk Drive volume name, a Subdirectory Name or Archive. A final combination of these bit values, 0Fh, indicates that the directory entry is for a long file name.

The next byte is reserved and not generally used. It is used, however, by the Windows NT and Novell operating systems to hold the first character of the deleted file name–the one replaced with E5h.

The next five bytes are for the file creation date and time. This feature exists only in Windows 98 and later systems using FAT 32. Prior to Windows 98 these bytes were reserved and had no meaning. The creation date and time identifies the date and time that the file was created on the drive. If the file is being copied from some other drive then its actual creation date and time could be much earlier.

Five bytes are required for the file creation date and time versus only four bytes for the file update date and time because the creation date and time is valid down within 10 milliseconds. The update date and time lacks this level of precision.

The last access date is also a feature found in Windows 98 and later systems. Notice that only the date value is captured. A time value has not been captured. The access date is changed whenever the file is used or its directory entry viewed in applications like Windows Explorer.

The high cluster number was a feature added for 32 bit Windows systems, Windows 95 and later. Notice both the high cluster number and the cluster number are 16 bit values. Clearly, a total of 32 bits are needed to reference the cluster number in 32 bit systems.

The update date and time is also known as the last write date and time. These values capture the date and time when the file was last modified. Unlike the creation date and time these values remain unchanged when a file is being copied from one drive to another.

The remaining date element is the file size in bytes. With only 4 bytes to work with, however, the maximum file size, in a directory entry, is 4 gigabytes.

Deleting Files

When files are deleted in a FAT file system they are not actually erased from disk. Rather, only the directory entry is changed and the next cluster value in the FAT is changed. With respect to the directory entry, all that happens is that the first character in the file name is changed to E5h. With respect to the FAT, all the values in the file's cluster chain are changed to zero. Notice that the first cluster number in the file's directory entry remains unchanged.

Since only the directory and FAT entries are effected by a deletion the original file data is still on disk. All that needs to be done in order to recover a file is change the first character in the file name back to some character other than the E5h deletion character and reload the FAT with the appropriate cluster chain entries. If the file was not stored in contiguous clusters it could be difficult to recover the entire file but if the disk is not terribly fragmented the chances are good that the file clusters will be contiguous.

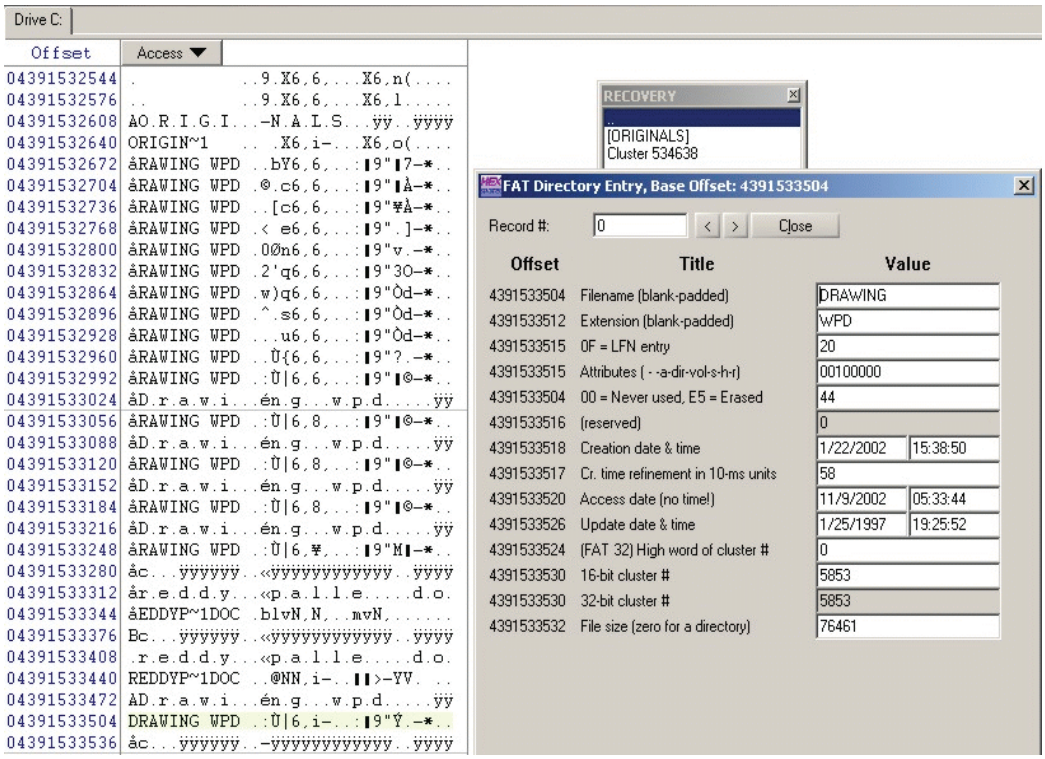


Figure 4 Illustration of Directory Index Contents

It is interesting that the file name is not deleted for a deleted file. So, whether or not a file used to exist on the disk can be determined simply by reviewing the directory lists. The figure illustrating the directory index contents, shows the first two sectors of a directory named RECOVERY. The contents of that directory are comprised of one subdirectory named ORIGINALS and a number of 32 byte directory entries that are recorded in cluster 534,638.

The figure is comprised of three windows. There is the big window showing the contents of the Recovery directory and the offset for each entry. There is another window on top that shows the decoding of the directory entry for a file named “Drawing. WPD”. In between these windows is another smaller window that shows the directory name, subdirectory list and the directory’s cluster chain.

Notice that most of the directory entries are for file names starting with the å (E5h) symbol, which means that those files have been deleted. On the next to the last line is a file name without the å symbol named “Drawing WPD”.

I use the file Drawing.WPD to demonstrate file deletion and recovery. It is easy to see how many times the file has been deleted and recovered. Each time the file was recovered a new directory entry was created.

This interesting feature applies to all kinds of computer objects. Short cut files, files with a LNK extension, are just one example. By examining directory entries for short cut files the examiner may be able to spot machine configurations that were not apparent on a physical examination of the machine or even links to files or other programs that have been deleted or uninstalled.

Moving files has a similar effect. The file name entry is deleted in the original directory and a new entry is created in the new directory. If the movement is on the same drive volume then the other parameters such as file creation date and time are unchanged. If the file is moved to a new drive volume then a new creation date and time is established.

New Technology File Systems (NTFS)

The NTFS file system was initially developed in the early 1990s by Microsoft for its NT class server operating system, although it was inspired by Microsoft's earlier collaboration with IBM on the High Performance File System (HPFS). Since its introduction in July 1993, the NTFS file system has become the primary file system used by all Windows based systems as well as many large capacity storage systems like external hard drives. It is a much more robust system than the earlier FAT file system that was developed in the late 1970s.

The NTFS system is actually a collection of different files that when taken together provide considerably more capability like recoverability, security, and capacity than its older sibling FAT. Unlike FAT, the NTFS system is comprised of files that sit in the storage area like every other file. By contrast the FAT file table, for example, was not a file. Rather, it was a reserved area where other data could not reside. The following table list the primary NTFS files.

Primary NTFS File System Components	
File Name	**Contents Description**
$AttrDef	A table of attributes names, numbers and descriptions
$BitMap	Bit map file indicating the condition of each cluster as allocated or not
$BadClus	Clusters with bad sectors
$Boot	Boot sector and boot code for file system
$LofFile	Contains the journal that records metadata transactions
$MFT	A collection of file records for every file and folder in the volume. Each file record has the header signature of FILE0.
$MFTMirr	Backup of entries in the MFT
$Secure	Information about security and access control
$UpCase	Uppercase version of every Unicode character
$Volume	Volume information like label, identifier and version
$Extend	A files system directory containing optional files like $Quota, $ObjId, $Reparse or $UsnJrnl

Much of the system's characteristics are also definable, like MFT record size and MFT location on the storage media. Unlike FAT, NTFS can be placed anywhere, although the so called MFT Zone has recommended sizes and placements. Two of the more significant NTFS system files are the Master File Table (MFT) and the Changes Journal ($UsnJrnl). Each are discussed in the following sections.

Master File Table ($MFT)

The MFT is the central repository for file and folder information about the storage media's content. It typically is a collection of one kilobyte (1,024 bytes) records about the files and folders on a storage media. The record is divided into several sections that comprise a header for the record followed by several metadata fields and even some resident data.

The metadata fields are of several types and contain a collection of information like date stamps and the list of clusters where the file resides. This latter element is quite significant since if a deleted file's MFT records can be found, the file's exact placement on the storage media is known. With the FAT system a deleted file's placement could only be assumed, since all that was really know was its starting cluster.

Part of the MFT record is actually used to store a file's data. If a file is small then the entire file can reside within the MFT record. This is a much more efficient use of storage space when the files are small. If the file is larger than the data area of the MFT record then the rest of the file is stored outside of the MFT in the normal data area.

Change Journal ($UsnJrnl)

The NTFS change journal is a file that captures data about the changes made to a file. The data it captures do not involve the contents of the file but rather attributes about the file in the file system such as the following.

- Time of change
- Reason for the change
- File/directory's name
- File/directory's attributes
- File/directory's MFT record number
- File record number of the file's parent directory
- Security ID
- Update Sequence Number of the record
- Information about the source of the change

While the data within the change journal is not useful for file recovery it can provide useful information for other forensic purposes, including spoliation analysis.

Deleting Files

As with the FAT file system, when files are deleted in a NTFS system the file record is marked for deletion. Within the header of the MFT record are two bit flags that function as semaphores to indicate whether the record is in use (active) or not in use (deleted). One bit is used if the record is for a file while the other bit is used if the record is for a folder.

Clearly, just as with FAT, neither the file record in the NTFS system nor the file data itself is actually deleted. While neither the file record nor the file data are actually deleted, other aspects of the NTFS file system are deleted or zeroed out in the same fashion that a file's cluster chain within the FAT table was zeroed out. Specifically, the index ets.

Besides knowing exact location of the deleted file, the NTFS system is also different from FAT in that its file system record can be overwritten. In an NTFS system, new files will occupy the earliest positions of deleted files in the NTFS. For example if a NTFS system has 10 files and the 4th file is deleted then when a new file is saved to the media it does not become number 11. Rather, it overwrites and becomes number 4. For a FAT system when new files were saved to a directory they were simply added to the end of the list of all the other files in the directory, including whatever files had been deleted earlier.

Files Systems that are not Friendly to File Recovery

There are, in fact, many different file systems for electronic media. While both FAT and NTFS take a "lazy" approach to file system maintenance and leave traces of a file's prior existence after they have been deleted, not all file systems are like that. The Unix file system, which predates even FAT, is well known for actually wiping a file's file system record after it is deleted. As a result of this clean-up there is no trace left of the file's prior existence, at least within the file system.

As it turns out the Unix file system is the model or ancestor of many other file systems such as the Ext2 and Ext3 file system used with Linux and even the Apple Hierarchical File System (HFS) and HFS extended (HFS+) that is used with Apple's latest OS-X operating systems.

Of course, when the file system record is deleted and wiped, it is not just the ability to recover a deleted file that is lost. All kinds of other information about the file is also lost like its date stamps. Thus, losing the file system record costs more than just the ability to recover the file. After all, it is not uncommon that even when the file system record remains that the deleted file is still not recoverable because it has been overwritten by another file as a result of other ongoing computer after the file was deleted.

Using Signature Analysis to Recover Deleted Files and Folders

Another way to recover deleted files involves the use of file signatures. File signatures were discussed earlier as a way to validate that a file matches its file extension and is the kind

of file that one expects a file to be. As explained earlier, signature analysis examines the first few bytes of a file. Within those first few bytes is usually a unique combination of characters that identifies the file type. Remarkably this same technique can be combined with a scan of free space and/or slack space as a means to locate and recover deleted files.

With the ability to use the file system as a means to recover deleted files there may not seem like anything else is necessary. Actually, though, signature analysis is a highly important and useful way to recover deleted files when file system information is not available, which could be the case in any of the following circumstances.

The first reason is that there may not be any remnants that files ever existed in the file system. This kind of condition can happen in several different situations. In the case of file systems like the NTFS file system the deleted file record could be overwritten when new files are copied onto the media and entries about those files are made into the MFT.

The second reason is that even with a file system like FAT where all instances of a file's activity are retained, the directory which once retained the file system's records of a file has been deleted and overwritten. Thus, similar to NTFS systems the file system record is not longer available.

The third and final reason is when the file system does not even retain references to deleted files. This could be the case with Apple file systems like the HFS and HFS+ file systems. Unlike FAT and NTFS file systems where references to files are simply marked as deleted, the Apple file system actually deleted the entire file system entry when a file is deleted. Thus, for Apple systems this is the only way in which deleted files can be recovered.

This is also the result when a partition has been formatted. That process resets the file system, although the data in the data area of the drive can still exist. In such a case it could be located and recovered by way of a file signature search.

Detecting Files for Recovery

Whether a file has a unique signature can be determined by examining similar files in a hex editor or by consulting the standard or specification describing that file type. Since the signatures reside in the first few bytes of a file, the review of free space looks only at the start of a cluster. As also explained earlier, files are stored storage units called clusters. Although the storage media has its storage area divided into units known as sectors, the file system groups sectors together to form clusters. Thus, the smallest unit that will be used for storing files is clusters. Since clusters are the smallest file storage unit, the start of any file will begin at the start of a cluster. As a result, the search process need only check the start of clusters in free space to see whether a recognized file type resides there. Consequently, it is not necessary that the process scan the entire are of freespace. Rather, it is only necessary that the process check the start of clusters for the file signatures of the file types that are of interest, at least if the interest is the recovery of documents. The particular file types that are of interest could very well depend on the type of case.

Despite that document recovery may focus on the start of file clusters it is still possible that documents could be more complex and contain embedded objects like images. In certain cases, even these embedded objects could be of interest, particularly when the entire document may not be recoverable but certain document fragments such as these embedded objects are desired. In such cases, it is possible for signature analysis to be used to recover these items as well. In such cases, the process would scan all of freespace and file slack, not just those parts at the start of a cluster, in an attempt to find and recover the desired objects.

Determining How Much to Recover

Simply spotting the signature of a desired file type is not enough to ensure its recovery, since there remains the question about how large is the document. Thus, once a recognized file type is spotted the next question becomes where does the file end and how much data should be recovered. Without this information or if the information is wrong the file recovered may still not be usable. Instead it could end up being a file that cannot be opened and view because the structure expected or needed by the viewing application to display the file contents will not be present. To solve this problem there several different approaches.

The first approach is that for some files types like ZIP, JPG and PST files, just to mention three, the length of the file is often stored in the file's header along with the file signature. Whether a particular file type includes its size as part of its header information is also described in the file's standard or specification. Thus, by consulting the specification one can learn the location where that information is stored in order to know where to look when trying to recover such files.

While many kinds of files can contain such information, it could be binary which makes the information more difficult to spot during a visual inspection. Consequently, consulting the file's standard or specification is likely the best means of learning where this information is stored and devising plans to recover such files.

A second approach for determining how much data to recover after locating the file header is to scan further in the file looking for other markers such as the end of file marker. This kind of information could be easily discerned by examining a number of files in a hex editor. Of course, consulting the file's standard or specification is also a good way to learn what the marker could be and how it differs from version to version of the file type.

Absent the above two methods that provide a more definitive approach to determining file length, the third approach follows a more trial and error method. This approach can include a collection of different techniques for calculating file size.

One of the other methods could be to search forward through the data examining the start of other clusters looking for other file signatures. If subsequent clusters are found having the file signatures of similar or other file types, the assumption could be that these subsequent signatures are the start of new files. Thus, the length of the file desired for recovery begins at the starting file signature and ends at the last piece of data in the cluster just prior to the new file signature in the next new file.

Another technique is to just make assumptions about how much data should be taken after the initial file signature is found.

Limitations to File Recovery

Signature analysis provides the ability to search the free space on a drive and find instances of files having the requisite starting byte signatures and ending trailers. The data carving technique then takes everything in the middle and reconstructs the file. Despite this great conceptual idea there can still be problems with the process.

While the starting point of a file is pretty well established based on the existence of file signatures, the weak point is that the amount of data used for extraction assumes that the file's data resides entirely on contiguous clusters. If the recovered file was actually fragmented then its various components are not stored in contiguous storage locations. As a result, when all of the data between the starting signature and ending trailer are recovered and the file reconstructed, it likely will not function. In fact, when one views the file through a Word or Excel viewer, for example, the person is likely to only see a large volume of non-sensical special characters.

Sometimes it is possible to consult other file system information and make intelligent decisions about where the other portions of the fragmented file resides and then recover the various portions and reconstitute the pieces as a single file.

Another limitation is that the entire file is not even still present on the media. It is possible that later portions of the file have been overwritten by some other file either active or deleted. In some respects this is another angle on the fragmentation possibility except that the deleted file is just not fragmented. Rather, it has actually be partially overwritten and will never be recoverable.

While the above works with traditional platter devices, SSD drives introduce complications to the techniques. The most significant complication is the SSD TRIM function. The Trim function is a process run by the drive that keeps it clean. In the process it will garbage collection.

Of course, the ultimate limitation to file recovery is that the entire file has been overwritten either by other files or with data security applications like file wipers. If the file has been overwritten then neither file system techniques nor file signature techniques can recover the file.

Summary

Just because a file is deleted does not mean it cannot be recovered. In fact, the potential for recovering a deleted file exists until it is overwritten by some other file.

The mechanics for recovering a deleted file can differ from system to system. For Windows systems there are two principle methods. One is by using the file system, since in a Windows system the file system entry also remains until it is overwritten by another entry or

another file. Whether the file system entry is overwritten by another file system entry or another file depends on the type of file system being used.

The other method for recovering a deleted file in a Windows system is by searching the start of freespace clusters for header signatures of the files of interest. Once they are found and a calculation of the file length determined the data in between the header start and the calculated end of file can be recovered.

For many other file systems, including the Apple file system, HFS+, there are no file system artifacts that can be used for file recovery. With these other file systems, the file record is actually deleted as well or, as in the case of Apple machines, it is wiped. As a result, the only method for recovering deleted files with these other systems is the same kind of data carving technique that can also be used on Windows systems where freespace is searched for recognized file headers at the start of clusters.

CHAPTER 9

Computerized Search

Introduction

A significant factor in the high cost of e-discovery is that counsel prefers to use manual techniques for document review. They have preferred to "put a lawyer's eyes on every document" because they have thought that it produced a better result. Consequently, they staff large teams of associates to laboriously plod through the documents at great expense.

The Rand report notes that counsel has tended to employ labor based review techniques which are expensive and have been proven to be both inefficient and ineffective. What is not often attempted is more technology based techniques such as various computer assisted review methods.

Clearly with the volume of digital evidence in many modern litigations, it simply is not practical to take a “boots on the ground” approach to document review and analysis. Certainly the volumes of data make it commercially impractical to use anything other than computerized techniques. Moreover, many other fields of human activity have demonstrated that the weak link in the chain is often the human element. As a result, automation and statistical sampling techniques are often used in other fields not only for economic reasons but for increased accuracy reasons as well.

The weakness in the human element of document review and analysis is even reflected in Practice Point 1 of the Sedona Conference’s best practice commentary on search and retrieval methods in electronic discovery. Practice Point 1 states that,

In many settings involving electronically stored information, reliance solely on a manual search process for the purpose of finding responsive documents may be infeasible or unwarranted. In such cases, the use of automated search methods should be viewed as reasonable, valuable, and even necessary.

For all of the above reasons, computerized search and document review techniques are essential in e-discovery. Furthermore, their use will likely continue to become more prevalent. Practitioners, who have not used them in the past, will be forced to implement these technologies and techniques as digital evidence and e-discovery force them to forego the traditional “boots on the ground” approach.

In the sections that follow the author examines various computerized search methods with which litigators should be familiar and ready to employ in their cases as needed.

Understanding the Search Problem

The solution to the search problem is not a single silver bullet issue. Indeed, the problem is multifaceted and includes things like linguistics, effectiveness and technology. The following sections examine each of the problems.

The Problem with Linguistics

The linguistic problem is one that is well known and has existed for some time. The most often cited example illustrating the effect of linguistics on the search problem is the 1985 Blair and Maron Study. The Blair and Maron Study is best known for its examination of a litigation matter involving a Bay Area Rapid Transit (BART) System vehicle that failed to stop at the end of the line.

The litigation team involved attorneys and paralegals experienced in complex litigation and document management. While the case clearly occurs prior to the ESI of today, the case did involve a computerized document management system with full text retrieval capability.

The litigation team believed that it has been able to find more than 75 percent of the relevant documents. The study, however, revealed that their actual recall was only about 20 percent. Further analysis revealed that linguistic issues were a significant contributor to the low recall rate.

Blair and Maron found that the words used by the two sides to refer to the relevant issues were entirely different. For example, defendants referred to the accident as “the unfortunate accident”. Plaintiffs, on the other hand, referred to it as a “disaster”. Third parties like witnesses or vendors used terms like the “event”, “incident”, “situation”, “problem” or “difficulty”. In the end, the linguistic differences were far more than realized by the legal team and this underestimate adversely affected their work.

The Ineffectiveness of Manual Review

In more recent times other groups have also studied document review success rates and even compared different methods. The Text Retrieval Conference (TREC) sponsored by the National Institute of Standards and Technology (NIST) has studied document retrieval issues at many conferences.

Document retrieval effectiveness is typically studied from two perspectives. The first is precision while the second is recall. Precision measures how well the retrieved documents meet the search criteria. Recall measures how well the retrieved documents matched or were relevant to the subject of the search.

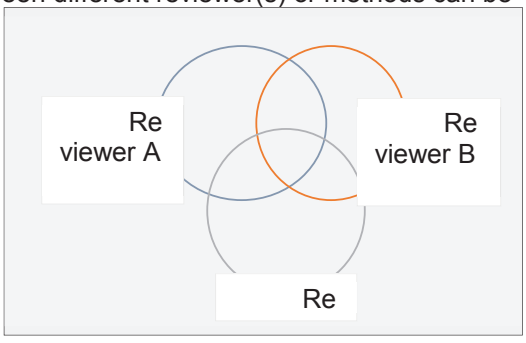
In 2009 the TREC conference compared results of manual document review with technology assisted review. Technology assisted review can encompass all kinds of search retrieval technologies.

The results revealed that technology assisted review outperformed manual reviewers by a significant amount. More specifically, manual reviewers had average recall rates of 59.3 percent while technology assisted reviewers had rates of 76.7 percent. With respect to precision, manual reviewers had average rates of 31.7 percent while technology assisted reviewers had average rates of 84.7 percent.

Results such as the 2009 TREC analysis suggest that technology assisted review is superior to manual review. So, even without consideration of the economic aspects of technology assisted review, there are quality and performance reasons as well and these tend to clearly prove the superiority of technology assisted review over the old manual review approach.

Finding the documents is not the only problem with manual review. Another significant problem is interpreting them. In other words, whether a document is responsive or relevant is often a subjective determination and can depend on the reviewer making that determination.

The consistency of document disposition between different reviewer(s) or methods can be measured using overlap. Overlap is the number of documents that have identical dispositions by different reviewers. In other words, it is the intersection of document populations by different reviewers



Several different studies have found the overlap percentages between document reviewers performing manual review range between 15 and 49 percent.[9] Even at the higher

[9] Ellen Voorhees and Donna Harman, Overview of the Eighth Text REtrieval Conference (TREC8), (circa 2000); Herbert L. Roitblat, Anne Kershaw and Patrick Oot, Document Categorization in Legal

percentage this means that there are significant differences between manual reviewers and putting a lawyer's eyes on every document does not provide a better product. Computerized search, therefore, not only hopes to bring greater economy to the review problem but also consistency and repeatability to the retrieval problem as well.

The problem with the effectiveness of manual review is actually multifaceted. One facet is that whether something is relevant or responsive is a highly subjective determination. Many factors can influence one's judgment of whether something is relevant or responsive such as subject matter expertise and familiarity with the party's business practices or systems. Furthermore, that judgment can change as one's theory of the case changes after months of discovery that includes document reviews, depositions and other discovery exercises. Also, that judgment can change from lack of concentration or fatigue after days and days of sifting through documents.

Another reality is that document review will not be completed with a single pass through the documents. Rather, there will be several iterations as the parties squabble and as different issues percolate to the top forcing changes to the theory of case. Consequently, what is needed is a method that can efficiently, effectively and iteratively query the documents to find those of interest. In the information age with ESI manual document review is simply not the answer.

Other industries with high volumes of repetitive tasks have long recognized the weakness of the human element in their processes and have looked for ways to remove it. These other industries have relied on automation and statistical sampling to solve the human problem. Automation will reliably apply a set of rules to repetitive tasks while humans are not as reliable.

Statisticians have long known that statistical sampling not only provides a cost saving facet but an improved accuracy rate as well, at least when human effort is part of the process. Even the organizers of the Legal Text Retrieval Conference (LegalTReC) have questioned whether their prior assessment of various retrieval techniques is accurate because they rely on human reviewers to judge and assess the results.

The second problem with the all manual approach is it is just not that efficient either. In addition to being more effective, sifting and searching can be much more efficiently performed by computers that tirelessly follow preprogrammed rules at great speeds. Even when automated search is not that effective, such as with poorly planned keyword searches, statistical sampling is both more economical and more effective than 100 percent human review. Combining the two, keyword searches or other automated methods and statistical sampling, can provide much greater efficiency and effectiveness than using only manual review.

The Problem with Technology

The problems with computerized search are not limited to linguistics or even disposition. There are technology issues as well. The primary obstacle is that document text

---

Electronic Discovery: Computer Classification Versus Manual Review (circa 2009); and Maura Grossman and Gordon Cormack, Inconsistent Assessment of Responsiveness in E-Discovery: Difference of Opinion or Human Error? (circa 2012) and also Technology Assisted Review in EDiscovery Can Be More Effective and More Efficient Than Exhaustive Manual Review (circa 2011)

must be “readable” by the search technology. Even that single issue has several other technical challenges that must be properly managed as described below.

Machine Readable Text

The first problem in having documents that can be read by computer is that they must have readable text. Documents like graphics, even PDFs, do not have readable text and they must first be converted to readable text.

Even though PDFs can have readable text, they could be graphic images too and there is not an easy way to know if they have searchable text or are only graphic images. Of course, even normally searchable text documents like Word documents can still have embedded images which can only be read if they are converted to searchable text.

The challenge for machine readable text is not just the difference between images and text. Sometimes it also involves document format. For example, a compressed archive (zip file) may contain machine readable text documents but the search engine must be able to open the archive and decompress its contents before its contents are readable.

Similarly, the document could have structured text like in an XML document that must be converted to its presentation format in order to be searched properly. Thus, the search engine needs to be able to make this conversion or some other kind of work around will be required.

Clearly, it is imperative that the users of computer search technology understand the capabilities of their search engine and ensure that it is actually capable of performing the task it has been asked.

Indexed or Not Indexed

The next issue is whether the search engine is indexed or not indexed. An indexed search tool relies on the index that it creates in order to actually locate documents having the search terms. Not indexed search tools scan through the document to determine whether or not the terms exist.

An indexed search tool will need time to construct the index but once it has been built searches can be run very quickly. Not indexed search tools do not need to build the index but for each search iteration they will need to traverse the entire document population. Considering that keyword searches will often require multiple iterations, it is usually best to use indexed search tools.

In addition, indexed search engines tend to have more robust features like Boolean connectors and proximity locators. These features are essential at reducing false positives and increasing the effectiveness of a search. Non indexed search engines typically do not have these features.

Technology Solutions

There have been a number of different solutions devised to provide computerized search capability. They include approaches like keyword search, context search, predictive coding and concept clustering. Each of these is described in the sections that follow.

Keyword Search

Keyword search is probably the best known and easiest to implement of the computerized search technologies. Keyword search has the highest precision rate of any other search technology. It also tends to have the lowest recall rates of the computerized search methods. Thus, it will accurately find documents with the search criteria but the documents may not actually have any relevance to what the user was looking.

There is a caveat to the recall rate of keyword searches, however. With keyword searches, recall can be a function of the keyword search. In other words, better constructed keyword searches will provide higher recall rates than poorly constructed keyword searches. The effectiveness of this method is highly dependent on the skills of those using it

Single term searches will have the lowest recall rates while more complex searches such as those with Boolean connectors and proximity locators will produce higher recall rates. The Boolean connectors are not only a means to provide additional discriminators to reduce false positives but they also allow consideration of linguistic differences in the search criteria. Other features like stemming and wildcards can also improve the recall rate of a keyword search.

Thus, the problems with keyword searches are often the linguistic issues as highlighted by the Blair and Maron study discussed previously. These limitations can be overcome, however, with more sophisticated use of keyword search technology that use features like stemming, wildcards for misspelling and various Boolean connectors to handle different linguistic differences.

If there has been a failure of keyword search in legal applications it has come from two causes. First is the single term, fire and forget approach. In other words, it is overly broad with single word search terms. At the same time, it is an inadequate use of more sophisticated criteria such as stemming, wildcards, Boolean connectors and proximity locators. In addition, the single terms lacked adequate linguistic analysis in order to determine whether there were alternative terms that should be used.

The second failure is that there is inadequate or no testing of the search term performance in an effort to improve performance or assess through sampling or other means that false negatives have been avoided and false positives minimized. Indexed search engines permit fast iterations of various search criteria. When the results are exported to tabular reports identifying attributes like the file name, location, date stamps, search term and about 100 characters either side of the term for context, keyword search users are able to review and assess the effectiveness of the criteria and make adjustments to the criteria based on their learning.

Both of these failures, overly simplistic search terms and untested search terms, are tremendously inefficient at finding the documents of interest. The inefficiency is even further compounded when the results are then subjected to full scale manual document review. While keyword search users may think that developing the terms is simple, there is a big price to pay with what comes next. Thus, the best approach to keyword search methods combines more sophisticated search terms and testing of the search terms in order to validate the results are actually what is desired.

Keyword search methods can be much more efficient than other methods discussed later because keyword search terms can be run against forensic images. Thus, there is no need to extract data and place it into some other document management system that would also require processing and production. Thus, much efficiency can be achieved if the original forensic images and the tools typically used for examining them are used to cull the document population as much as possible.

With this in mind, the keyword search process can be further bolstered with two other techniques. One is data analytics and the other is statistical sampling.

It is hard to predict where relevant evidence might be found. Thus, any attempts to cull the document population prior to search as a means to limit false positives has the potential for missing otherwise important evidence. At the same time one would be very surprised at the places where keyword search terms can be found and would thus trigger the review of that document.

One way to restrict the chance of false positives from keyword search while realizing the economical benefits of searching the forensic images is to include data analytics when reviewing the search results. As an example consider that both Windows and Apple based system provide search capability of their storage contents. This search capability is provided by indexed search engines within their systems. Consequently, if the keyword terms exist on the storage media there is a good chance that those terms will also exist in these system indexes. By including data analytics into the search result review one could quickly determine that the existence of the system search indexes into the population of documents with hit terms is actually a false positive. This same aspect can be achieved when a Windows registry file containing the name of a document containing a search term appears in the search results. In that case data analytics can tell the user that this is a false positive and should be ignored.

Statistical sampling is another tool that can be used to review search results and more economically determine whether search terms should be revised. In other words, after searches are run and the populations divided into their related groupings, samples can be taken and reviewed as a quality assurance measure that the results are as expected. This could be especially useful when documents are cleared after privilege review. Since keyword search has such good precision results, the documents not containing the search terms could be reviewed using acceptance sampling in order to confirm the validity of the results.

Context Search

For some, the silver bullet to the shortcoming of keyword search had been context search. Simply stated context search adds context to the search criteria. For example, when one is searching for jaguars are they searching for football teams and their players, automobiles or large cats on the African plain?

In essence, context search improves the keyword search solution by addressing the problems present in keyword searches related to synonymy and polysemy. Synonymy is a common linguistic issue where different words are used to express the same concept. Polysemy is where the same word can have different meanings such as the jaguar example mentioned above.

Context search solves both problems by embellishing on the traditional keyword index search model. More specifically, the index process of a context search engine collects more data, commonly called vector data, about a document's terms such as its location (like headers, titles, page or paragraph text) within the document and relation to other terms. The additional data along with synonym expansion, fuzzy logic and stemming technology are used in an algorithm to identify and usually rank the documents having the best match to the likely search objectives.

So, the context search technology bundles numerous advanced techniques in a simple user interface. Remarkably its simplistic black box approach can also be its shortcoming. After all, all of these additional components such as the additional data captured during the indexing process, the synonym library and algorithm are usually closely guarded secrets. Furthermore, they cannot be modified by the user.

As mentioned previously, concepts like relevancy and responsiveness can be quite subjective. What might be responsive or relevant to one person is non-responsive or irrelevant to another. Yet, that determination of responsiveness or relevancy is controlled by the algorithm used in the context search engine.

In the final analysis, context search is a sophisticated keyword search. The real difference is the extent to which features like synonym usage, relevancy ranking and concept discrimination have been programmatically scripted into the search engine functionality. The same capability is available with traditional keyword search tools but the implementation is totally dependent on the user's skill to incorporate those features in the keyword search query.

Since the user cannot modify the algorithm's used by the context search tool, it is possible for sophisticated users of sophisticated keyword search tools to even exceed the capability of context tools. After all, relevance and significance are subjective determinations.

What context tools offer is a sophisticated capability for less sophisticated users. What they do not offer is a silver bullet solution. They have limits. Furthermore, users are likely not to know how to assess those limits since their machinery is hidden "under the hood". Of course, sometimes this can be useful when negotiating search protocols, since one party may be more motivated to impede the search process than to promote it. In those cases, a context search engine may make it more difficult for such an opponent to game the search process.

Predictive Coding

The latest search solution is predictive coding. Predictive coding is not a search tool in the more traditional sense, since it not really term based. Rather, predictive coding employs statistical concepts to measure a document's contents. Those measures are then captured in a baseline set of documents commonly called the training set. Those baselines are then applied against the scores of other documents in the population to determine similar or dissimilar documents.

The overall process is comprised of several steps that range from

- selecting and scoring the baseline documents,
- comparing the population against the baseline, and
- evaluating the resulting scores for accuracy.

Statistical techniques are heavily employed throughout the process. Statistical theory is used when determining the number of documents to be used in the baseline set of documents. They are used again when applying the baseline documents to the population and then finally again when assessing the accuracy of the results.

The following table illustrates how predictive coding works. After the training documents are manually reviewed and scored the document text is read by the computer and a fingerprint of sorts is developed. The fingerprint ignores "junk" words also known as "stop" words like "the", "an", "is", "on", "a", "this", "that" and others and only considers the more significant terms. Depending on the application, users may be able to edit the list of "junk"/"stop" words.

After eliminating the "junk" words the documents are scored by cataloging the specific words and the count of their occurrence in the document. The scoring of the document in terms of its significant words and their count provides a kind of fingerprint for that document. When the score or fingerprint of all of the training set documents is determined statistical values can be calculated that can be used to evaluate other documents in the population based on statistical theory. The score of the training set documents is compared to the score of the documents in the population and a difference computed that can be used to quantify how different each of the population documents is from the training set documents.

TRAINING DOCUMENT			POPULATION DOCUMENT	
TERM	COUNT		TERM	COUNT
Word 1	3		Word 1	1
Word 2	2		Word 2	
Word 3	4		Word 3	3
Word 4	1		Word 4	
Word 5	3		Word 5	5
Word 6			Word 6	
Word 7			Word 7	3
Word 8			Word 8	4

Predictive coding cannot be used for all kinds of document review. There are some document types that it cannot do or will not do well such as:

- Image based documents without searchable text;
- Non-text based documents converted to text such as with Optical Character Recognition (OCR) where the accuracy rate is lower than 99 percent;
- Text based documents where the quantity of word terms is small such as fewer than 100 words; and
- Numerical documents such as spreadsheets.

Clearly, predictive coding is not simply application of a magic technology. It is not a simple push of a button. Rather, it is a process that may incorporate some automated technology; yet, much of the process involves manual review for the evaluation of the baseline documents and verification of the result sets.

So, there is considerable overhead when using predictive coding technology. Consequently, it is probably best suited for extremely large document sets and may have a much smaller payoff for smaller and even more garden variety cases.

The extra overhead is also not its only drawback. Indeed, it is very technical and there will be a cost associated with the expertise necessary to pull it off.

Besides economy and reliability another of the attractive attributes to predictive coding and other technology assisted review techniques is its repeatability. Yet, predictive coding can have variability as a result of the statistical techniques actually employed when applying the baseline documents to the population. Indeed there are actually quite a number of different statistical, machine learning models that can be employed such as:

- Expectation maximization,
- Naïve Bayes classifiers,
- Latent semantic indexing,
- Support vector network,
- K-Nearest Neighbor,
- Locality Sensitive Hashing,
- Neural Networks, and
- Hidden Markov Models to name a few.

While all of these models should produce repeatable results within themselves, different vendors could be using different methods and thus different results could be produced by the different products. The differences likely will be small but they could produce a slightly different point estimate. When viewed as a range of documents the differences would likely fall at the fringes and not near the center of the normal distribution.

The science at the heart of predictive technology is often quite old. Its more recent appearance can be attributed to the computing power required to run the calculations. They simply were not practical until more recent times and more powerful computers.

Like the other technology assisted review methods, predictive coding is not without its issues as well. First, one must find the training documents and a suitable number must be selected. In addition, considerable effort can be expended evaluating those since they are key to the coding of the remaining population.

Second, there are two competing aspects to any statistical approach; confidence and precision. To have high confidence often means a broader precision range. To have high confidence and a narrow precision one must have larger samples or more homogenous populations. Achieving the more homogenous populations can require separating the document populations into similar document types. For example, it may require separating e-mail messages from other text documents.

In addition, it could also require developing baseline sets that are more focused on specific issues. A quantum claim, for example, has three parts: liability, causation and quantum. Similarly, in a construction case there could multiple causes of claims.

In statistical theory, stratification provides a means to bring higher confidence and greater precision while using smaller sample sizes than if one large sample had been taken. Since the overall goal with predictive coding is both economy and reliability, developing separate baseline sets would be overall more effective than having a single baseline set.

Third, manual review is still a component of the process both in developing the baseline training sets and in assessing the final results. Since manual review is inherently unreliable and inconsistent, the reliance on manual effort to identify baseline sets and evaluate performance could provide a significant defect to the methodology.

Fourth, the methodology is considerably complex once statistical theory is factored into the equation. The added complexity makes a considerable target for an opponent. If they are successful in finding a soft underbelly, all that may remain is a scientifically, quantifiable measure of incompetence.

The bottom line is that predictive coding is an accepted methodology for document review and disposition. But then it relies on scientific principles that have been accepted in all kinds of other disciplines, like DNA, fingerprint analysis and even document deduping with algorithms like the MD-5 hash. All of these methods rely on statistics to develop probabilities that are persuasive even though not absolute.

Whatever it is or ultimately may be, predictive coding is not an “easy” button or silver bullet. It offers increased economy and reliability over manually reviewed documents. It is also like taking a swim into deep water with strong currents. It really brings to life the old saying, “swimming with the sharks”.

Concept Clustering

Concept clustering is a means to gain greater efficiency by grouping like documents. The efficiency from the grouping can occur in several different ways.

First, clustering can group documents of similar subjects. Once grouped, reviewers may not need to review all documents in the group before making a determination about the significance of the documents. Rather, after looking at only a few documents in the group a reviewer can dismiss all of the documents in the group.

The technology used for clustering is similar to predictive coding. A baseline set of documents may not need to be created. Rather, the statistical technology simply reviews the document contents and quantifies those having similar content.

The second approach to clustering is grouping like kinds of documents. In other words if all invoices were grouped together, a manual reviewer may be able to develop a rhythm for reviewing and dispositioning a document by looking at the content at a particular location. If all of the documents are the same then a reviewer may be able to iterate through them much faster than if they are all kinds of documents.

Document Hashing

Another way of locating relevant files for discovery is by way of their digital fingerprints or hashes. This technique is useful for finding files that are identical and for finding files that are not usually susceptible for word term searching. Typcially the kinds of hashes used are the MD5 (message digest 5 hash) and the SHA hash.

Exact Match Hashing

Another way of locating relevant files for discovery is by way of their digital fingerprints or hashes. This technique is useful for finding files that are identical and for finding files that are not usually susceptible for word term searching. Typically the kinds of hashes used are the MD5 (message digest 5 hash) and the SHA hash.

The MD5 message digest was developed in 1994. It is a one-way hash algorithm that takes any length of data and produces a 128 bit "fingerprint" or "message digest". The MD5 algorithm is intended for digital signature applications. At 128 bits the number of potential outcomes of the MD5 message digest is 2^{128} which is larger than 3.40282×10^{38} or the number 340282 followed by 33 zeros, which is larger than a trillion, trillion, trillion. It is believed that this number of unique outcomes is so large that it is highly remote that two different messages would have the same MD5 message digest.

In the event that the MD5 algorithm does not provide a low enough probability that two documents would produce the same message digest then there is also a SHA-256. This algorithm is 2^{256} or 1.157×10^{77} or the number 1157 followed by 74 zeros which is about twice the number of possible outcomes as the MD5.

Thus, hash analysis is one method of locating specific files and it is more likely to find the desired file than the chances of a word term search. This technique also has limits, however. If

a file has had any alteration made to it, then it will no longer have the same hash. So, if the file of interest is a customer list and new names have been added or old names have been deleted the hash will be different.

Fortunately, simply changing a file's name does not alter its hash. The files name is not generally part of the file itself but, rather, is stored in the filing system. Again, if a hard drive is likened to a library then the file system is the card catalog while the file is the book on the stacks.

Fuzzy Hashing

Other technologies such as fuzzy hashing have been developed to solve the problem in trade secret cases where sensitive documents and data have been changed. Fuzzy hashing techniques typically divide the document into smaller segments and then calculate hashes for those segments as compared to the entire document. A near match will typically have some number of segment hashes that match.

Even so, fuzzy hashing can be difficult for things like Excel spreadsheets that have many structural aspects that are identical in all spreadsheets. Thus, having similar segment hashes can just be a false positive for those kinds of files.

Summary

Digital litigation involves many challenges. The solution to these challenges does not lie in the procedures of the past like manual document review. Rather, the solution involves using technology to solve technology caused problems.

While it is natural for practitioners to search for a silver bullet or "easy" button, there just is not one. The reality is that digital discovery requires blending a lot of different technologies and techniques for an optimal solution to render swift and economic justice. After all, regardless of how large the original document population the number of those that will be needed at trial is probably less than a few hundred. The issue is how to find those few hundred documents.

The solution is not a matter of simply iterating through the original population in order to find the few documents that will be needed at trial, as has often been done in the past. The population of documents is not uniform and indistinguishable except for their content. On the contrary, there are many facets about the population of documents that can be used to differentiate them and narrow their numbers to those of interest and the final trial exhibits. The different technologies provide the means to differentiate those facets and find the final documents of interest.

Perhaps the best example of choices is in technology assisted review. Between keyword search, context search and predictive coding, litigators have several choices. While many want to dismiss keyword searches in favor of predictive coding that decision may not be reasonable. If there is a problem with keyword search it is simply that it is subject to misuse like any other technology. When properly used keyword search can be very effective.

At the other end is predictive coding. While it brings considerable science to the document retrieval problem, it also brings considerable overhead. As a result, it may not be well suited for garden variety cases. In addition, its added complexity likely means it is more subject to abuse than even keyword searches.

A kind of middle ground is context search. It offers sophisticated capability in a black box format. So, it may be the best way to bring sophisticated capability to less capable users.

Regardless of the method selected, they all are subject to human limitations, particularly with respect to the determinations of responsiveness and relevance.

Document retrieval is not the only technology about which litigators need to know how to use. Indeed there are quite a number of different technologies. All of these can be used to solve the overall problem faced by litigators in the digital age—how to deliver swift and economic justice.

The best answer is not a single silver bullet or “easy” button but likely a blend of all of these methodologies to deliver an optimal solution.

CHAPTER 10

Designing Plans and Protocols: A Systems Engineering Approach to Cyber Litigation

Introduction

Successful managers of complex projects know the importance of good planning. In fact, successful managers of all kinds of complex endeavors like software products, hardware items, building construction, military operations and even professional services know the importance of good planning in delivering a final product that performs as intended as well as one that satisfies its cost and schedule criteria.

Litigation is a complex product, too. It has many parts like pleadings, orders, discovery, reports, hearings and the trial itself. One of the largest components to any litigation is discovery, which itself has many elements that must be optimized for efficiency and effectiveness, including a document management system that is often the central resource for capturing, organizing and marshalling the facts of every litigation.

If one were building a house, the end result could be described on the back of a napkin. Everyone knows, however, that such an approach is a prescription for disaster. As a result, it is widely accepted that a well-conceived and detailed drawing package is the best approach for building a house because it will resolve many issues on the front end and thereby avoid many disputes on the back-end as well as reduce waste as a result of ordering mistakes or even assembly errors.

The importance of planning for litigation in general and creating the discovery system in particular has many similarities to building a house. A litigation plan could be simply designed as well but just like the house building analogy, a simple litigation plan, particularly in the age of e-discovery, is a prescription for disaster that will surely cause many disputes, many false starts, and the wasteful allocation of resources.

There are many rules that govern civil litigation in the federal courts. The primary constraint as expressed in Rule 1 of the Federal Rules of Civil Procedure (FRCP) is to, ". . . [S]ecure the just, speedy, and inexpensive determination of every action and proceeding." The importance of planning in order to achieve that goal is clearly understood since planning is expressly required by the Rules. In fact, a Discovery Plan is required by Rule 26(f)(2) of the FRCP.

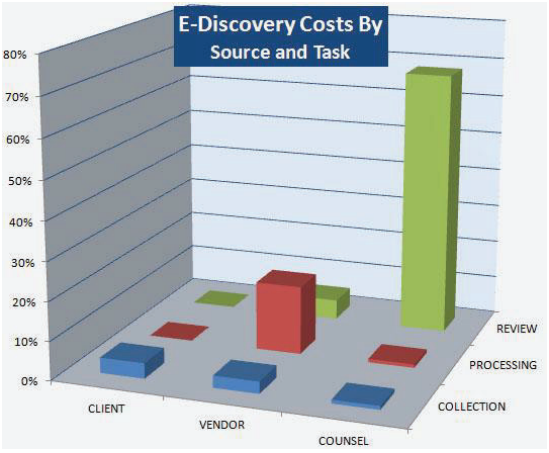
The following sections review the importance of discovery plans and protocols in litigation and how a plan can be used to improve the performance of litigation for cost schedule and performance/quality objectives, how plans are incorporated in Rule 26 of the FRCP, and the eleven steps to designing a discovery plan.

Why Litigation Often Fails

A disappointing outcome in litigation is not determined solely by the verdict. Indeed, one can win the verdict but if it costs more than it was worth it is just losing a different way.

In some cases one never gets to the verdict because a party is able to conclude well in advance that the outcome will not be worth the costs. In other words, the cure may well be worse than the disease. In such cases the settlement may be more about avoiding the punishment of litigation than obtaining a reasonable outcome. The reality is that litigation has become very expensive and one must be willing to take the punishment for the sake of principle.

Although many like to blame the current driver for the high cost of litigation on e-discovery, the true cause is not the nature of the digital evidence, the inherent procedures and processes related to the digital evidence or the use of vendors and consultants who are experts in managing digital data. Rather, the true cause for the high cost of litigation is document review and a failure to follow the rules of procedure as they exist.



According to the 2012 report by the Rand Corp.'s Institute for Civil Justice, 73 percent of e-discovery costs are expended on manual document review at a cost of 15,000 dollars per gigabyte of data reviewed. Furthermore, 75 percent of the data reviewed are useless and will never be produced. More efficient methods of review or selecting documents for review like technology assisted review are not being used and likely because there is a reluctance by counsel to forego historical revenue streams that have long been part of counsel's document review efforts.

The high cost of document review is not just caused by the inefficient and ineffective methods that are being used by counsel. Indeed, there is another significant factor contributing to the high cost of document review and that is the excessive expanse of discovery along with a failure to follow the rules as they have existed for years.

Since the 1970s there has been considerable discussion and criticism within the legal profession regarding discovery abuse. The rules of procedure, particularly Rule 26(f), have been changed numerous times to try and encourage both cooperation as well as promote the "proportional" use of discovery in order to deliver, "the just, swift and inexpensive determination of every action and proceeding" as promised under Rule 1.

What tends to happen is that the parties do not cooperate. They do not cooperate in planning efficient and effective discovery nor do they cooperate in following the rules regarding any number of other discovery subjects like preservation and production just to mention two. Some have suggested that these failures are due to confusion about the definition of

"zealous advocacy" and that the profession's members do not realize that "zealous advocacy" means arguing about the facts and not about hiding them.

Not only has this problem been recognized and addressed by various procedural rule changes over the last 35 years, that is discussed in a subsequent section below, it has been the subject of numerous other sources as well. A few of the other sources are the following.

- commentary by the Sedona Conference
  - Cooperation Proclamation (2008),
  - Cooperation Guidance for Litigators and In-house Consel (2011),
  - Cooperation Proclamation Resources for the Judiciary (2014);
- studies like the 2008 interim report by the American College of Trial Lawyers and the Institute for the Advancement of the American Legal System that claimed the most significant cause for the high cost of e-discover was discovery abuse; and
- numerous case decisions like
  - Mancia v Mayflower Textile Services, Co., 253 F.R.D. 354 (D. Md. 2008), and
  - *National Day Laborer Org v US ICE*, 2011 WL 381625 (S.D.N.Y. 2011).

Clearly it is well known that the failure to cooperate in discovery and the failure to follow the rules are causing litigation costs to skyrocket. Furthermore, they are not simply one directional. Indeed, such tactics tend to boomerang and inflict great expense onto counsel's own client. To avoid this consequence and actually accomplish the goal of Rule 1, it is essential that discovery be well planned.

How Systems Engineering Improves Planning for Complex Projects Including Litigation

When one thinks about a plan, one often thinks of it like a map or a recipe. In other words, one typically thinks of a plan as a set of instructions or as a procedure or method of acting in order to achieve a particular outcome.

In traditional planning approaches the focus of the plan is on production. The planning and design phases are less rigorous and the flaws of the initial plan might only be recognized

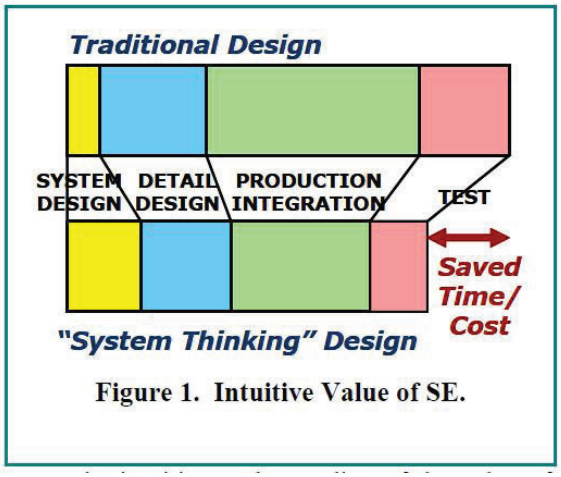


Figure 1. Intuitive Value of SE.

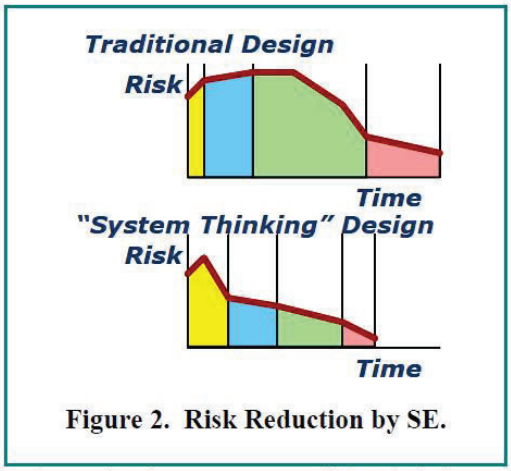
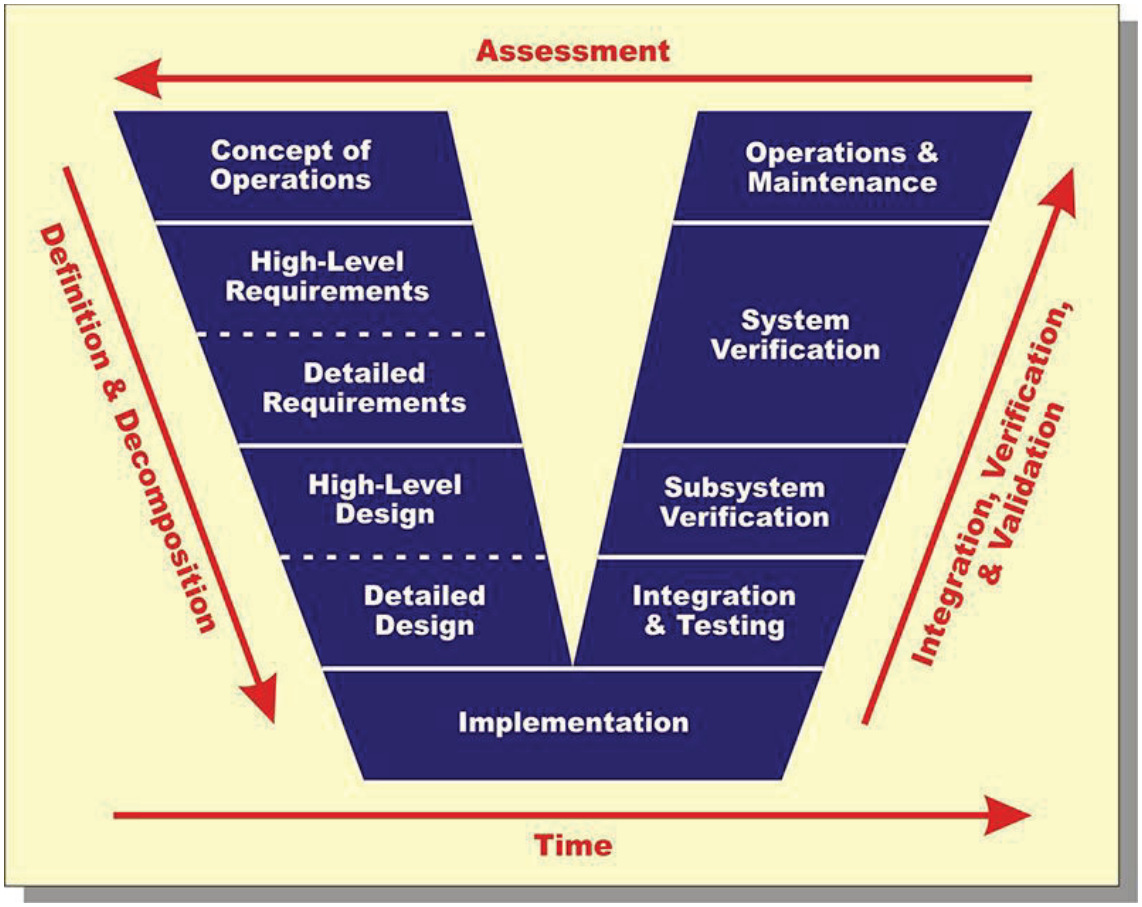


Figure 2. Risk Reduction by SE.

when production itself fails.

Systems engineering takes a more thoughtful approach to plan development. Perhaps the most significant difference is that the thoughtfulness is moved forward in the development process in order to avoid wasteful production failures. In the process it improves problem decomposition and definition, requirements synthesis and then recomposition and process development as illustrated by the classic "V" diagram below. The result of more thoughtful planning, however, is that there are fewer production failures requring system redesigns and the overall project takes less time with less cost as shown in Figure 2 above.



As a result, while developing the plan the actual objectives are sharpened as one evaluates decisions and the effects of trade-offs between the cost, schedule and performance/quality criteria. It does this in several ways.

First, the process of developing the plan provides the parties a means to determine their desires. It may be easy to say that one wants to build a house but by following systems engineering techniques to problem definition and decomposition one can better determine what that means. For example, will it be a one-story house or two? How many bedrooms and bathrooms will it have? Clearly it would be better to define these requirements before production begins and resources have been allocated and expended.

The development of the discovery plan and protocol provides similar assistance to the litigation. The issues of liability, causation and quantum were likely expressed in the pleadings. The plan will become more specific and identify which people, places and events are likely relevant to the issues and to what extent computerized devices and storage media should

be examined for relevant evidence. With e-discovery this particular step can have significant consequences since there are typically lots of different devices and storage systems that could potentially store important evidence.

Second, when developing a plan, there are considerations of more detailed trade-offs and alternatives that are performed in order to further optimize the design for cost, schedule and performance/quality. When building a house these kinds of trade-offs and requirements synthesis can include decisions regarding things like carpet or hardwood floors, exterior brick or wood siding, asphalt shingle roof or metal roof just to mention a few.

In litigation there are similar kinds of trade-off decisions that can be made. They cover a wide range of subjects like the following.

- Should the data productions be done in native format or converted into image formats?
- Should all exchanges include processed results such as format conversions, text extractions, internal metadata extractions or should each party be responsible for developing its own value added data from whatever data is actually exchanged?
- Should the exchanged data include various field attributes and what should those be?
- What attributes like file system attributes, message attributes, or keyword attributes to mention a few should be used to decide what data will be exchanged?

Third, during development of the house plan there are often tests performed to confirm performance capabilities of materials, parts or subassemblies. More complex tests can be used to demonstrate proof of concept before actually proceeding with a design concept. In addition, prototypes can be constructed and tested to confirm whether the design meet the desired performance criteria prior to committing the huge resources and beginning full scale production.

In litigation various types of early case assessment techniques can be used to probe the data population in order to identify patterns in the data, validate expectations of its contents, identify gaps in the data, or highlight unexpected occurrences. Even more substantial analytics like computerized search techniques can be used to test concepts and validate the quality of the data and whether it is relevant to the issues in the case. A multi-stage approach can be used to prototype and validate processes and procedures prior to final acceptance of the plan and more fully committing resources for full scale document production.

Fourth, after problems are decomposed and requirements synthesized the outcome and lessons learned are recomposed into a final design and interfaces between the various parts identified so that the final outcome will work as intended.

In litigation, the recomposition of the requirements result in the design of the production requests that will result in the actual production of the desired documents for review and use at trial.

Clearly the systems engineering approach incurs more analysis and evaluation on the front end than traditional methods that target an early start to production. While the traditional approach may initiate production sooner, it inevitably results in a longer project performance period and higher costs as a result of unforeseen problems that sidetrack progress and consume resources unnecessarily.

A systems engineering approach is not only more thoughtful it is more formal as well. Once decisions are made they are documented and managed by way of configuration and project management tools. These disciplines also provide at least two other advantages.

First, during project performance the documented plan provides a means to measure progress on a cost and schedule basis. Once differences between the plan and actual performance are detected, corrective action can be taken before the consequence of mistakes or errors can magnify into even larger problems.

The other advantage of having a documented and controlled management plan is that when differences do arise between the plan and actual performance, the documented plan can provide a means to test recovery strategies. After all, the documented plan should be working model of reality. Thus, by iterating back through the plan and performing additional trade studies and studying the consequence of other corrective measures, recovery strategies can be identified.

How Plans are Incorporated into the Civil Rules of Procedure

While the advantages of good planning have been lost on many of those conducting litigation, they have not been lost on those creating the rules of procedure which are supposed to be followed by all of those conducting litigation. The requirement for discovery plans have existed in Rule 26(f) of the FRCP since the 1993 amendments, although discovery conferences have been part of Rule 26(f) since the 1980 amendments when 26(f) was first added.

The discovery conference was added in 1980 in an effort to curb discovery abuses. At that time, however, the discovery conference was simply something where counsel could request the assistance of the court if counsel had been unable to agree on a reasonable discovery plan.

Since few had utilized the use of discovery conferences, the 1993 amendments required the development of a discovery plan so that it could be incorporated into the court's scheduling order under Rule 16, which is one method for how the court manages the case. The 1993 amendments even described certain matters that should be addressed by the parties and included in the discovery plan for inclusion in the court's scheduling order.

The 2006 amendments to Rule 26(f) made it clear that the parties were to discuss the discovery of Electronically Stored Information (ESI) during their conference. Actually, the discovery of computerized data had been "black letter law" for more than a decade prior to the 2006 changes. (see, *Anti-Monopoly Inc. v Hasbro*, Not Reported in F.Supp., 1995 WL 649934 (S.D.N.Y.)) In fact, the term Electronically Stored Information (ESI) had been used more than 20 years prior to the 2006 changes when it was decided that, "It [was] now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure. . . ." (see, of *Bills v Kennecott Corp*., 108 F.R.D. 459, 461 (D. Utah 1985)) Thus, in many respects the 2006 amendments were simply formalizing what was already an accepted practice in order to end wasteful motion practice as a result of failures to cooperate that claimed the contrary on almost every case where computerized data were sought in discovery.

The 2006 amendments to Rule 26(f) even embellished the subjects to be discussed at the discovery conference and included in the Discovery Plan. The Committee comments to the 2006 changes to Rule 26(f) also referenced section 40.25(2) of the Manual for Complex Litigation that listed a number of preservation subjects that should be discussed during the discovery planning conference.

The 2015 amendments also made some editorial changes to the discovery plan section of Rule 26(f) to include a reference to preservation as a topic for discussion and a reference to Court Order under Rule 502 and the party's discussion of how privilege material will be handled. Like many of those preceding it the 2015 amendments to Rule 26(f)(3) that expressly included preservation as something to be discussed in the discovery conference were nothing new, since the Rule 26(f)(2) had already suggested the discussion of preservation during the discovery conference so that it could be included in the Scheduling Order.

Discovery Plans are required by Rule 26 of the FRCP. In fact, a Discovery Plan or protocol is the product of the Discovery Planning Conference required by Rule 26(f)(2). Rule 26(f)(3) identifies a list of items that should be addressed in the discovery plan. As of the 2015 amendments, those items are:

- 26(f)(3)(A)
    - Timing, requirement or form of initial disclosures, and
    - Statement when disclosures will be made
- 26(f)(3)(B)
    - Subjects on which discovery may be needed,
    - When discovery should be completed,
    - Whether conducted in phases or limited or focused to a particular issue
- 26(f)(3)(C)
    - Issues about
        - Disclosure,
        - Discovery or
        - Preservation of ESI,
    - Form of production
- 26(f)(3)(D)
    - Claims of privilege,
    - Protection of trial preparation materials,
    - Requests for protective orders
- 26(f)(3)(E)
    - Limitations on discovery required by these rules or local rules
    - Any other limitations
- 26(f)(3)(F)
    - Any other orders under 26(c) or 16(b)

One of the ways the court manages a case is through the Rule 16(b) scheduling order. Interestingly, the Discovery Plan provides many of the details that will be incorporated in the scheduling order. Thus, the discovery plan is essential for the court's proper management of the case.

Just like rule 26(f)(3) lists items that should be included in the discovery plan, rule 16(b) identifies things that should be included in the scheduling order. Since the discovery plan feeds

the scheduling order, the items listed in Rule 16(b) should also be considered in the discovery plan.

The items listed in Rule 16(b) as the contents the order are the following.

- 16(b)(3)(A) – limiting time to
  - join other parties,
  - amend the pleadings,
  - complete discovery, and
  - file motions;
- 16(b)(3)(B)
  - Modify the timing of disclosures
  - Modify the extent of discovery,
  - Provide for
    - Disclosure,
    - Discovery, or
    - Preservation of ESI
  - Include any agreements of the parties regarding privilege or protection of trial preparation materials after production,
  - Set dates for pretrial conferences and for trial, and
  - Other appropriate matters.

Rules 16(b) and 26(f)(3) are not the only places in the FRCP where subjects for the discovery plan are identified. Form 52 in the Appendix of forms to the FRCP also provides a list of things to consider.

V List of persons participating in 26(f) discovery conference

VI The date on which or by which the parties will complete initial disclosures

VII The proposed discovery plan

VIII Subjects about which discovery will be needed

IX Dates for commencing and completing discovery including completion of staged discovery where one subject is completed before another,

X Maximum number of interrogatories along with the dates that answers are due,

XI Maximum number of requests for admission along with the dates responses are due,

XII Maximum number of depositions by each party,

XIII Limits on the length of depositions in hours,

XIV Dates for exchanging reports of experts,

XV Dates for supplementing disclosures and responses under 26(e) to supplement or correct for any material fact or omission unless already made known to the other parties.

XVI Disclosures under 26(a),

XVII Responses to

XVIII Interrogatories

XIX Requests for production or

XX Request for admission.

XXI Other items

XXII A date if the parties ask to meet with the court before a scheduling order

XXIII Requested dates for pretrial conferences

XXIV Final dates for Plaintiff to amend pleadings or join parties

XXV Final dates for the defendant to amend pleadings or to join parties

XXVI Final date to file dispositive motions

XXVII State the prospects for settlement

XXVIII Identify any alternative dispute resolution procedures that may enhance settlement prospects,

XXIX Final dates for submitting Rule 26(a)(3)

XXX Witness lists,

XXXI Designations of witnesses whose testimony will be preserved by depositions, and

XXXII Exhibit lists.

Clearly the lists of subjects found in Rule 16(b), 26(f)(3) and Form 52 provide quite a list of subjects that should be addressed and included in the Discovery Plan and protocol. Many are milestone dates while others are more substantive issues such as preservation and discovery or production of ESI. Of course, even some of the milestone dates like dates for exchanging expert reports and commencing and ending discovery require consideration of the efforts required to accomplish those tasks before realistic dates can be developed. After all, it is simply impractical to set an arbitrary date for the completion of discovery without consideration and detailed planning of the processes that must be performed in order to complete that task.

Also, based on the various subjects appearing in the lists of things to be covered by the discovery plan like depositions, interrogatories, request for admissions and form of production, it is clear that the requirements of other rules must also be considered. So, the discovery plan requirements are not strictly limited to consideration of the subjects identified in Rules 16 or 26 or Form 52 without also considering the requirements of the rules governing the efforts referenced in the subjects to be included in the discovery plan.

Under 26(f)(1), the discovery conference, which produces the discovery plan, is to be held as soon as practicably but at least 21 days prior to the Scheduling Conference or a scheduling order is due under Rule 16(b). Under the 2015 amendments, the scheduling order is due 90 days after any defendant has been served with a complaint or 60 days after any defendant has appeared. Thus, there are 69 days within which to commence the discovery conference. The report itself is due within 14 days of completing the discovery conference.

While the order is to be issued within the prescribed period, that period can be extended under Rule 16(b)(2) for good cause. In addition, the schedule can be modified for good cause as well under Rule 16(b)(4).

None of the rules discuss how to progress or complete the discovery plan when the parties cannot agree on a particular subject. In addition, there is no requirement that one party must capitulate to an unreasonably intransigent party that fails to participate in good faith.

If the lack of agreement on a plan is the result of one party's lack of participation then Rule 37(f) permits the court to impose monetary sanctions on the failing party for any increased costs caused by the failure. Also, at least one case resulted in dismissal in part because of a failure to cooperate as required under Rule 26(f)(2). (see, *Siems v City of Minneapolis*, 560 F.3d 824, 826-27 (8th Cir 2009))

Also, Form 52 suggests that separate paragraphs or subparagraphs be used when completing the written discovery plan and the parties cannot agree on an item. Once submitted to the court, such variances should be clear notice that judicial action is needed.

Section 11.42 in the Manual forCcomplex Litigation describes a process where judges are supposed to be active in case management. For example, it says that,

Judges should ask the lawyers initially to propose a plan, but should not accept joint recommendations uncritically. Limits may be necessary even when regarding discovery on which counsel agree. The judge's role is to oversee the plan and provide guidance and control. In performing that role, even with limited familiarity with the case, the judge must retain responsibility for control of discovery. The judge should not hesitate to ask why particular discovery is needed and whether information can be obtained more efficiently and economically by other means.

Despite the above, judges are not always proactive in case management. More times than not they tend to be reactive and respond only when there are complaints about the process by the parties. Surely, submitting discovery plans with divergent paragraphs when the parties cannot agree as suggested on Form 52 should signal the judge that his input is needed.

Eleven Steps To Designing a Discovery Plan: A Systems Engineering Approach

As described previously, systems engineering takes a more thoughtful approach to plan development. Perhaps the most significant difference is that the thoughtfulness is moved forward in the plan development process in order to avoid wasteful production failures. In the process it improves problem definition and decomposition, requirements synthesis and process development. As a result, while developing the plan the actual objectives are sharpened as one evaluates decisions and the effects of trade-offs between the cost, schedule and performance/quality criteria.

As described in the following eleven sections systems engineering techniques can be blended with the various subjects identified in the rules for developing a discovery plan and accomplishing the objectives of Rule 1, for the "just, speedy and inexpensive determination of every action and proceeding."

1. Determine the Scope of Discovery and the Order of Production

One of the first steps is always to identify the target of discovery. Rule 26(f)(3)(B) identifies the subjects of discovery and whether discovery should be conducted in phases as elements to the discovery plan.

Often the concern is that the subject of discovery is too broad and that examining every computerized device and source of ESI is simply not practical. The parties are in litigation in order to settle their grievance but they are unsure exactly how the process will solve their problem. In large respects, therefore, they are shooting in the dark to discover what facts can settle their problem.

If one of the party's is General Motors, it is not practical to request all of their computer records. Consequently, the first step in any discovery matter is to determine the scope of discovery. Perhaps the best way to determine the scope is to identify the significant people, places and events that are important to the case so that discovery can be appropriately targeted.

The parties and their counsel should, of course, meet to discuss and define the scope of the litigation or they could schedule phone conferences for this purpose. At the same time, it may be useful to even stratify the population and develop a multi-stage discovery effort. In other words, when identifying people, places and events there could be agreement that the data of certain custodians at certain locations involving certain events are expected to have greater significance than others. This determination can then be used to prioritize the discovery.

Prioritizing the discovery can have different significance depending on the situation. The first is simply the order in which media related to people, places and events should be processed and produced. The other, and perhaps more useful, is the actual stratification of the people, places and events so that their respective data can be processed and produced under a multi-stage discovery plan.

A multi-stage plan is actually contemplated in the rules in recognition that it may be better to process and produce the low hanging fruit first while leaving the more difficult and more costly data to process and produce for later in discovery, if even needed at all.

The multi-stage plan provides several other benefits, as well. First, there is likely little need to process and produce documents from low priority data sources, particularly if critical information has already been found. Even when critical information has not been found that could be the signal that there is even less value in processing and producing data from even lower priority data sources.

The second benefit provided by a multi-stage discovery plan is that the separate stages provide the parties with opportunities to prototype the procedures and processes and validate their effectiveness before committing to full scale production. So, proving the validity of the discovery procedures on smaller data populations could save substantial sums down the road, particularly should it become necessary to revise any of the various procedures.

The final benefit is that establishing an order determines the flow of the data and the sequence of subsequent discovery. After all, the order of depositions as well as other forms of discovery could well depend on the order of documents produced.

A systems engineering approach improves the overall process and the ultimate outcome through problem decomposition and requirements refinement. During this stage of the discovery plan the parties should focus on refining the problem and what will actually be required to resolve it.

There are many different manners in which multi-stage plans could be implemented. One way involves stratification of key players versus lesser and lesser players. Another involves highly duplicative data sources like backup tape archives. In that case the various stages could be based on perceived likelihood that critical information will more likely be found on certain media. If so, then perhaps the remaining media could be avoided all together.

Another of the guiding factors to consider when identifying people, places and events should be relevant evidence. A review of people, places and events may not only narrow the scope but further consideration may even narrow the scope within those categories because what is really of interest is relevant evidence and not just data to collect, process and produce. After all, litigation is not an exercise in data processing, review and production skills. Rather, the action will succeed or fail on the basis of a few exhibits. The ideal situation would be to only process, review and produce the data that will be used as exhibits at trial.

Re-openers can be included in the plan so that if during discovery additional information is learned the scope could be expanded. Of course, if the additional information suggests a narrowing of the scope then the additional steps need not be executed, although a formal modification could be executed.

2. Preserve the Data

The second step involves the preservation of the data for subsequent discovery and analysis. Rule 26(f)(3) requires the parties to discuss any issues about preserving discoverable information and include those in the plan.

Preservation is probably the most important part of the litigation since if done improperly a party can lose before the case even really begins. After identifying people, places and events in the previous step, one should also identify the related computer resources, devices and media. Each of the parties could come to meetings or conferences with a map of their own devices and systems. Those maps could be exchanged and discussions held so that the parties can have comfort of the preservation considering their agreements about the scope of the discovery. Thus, the meetings would essentially finalize the data maps that each brings to the discussions.

This is a good task in which to have an expert participate as well as the parties' respective system representatives (a 30(b)(6) caliber of individual). The expert could assist not only in performing the preservation but in helping to scope the universe of media to be preserved. The kind of expert should not just be someone with preservation experience but someone with systems experience, as well. Someone that will know how things work and know what kind of

questions to ask about systems and devices based on an understanding of the case and the types of activities in which the parties are engaged. In fact, with the maps exchanged it is the kind of thing that the lawyers could take a back seat and allow the experts and designated individuals discuss to develop the final "map". Once developed the lawyers could ask their own questions to confirm how well the map fits with the planned scope of discovery.

The focus of the preservation effort should be the media, such as hard drives and backup tapes, on which the believed important data resides based on the identification of computer resources used by people and places for the events identified in the previous step. Of course, the parties should have already performed their preservation long before the discovery conference or development of the plan. So, what should be addressed in the plan is confirming the devices and media that have already been preserved as well as identifying those devices that have not already been preserved but are part of the people, places and events previously identified in step 1.

It is important that the media be preserved and not just specific files or documents saved as is common in a targeted data preservation. Rather, it is essential to capture the entire media with the full spectrum of data. That way no matter how the case dynamics might change, the data will be available for analysis.

The importance of preserving the media is not just a technical evidential issue. Indeed, it is an economic issue as well. Determining what specific files are important to a case and should be preserved can take time. In fact, determining what data should be preserved could take more time than just preserving the media itself.

There is a difference between preservation and analysis. A targeted data acquisition that tries to capture files of interest crosses the line from preservation into analysis. Since a party may have a duty to preserve but not have a duty to produce, a key element in minimizing costs is to not waste effort trying to figure out what data on a particular media is or could be relevant and what data is not once the universe of data to be preserved has been determined.

In addition, there are a lot of data hiding techniques that will not be easily uncovered during a targeted data preservation. For example, an important document could have had its file name and extension changed to something outside the types that have been targeted for preservation. If that has happened it will not be selected for preservation and totally missed.

Another reason for preserving the entire media is that if something ultimately has evidential value it will need to be authenticated. Part of that authentication should include the authenticity of the media from which it was harvested. Authentication of the media typically involves examination of the media's system metadata. If the metadata indicates that the media has been doctored or counterfeited then the authenticity of the evidence should be questioned.

In recognition of the above, the plan should adopt media based preservation. The parties should meet to determine what has already been preserved and identify any additional media that should be preserved.

It is not necessary that every bit of data be preserved particularly when there could be several different copies of it. For example, if a particular device is captured through normal

backup systems then it may not be necessary to also perform an additional preservation of that device's actual media. The backup history could be far better than any current period media preservation.

Part of the discussion should also involve the particulars of the preservation method. If a media based preservation was performed was it a forensic grade preservation capturing the entire media or was it something that captured only the active data. In the case of the latter the parties may agree that an additional forensic image also be made of the data.

Whatever the parties decide regarding the specific data that has been preserved or will be preserved should be formalized in the discovery plan. Since it is not necessary that all preserved data actually be analyzed or produced, the determination of what data sources should be preserved is not based on which will be analyzed or produced.

3. Schedule of Discovery

Other sections of the plan address quality and cost issues. This portion of the plan should address timing of the work by creating a schedule that includes, at a minimum, the various milestone dates identified in Rules 16(b), 26(f) and Form 52 such as the following.

ITEM	Rule 16	Rule 26	Form 52
Date for initial disclosures	X	X	x
Date when discovery starts and ends		X	X
Date when each Discovery phase will start and end		X	X
Date for joining other parties	X		X
Date for amending pleadings	X		X
Date for filing motions ends	X		X
Date for modifying extent of discovery	X		
Date for pretrial conference	X		X
Date for trial	X		X
Date for proposed discovery plan	X		
Date for exchanging expert report			X
Date for supplementing disclosures and responses			X
Date for Interrogatory responses			X
Date for Document production			X
Date for admission responses			X
Witness lists	X		
Designation of witnesses	X		
Exhibit Lists	X		

Schedules are used for planning and managing all kinds of complex projects like building construction, product development, system development and even movie production to not only plan performance and what it will take to accomplish a particular objective but to monitor performance as well. Schedules are even used in litigation and incorporated in the scheduling order but litigation schedules are typically very different than the schedules used in other complex projects.

Litigation schedules are more like milestones where goal accomplishment is tagged to a certain date. By comparison, schedules in the other complex projects mentioned above are typically networked schedules. In network schedules the individual tasks that will be required to accomplish a particular milestone are linked to each other based on their known dependencies. As a result, as work is performed and the schedule updated the consequence of actual performance on the accomplishment of milestones can be calculated.

Litigation schedules, at least those used by the parties to manage the project, should be networked in order to accurately model reality. Depositions can be linked to related document productions that must be related to their selection and processing and even to their initial preservation. There are likely other tasks as well whose performance is dependent on other tasks that precede them.

Multi-stage approaches can provide several issues as well. First, the multi-stage approach may simply have been selected as a means to test production procedures on smaller populations prior to moving to full scale production. Those situations could be fully scheduled using a networked approach.

The other situation, where a multi-stage approach is adopted as a means to potentially avoid portions of the data production that are suspected of having less significance, is more complicated. In those cases, the schedule would essentially be incomplete and dependent on certain events triggering that performance.

Dependencies are not the only characteristic of an accurate schedule. Network schedules should also integrate the resources required to perform a task. Those resources can have availability constraints as well as performance capabilities that influence timing. For example, before document review can begin there must be reviewers and they are only capable of reviewing those documents at a certain rate. Thus, performance constraints are not just limited to task dependencies but to various kinds of resource constrains as well.

Once the resources have been linked to tasks the costs of those resources can be linked as well. Once that is done both elements of cost and time can be calculated.

Typically counsel has to provide clients with time and cost estimates as well as periodic updates on actual performance of the litigation. Networked schedules with integrated resources are a great way to provide clients with that information. Clearly, litigation schedules are not only an interest to the court but to clients as well and counsel on both sides of the litigation serve those masters. Consequently, not only should schedules be incorporated in the discovery plan development but they should be networked schedules with integrated resources as well.

Including realistic cost and scheduling techniques into the discovery plan should not be that much of an extra step. Assuredly, clients have already had their counsel prepare cost and schedule estimates prior to even initiating litigation. If those disclosures were realistic there likely will not be much difference between what was initially prepared from what is prepared during development of the discovery plan with opposing counsel. If there is a significant difference this would likely be a good time for the client to find out. In addition, those interested in settlement are likely very interested in developing a realistic cost and schedule model and doing so with opposing counsel just so the adverse party can accurately assess the cost of such a venture and then calculate their own return on investment.

It is not essential that the two sides share their cost estimates when developing their network schedule. One side can likely be confident that if a realistic schedule is developed that someone else will be able to fill in the numbers and calculate the costs for the client.

Developing realistic network schedules are not cost prohibitive. Simple cases will have simple solutions with simple schedules. The associated cost will be minimal, therefore.

It is the complex cases that will have complex solutions and complex schedules. In those situations the risks are very large. Small errors can have significant consequences. The effort related to spoliation motions and hearings can run hundreds of thousands of dollars even before their outcome is imposed, if successful. Disputes about production format and accessibility can also be considerably large. Rambo style lawyer tactics can boomerang with significant consequences. In essence, it is easy to get off track, particularly when the discovery plan is ill-conceived from the start. Developing a realistic network schedule is a good way to avoid those kinds of problems or at least calculate their consequence before settling on a litigation strategy.

Remarkably network schedules are not just barometers of bad news. Since they are working models they can also be very useful in developing recovery strategies should the wheels come of the bus, as they say. As working models, network schedules can be used for gaming, what-if analysis and trade-off analysis both when developing strategy alternatives and trying to recover from some kind of unexpected event or blown estimate.

Schedule information is often required in complex projects for reasons other than management. Indeed, meeting performance objectives is often very important to any contractual relationship. As such, when performance fails to meet contractual requirements it is often important to understand the cause and which of the parties is responsible. Network schedules are often used for this purpose and often are the kind of evidence required for one party to obtain compensation from the other for performance failures like failing to follow the discovery plan or the rules themselves.

4. Validate the Population

There is an old saying in the technology world about "Garbage in. Garbage out." In litigation, it is simply foolish to commit resources and proceed with discovery if there are significant omissions in the population, or perhaps worse something even less accidental, that if known would have altered the direction of discovery and the allocation of resources. After all, if

one is looking for a needle in a haystack, one at least wants to have the right haystack and have some comfort that the needle is still there; otherwise, it is a lot of wasted effort.

Similarly, if one has limited ammunition, one shoots only at verified targets and not blindly into the darkness. Using the home building analogy once again, it is better to wait and purchase the building materials once the construction plans are known; otherwise, it could just be a waste of resources.

Before committing resources to process and review documents it only makes sense to validate that the media from which they come is worthy of that commitment. After all, there will likely be many different data sources but are they all worthy of consideration? Are some likely to be more worthy than others? Would the worthiness of certain storage media change if it was known that it did not cover the period of interest, the custodian of interest during the period of interest, or if it showed signs of deliberate manipulation? Even if all of the media are valid, would some media still have a higher probability of producing relevant evidence than others and would decisions about the allocation of resources and their timing be different if that information was known?

While counsel typically does not like to "investigate" its client, validating that the population of preserved devices is something that both sides should want to have performed, at least on the opposition's preservation. Of course, to avoid later claims of spoliation they should be proactive and validate their own client's holdings. There are several areas of interest when validating the population of preserved devices and data.

- Whether there have been any other storages devices like external hard drives or flash drives that were attached to bootable devices like personal computers but not preserved that could have relevant evidence?
- Whether bootable devices are the original device for the period in question or was there another hard drive or an earlier hard drive that has not been preserved?
- Whether there are other network attached devices that could have been used to store data and whose contents need to be included in the preserved and potentially producible data?
- Whether the attached storage devices that have been preserved were attached to any other bootable devices other than those that have been preserved?
- What files have been used from bootable devices and are those files on storage devices, including web based storage sources, or media not covered in any of the above?

Although the parties could agree for the examination of their electronic media for these purposes by an independent expert or by their own experts, it is also possible to answer these questions without having to examine the devices themselves. Instead, there are certain system files on the bootable devices that could be produced as part of discovery and those files could be examined to answer the questions about what devices have been attached and whether the bootable device's media appears legitimate.

The particular files that one would want to examine depend on the type of bootable device. In other words, is it Windows or is it Apple, for example. For Windows systems the files of interest are generally several Registry hives. For Apple machines is it several Property List (PLIST) files. Even after identifying the type of bootable device there could still be differences

between the operating system versions on those devices that could affect the particular files that will be of interest.

Answering the first two questions above is easily accomplished by requesting the same system files on bootable media. The other questions above could also be answers but there are different files and it is not as simple as a "look" at a few files on bootable devices. Nonetheless, the information is easily obtainable with file system and file pointer kinds of analyses. Consequently, it still is something that the parties would likely want to confirm before "wasting" valuable resources on incomplete, or potentially worse, questionable data.

In a multi-stage discovery plan the parties could defer confirming devices in the lower priority strata until it actually looks like they will be examined. Assuming the first stages are related to more important and likely productive targets, validating the population of preserved media for those strata should be done early.

With respect to other network attached storage there are a couple of different places where one could look in order to make that determination. The "look" is a little more involved than just a couple of files, however.

Once again, both sides have an interest in validating that the population of potentially producible documents is complete. Hence, both sides should want to embrace this effort and include the correct process in their discovery plans.

5. Prepare Data for Analysis

It is hard to make good decisions if one does not have good empirical data on which to base those decisions. The purpose of the data preparation phase is to transform the preserved data into something that has its useful characteristics revealed and available for analysis. In addition, the preparation phase puts the data into a usable form for efficient analysis by automated tools.

The information derived during preprocessing will be used by the parties to make decisions about their own data holdings. They can also share that information, or portions of it, when developing their discovery plan to better plan the particulars of the discovery such as the document file types of interest and the most efficient data sizes for review and production batch volumes. The more buy-in that each side can negotiate into the plan the less likely that there will be a dispute about a particular process employed later on during the actual execution of discovery.

The traditional document review platforms are not the best tools for performing this kind of analysis. In fact, there are many other tools that provide these kinds of capabilities like many of the computer forensic tools and third party specialty applications. Furthermore, they can do it straight from the preserved data without having to extract it, convert it or spend other budget resources. Thus, there are economic reasons for using these special kinds of tools and avoiding the document review platforms until after the desired documents are actually selected.

The kinds of preprocessing should be formalized in the discovery plan. It may not be possible to complete the data preparation prior to completing the discovery plan, although it would be ideal if the results were known and could be used for developing the entire discovery plan. The reality, however, particularly in a multi-stage discovery plan where hopefully not all stages will have to be performed, is that data processing will not be complete and the discovery plan is flexible enough to adapt to whatever situations and conditions are found as the actual production moves forward.

Systems engineering is frequently an iterative process of decomposition and synthesis followed by recomposition and integration of the result. While it is always possible that things will work on the first attempt, it could very well be that further follow-on is required.

Both sides have an interest in memorializing the data processing efforts in the discovery plan. Primarily, it guarantees that certain minimum standards will be followed by both sides. In fact, both sides have an interest in obtaining agreement on the minimum standards to avoid having an entire effort torpedoed due to faulty shortcuts or errors and omissions in performance, particularly after having incurred considerable expense.

When proceeding under a multi-stage discovery plan it is not essential that all of the data be subjected to data processing prior to finalizing the discovery plan. Rather it is possible to only subject the media selected for a particular stage or even stages to the analysis. With each stage the results can be updated and compared against prior groupings.

When developing a plan the parties can agree to what extent the data will be subjected to these processes prior to production. The facets that they should consider are discussed in the sections that follow.

Compound Documents Parsed and Cataloged at Desired Levels of Granularity

Many of the document types sought by litigators are not simple documents but rather are compound documents. A spreadsheet is a potential example of a simple document. On the other hand, an e-mail is an example of a compound document. E-mails have both a message and they have attachments; hence a compound document. A compressed archive or zip-file is another example of a compound document since it contains many documents within it.

When selecting files for review or production it is essential to identify the contents of compound documents so that they could be included for consideration. Thus, one thing that should be considered in the profile is the granularity of compound documents. In other words, at what level will they be decomposed in order to ensure that their contents are properly included for consideration.

Another important consideration is the effect of granularity on deduplication. The most place where this is most important involves e-mail. In other words, should duplication be performed at the entire e-mail level (message and attachments) or at each element (message and each attachment separately)?

If the entire message level is chosen then the same message will be seen each time there is a different date, or distribution list or attachment. Similarly the same attachment will appear

each time it is attached to a different e-mail as well as saved to different locations on the server or personal computer.

If the purpose of the deduplication is to remove redundancies like those that exist in multiple backup tapes then deduplication at the message level is adequate. If the purpose is to develop the most efficient data set for document review then greater granularity is desired.

If the same message is sent to two different people on different coasts each of those messages will have different hash values even though they contain the same message and attachments. The difference is caused when the message travels the internet and receives date stamps at each server along the way. The message's route to one coast will likely be different than it's route to the other coast. Of course, the original message will never have traveled the internet and not have any server date stamps.

Thus, in order to develop the most efficient list of documents for review and to ensure never reading the same e-mail more than once, the deduplication should be done at the most atomic level. Even then, since the message is actually a collection of metadata fields only certain fields about the message should be selected for deduplication.

Again, consider the case where a message is sent to a distribution list and then after sending it one realizes that someone was omitted from the distribution so it is sent again to those that were omitted. In order to avoid seeing that e-mail more than once and in order to develop the most efficient lists of documents for review only the data stream comprising the message portion of the e-mail should be selected for hashing and deduplication as well as the attachments separately.

Thus, for efficiency sake as well as other objectives like completeness the parties should decide the level of granularity for determining deduplication. To some extent it could be left for each of the parties to determine granularity for their own purposes in order to achieve the greatest efficiencies. On the other hand, each of the parties has a stake in efficiency at the production level when trying to minimize production costs.

Hashes Calculated

Since it is well recognized that the volume of electronic data will be significantly large one of the key tools that the litigants will require to conduct efficient discovery is a means to identify and remove the duplicates. Removal of duplicates should not be performed based on file name or subject matter or other visible characteristics of the data. Rather, the best method for identifying duplicates is through the use of digital signature or digital fingerprint algorithms.

The MD5 message digest (MD5 Hash) was developed in 1994. It is a one-way hash algorithm that takes any length of data and produces a 128 bit "fingerprint" or "message digest".

The MD5 algorithm was intended for digital signature applications. At 128 bits the number of potential outcomes of the MD5 message digest is 2 to the 128th which is larger than 3.40282 x 10 raised to the 38th or the number 340282 followed by 33 zeros, which is larger than a

trillion, trillion, trillion. It is believed that this number of unique outcomes is so large that it is highly remote that two different messages would have the same MD5 message digest.

In the event that the MD5 algorithm does not provide a low enough probability that two documents would produce the same message digest then there is also a SHA-256. This algorithm is 2 raised to the 256th or 1.157 x 10 raised to the 77th or the number 1157 followed by 74 zeros which is about twice the number of possible outcomes as the MD5.

Thus, either the MD5 or SHA-256 algorithms can be used to determine a signature of all electronic documents comprising the population of those that are discoverable. From that population, the unique documents can be identified based on their message digest values.

Furthermore, the fingerprint is "non-reversible". In other words, it is computationally infeasible to determine the contents of the input file based on an MD5 hash value.

When performing the deduplication process there are two elements that requesters and producers will want to determine. The first is the granularity at which the deduplication will be performed. After all, the purpose of the de-duplication exercise is to reduce the population of documents in order to streamline the litigation lifecycle and reduce review time and analysis time and costs. How granularity can affect this process is described in a subsequent section.

The second issue is how to treat and track the duplicates since the existence of these duplicates could have significance to the case. Thus, while identifying and removing duplicates is important for efficiency reasons, knowing that duplicates exist and where they are located could be very important when understanding how those documents were used is important.

In a multi-stage discovery plan, it is possible that as the discovery is expanded to each group that the number of unique files will diminish from grouping to grouping because they have already been considered in earlier stages, although the tracking of where each of the duplicates was found will need to be updated.

Signature Analysis

Electronic media can have many different types of files stored on them. In e-discovery parties are often interested in only certain types of files and not necessarily all of the files on a media. Generally, people identify the file type by its extension. However, in a Windows environment the extension is not as reliable as in other systems. In addition, it is easy for evil doers to change a file's name and extension as a means to disguise a file's significance.

One method of validating a file's true nature is through signature analysis. Essentially, signature analysis looks for certain known markers in the file's internals that identify its type. In fact, software programs frequently rely on these internal markers rather than the file's extension before proceeding.

Signature analysis and confirmation of each file's type should be part of every e-discovery process and included in the plan.

Known Files Identified

In addition to de-duplication, digital signatures such as MD-5 hash can be used to accept or reject the files that are to be considered. In other words, if a particular file is sought, such as a trade secret, then search parameters could be constructed to look only for files with that hash value.

The hash value is not affected by a change in file name, since the file name is not part of the file itself but resides in the filing system. Thus, if the file name was changed as a means to hide its nature, the hash analysis would still detect it.

Hash analysis can also be used to reject or exclude certain files. For example, with each software installation there are often sample and tutorial files to assist users in learning the product. These sample files could well fall within the desired file types when file's are being selected for document review and subsequent processing by their file types.

There are lists produced containing all the known hashes for commercial software packages. These would include the sample files. Thus, if these lists were included in the respondents production process then such files could be omitted from production. Similarly, the lists of known hashes can be used to exclude files from prior searches or analysis, particular when a multi-stage discovery plan was being followed.

Encryption Detection

When planning discovery it will be useful to know which, if any, files are encrypted. Encrypted files cannot be searched since their contents are scrambled and meaningless. Most likely cannot be examined either, although it is possible for the encryption protection to simply be protection against changing the document contents. Thus, it is necessary to know what files are encrypted so that they can be handled properly.

Depending on the volume of encrypted files and where they happen to be encountered the parties may decide to postpone decryption efforts, after all it may be possible to obtain considerable information about an issue from other unencrypted files. In addition, decrypting files will be an added cost to the discovery process. So, accumulating them into groups and processing them on a batch basis will likely be more economical than handling them when encountered.

An entropy test is a means for detecting encrypted files. Essentially, an entropy test measures the chaos within a file. While the test is not foolproof, the more chaos that a file contains the more likely that it is encrypted. Clearly, one of the preprocessing tests should be an entropy test or other similar process to try and spot encrypted files early so that they can be subjected to the special treatment that they require and before the other processes and efforts that will not be effective on them are wasted.

Deleted File Recovery

Consideration should be given to recovering deleted files. There are several different methods by which deleted files could be recovered. There are the traditional methods that recover deleted files from freespace either through file system pointers or by data carving based on file type signature data. Then there are methods that recover files from Volume Shadow Copy (VSC). While the traditional file recovery methods are something that the parties will want to discuss based on particular case circumstances, the VSC data is something that should be performed in every situation.

The VSC was a feature introduced with Windows Vista. It provides a means of archiving files so that they can be recovered later. Thus, VSC files are not really deleted files. Rather they are archived files and they are accessible to the user simply by right clicking on the file in Windows Explorer and then viewing the Previous Versions tab in the Properties Dialog box. Consequently, one could easily argue that the files are "easily accessible" to the user when operating the computer and should be treated the same as other active data files even though they are more technically a file archive.

While VSC was enabled by default on Windows Vista systems it has to be enabled on Windows 7 and later versions. Thus, there is no guarantee that VSC versions of files will exist on Windows based computers that are Windows 7 and later, although it is a good practice for organizations to activate the feature on employee machines, particularly when they implement full disk encryption and want to be able to recover deleted data when the need arises.

While recovering VSC data from a device that is up and running is simple enough, it is a different matter when recovering the data from a detached drive or forensic image. Nonetheless, there are forensic software tools that makes this process very easy and will even identify files in VSC that are no longer in the active file system. Thus, the parties when negotiating their discovery plan just need to make sure that those tools will be used when extracting data from preserved media.

As indicated previously, there are other methods of recovering deleted files than from VSC. These other methods are the traditional techniques that involve file system pointers or data carving based on file signature data.

File recovery software has become quite effective. Furthermore, the use of automated tools makes recovery relatively inexpensive. Unless there are concerns about whether active files contain the needed evidential data, deleted file recovery can be omitted because all that it is likely to provide is temporary versions of currently active files.

If there are concerns about the evidential quality of the active data then recovering deleted files is a real option that is worthy of consideration. The recovery can even be tailored to target on the kinds of files of interest. For example, it could be tailored to target only Office documents for example while ignoring graphical images that could have come from browsing websites.

Regardless of the tailoring, the parties should recognize the there are all kinds of situations where files are deleted. Many are system related. Thus, the deleted files recovered could be temporary versions of active files that were deleted when the active file was saved. Then again, these deleted files could be prior be instances with slight modifications to currently active files or even be files that are no longer exist as active files.

In any event, the parties can discuss the specifics of their case and decide how they want to handle deleted file recovery. Of course, they could always decide to postpone any deleted file recovery effort to some future stage in a multi-stage discovery plan and base their decision on the results obtained from active files.

File System Data Collected

If a storage media can be analogized to a library the file system is like the card catalog while the files themselves are like the books on the shelves. By examining the file system one can identify the files that are currently on the media and of potential interest in the same way that by examining the card catalog one can determine what books are in the library and are of interest.

Just like the card catalog contains certain attributes about the books on the shelves, the file system contains information about the files on the media like the file's name, extension, location, size, and various date stamps. These attributes can be used to select files of interest and also assess whether the media should even be selected for further processing. After all, what might be of interest to the case is files of a certain type, from a certain time and related to a particular user. This kind of information can be readily determined by examining the file system data prior to actually processing any of the files themselves for processing.

Other important information can also be obtained from the file system data. For example, the file system could also still contain entries of files that were deleted, although it is possible that it will not reveal all files that have been deleted. Nonetheless for those deleted files that are contained in the file system there is likely enough information to assess whether there has been a spoliation issue that needs further examination before proceeding with processing and production.

As part of the file system analysis one can also search the media for prior instances of a file system. Finding these remnants can be important particularly if they are remnants from a file system that existed just prior to the preservation or after a duty to preserve had arisen. A lot of data hiding techniques would leave remnants of a prior filing system. Thus, finding these can also signal a spoliation issue that needs to be further examined before proceeding with processing and production.

In light of the above, one of the things that should be done during preprocessing is development of file system information with which to perform various analytics in order to better understand the contents of the various media in order to determine its usefulness to the case and assess what resources will be needed for processing, production and continued discovery.

Although lists are sometimes not informative enough, they, nonetheless, are a good first step that allows the requesting party to see what is available and how their requests can be better targeted. In addition these lists provide useful attribute information that confirm or deny attempted spoliation as well as provide important usage and trend information about the media and the data it contains.

Search indexes constructed

At some point the data will be probed with various kinds of search efforts. These efforts most frequently rely on indexes of document contents. Thus, before the searches can be run the indexes should be constructed.

Of equal importance is from what the indexes should be constructed. There are a couple of different issues that must be resolved about search index creation.

The first is that not all documents are searchable. Documents like images, for example, must first have their contents converted into a searchable form. Thus, one thing that must also be decided is how unsearchable file will be converted into searchable form. Typically, non-searchable documents are converted into some kind of format that can then be optically recognized.

The list of unsearchable document types can be surprising. A PDF document, for example, may not be searchable. In addition , it is hard t know for sure which ones are and which ones are not. Thus, it is often common practice to convert them all and then optically recognize them.

Even document types that are searchable like spreadsheets and word processing documents can still have embedded images. So, decisions should be made about how those should handled as well.

Second, not all search engines can index a document's internals. In such cases, things like application metadata will be missed. Thus, another decision is the extent and manner in which application metadata will be indexed.

A third consideration is the accuracy level of optically recognized text. Optically recognized text with low error rates can still miss important documents. Thus, it is important to decide at what accuracy level the recognition will be performed.

File activity constructed

Depending on the case the existence of a document may not be as interesting as whether it was viewed. There are several different ways to determine whether a document was actually being opened and viewed. If this is one of those kinds of cases, obtaining the file activity data from various file pointer sources will be useful.

Even if it is not a case where viewing a document is dispositive to a particular issue in the case, it may still be a useful means to narrow discovery to more meaningful documents, at least in a multi-stage discovery setting.

6. Data Analytics

At the end of the day every case comes down to a few hundred exhibits. Many of these may already be known at the time of initial disclosures under Rule 26(a)(1). Still others may still be buried within the data population.

In large part, discovery is about finding the exhibits needed for trial that are buried within the data population. For all practical purposes, however, the effort expended to sift through the larger population of documents just to find these few remaining exhibits is wasted effort. Data analytics is the process intended to reduce the wasted effort of finding these few remaining exhibits.

From a systems engineering approach, data analytics is the techniques for finding the documents without having to examine each one. Systems engineering is an iterative process that starts at the higher level item, such as those expressed in the complaint, and then moves into lower level components and processes with problem definition and decomposition, requirements synthesis and then back up with recomposition of the results into solutions and interfaces. With better clarity about the data population one can devise better document requests that better targeted at the documents that will matter.

As with the data preparation phase discussed previously, the traditional document review platforms are not the best tools for performing this kind of analysis. In fact, there are many other tools, like the computer forensic tools and third party specialty tools that provide these kinds of capabilities and can do it straight from the preserved data. Thus, there are economic reasons for using these special kinds of tools and avoiding the document review platforms until after the desired documents are actually selected.

A big question that needs to be answered is how much of the data analytics if any will be performed prior to submission of the discovery plan and issuance of the discovery order. The reason that this is such a big question is that the data analytics could very well narrow discovery dramatically, since the outcome of the analytics should be a clearer understanding of the documents that should requested and will be produced.

Without the analytics, production requests tend to be quite broad and overly inclusive. With the analytics the parties can have a much greater understanding of the data population both in terms of data volumes and data types and even what documents likely will be dispositive. Thus, there is considerable incentive for conducting the analytics prior to finalization of the plan and issuance of the order.

During the analytics it is not intended that there will be any documents swapped, although in some cases they could be consulted and the details shared between the parties. The intended benefit of the analytics is to obtain considerable insight about the data holdings as well as better identifying which documents are more likely relevant to the issues.

Since relevancy is a highly subjective decision, the analytics provide the requesting party with greater confidence that relevant documents will be produced as part of whatever production requests are ultimately fashioned. As a result, requesting parties can more comfortably narrow their production requests.

Before this kind of substantial information can be obtained there likely will need to be put in place protective orders and non-disclosure agreements, which could be one reason for why the analytics come after development of the discovery plan and issuance of the order.

Even if the analytics are not shared or at least saved until after approval of the discovery plan and issuance of a scheduling order, there is plenty of reason that the data owner will want to conduct its own analytics. In the event of a disagreement over the discovery plan, the data holder can use this information to persuade the judge that their plan for discovery is more consistent with the goals of discovery in the first place and the accomplishment of the Rule 1 objectives. After all, if one wanted to avoid a discovery dispute, the best way could very well be to prepare divergent paragraphs of the plan as suggested by form 52 and then support that position with empirical data derived from analytical testing of the population.

There are actually several types of analytics that should be performed and, of course, under a multi-stage approach there could be several iterations of the process. The kinds of analytics that should be performed are described in the sections that follow.

File System Analysis

The results of the data processing efforts discussed previously are often merged with the file system data by the kinds of tools that provide those kinds of results. The result of those efforts are often lists and tabular reports about the file system contents along with other attributes like hash values, encryption indicators, file signature results.

With this information there are many types of lists that can be used by both sides to identify desired documents for production. By using file system attributes along with other elements developed during the data preparation phase one can tell a lot about a document and if it could be of interest.

Storage location, dates, name, type are just some of the attributes that can reveal much about a document's desirability. Filtering data sets by these attributes can even be used to stratify the population for use with other selection techniques like content search.

Sharing the results of this analytical information along with distributions like those discussed below can help both parties to streamline a production request and target it for better accuracy and relevance as well as budget and schedule what it will take to more thoroughly review the data.

File type distributions

File type distributions based on the results of signature analysis provide informative information about data population content. The existence of file types of interest can be confirmed as can their quantity. After all, a smaller than expected population of desired file types could raise many questions including authenticity of the media or even spoliation.

The same can be said when file types that were not expected are uncovered. Such types could be added to what the parties had planned to consider.

File type distribution also provide planning and resource information. For example, not all file types are searchable. Thus, file type distributions provide insight about the volume of data that will need additional processing either before or after production.

File type distributions also provide planning and resource information about the population as a whole. The results could alter planned stage sizes, either larger or smaller, when a multi-stage discovery plan is being followed.

Custodian Distributions

The parties may have had certain expectations about the volumes of data held by certain custodians. Differences in expectations could again raise questions about authenticity of the media or spoliation. When custodian distributions are further refined by file type or other attributes still other questions could arise.

Of course, authenticity or spoliation are not the only questions. There could be others about resource requirements and the adequacy of plans to process, produce and review documents.

Time Period Distributions

Time period distributions, particularly when further refined by file types and custodians, are another useful tool when planning discovery and identifying documents of interest.

Other Distributions

There are plenty distribution analyses that can be used. Some of the other distributions of interest involve e-mail containers, message senders and recipients, unique versus duplicate files based on hash value.

File Activity Analysis

In addition to knowing what files exist, knowing which ones were actually opened and viewed could be of far more interest. The results of these analytics can be merged with other file lists and distributions to help narrow what documents are of the most interest and should be produced.

Document Search

Obviously some responsive documents will require more sophisticated methods to find. There are a lot of different automated techniques that can be used.

Regardless of the search method used like keywords, hashes, context, predictive coding, etc. one feature that should be included in the plan is that the parties will again share lists of the

search results. This provides the parties a means to examine just how effective the search methods are and make changes before going to full scale production.

The lists can be of two types. One type is a simple list of the files that includes various attributes like name, extension, file type confirmed by signature analysis, custodian, path location, various date stamps and hash calculations just to name a few. The report can be provided in tabular form like a spreadsheet so that the parties can perform additional analyses like sorting and filters about the results.

The other type of list is a context list that in addition to the basic attributes about the file includes some context around the selection criteria. The context list is probably better suited to keyword searching and provides a fixed number of words or characters either side of the keyword hit. The context provides the parties a means to assess the effectiveness of the search term and whether the document is relevant or more likely just a false positive.

A context result could also be provided with other search techniques like hash and predictive coding. In those situations, however, the supplied context could be the first 100 words of the document or something similar that again could be used by the parties to assess the relevance of the document.

7. Handling Privilege and Confidential Items

How to handle privileged documents is always an issue to be discussed. It is even one of the items expressly identified in Rule 26. Of course, privileged documents are not the only issue. The handling of confidential data is also something that should be discussed and resolved. In fact, the handling of confidential data is also something that is expressly identified in Rule 26 to be resolved in the 26(f) conference and Discovery Plan.

Naturally, each side will handle the manner in which they choose to find and identify privileged and confidential information. What needs to be resolved is the mechanics of protecting that data.

Handling Privileged Documents

Generally privileged information will be withheld but the particular documents identified in a privilege log. In complex documents it is possible to resolve the issue by redacting the privileged information while producing the remaining portions of the document.

Despite the above, there are several issues that are still up for discussion. For example, with compound documents like e-mails and compressed archives (zip files) what should happen if only one of the documents contains privileged information but the other documents in the collection are not privileged? Should they all be withheld or only the one containing privileged information?

E-mail chains provide another issue for privilege. While a single message that incorporates an e-mail chain is a single document for asserting the privilege, each original message of the chain parts are separate communications. Thus, to protect the privilege under

Rule 26(b)(5) each instance in the chain must appear in the privilege log. (see, Properly Logging E-mail versions Key to Maintaining Privilege and Avoiding Sanctions) When creating the plan the parties should make it clear that each message should appear in the privileges log.

Another consideration that can be included in the plan is a clawback agreement. A clawback agreement permits the return of documents without waiver. Generally clawback agreements are used in the context of privileged documents but they need not be limited to privileged documents. In fact, they could be more broadly constructed to permit the return of any document mistakenly produced.

Clawback agreements are an attractive feature intended to keep discovery costs low by minimizing the need for strict document review during discovery. While the agreements are often enforced that is not always the case. Exceptions have been made based on the reasonableness of the procedures employed to prevent the inadvertent disclosure of documents. Some clawback agreements have even been crafted in a way that emphasizes the reasonableness requirement in order to protect privilege. In addition, state law cases have not always followed federal procedures, particularly when waiver protections are more narrowly construed. In any event, clawback agreements are a nice feature for every discovery plan but parties should recognize that they may not be foolproof.

Handling Confidential Documents

The handling of confidential information has many similarities to privileged information, although the issues is not one of non-disclosure but of limited disclosure. As with clawback agreements the parties can negotiate what documents are subject to confidential status as well as the special handling procedures associated with those documents.

Confidential status could be provided in several layers. Some documents may just have public sensitivities and need to be protected from public disclosure of the case documents. Others could have more sensitive status that restricts disclosure from the opposing party, although it may be disclosed to the opposing party's experts and legal team.

The special handling of confidential documents will involve special marking procedures as well as restrictions on disclosure. When electronic or native format files are concerned the marking may need to be suffixed or prefixed in the file name, since it may not be possible to alter the original document without altering the evidence itself.

As with privileged documents, confidential documents could have a clawback arrangement of sorts. In other words, documents that were inadvertently produced without the proper markings and restrictions could later be so designated and restricted. As with privileged documents some kind of disposition treatment of the inadvertently produced documents, like return or destruction of the inadvertently produced documents along with any copies subsequently made, will need to be included once they are detected.

Special Access Procedures

Sometimes it is just simpler to be open kimono and one party allow the other full access to its electronic data. It might be a gesture of openness or it might be a way to shift discovery costs to the requesting party. In either case, the parties will need to develop a plan for handling privilege and confidential data issues.

In some cases, the access is desired by requesting party that can be resisted by the producing party, particularly if it appears the requesting party's real agenda is just weaponization of the discovery process. In other cases, the producing party may be very content to let the requesting party have complete access. (see, Gaining Access to Computer Forensic Images)

In such cases, the parties generally agree that an expert will have full access to the digital data. The expert could be a neutral expert or it could even be the expert retained by one of the parties like the requesting party.

The expert will conduct whatever tests or searches are desired by the requesting party. In the event that the expert finds anything of interest, he first produces the data to the producing party for privilege review and other restrictive markings before producing the cleared data to the requesting party.

In such situations traceability and configuration issues are very important. Thus, the expert not only produces the data of interest but also other attributes about the data so that it can be traced back to its original source. The other attributes could include things like unique identifiers, original and produced file names, the path location, MD5 hash value, and file system date stamps.

For efficiency purposes, the process could also follow some of the analytic procedures discussed previously where the process starts with lists that are cleared by the producer before being supplied to the requester. The lists then become a basis for the requester to request certain documents for further review. The specifically requested documents are then provided to the producer for clearance before being provided to the requester. Essentially, these types of techniques provide a means to narrow the document productions and only produce those that have passed several layers of selection.

The procedures need not be limited to just documents. The produced results could be the results of forensic analysis as well.

Of course, under these special procedures, whatever they might be, the expert is only allowed to discuss those things with the requester that have been cleared for production. Consequently, it is important that both sides have confidence in the integrity of the expert.

8. Production of Documents

The production of documents is normally done in response to Rule 34 production requests. That prospect may still exist even when as part of step 6 discussed previously, data analytics, agreements were reached regarding the criteria for document production such as keyword hits and other data attributes.

Once the documents have been selected it is just a matter of processing and producing them. Of course, document review is usually done at this time as well, which makes this stage of the disclosure process the most costly portion.

Indeed, the processing and production portion of the plan is where a lot of different technical details will be resolved that if not specified could cause problems later on. The kinds of things that will be resolved in this section are the production format, usable form, metadata, duplicates, compound documents, special file types and the rate of production.

Format

The form of production is one of the topics to be addressed by the discovery plan under Rule 26(f)(3)(D). With respect to form there are several options. The most obvious is native format. The other option is to produce the documents in some kind of imaged format like TIFF or PDF. There are pros and cons to each of these.

While the image formats have been very popular for a lot of reasons, there is also added cost of production associated with the conversion process from native to the imaged format. From an efficiency perspective, native format is the most economical since it avoids the cost of conversion.

Of course, the native option only exists for ESI. Many cases can still include some amount of paper based documents. For paper based documents the options are to produce in paper or to produce in imaged format.

Making the choice between format is not simply an economic decision. There are other considerations as well that involve useful form.

Usable Form

The usable form issue can be quite significant when producing documents. One of the issues that has gained considerable interest in recent years is the application metadata, which is the internal data attributes about a document that are not visible when the document is displayed in its presentation format. Rather, this data is never displayed but is can be useful nonetheless.

While native forms contain the application metadata, the imaged formats will not reveal that data. Instead, when imaged formats are produced the metadata must be extracted. The problem there is that the available metadata is not the same between different document types. In fact, it could be very different between types and it is impractical to construct a process for capturing them all and a database for holding them all. Consequently, it has become common for parties to swap native documents even when they are swapping imaged based formats.

The application metadata is not the only usable form issue. When images have been produced without also providing the native format it has been decided that not producing searchable text along with the image format is not usable form. Of course, the parties could agree to produce only image formats if that was their choice and there are reasons for doing so.

When native documents are not produced and only an image format is produced then the only way to be searchable text is to create the searchable text by OCRing [Optical Character Recognition] of the image format. While OCR technology is much improved it is still subject to some error. The error could have adverse consequences of the usefulness of the searchable text. Consequently if the parties are going to agree to swap searchable text then they should also impose performance standards on the accuracy of the searchable text. Of course, achieving something highly accurate like 99 percent could be very expensive and difficult to achieve. Rather than imposing those costs on the producing party, what might be more reasonable is for the parties to swap images without searchable text and then each of them could decide how much they want to expend on getting the searchable text.

If they decide to forgo producing the searchable text and letting each party obtain its own, another factor that they will need to consider is the quality of the images. Low quality images will produce low quality searchable text. Consequently, to assure an image is in usable form the parties will also want to agree on specifications for the images such as resolution and sharpness. Of course, they could avoid the entire issue by just producing natively, at least for ESI. If the production includes any amount of paper based documents then the image based option is still possible as would be the option to simply exchange copies. In either case, the parties could include these details in their plan and avoid disputes later.

Metadata

It is often said that metadata is data about data. In the context of e-discovery metadata is not just the application metadata that is internal to a particular electronic document. In the context of e-discovery metadata is also the data that is captured in the document management database that pertains to the document.

When parties produce documents they expect to receive metadata about those documents from the producing party. Consequently, part of what the parties should decide upon is what metadata they will be exchanging along with the document.

Some of the obvious metadata elements are the custodian and/or identifier for the particular media when a custodian has more than one type of media. It is very common for a single custodian to have more than one piece of media once one considers things like attached devices. Similarly, when system resources like servers or backup tapes are considered it is also possible for the custodian to have several different media. Thus, issue to be resolved about metadata is not just the application metadata contained within the document itself.

Other common attributes besides file name and extension are the location of that particular file on a media. Still other attributes are file system date stamps. If the document is an e-mail message then it could be things like the subject, sender, recipient and message date.

While the above attributes are metadata that can be harvested from the media on which the document was located, there are other attributes that are determined during processing, like the MD5 hash used for subsequent verification and de-duplication, and bates numbering that is determined at the time of production.

While there may be many different metadata elements that could be desired by the parties and incorporated in their plan, there are many standard elements as well. Perhaps the bigger point is that if the parties have an expectation about what data should be swapped they should include it in their plan before expending considerable resources and then realizing the work was totally inadequate.

Besides what specific metadata attributes will be exchanged there is still another element on which the parties should agree. That additional element is the format and structure of the metadata and the produced documents.

It is not unusual that for the two sides to be using different document management systems. Ideally, each party will want to receive the documents and their respective metadata in a format and structure that can be ingested by their own system without any additional work. Although there are tools that are useful in making conversions, the most efficient will be when no conversions are needed.

Handling of Duplicates

Although duplicates have frequently existed in every production, at least since the birth of the copy machine, duplicates are particularly frequent in e-discovery. The use of e-mail further aggravates the problem as does various data retention practices and disaster recovery systems.

Parties may be able to help themselves by deciding how to handle duplicates. In its simplest form, the fact that duplicates are found in different periods of a backup rotation scheme is of no interest. As a result, the parties could decide to ignore the duplicates and only consider producing a unique version.

Things get more complex when the same document can be found on the machines of different custodians, although depending on the document type and nature of the case it may make no difference at all. If the document were a simply vendor invoice, it could make no difference how many copies existed and there they were found, particularly if there was no dispute about the invoiced item. On the other hand, if the document were the trade secret of a competitor, it could make a lot of difference about how many places it was found and the timing of its arrival at each location.

As part of their discovery plan the parties could decide how to handle duplicates. It need not even be a single rule for all documents. Rather, it could be quite stratified.

As a result of the preprocessing analytics the parties could know quite a lot about the population based on document types and the distribution across custodians. As a result of the scope definition and preservation effort they would also know a lot about the various storage systems being used by each custodian. With this information they could decide that certain document types should be produced as singles only across the entire document population, while other document types should be singles only within a particular custodian or storage media.

Even if the parties agree to produce singles only across the entire document population, which would produce the smallest document population and probably the greatest overall

efficiency, they could rely on various document lists developed during preprocessing analysis to reveal all instances of a document's location when such information was of interest for a particular document.

Handling of Compound Documents

As discussed before, compound documents are those with many parts. In the normal sense of things, they tend to be compressed archives (zip files) and e-mails. The issue worthy of discussion by the parties is how to handle compound documents, particularly when not everything about a compound document is relevant to the case.

It is common practice that all parts of a compound document should be produced if any of it is responsive. With regards to e-mails this is likely the best practice to follow. With regard to compressed archives such a practice is questionable. A better approach may be production of just the responsive documents within a compressed archive while having a re-opener of sorts that permits subsequent production of other element should questions about their relevance develop.

Again, if the parties have followed the preprocessing analytic procedures discussed previously and shared the results, they likely will have lists that can inform them about the other documents that were captured in a compressed archive but not produced. Should a particular document prove significant the parties could first consider those lists to help them decide whether any additional files are needed.

Handling of Special File Types

When native files are being produced then all responsive documents will assuredly be produced. The question becomes when the production is format is an image format or includes an image format. In the case of image format based production there are several different native file formats that just sensible for images based production.

Spreadsheets are one file type that is not always suited for image based production. The issues with spreadsheets are many. First, the layout of the spreadsheet may not be symmetrical. Thus, when the data is reduced to a two dimensional matrix the result could include large amounts of blank pages.

Second, the spreadsheet could have many hidden columns and rows or even columns that are too narrow. Revealing the hidden columns and rows or resizing the rows could again disrupt its presentation and result in huge amounts of additional pages to be created and even make the presentation harder to comprehend.

The solution for spreadsheets is to either produce them all in native format or to limit the image based format to only a few pages while still producing the total file in native format. The exact procedure for handling spreadsheets is something that the parties could negotiate and specify in their plan.

Database tables are another problematic file type. Database tables are essentially tabular data like spreadsheets. Database tables could easily result in image based documents that are huge. In addition, the presentation of database contents in a tabular image based presentation could be very hard to comprehend. Another problem is that for database table data to be meaningful it often has to be related to the contents in other database tables. Without making the relationship the database table data could be totally incomprehensible. A final issue for databases is that in some forms the tables are not separately exposed but rather encapsulated in another kind of wrapper.

The solution for databases is very much like spreadsheets. It is best to rely mostly on native format production or to limit the image based production to a few pages while still producing the total database table file in native format.

The reality is that not all kinds of digital evidence is a document. There are other kinds of challenges as well with things like voice mails, audio and video. If the parties have used the preprocessing procedures they will have a good understanding about the kinds of data in the population. They can use this information to assess the data types and agree on what will be the best production formats and methods.

Rate of Production

It is very common that productions will be made in increments and not all at one time. The increments are particularly applicable when some kind of privilege review is being performed and a determination has to be made in a timely matter. In such cases, the parties will want to set time limits. The question is what those limits should be.

Frequently, limits in these cases are expressed in pages. The issue there is that pagination is an abstraction imposed by printer requirements. When producing native format documents pages have no significance. Even the gigabyte size could have little significance because current Microsoft Office documents utilize compression technology that can make conversion to document sizes hard to interpret.

It is hard to apply a magic parameter to solve the production rate issue. The parties will simply need to examine the document population and perhaps group the documents into similar type and then apply some kind of production rate.

9. Include Disputes Provision

Disagreements inevitably happen. Consequently, every good contract contains a disputes provision. The discovery plan should be no different.

The alternatives are not limited to a telecom with the judge or even a motion hearing. Indeed, the disputes provision does not have to strictly follow traditional disputes processes. In other words, it does not simply have to provide the adjudication of an issue. There are, in fact, several different approaches that could also be incorporated.

First, counsel could involve each side's technical experts and allow them to have open discussions about the issue. Counsel may have already discussed an issue with his technical expert but that is still not the same as free communications between two similarly skilled persons.

It is not even necessary that the two technical experts reach a conclusion or that their ideas be adopted without first subjecting them to more penetrating analysis off stage. Indeed, initial discussions where ideas are simply brainstormed and discussed could always be the precursor to a final negotiation and settlement.

Second, counsel could also include is a joint consultation with another expert--a neutral expert of sorts. Electronic discovery can be very technical. In addition, there could be several different ways to solve a problem. Thus, another thing that the disputes provision could include is consultation with a third party expert who can comment of the wisdom of opposing ideas, suggest an entirely different solution, or just share experiences about how certain processes are typically handled and let the parties pick their poison so to speak.

Clearly, there are all kinds of potential issues and all kinds of alternatives for settling them. Actual motion hearings would surely be the least desirable but may be unavoidable nonetheless. If the dispute actually escalated to that point then the dispute provision may also want to include a provision for the prevailing party to receive costs and fees.

10. Assign Cost Responsibility

The plan should also assign who will pay for the cost of the discovery process. Generally, each side will pay their costs.

Experts will likely be involved in assisting with the discovery in several areas such as helping to identify ESI sources, preprocessing analysis and final processing and production. Again, each side will typically pay for their own experts.

It is possible that the parties could also pick a common expert to assist with the discovery effort in hopes of gaining greater efficiency. In that case there may be cost allocations or other methods for determining cost responsibility. The allocation of costs could be simply based on the data being processed and who owns it. Then again their could be other agreements such as expanded access to one party's data in exchange for the costs of processing being shouldered by the requesting party. In the end, there are all kinds of deals that could be made as part of the negotiation of the discovery plan procedures.

When a multi-stage discovery approach is selected there could be other factors for determining cost allocation. For example, if the first stage, which would likely be the data sources with the greatest chance of having responsive and relevant ESI, produces no fruit then perhaps the cost of proceeding with the next stage should be totally born by the requesting party.

Similarly, there could be a disagreement between the parties about the scope of discovery. One party wants expansive discovery while the other sees it as just a fishing

expedition. One way to resolve the scope issue is to include cost shifting provisions into subsequent stages of the discovery population. Perhaps costs would be shifted to the requesting party and then only shifted back to the producing party if relevant ESI was uncovered. The definition of relevant could even be structured to exclude duplicates of data already found unless the finding was more than just mere possession and amounted to material usage.

If neutrals are used for any aspect of the litigation or discovery process there are likely some special procedures that should be considered. Neutrals are in a tough spot and not just because of their duty for neutrality.

Someone is going to lose the case. If the neutral is in any way involved in that effort, even if it is strictly in the execution of their assigned duties, they will likely become a target for removal. For example, if the result of the neutral's preprocessing analytics it becomes clear that one side has spoliated evidence, the neutral is likely to become a target for removal by the disrobed party.

One way for the disrobed party to target the neutral is to manufacture a dispute with the neutral such as by not paying for the services provided. In such a situation the neutral is an a difficult position. If he does nothing the disrobed party will always claim that his work is always retribution for whatever services have gone unpaid. If the neutral tries to collect the unpaid amounts then again the disrobed party claims that his work is always retribution for whatever services have gone unpaid.

As a result, any compensation plan involving a neutral should be designed to protect the neutral's work from the shenanigans of disappointed parties. As such it may be best to have the neutral paid in advance or on a replenishing retainer basis for any work performed.

There could still be other considerations about the assignment of costs. For example, if spoliation is detected then the parties could have agreed in advance that the spoliating party pays the costs of the more detailed forensic analysis that is needed to evaluate the spoliation. (see, When Does Respondent Pay for Inaccessible Data)

Whatever cost allocation the parties negotiate they could also limit the costs to "reasonable" costs and describe what "reasonable" costs might be and include whenever the responsibility of one is shifted to the other. For example, if some kind of shifting is desired as a result of apparent spoliation then the analysis is not an open check book but one where the efforts employed are reasonable and proportional. Arguably such vague terms could lead to more motion practice so the parties may want to be more explicit and rule out inefficient methods like manual document review in favor of various technology assisted review techniques, for example. In other industries it is not uncommon for agreements to limit these kinds of costs either by their nature, amount or rate.

11. Disposition of the Data

The final element to be considered is the disposition of the data at the end of the case. This particular element does not really help with execution of the case. Rather, it just ensures

that there is an ending and both sides can know when to cut any continuing costs that go with storing and safeguarding the data.

Both sides will need to retain their own data for the duration of the case. Since they will have exchanged data they each are also holding the other's data. So, the disposition issue not only involves their own data but the other's.

The parties can include what kind of notice is needed in order to trigger the destruction of the data. They can also include what procedures should be followed for the destruction such as wiping in addition to simple deletion. A final element can be certifications of data destruction that each side can exchange with the other.

Costs and Consequences of Developing a Good Plan

Developing a good plan takes both time and effort in addition to expertise. Frequently, project managers under estimate the importance of a good plan and move quickly to project construction for cost or schedule reasons. Such thinking is flawed, since it inevitably results in a longer project performance period and higher costs.

Over the years there have been many efforts to determine the optimum amount of advanced planning for any particular project. While each project is different and there is no magical ingredient, the rule of thumb has become that 15 to 20 percent of the overall budget should be allocated to advanced planning.

This 15 to 20 percent is not an additional cost, however. Rather, by spending that much on advanced planning the overall costs of the project is often cut by 50 percent or more when compared to similar projects without the planning effort.

Some have even thought to stratify projects needing advanced planning. The thinking was that only complex projects would benefit from the overhead of advanced planning. This has proven not to be the case, however. Studies have found that smaller projects took longer and cost more than more complicated projects when systems engineering disciplines were not fully applied to smaller projects.

Smaller projects will have less complicated issues. As a result of these less complicated issues, they will result in less planning costs. The idea that smaller projects should have less discipline in the planning effort simply undermines the benefits that planning will bring.

Summary

Successful managers of complex projects know the importance of good planning. In fact, successful managers of all kinds of complex endeavors like software products, hardware items, building construction, military operations and even professional services know the importance of

good planning in delivering a final product that performs as intended as well as one that satisfies its cost and schedule criteria.

Litigation is a complex product, too. It has many parts like pleadings, orders, reports, hearings and the trial itself. One of the largest components to any litigation is discovery, which itself has many elements that must be optimized for efficiency and effectiveness.

The primary constraint for civil litigation is the, "just, speedy, and inexpensive determination of every action and proceeding" as expressed in Rule 1 of the FRCP. Unfortunately, that goal is seldom achieved because of poor planning and a failure to follow the rules in the first place.

The 26(f) conference and discovery plan are not just a requirement in a rule book. Indeed, they are the means by which clients and counsel bring sanity to the disclosure problem in order to accomplish Rule 1 objectives.

In traditional planning approaches the focus of the plan is on production. The planning and design phases are less rigorous and the flaws of the initial plan might only be recognized when production itself fails.

Systems engineering takes a more thoughtful approach to plan development. Perhaps most significant difference is that the thoughtfulness is moved forward in the development process in order to avoid wasteful production failures. In the process it improves problem decomposition and definition, requirements synthesis and then recomposition and process development. As a result, while developing the plan the actual objectives are sharpened as one evaluates decisions and the effects of trade-offs between the cost, schedule and performance/quality criteria.

Developing a good plan takes both time and effort in addition to expertise. Frequently, project managers under estimate the importance of a good plan and move quickly to project construction for cost or schedule reasons. Such thinking is flawed, since it inevitably results in a longer project performance period and higher costs. Thus, avoiding good planning as a cost savings measure never results in any cost savings. Rather, it results in just the opposite.

The rule of thumb has become that 15 to 20 percent of the overall budget should be allocated to advanced planning. The 15 to 20 percent is not an additional cost, however. Rather, by spending that much on advanced planning and employing proper system engineering disciplines the overall costs of the project is often cut by 50 percent or more when compared to similar projects without the planning effort.

CHAPTER 11

Understanding ESI Admissibility: When You Absolutely, Positively Have to Win

Introduction

Evidence is defined as something or a set of things that shows something else exists or is true or, at least, is helpful in forming a conclusion or judgment about an issue. In legal proceedings somethings may never be considered as evidence if it does not satisfy the rules determining whether it even qualifies as evidence. In other words, in legal proceedings before "things" can be used as evidence they must have a certain purity. As a result, when resolving a

legal proceeding it is not enough to have formulated an answer, since the ingredients must pass various purity tests.

The rules are designed to secure fairness in Judicial Administration, to eliminate unjustifiable expense and delay, and to promote the growth and development of the law of evidence so that truth may be ascertained and proceedings justly resolved. The rules are not intended to result in an exhaustive search for a total and complete understanding of every civil and criminal case that comes before a federal court. Rather, the rules are meant to assist lawyer-adversaries and common sense triers-of-fact in resolving particularized legal disputes. Accordingly, the rules give courts authority to adapt the laws of evidence to circumstances as they arise.

The Federal Rules of Evidence were adopted by order of the Supreme Court on November 20, 1972, transmitted to Congress by Chief Justice Warren Burger on February 5, 1973, and became effective on July 1, 1973. In enacting these rules, the Supreme Court and Congress did not intend to wipe out years of Common Law development in the field of evidence. To the contrary, the Federal Rules of Evidence largely incorporate the judge-made, common law evidentiary rules in existence at the time of their adoption, and where the federal rules contain gaps or omissions, courts may answer unresolved questions by relying on common law precedent. Like their common law predecessors, the federal rules govern the overall admissibility of evidence, the limitations of relevant evidence, the definition of prejudicial and cumulative evidence, the admissibility of Hearsay, lay and Expert Testimony, the nature of evidentiary presumptions, the grounds for authentication and identification of documentary evidence, and the scope of evidentiary privileges, like the work product, attorney-client, and doctor-patient privileges.

In 1974, the National Conference of Commissioners on Uniform State Laws adopted the Uniform Rules of Evidence, which were designed to be identical to the Federal Rules of Evidence. Cases interpreting the Federal Rules of Evidence are helpful in the analysis of state rules that are based on the Federal Rules of Evidence. In fact, some jurisdictions have held that a rule of evidence patterned after a Federal Rule of Evidence should be construed in accordance with federal court decisions interpreting the federal rule. Thus, state courts in these jurisdictions will look at the federal rule's history and purposes in interpreting the provisions of an identical state rule of evidence.

Whether potential evidence is admissible becomes important at two points—summary judgement and at trial. It is at these two points where rules of evidence come into play. A party's evidence simply cannot be considered if the rules' hurdles have not been crossed. Remarkably, it is a long journey from the initial declaration of war to the final dispositive battles of summary judgment and trial. Furthermore, the road is torturous and there are many pitfalls along the way that can turn what seemed to be powerful ammunition into a complete dud.

There are no special rules governing the admissibility of ESI. To be admissible, potential evidence must first satisfy two conditions. First, it must be relevant under Rule 401. Second, it must be authentic under FRE Rule 901, although a foundation for authenticity is usually laid prior to its consideration of relevancy.

If it is relevant and authentic, then it still must clear three other hurdles. First, it cannot be hearsay under rule 801. Second, it should be the best evidence available under rules 1001 to 1008. Finally, its probative value must outweigh its ability to unfairly prejudice a party under rule 403. Each of these five tests are discussed in the sections that follow.

Relevant

The first test for admitting ESI as evidence is that it must be relevant. Article IV and its related 400 series of rules govern whether evidence is relevant.

Rule 401 generally governs the relevancy issue and defines relevance as “any tendency to make a fact more or less probable than it would be without the evidence and the fact is of consequence when determining the outcome of the action.” Rules 402 to 415 then go on to examine the relevancy issue in light of select circumstances such as the existence of liability insurance under 411, compromise offers and negotiations under 408, and issues related to sex crimes under Rules 412 to 413 just to mention a few.

None of the rules on relevancy provide any unique challenges for ESI, although several of the relevancy rules involve subject and issue for which ESI would likely be the evidence whose relevance is under consideration. With regard to ESI, therefore, the primary constraint for relevancy is does the item tend to make a fact more or less probable than it would be without the evidence.

Authentic

The second test for admitting ESI as evidence is that it must be authentic. When it comes to ESI, it has been long established that computer records are subject to the same foundational issues as other evidence.[10] What these earlier cases have held is that the computer information is trustworthy and it is what it purports to be. This determination has often involved an examination of the computer itself along with its programs and data input to determine that the information it contains is trustworthy. It may not be enough for someone simply to testify about the product produced by the processes without establishing the proper functioning of the underlying equipment and processes.[11] Indeed, the increasing complexity of computer

[10] *U.S. v DeGeorgia* 420 F.2d 889, (9th Cir. 1969) at FN11, ". . . [I]t is immaterial that the business record is maintained in a computer rather than in company books, this is on the assumption that: (1) the opposing party is given the same opportunity to inquire into the accuracy of the computer and the input procedures used, as he would have to inquire into the accuracy of written business records, and (2) the trial court, as in the case of challenged business records, requires the party offering the computer information to provide a foundation therefor sufficient to warrant a finding that such information is trustworthy. " ; See also, *U.S. v Russo*, 480 F.2d 1228 (6th Cir. 1973) at 1240, ". . . [O]nce the reliability and trustworthiness of the information put into the computer has been established, the computer printouts should be received as evidence . . ." ; and also *U.S. v Croft*, 750 F.2d 1354 (C.A.Wis. 1984) at 1365, "The record reveals that defense counsel thoroughly cross-examined Laufenberg concerning the accuracy of the computer and the input procedures."

[11] *In re VEE VINHNEE*, 336 B.R. 437 (2005)

technology necessitates similar concerns and questions about the evidentiary foundation of ESI that includes the proper functioning and reliability of the computer system from which it came.[12]

Article IX of the FRE and its related 900 series of rules govern the authentication and identification of evidence. Remarkably the issue of authenticity is a low bar. A court need only infer that a document is legitimate. If the means of confirming authenticity is overly complex or burdensome the evidence, may well be accepted nonetheless and then the issue of its authenticity will simply go to the weight of the evidence when considered by the trier of fact. It is only where there is no evidence from which the trier of fact can reasonably conclude that it is authentic that the judge can withdraw the evidence from consideration by the trier of fact.

Clearly to have the evidence admitted the proponent must make some kind of showing that the evidence is authentic and that it is what it purports to be. At the same time, the opponent can question the authenticity of the evidence in hopes to have it excluded or its significance diminished. It is not enough, however, to simply question the adequacy of the foundation laid without having an underlying dispute about the authenticity of the evidence itself.

There are three rules in the 900 series that address authenticity. There is 901, which imposes the general requirement that the proponent must, "produce evidence sufficient to support a finding that the item is what the proponent claims it is." Rule 902 describes certain kinds of evidence that could be self-authenticating and Rule 903 says that witness testimony is required for authentication only when required by law.

In most situations only Rules 901 and 902 will be relevant to the authenticity issue. Within these rules there are multiple parts but there are only certain elements of their requirements that are more likely relevant to ESI than any other of the elements in these two rules. Each of these rules and the portions more likely relevant to ESI are discussed in the sections that follow.

Witness Testimony under 901(b)(1)

Probably the most often used and simplest method of authentication is the first example listed in 901, Testimony of a Witness with knowledge. Typically, this is the person who created a document or witnessed it being created or sent. When it comes to ESI, however, this could be a very unreliable method of authentication and one that can easily be impeached

Unlike its paper counterpart, ESI is easily changed whether on purpose or by accident. Thus, the easiest way to impeach witness testimony about authentication is through some rather simple questions such as the following.

- How do you know that this is the exact document about which you are thinking and that this version is not different and has not been changed?
- Do you know when the document was last changed and what those changes were?

[12] Manual for Complex Litigation, §11.446, *Use at Trial,* "Computerized data, however, raise unique issues concerning accuracy and authentication. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. . . The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy."

- Can you recite the document contents to me?
- Do you know if the hash value of this document is the same as the one that you are thinking about?

Chances are that the kind of witness that typically testifies about document authenticity will neither be prepared for this kind of questioning nor have the technical skills to competently and persuasively answer the questions. The more complex the document the less likely that witness testimony is credible. Of course, if it is a simple document like a simple one line message then testimony from the document creator or a witness to the document creation or being sent can be credible.

Comparison by an Expert Witness or the Trier of Fact under 901(b)(3)

When something was taken there could be a need to know whether what has now been found is actually something that has been taken. Whether what has been found is something that has been taken may not be obvious because it may have been disguised. For example, the ESI could be given another name and even a file extension in an attempt to camouflage its true identify.

A visual inspection could indicate that the two are at least very similar but visual inspections can be fallible, since the human eye itself is fallible. In addition, the one taking the data may have devised a story to explain that the two look alike, although the version that has been found was created from memory. Thus, there a lot of reasons why comparison by an expert using more specialized techniques can be a superior authentication method.

One method that could be used by an expert for comparison purposes are hash values. These are discussed in earlier portions of this manual. Hash values would not be changed simply because the name had been changed. Similarly, different file system dates would not alter the hash value since both the name and file system dates are separate data elements from the document itself. In fact, the hash value would change only if any of the contents of the document had been changed.

It is not unusual that contents of a document have been changed to further camouflage the document. For example, headers and footers or titles of the document could have been changed. If that is the case that may not by itself negate the usefulness of a hash function because the hash value is calculated on a data stream. Thus, if known changes could be eliminated then the remaining portions of the document could still have their hash values calculated and compared. An identical hash value of the remaining similar portions could still be telling, particularly if the similar portions were significantly large. The hash calculation is quite sensitive and different results would be calculated if so much as a “bit” was different. If the remaining similar parts are significantly large than the probabilities that such similarities could have been achieved without a taking become quite remote.

Hash values are not the only comparison. There are others that can compare and catalog where the differences exist. An examination of those differences could also help to determine how likely the two documents are not similar or derived from the same original source.

Another method of comparison is based on internal metadata within the document. These types of comparisons are discussed in the subsequent section on self-authentication.

Distinctive Characteristic and the Like under 901(b)(4)

Rule 901(b)(4) allows the proponent of an item of evidence to authenticate that item based on its "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with other circumstances."

As explained in the introduction to this admissibility section, the FRE were developed in the early 1970's and based on then existing common law evidence rules. Thus, the FRE were developed prior to when ESI was ubiquitous and the basis of most evidence was a paper record. In the paper world a distinctive characteristic could be something like someone's initials or some other mark on a document that is inseparable from the document itself. The authenticating patterns envisioned by the rule are not limited to physical marks, however, and can extend to language patterns.

In the ESI world, a distinctive characteristic could be entirely different than a physical mark or visible attribute. While many might consider something like a water mark or a logo or signature as qualifying as a distinctive characteristic, that is not likely the case in the context of ESI. All too often these kinds of characteristics are not "burned" into the digital data itself such that they are inseparable from the base document. Rather they are typically just some other object that has been embedded in the document along with many other objects that when considered in their entirety comprise the entire document. Since they are simply another object embedded in the document and not "burned" into the document, they are easily copied from other sources or even overlaid or edited with sophisticated editing programs.

The distinctive characteristic of ESI that could be useful for its authentication are things like the hash value discussed previously and the metadata elements discussed in subsequent sections.

Evidence About a Process or System under 901(b)(9)

Rule 902(9) allows the proponent of an item of evidence to authenticate that item based on, "evidence describing a process or system and showing that it produces an accurate result."

As stated previously, ESI is more easily altered or changed than its paper counterpart. In fact, it may even be a complete fabrication. The integrity of ESI can be further complicated by the integrity of the system in which it resides. For example, dates and the timing of when things happened are often important facts when resolving a legal action. The dates surrounding ESI often depend on the integrity of the system clock for the computer device from which it was collected. Thus, if the system clock is inaccurate so can the dates associated with ESI.

Dates are not the only issue that causes concern. There are other adverse consequences that can be caused by other factors such as power failures and environmental issues. When the item is the result of processes there can be issues about the logic of programs or other

automated processes. The issues can become even more complicated if the device from which the item is harvested is a complete counterfeit. For all of these issues, however, there are ways in which they can be detected and the problems identified.

There are many facets about a process or system that should be authenticated. Some of these are discussed in previous sections about validating the evidence. Some of the specific things to consider and that are discussed are validating that the device is an original and not a counterfeit and that the system clock was accurate.

Self-Authenticating Inscriptions under 902(7)

Rule 902 lists twelve different methods that will be accepted for self-authentication of a piece of evidence. Only one of these could potentially apply to ESI. That one method is the existence of "trade inscriptions and the like" under 902(7).

Under 902(7) evidence can be self-authenticated by way of an inscription, sign, tag, or label purporting to have been affixed in the course of business and indicating origin, ownership, or control. In terms of ESI these kinds of self-authenticating inscriptions are likely to be found in the document's metadata.

The term metadata is often defined as data about data. With respect to ESI there are generally two types of metadata. There is system metadata and application metadata.

System metadata involves various files and their contents that are used by the "system" to operate and manage the device and its contents. System metadata can include well known attributes like file system dates (create, modified and accessed), and system logs just to mention two. What system metadata is available is highly dependent on the system being used to manage the device. System metadata for Microsoft based systems will be different from Apple based systems. System metadata is an important means of authenticating that the system is functioning properly as discussed in earlier sections.

The other type of ESI metadata is application metadata. This is the kind of metadata contained in the individual files such as spreadsheets and text documents. The metadata can be different for the many different types of files. In fact, there are many different metadata standards for the various different file types. In addition, the metadata attributes for each file type can change with different versions of the file standard when file format changes happen such as .DOC to .DOCX.

Some of the more frequent types of evidence to which these self authenticating inscriptions can be helpful are in the areas of e-mail, photographs, Adobe documents and essentially any document with application metadata. The subject of application metadata is discussed in greater detail in the chapter on metadata analysis.

Certified Records Generated by an Electronic Process under 902(13)

Rule 902(13) is one of the new amendments to the FRE that takes effect on December 1, 2017. It essentially applies to records generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirement of 902(11) or (12)

Certified Data Copied from an Electronic Device, Storage Media or File under 902(14)

Rule 902(14) is one of the new amendments to the FRE that takes effect on December 1, 2017. It essentially applies to data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12).

The Hearsay Exclusion

Hearsay is defined as a “statement” that was made outside of the courtroom. Out-of-court statements are deemed less reliable because declarants of out-of-court statements are not sworn under oath, are not subject to scrutiny by the trier of fact at the time of their making, and are not subject to cross-examination which could expose inconsistencies and weaknesses in them. Rule 802 excludes hearsay unless it satisfies one of the many exceptions provided by the rules or by statute.

All kinds of ESI evidence will inevitably encounter the hearsay exclusion. If they satisfy the requirements for one of the many exception they can be admitted, however. The following sections examine the most likely exceptions that would apply to ESI.

Non-Hearsay Statements

The best way to avoid the hearsay exception is if the statements are not actually hearsay as defined in the rules. An out-of-court statement will meet the definition of hearsay only where it is "offered in evidence to prove the truth of the matter asserted.” Where an out-of-court statement is not offered for its truth content, however, no concern arises that the accuracy of the statement should be subject to the scrutiny afforded by the trial process. Since the declarant's credibility is not at issue, there is no need for the trier of fact to assess the declarant's "perception, narration, and memory."

Business Records

Since more than 98 percent of worlds data is now in electronic form, it is highly possible that ESI qualifies for the business records exception.

Rule 803(6) establishes a number of foundational elements for the business records exception. There are seven criteria for the business record exception.

1. The record must be in the form of a "memorandum, report, record, or data compilation, in any form . . ."
2. The record must set forth "acts, events, conditions, opinions, or diagnoses. . . ."
3. The record must have been "made at or near the time" of the acts, events, conditions, opinions, or diagnoses recorded.
4. The record must have been made "by, or from information transmitted by, a person with knowledge...."
5. The record must have been "kept in the course of a regularly conducted business activity...."
6. It must have been "the regular practice of that business activity to make the memorandum, report, record or data compilation...."
7. There is no indication that the source of information or the circumstances of its preparation are untrustworthy.

Excited Utterances, Present Sense Impressions and Existing State of Mind

When the ESI involves electronic communications like e-mail and text messages or even social media posts there are several different hearsay exceptions that could be applicable. Those are the present sense impressions exception under 803(1), the excited utterance exception under 803(2), and the existing state of mind exception under 803(3). Each are described in sections below.

Present Sense Impression under 803(1)

Even where an e-mail message was not composed with the type of spontaneity to qualify as an excited utterance, it may, nonetheless, reflect a different type of spontaneity sufficient to admit the e-mail message under the present sense impression exception to the hearsay rule. Specifically, under Rule 803, the hearsay exclusion will not apply to "[a] statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter." The present sense impression exception is premised on the theory that a witness who makes a statement sufficiently contemporaneous with an event or condition described in that statement is unlikely to misrepresent the event or condition deliberately or consciously. Among other things, the present sense impression exception may be useful for obtaining documentary evidence of a conversation (assuming that the statements in the conversation are not themselves excluded by the hearsay rule).

Excited Utterance under 803(2)

As a result of different forms of electronic communications and the speed at which they can occur, the excited utterance exception is a likely way to get many forms of communications admitted into evidence. Specifically, under Rule 803, the hearsay exclusion will not apply to "[a] statement relating to a startling event or condition while the declarant was under the stress of excitement caused by the event or condition." The exceptions in Rule 803 are designed to admit certain types of hearsay statements that have sufficient "circumstantial guarantees of

trustworthiness" to justify admitting them into evidence despite the fact that the declarant is not subject to cross-examination. The excited utterance exception is premised on the theory that persons who are excited by particular circumstances will not have the ability to reflect on those circumstances and consciously fabricate a response when acting in an excited condition.

To lay the foundation for the excited utterance exception, the proponent must establish: that a startling event occurred, that the declarant experienced a state of excitement, that the statement at issue was made while the declarant was under the stress of that excitement, and that the statement is relevant to the event that induced the excited condition.

Existing State of Mind under 803(3)

Rule 803 excepts from the hearsay exclusion "[a] statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain and bodily health)" subject to certain limitations.

Recorded Recollection under 803(5)

The recorded recollection exception allows a party to introduce into evidence "[a] memorandum or record concerning a matter about which a witness once had knowledge but now has insufficient recollection to testify fully and accurately."

Witnesses Prior Statements under 801(d)(1)

Rule 801(d)(1) excepts from the definition of "hearsay" any statement that is "consistent with the declarant's testimony" if the statement "is offered to rebut an express or implied charge against the declarant of recent fabrication or improper influence or motive." The statement must have been made before the time when the declarant was allegedly subjected to bias, influence, or motive to fabricate. Furthermore, in order for a statement to be eligible for this treatment, "[t]he declarant [must testify] at the trial or hearing and [be] subject to cross-examination [about] the statement." By claiming that the witness's current testimony is fabricated or has been induced by improper influence or motive, the opponent is deemed to "open the door" to entry of the prior consistent statement.

Statement Against Interest under 804(b)(3)

Under Rule 804(b)(3), a hearsay statement will be admissible in instances where the statement was made against the declarant's interest. To satisfy this exception the statement must have been so contrary to the declarant's pecuniary or proprietary interest, potentially exposing them to civil or criminal liability, or to render invalid a claim by the declarant against another, that a reasonable person in the declarant's position would not have made the statement unless believing it to be true.

The statement is measured against this standard at the time of its making. The exception is based on the theory that people are unlikely to make statements that are damaging to

themselves unless such statements are true. Notably, whereas the old common law rule was limited to statements regarding pecuniary or proprietary interest, Rule 804(b)(3) encompasses statements that tend to establish liability or extinguish a claim of the declarant's, statements that expose the declarant to criminal liability, and statements that expose the declarant to hatred, ridicule, or disgrace. Thus, for example, where e-mail messages revealed that the author could get into trouble or be disgraced if the activities discussed in the messages were made known, the messages were held to be admissible as statements against interest.

The Best Evidence Rule

The so-called "best evidence rule" is embodied in Rule 1002, which requires "the original writing, recording, or photograph" where proving the contents of such an item, except as expressly provided by the rules of evidence or otherwise by law. The definition of the term "original" includes data stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately. Similarly, the term "duplicate" is defined to include any "counterpart produced," among other things, "by mechanical or electronic re-recording."

The best evidence rule is relevant to ESI, particularly since ESI is typically copied or taken from an original media. An image is technically a duplicate of a media. A copy that is not an image is not a duplicate of the media. The validity of the duplicate is determined by the hash value which confirms duplicate within very high probabilities. The calculation must be performed across the entire media too. Thus, one must know how the hash was calculated with regard to its inputs. For example, a logical image which is just of a partition is not a duplicate of the media because it is not of the entire media. Similarly, an image that does not include freespace for the partition is not a complete logical image. Thus, assuming the hashes matched, the duplicate would be a duplicate of only whatever the input for the hash calculation was.

Files could be harvested from a media and also accepted as duplicates. Whether they were authentic duplicates would also be determined by some kind of hash value.

Unfair Prejudice Exclusion

An examination of ESI often involves an examination of an opponent’s computer devices, including their personal devices that could have all kinds of data reflecting all kinds of activity. Some of the activity could be distasteful while having nothing to do with the issues of the case.

Certain evidence, although relevant, is nonetheless excluded where it is unfairly prejudicial. Specifically, Rule 403 provides, "Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence."

Evidence will not be deemed unfairly prejudicial where it is "prejudicial only in the sense that proof of the case is prejudicial to the opponent. Unfair prejudice means an a tendency to

resolve the issue on a peripheral or less than a factual basis, which usually means an emotional basis.

Summary

While the rules of evidence apply equally to ESI as other forms of evidence, there are still some differences about ESI. The differences do not necessarily lie in the rules but in the requirements for handling ESI in order to satisfy the rules.

Perhaps the most significant evidential rule for ESI is authenticity. There are essentially four issues that effect the authenticity issue. The first is whether the evidence is exactly what was collected. This issue is typically resolved by validating the hash value of the evidence at trial with the evidence that was collected.

The second issue is whether it was collected properly. Typically this means was it collected without being altered. In some cases, it is not practical to collect the evidence without making some changes to something. The changes may not effect the evidence itself but could effect other aspects like file system metadata. In these cases, it is necessary to show that the changes did not effect the evidence or that any changes to the evidence have been identified and not effecting the decision making benefit of that evidence.

The third issue is whether the device from which the evidence was collected was functioning properly such that the document is what it purports to be. Demonstrating the proper functioning of the device could require any number of proofs both of the device itself and the program with which the evidence was created.

The final issue is whether the evidence is otherwise a spoof. The reality is that ESI is very easy to manipulate. Thus, authentication can extend not only to proper functioning but that the device or the evidence itself is not an entire fabrication.

Glossary

Electronic Storage Device – Any item that can be used by a person for storing and retrieving digital data and contains both the storage media and the means for storing and retrieving data to its media even though it may need to be connected to some other piece of equipment for the data to be interpreted by a person. Examples of Electronic Storage Devices are computer workstations, laptops, servers, cellphones, Personal Data Assistants (PDA), flash drives, thumbdrives, hard drives, etc.

Electronic Storage Media – Any item that can be used by a person for storing and retrieving digital data but relies on another device to write or read the data to the media. Examples of Electronic Storage Media are tapes, diskettes, CDs, DVDs, zip disks, etc.

Entropy test – A method frequently used to identify encrypted files. Entropy tests may not always identify protected files, since it is essentially a test of randomness. Files having both random and non-random components may not fail the test.

ESI – Electronically Stored Information

Event Logs – A windows system log that captures various machine operation activities such as logon and logoff, network connection or disconnect, etc.

FAT File System – See File Allocation Table File System

File Slack – See the definition for Slack Space

File System – The file system of a storage media is the equivalent of the “card catalog” in a library. It is what electronic systems use to know the names and locations of files and folders on the storage media along with other attributes like date stamps and active or deleted status.

Forensic Data Copy - A Forensic Data Copy (FDC) is a method of securing or “petrifying” data files into a protective container that prevents future alteration of the collected data. This method is focused at capturing selected data files from a storage media and not the entire contents of the storage media itself.

Forensic Grade Copy – A Forensic Grade Copy (FGC) is a method of copying data from an electronic storage media in a way that captures the data available to the copying method. Typically, this method is used with cellphones where the data captured may not be everything on the device but is everything that the device manufacturer allows to be captured from the device through whatever interfaces the device manufacturer has designed for such purposes. The data is then stored in a container to protect the copied data from future alteration of the collected data.

Forensic Grade Image – A Forensic Grade Image (FGI) is a special kind of copy of an electronic storage media that captures the entire contents of the media including active data as well as deleted data or free space as well as those areas of the media that are typically not available to the media users such as boot sectors and unpartitioned space. The copy is typically made using special protection measures to ensure that none of the media's data is altered during the process.

Free space – The area of a storage media available to store new data. Free space can contain deleted data, since the act of deletion usually only changes the status of the storage area containing a file from "in use" to "available for use". Free space is sometimes referred to as unallocated space since it is not currently allocated to storing active files.

Hashing – The act of computing a mathematical score of a data stream for use in subsequent validation or identification. The most common hashes used in this project shall be the MD5 or SHA1 hash.

HFS+ -- See Hierarchical File System

Hibernation file – The hibernation file is a feature of many computer operating systems where the contents of RAM are written to non-volatile storage such as a hard disk, as a file or on a separate partition, before powering off the computer. When the computer is restarted it reloads the content of memory and is restored to the state it was in when hibernation was invoked.

Hierarchical File System – The original file system used by Apple computers. In more modern times it was upgraded and referred to HFS+ or HFS Extended.

INFO/INFO2 File – A windows system file used by the Recycle Bin to track deleted files

Internet Cache – Files used by web browsing software that tracks internet history data as well as local file access data.

Link File – A windows system file that is created whenever a file is opened. Link files contain various metadata attributes such as the location of the file that was opened.

Master File Table – A table with in the NTFS file system that contains

MD5 – See Message Digest 5

Message Digest 5 – A 128 bit algorithm

Metadata – Metadata is data about data. Metadata may generally be viewed as either System Metadata or Application Metadata. System Metadata is data that is automatically generated by a computer system and relates to other data files or activities of the system. For example, System Metadata often includes file system information such as date and time stamps, file path (location on the media), attributes such as read-only or other system generated information such as pointers, and activity or operation logs. Application Metadata is data within a file and relates to that particular file. Application Metadata is divided into two types, Substantive Metadata and Embedded Metadata. Substantive Metadata is data that reflects the

substantive changes made to the document by the user. For example, it may include the text of actual changes to a document. Embedded metadata includes other data embedded in the document by the system or software application such as author or creator, organization, and various date stamps. While no generalization is universally applicable, System Metadata and embedded metadata is less likely to involve issues of work product and/or privilege.

MFT – See Master File Table

MSG – MSG is the format of a container (file) used to hold individual e-mail messages and their attachments in a Microsoft Outlook/Exchange mail system.

Native File(s) – ESI in the electronic format of the application in which such ESI is normally created, viewed and/or modified. Native Files are a subset of ESI.

New Technology File System – A file system

NSRL – National Software Reference Library is a list published by the National Institute of Standards Technology of known file hashes, specifically MD5 and SHA1, for published software. The library is updated quarterly to reflect revisions and new releases. The library is typically used to identify and remove from further consideration files contained in standard software applications that, while matching files types of interest like spreadsheets or text documents, shall have no significance to this litigation.

NTFS – See New Technology File System

OCR – Optical Character Recognition is the process of converting image based textual characters into textual data that, in the context of this project, can be searched with other electronic means.

PDF – Portable Document Format is an image file format commonly used for document management in litigation. The conversion from native format to PDF shall eliminate metadata contained within the native format document, although the PDF format shall contain the searchable text of the remaining image.

PST – PST is the format of a container (file) used to hold an individual's e-mail messages and attachments in a Microsoft Outlook/Exchange mail system. In a metaphorical sense the PST container is the equivalent of an individual mailbox containing letters (e-mail messages).

Registry – A file used by the Windows Operating System to store data attributes used by the operating system for machine operation. The Registry is composed of several files. The attributes they contain include installed hardware and software, security data, configuration data, user data, etc.

RTF – RTF (Rich Text Format) is a text based file format developed by Microsoft for use with Microsoft products like Outlook and Word and for cross platform document interchange.

Secure Hash Algorithm – A cryptographic hash function used in information security for such things as digital signatures and data integrity checks. The SHA algorithms come in several different used to It comes in several varieties such as SHA-1, SHA-2, SHA-256,

Security Identifier (SID) – A security identifier is an intelligently coded value used on Windows NT class machines that uniquely identifies the machine or domain and the user associated with certain data or functions. The machine or domain portion is a set of 3 ten character strings separated by dashes. The user portion is a 3 or more character suffix added to the machine or domain identifier. The user portion uniquely identifies the user for that machine or within that domain. User identifiers of 1000 or less are system level users, including built-in users like the machine or domain administrator, while identifiers of 1001 or more are other users.

SetupAPI.Log – A Windows system log found on Windows systems prior to Vista that captures information related to installation of hardware devices.

SetupAPIDev.Log - A Windows system log found on Windows systems Vista and later that captures information related to installation of hardware devices.

SHA – See Secure Hash Algorithm

Slack space – Electronic media is typically divided into smaller storage segments. Slack space is the area from the end of an actively stored file to the end of the storage segment containing the active file.

Static Image(s) -- A representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. In the absence of agreement of the parties or order of Court, a Static Image should be provided in either Tagged Image File Format (TIFF, or .TIF files) or Portable Document Format (PDF).

SWAP file -- A swap file (or swap space or a pagefile) is a space on a hard disk used as the virtual memory extension of a computer's RAM (Random Access Memory). The swap file allows a computer's operating system to pretend that it has more RAM than it actually does. The least recently used files in RAM are "swapped out" to the hard disk until they are needed later.

TIFF – Tagged Image File Format is an graphical image file format commonly used for document management in litigation. The conversion from native format to TIFF shall eliminate metadata contained within the native format document. A TIFF image is not searchable without first having its text based characters converted to searchable text.

TXT – TXT is a text only file format usually based on the standard ASCII (American Standard Character for Information Interchange) character sets.

UTC – Uniform Time Convention. Many computer system file dates are stored internally in UTC format and then converted to local time, when presented, based on the computer's time zone settings. In a general sense, UTC is similar to Greenwich Mean Time (GMT). Consequently, when converting UTC times to local East Coast United States time, for example, users would subtract either 4 or 5 hours from the UTC time, depending on the existence of daylight savings time, to convert to local time.

APPENDIX 1 - Finding and Selecting a Computer Forensic Expert

Introduction

We live in a digital world and there is hardly a dispute or litigation that does not involve computerized devices or their data. The dispute may not involve a lot of data but it likely will involve some kind of computerized device or data even if it is a single text message, e-mail, voice mail, transaction record, web search, document, etc. As a result, there is hardly any case that is not a candidate for a computer forensic expert or consultant whether that need is technically or economically based.

Despite the widespread presence of ESI [Electronically Stored Information], does every case actually require it? For example, consider a payment dispute for services or

products. One might think that the simple production of the contract and proof of non-payment is all that would be required. It is amazing, though, how such a seemingly simple case could morph into something requiring ESI.

For example, when the contract was breached by failure to make payment the issue of liability may be settled but the other elements involving causation and quantum, could still be unresolved particularly if the contract is not yet complete. Consequently, proof elements could quickly expand into complex damages issues like mitigation.

Such a turn could also quickly shift the burdens from the defendant back to the plaintiff. While the defendant may ultimately owe something, it may not be the full amount sought by the plaintiff. Furthermore, the ESI necessary to prove such a defense could reside in untold gigabytes of ESI proving or disproving the plaintiff's efforts to mitigate and whether new volume was actually replacement volume.

What is more, once litigation became eminent, did the plaintiff adequately preserve the relevant evidence particularly after receiving the defendant's answers indicating that the claimed amount was not owed and various defenses articulated? Clearly, a computer expert could be essential for a variety of reasons.

The importance of a computer expert is not driven solely by the ubiquitous nature of ESI. Nor is it tied solely to technical evidential issues and expert testimony. Indeed, there are numerous economic reasons as well. After all, computer related expertise is essential throughout today's litigation lifecyle. In other words, it is not just evidential issues. Indeed, the management and administration of the entire litigation process is highly automated or should be in order to analyze the data and marshal the facts economically and effectively. The inexpert handling of the computer issues not only affects the evidential issues but can mire the entire case in a quagmire jeopardizing a merit based outcome.

Consequently, there is probably greater payoff for using a knowledgeable computer expert than any other discipline involved in litigation. Both clients and their counsel should recognize this reality and learn how best to employ the skills of computer experts to not only win the case from a technical evidential perspective but also to manage it efficiently and economically. After all winning on the legal question without an economic victory as well is just losing in a different way.

The following sections provide guidance to clients and litigators on the work of computer forensic experts and the factors that should be considered to find and select them.

What is a Computer Forensic Expert

In order to find and select a computer forensic expert, one must first know what they are seeking. Computer forensics is the application of technical knowledge, skill and experience to legal problems involving digital evidence. Since over 98 percent of all information is stored on a computer, computer related legal problems can manifest themselves in a myriad of ways that range from identification of data sources and then progress to preservation, selection, examination and presentation of the data.

The term expert has a special meaning when used by litigators and others in the legal profession. In their vernacular the term “expert” most often means a witness that testifies about subjects involving scientific, technical or specialized knowledge and renders an opinion about the evidence in a case.

Experts are the only witnesses that can provide testimony and opinions on subjects involving scientific, technical or specialized knowledge. Other witnesses, known as fact witnesses, cannot. In fact, fact witnesses are prohibited from providing testimony about scientific, technical or specialized knowledge.

Fact witnesses are so named because they limit their testimony to facts about which they have personal knowledge, although in certain circumstances a fact witnesses may also provide opinion testimony or what is known as a "lay opinion". Lay opinion, however, is limited to the actual perception of the witness or what might otherwise be helpful to understanding their testimony.

The prohibition against fact witness testimony based on scientific, technical or specialized knowledge is intended to avoid situations where experts testify in "lay witness clothing" and avoid the special disclosure and evaluation procedures established for experts. When the special procedures for experts have not been followed expert testimony and opinion have not been permitted, although witnesses have still been permitted to testify about factual matters.

The reservation of scientific, technical or specialized knowledge to expert witnesses and its exclusion from fact witnesses can have significant consequences for even routine cases where computer forensics was used for tasks as seemingly simple as preserving Electronically Stored Information (ESI) or culling the ESI for responsive documents. After all, when testifying about the collection the explanation would involve discussion of the tools, equipment and procedures used to ensure accurate collection of the data such as write protection, error detection, data verification, data security and chain of custody to name a few. Similarly, testimony about the culling or search of the ESI for responsive documents would involve explanation of technical issues related to linguistics, statistics and technology.

While the collector or operator could testify about the procedures used to preserve or select ESI for production, only an expert would be able to testify about the technical aspects of the collection or the selection and render an opinion about the adequacy of the procedures and whether they satisfied the technical requirements of the discovery. Thus, if the validity of the production were ever challenged, opinion testimony regarding the accuracy or inaccuracy of the production would only be permitted by way of expert testimony and not through lay opinion by others involved.

While some have tried to side step the expert classification by claiming that collectors, selectors and even analysts are essentially fact witnesses because they simply push the buttons of the specialized tools and software that they use to collect, select, analyze and present the evidence; such claims have not been successful. Where this logic has failed is in the interpretation of the data produced by the computer forensic tools and software.

The interpretation of the data is often dependent on the expert's knowledge of the forensic tools and software, which are not usually "familiar in everyday life". In addition, the expert's

knowledge of the data types and the evidential media on which the data are stored such as its filing system and data storage structures are, also, not usually "familiar in everyday life". In fact, courts have analogized the interpretation of computer forensic reports (as would be produced by imaging tools, search engines and analysis software) to specialized medical tests and interpretation by police officers of slang and code words used by drug dealers, which they have deemed specialized knowledge of an expert.

While expert witnesses are qualified by way of their knowledge, skill, and/or experience it is not necessary that they possess a high degree or the highest degree of knowledge, skill and/or experience. Rather, as previously indicated, they must simply possess a level of knowledge that is not “familiar in everyday life” or “in possession of the jurors”. Perhaps most important, however, is that regardless of their actual degree of expertise, the testifying expert must be helpful to the trier of fact in understanding the evidence.

Clearly, qualification as a forensic expert can be a low bar, since there is probably little about any aspect of computer forensics at any stage (whether collection, selection, examination or presentation) that is “familiar in everyday life” or “in possession of the jurors”. So, it is possible for ESI collectors, for example, to qualify as an expert and testify as an expert, assuming that the rules for experts, such as timely disclosure and production of a report, have been met. When these requirements have not been met then “expert” testimony has been prohibited.

Of course, whether the expert survives beyond qualification and actually advances the case can be a different matter. Thus, while the bar for qualification as a testifying computer forensic expert may be low, a higher standard is probably desired by the client and its attorney. In fact, they should seek someone that fits the more commonly used definition of an expert which is a person having a high degree of knowledge or skills in a particular subject and not just someone whose knowledge exceeds the jurors.

While the term “expert” in a legal context will most often refer to testifying experts, the term can also refer to non-testifying experts whose purpose is to assist with trial preparation. Generally, these kinds of experts can include jury selection experts, presentation experts and even experts in the same fields as other testifying experts. In fact, in large complex cases it is common to have both a testifying and non-testifying expert in the same technical field. The difference is that since the non-testifying expert is not normally subjected to examination by the other party, the non-testifying expert may be more informed about strategy or case weaknesses so that his expertise can be used to enhance those areas of the case without fear that the results of those consultations will be disclosed to the opposing side.

The importance of the non-testifying or consulting expert is not limited to technical evidential issues. Indeed there are many areas including procedural areas where an expert’s knowledge and skills are invaluable for efficient and economic case management. After all, a lot of litigators lack even basic spreadsheet skills. Even if they possessed advanced spreadsheet skills, there is still a quantum leap between those and what is needed for the collection, analysis, exploitation and management of diverse data types in a complex data management system. Furthermore, performing them in the most efficient manner possible is important for the client and is critical to ensuring a merit based outcome.

An example of a procedural matter where a computer expert's skills could be very useful is the development of the discovery plan and protocol. A plan and protocol that incorporates the most efficient and effective methods for collecting and culling large data populations could provide huge savings considering that about 74 percent of the discovery budget is consumed by document review. Therefore, those processes and procedures are a huge target for improved efficiency.

So, unlike other experts, the computer forensic expert can affect the evidential issues as well as procedural and case management issues across the entire litigation effort. As a result, the inexpert handling of the computer issues not only affects the evidential issues but can mire the entire case in a quagmire. Only this quagmire also contains land mines in the form of sanctions for unreasonable errors, should they occur. Consultation with a computer expert can help less sophisticated legal professionals avoid those problems entirely.

Finding a Computer Forensic Expert

Once the lawyer has determined to use a computer forensic expert the next likely hurdle will be how to find one. Of course, there is always the old fashion way that is probably used most by lawyers. That is asking around with other firm members and colleagues about experts that they may have used in the past and would recommend.

Performing searches on the internet is another common method of finding experts. If their websites exist then evaluating the content of those sites can help identify candidates.

Besides searches of the internet, those with access to case decisions can also search those for instances where experts are identified.

Of course beyond that are the usual directories. Some of the better known are Martindale Hubbell, AMExperts and then various industry or geographically specific directories such as construction industry directories or local bar association directories.

As computer forensics has become more common, there are also professional associations that can provide member lists. For example, the International Society of Forensic Computer Examiners (www.isfce.com) is one professional association where individuals can be found. In addition there are also tool specific certifications like Guidance Software's EnCE [Encase Certified Examiner] and Access Data's ACE [Access Data Certified Examiner].

Clients often have technology staff in-house that help with the administration of their systems. Nevertheless, client personnel are not a good source for forensic expertise and there are several reasons that this is true.

First, they are not normally involved in forensic processes to begin with. Rather they support the organization in the execution of its mission, which it not litigation or forensic services. The difference is often like the difference between the infantry and the special forces. Both may be able to fire a rifle but the ways in which they use them are entirely different. Even the ammunition is different because a forensic expert will likely have different tools to examine media and its contents than a client's in-house technical support staff.

Second, another drawback to using client personnel is that there will be "combat". Litigation is not just using a weapon to fire at paper targets. Further down the line there will actually be contact with the enemy, so to speak. Unless the client personnel has done that kind of thing before, they likely are a less attractive choice than someone that is combat experienced.

Third, a lot of what happens in even the early stages of the collection and analysis process is to prepare for the "combat" that will happen later. Thus, considering less capable client personnel could be like bringing a knife to a gunfight.

Finally, in a recent survey of IT security professionals less than 8 percent would recommend using an outside consultant to assist with the analysis of a data breach; but, more than 50 percent of those same respondents claimed that their staffs lacked the tools or the training to determine the cause of the breach.[13] These survey results are highly relevant to the selection of a forensic expert particularly when one considers that client IT personnel are more closely aligned to the breach issue than to providing litigation support services. Thus, if they are not well prepared for something more closely aligned with their actual job function, how well will they perform on something that is not aligned to their job function?

Selecting a Computer Forensic Expert

Once you have located potential candidates, or at least sources for potential candidates, the next step will be selecting a computer forensic expert. Naturally, the case specifics will influence your selection. The case specifics not only include the nature of the case such as bankruptcy, system intrusion, contract dispute or fraud to name a few but can also include the complexity of the case--at least with respect to the digital evidence. What will be challenging for litigators is identifying and understanding how those case differences will manifest themselves in the skill sets of a forensic computer expert.

There are a number of features that can influence a selection decision. The criteria that are likely most useful are the area of expertise, relevant experience, industry specifics, educational background, training, licenses and certifications, criminal versus civil experience, presentation skills and forensic tools. Each of these are discussed in the sections that follow.

Price

How much things will cost is always a consideration. Remarkably, price is more often the last thing to consider when selecting a computer forensic expert. If the expert crumbles under pressure or cross examination; if his analysis is faulty; or if he lacks the aptitude to advance the case either by finding important evidence even when deliberately hidden by the opposing party or overcoming obstacles erected by opposing counsel to frustrate discovery, then having paid him anything is too much.

[13] Threat Intelligence & Incident Response: A Study of U.S.and EMEA Organizations, Ponemon Institute, February 2014

The reality is that computer forensic expertise is not a commodity like some kind of hardware component that one plugs into their computer. Furthermore, the expert is not simply a facilitator or button pusher on software that every computer expert uses. While a lot of computer forensic experts use the same tools, so do carpenters; yet, some are much more skilled in using those tools than are others.

Price is also hard for clients to evaluate because they have to understand what it is they are actually buying for that price. In many cases, the difference in price is a difference in the services being delivered and both clients and counsel often lack the skills and expertise to understand and evaluate the consequences of those differences. Furthmore, clients or counsel may think that they only need a certain service provided but often times what that really means is that client and counsel do not have a good understanding of the situation or the requirements, at least from a computer forensic perspective. Recall no one thought that the ship Titanic would ever need its life boats.

Often times technology buyers take a commodity based approach because they think everything about technology is just a commodity and one solution is just as good as another. If one were digging a ditch, one might think that they could buy the cheapest shovel if one shovel is as good as another. The problem with such an approach is that the job might be better performed with a back hoe. In those cases, buying a shovel is simply the wrong choice because the backhoe can dig the ditch faster and more economically then an army of men using shovels--even if the men are lower priced. If the ditch is of any real size, using the more expensive back hoe can save overall project costs. After all, when one is digging for gold using the right tools can not only better ensure hitting the mother load but finding it faster and at less over all costs than using less effective tools..

While it might end up that clients only need a certain service performed, litigation in general and computer analysis in particular is often like digging in the dirt for buried treasure. It is hard to know exactly what one will encounter once the excavation begins. Will the treasure actually exist? Will some other excavation method be required? How will one know if what is found is actually fools gold? Consequently, what clients should value most is a talented treasure hunter that knows how to both find the treasure as well as how to plan, manage and execute the most economical expedition.

There are plenty of reasons why finding the lowest priced forensic expert simply does not make sense, particularly when that savings means less capability. At the end of the day, the computer forensic expert will be a small part of a client's litigation costs. It is not unusual for counsel costs to surpass the computer forensic expert by magnitudes of 10, 20 or even 30 to 1. Thus, the cost outlay for the computer forensic expert will likely be small when compared to the total project costs. As a result, a litigation matter will not become more economically viable simply by choosing the lowest priced expert. On the other hand, the consequence of choosing a less capable expert can be colossal both in technical terms and how it hobbles the case such that overall project costs skyrocket. Facts can be pesky things. A good computer expert can provide a case with all kinds of good facts that can really make a difference in both the outcome and what it costs to get there.

If there is a redeemable characteristic to the low priced vendor, it is that the opposing side may well have followed that line of reasoning. If one is ever confronted with adverse findings

from an opposing forensic expert, the reality could well be that they have come from the low priced vendor or from even an otherwise capable expert whose capabilities have been hobbled by the shortsighted thinking client or counsel. So, if the claims come as a surprise, do not be too quick to abandon ship.

Clearly, while price is part of every calculation, the price problem for selecting a computer forensic expert has more than one variable which must be resolved. Thus, it is not as simple as finding the lowest priced expert, since such a solution might only cause the other variables to increase disproportionately. As a result, there are many things that need to be considered when selecting a computer forensic expert and many of those are much more important than his unit cost.

Area of Expertise

Perhaps the first area that should be considered when selecting an expert is whether he has the kind of expertise that is required. Computer forensic is not a monolithic subject. In fact, like law itself, there are many nuances and they can vary quite a bit.

Legal practitioners tend to think of computer experts in terms of the computer equipment related to personal or business activities. In other words, imaging hard drives and examining their contents. Even under that umbrella, however, there can be significant differences between phones, personal computers, servers, network switches, routers, firewalls, application software or databases.

Things can be even more esoteric with other peripheral systems like surveillance/security systems, restricted access/security systems, video/audio systems, phone systems, etc. All of these could be important in the right case and are further support for why litigators may need to use an expert just to help them identify what kind of expertise is actually required.

Even after the right systems are identified there can still be differences with which to distinguish experts. For example, phones can be distinguished by their technology such as Apple, Android, Blackberry, Windows or other smart phones. Similarly, the different kinds of personal computer systems such Apple, Windows, Unix/Linux, etc. can have significant distinguishing differences.

Of course, these are just examples and not intended to be an inclusive list. Furthermore, the area of interest may be more software related than hardware related. The point is that the litigator needs to realize that the field is not monolithic and there are significant differences between all kinds of systems and applications. Consequently, when selecting an expert the litigator should have some appreciation of the differences and select an expert with the appropriate expertise.

Of course, in mainstream areas like the Windows world, the population of experts from which to select is abundant. In the more esoteric areas, experts with the desired expertise may be harder to find. In those cases, the litigator may need to settle on an expert capable of identifying the problem and developing a solution. After all, a talented expert without specific

expertise may still be a far better selection than one with some expertise that is otherwise unremarkable.

Relevant Experience

The analysis of the expert's relevant experience is another important discriminating factor. The particular factors that one should consider about relevant experience depends on where in the litigation lifecycle the expert will be used. After all, the interests are different depending on whether he will be used for preservation, analysis, processing and production, procedural issues or testimony. In addition, within each of those categories the expert's relevant experience can be assessed from two different angles--specific and related experience. All of these considerations are discussed in the sections that follow.

Preservation

The preservation phase is probably one of the most import phases of the entire litigation lifecycle. Unlike its paper counterpart, electronic data degrades with continued usage and even the passage of time. Simply continuing to use a computer can alter important evidence like date stamps and application meta data. With respect to system meta data. the continued use of a computer completely destroys important artifacts like file pointers, browser history, recycle bin activity logs, and system event logs to name a few that can be essential to evidence authentication and/or revealing actual system usage.

In the preservation phase there are two areas where the forensic expert can be essential. Those areas are identification of potentially relevant ESI that should be preserved and then actually conducting the preservation effort

When identifying potentially relevant ESI for preservation the forensic expert can provide several valuable functions. The first is identifying the sources of ESI. Properly identifying ESI is not necessarily as simple as asking the client where their data resides. The client and its technology personnel are likely inexperienced in litigation matters and may think quite narrowly. Their limitations may involve the actual devices as well as the extent of the data that they contain.

The expert should be seasoned in litigation requirements and know to how to develop a conceptual model of the client's systems that not only includes formal system components like servers, personal computers and phones but informal components like flash drives, external hard drives and home computer devices. There could still be other formal system elements worthy of consideration such as backup system, communication systems and document management systems.

A computer expert should know how to define the population and then peal each layer in order to identify those elements likely to contain potentially relevant ESI warranting preservation. As the expert learns about the target's system, he is likely better able to identify that when one type of system or usage occurs then another is likely to exist as well.

While the final decision belongs to the litigator, the expert can present the litigator with intelligent options. For example, if there is detailed backup history then a separate preservation of a server or a least a forensic preservation may not be necessary. Similarly, if the key personnel only used their assigned equipment and never logged into a server as an operator then the server is not likely to contain the kinds of forensic artifacts that could be obtained only from a forensic imaging of a server. So, again there is no need for that kind of expenditure and effort.

The expert may also know to inquire about retirement and replacement policies at the target and history of equipment used by key personnel in particular. He would also know to inquire about device usage policies and be able to confirm representations when conducting his inquiry or at the time of actual preservation.

Another reason for using the expert for the identification process is that as he learns the system he can determine the best methods for performing the actual preservation. This latter phase can include both the timing of the preservation and the best method of preservation while considering how to reduce disruption and overall costs.

During the identification process the expert can likely also provide feedback to the client and litigator about estimated costs and timing so that reasoned decisions can be made. In the end, the expert is well positioned to testify about the process and justify the reasonableness of the approaches taken. After all, the preservation standards are for potentially relevant evidence and it is not a standard of perfection.

So, there are a lot of benefits to using an expert for both the identification and actual preservation of ESI during the preservation phase. When selecting an expert for this process, the litigator should consider what experience the expert has had in this kind of effort. Specifically, exactly how skilled is he in conducting the preservation phase. It could be that his vast experience is comprised mostly of analysis and testimony based on media that was captured by others and supplied to him. So, it could be that his preservation experience is rather limited both in terms of the identification, the actual requirements for identification, and even in conducting the actual preservation for the various types of equipment that could be encountered.

So, if he is being used in the identification phase, one obvious consideration is whether he has served in that capacity before. An equally important factor could be whether he has had to defend any preservation that he has performed in the past or attack any preservations performed by others or whether, once again, his work has been limited to the actual analysis and findings phase.

If he is being considered for the actual preservation phase, then the things to consider are whether the expert is experienced in preserving the types of devices that need to be preserved? Personal computers can have different preservation approaches than enterprise servers. Phones can have still different approaches. Also, there can be different approaches for Microsoft based systems than Apple based systems. If the interest is e-mail servers, document management systems or other application databases there could still be other approaches to the preservation problem.

If the expert has participated in the identification phase then the device population should be fairly well understood and determining his experience and capability should also be rather straightforward.

When it comes to preservation another factor to consider is that the reality is often different than the plan. The differences often involve the number of devices, types of devices and size of devices. So, the last thing to consider about the expert's relevant preservation experience is his ability to improvise and adapt when field conditions differ from the plan.

Analysis

If the need for an expert is further along in the lifecycle, such as analysis, the question is whether the expert even has analysis experience or is his experience mostly in the preservation phase? If he does have analysis experience how much does he have and is it with the kinds of equipment that are part of the preservation collection. Once again, there are different analysis approaches and requirements between the types of equipment like personal computers, servers or cell phones, and even between the systems like Microsoft and Apple. So, how well does the expert match against the actual equipment to be analyzed.

For the litigator, it can be difficult to assess whether the expert has analysis experience. Yes, he may have analyzed similar devices but what kinds of analysis has he performed and what is his actual level of expertise?

There is more to device analysis than the files themselves. A lot of forensic artifacts are in system meta data. The location and structure of those artifacts is different on a Windows machine than on an Apple machine, for example. So, when selecting experts the litigator may want to consider talking with the expert about the nature of the case and inquire about approaches that are available for conducting the analysis and then try to speak with the expert about the specifics of the different device types and his experience with them.

The analysis may not be related to the facts in the litigation, however. Rather, the analysis may be about the authenticity of the evidence and whether it is reliable. So, even in garden variety e-discovery cases there is need for analysis.

The reliability of the media and the digital data it contains can be readily determined. It does not even require production of the entire media. Indeed, it can be accomplished by examination of certain files that will not be directly relevant to the issues in the case but will be directly relevant to the to determining the adequacy of the digital data.

Without validating the evidence significant resources can be squandered on a wild goose chase. In addition, the arguments will be more protracted and less definitive since the ammunition needed to actually win the argument may not have been included or otherwise improperly obscured.

Another factor to consider with respect to analysis experience is whether the expert's experience includes the type of case for which he is being considered. For example, if the case is a family law matter, it may be useful that his experience includes family law matters.

Going further, it will be useful if his experience tracks with the specific interest in the case. For example, one of the interests in a family law matter is detection of hidden assets when resolving the property settlement agreement. So, the question is whether the expert has that kind of experience in family law matters or has he worked mostly in other areas of family law matters like the fidelity or aberrant behavior areas.

If it turns out that he has not worked on hidden assets that may not be a fatal weakness if he has worked in other kinds of cases where hidden assets are also of interest. For example, in trade secrets and bankruptcy cases there is also interest in hidden assets. Remarkably, the skill sets are similar if not identical even though the fact pattern is different.

Similarly, the aberrant behavior aspects of a family law matter could have similarities with a workplace harassment issue or even aberrant workplace behavior. So, if the expert is not an exact match for the specific interests of the case then the litigator should consider inquiring about other types of cases where the skill sets could be similar. Of course, the litigator may have to rely on the expert to identify similar cases after speaking with the expert about the nature of the specific case.

One might need to give the expert time to explain how he thinks that his experience will fit into what litigator perceives is needed for the case. The litigator may need to follow up and assess what other benefits could be offered from a management issue and discuss where the expert thinks problems could be encountered and how he could help get around those issues.

Another element of interest should be how complex his cases have been. Was everything sitting out in the open or were things a little more subtle. What is his experience with anti-forensics techniques like file wipers, of course, but also reformatting, drive swapping, counterfeiting, file churning, clock manipulations and a whole host of others. Again the litigator may not be knowledgeable enough to ask about specific scenarios and may have to rely on the expert to identify and discuss his experiences regarding anti-forensics along with any standard procedures that he employs for that purpose.

In the final analysis the question is what does the expert do to validate a production. Does he take steps to identify omissions and/or manipulations or does he simply proceed with what has been given. If the media has been specially prepared for his review by the opposing side, then it may not reveal anything when examined solely based on its actual content. It is only when the “pedigree” is examined that forgery could become obvious.

A final consideration is can he work with imperfect information in the event that not all discovery requests are granted by the court? In addition, is he able to reverse engineer the work of opposing parties without documentation or when other information gaps exist?

Processing and Production

The largest consumer of the litigation budget is processing and production of the digital evidence and its related document review effort. From an economic perspective, it is a big target that can have a big payoff if done right.

The processing element typically refers to the effort required to convert the digital data into usable form for review and subsequent production. The most economic solution to the processing and production problem is not as simple as selecting the lowest unit price.

In the digital age, manual review is not really practical for both economic reasons as well as accuracy reasons. Manual review is the most costly part of the processing and production effort. Also, the human factor in manual review is well known for errors.

As a result, the best way to manage the problem is through the processing phase where automated techniques are used to perform volume reduction and eliminate manual review as much as possible. Thus, the kind of computer forensic expertise that both a client and a litigator seek during this phase is one that can reduce the volume of data that will be subject to document review.

There are actually a number of techniques that can be used to accomplish these goals such as various computerized search techniques, meta data. filtering and analytics to eliminate unresponsive and irrelevant files, removing known files, identifying and removing duplicates along with other productivity related processes. An expert could help design the battery of techniques that would be used to maximize the effectiveness of the processing phase in order to minimize the effort needed for the review and production efforts.

Procedural Matters

Procedural matters are another area where an expert can make a significant contribution to the economics of a case. Legal problems involving digital evidence, computer forensics, is a very complicated subject and involves more than checking off paragraphs in the rules of procedure.

The completion of Rule 26, for example, results in a discovery plan. That plan could be analogized to the plans for building a house. Certainly, the plan could be the equivalent of something crafted on the back of a napkin. Or it could an “architectural” view or a “plan” view of the final product.

The best approach for house building, however, is known to be an engineered drawing. While it takes more on the front end to develop the engineered drawing, it will have payoff on the back end by speeding final production and avoiding disputes that could derail the entire effort.

Under the home building analogy the expert serves as a design consultant having specialized knowledge about technology and processes that can be woven into the final design document—the discovery plan. The final plan should involve numerous technical methods such as those previously discussed in the processing and production as well as procedural techniques like multi-tier discovery.

The multi-tier discovery would use a staged approach designed to avoid full scale processing and production, at least until the risks are better known. The multi-stage approach would attack the discovery process in stages starting with the devices and custodians believed

to have the most relevant evidence for the case. Perhaps the entire dispute could be resolved after that initial review without having to process the entire population.

In addition, the expert may be able to suggest specific tests that would be better able to identify the specific documents of interest or identify various other system related artifacts that would be dispositive to the matter. Even if not dispositive to the entire matter, the expert's work may be able to eliminate custodians or devices from further consideration the related processing and production.

Using a multi-tiered approach could also prove the validity of the discovery plan prior to committing huge resources in the same fashion that construction and manufacturing practices use "prototyping" or "proof of concept" methods prior to committing to full production. For example, the search techniques being used to identify responsive and relevant documents may or may not work as intended. It is better to prove the merits of the methodology before committing full resources to full production. The expert and his special tools could likely help in this process long before the data is processed and placed in any document management system used for the litigation.

The discovery plan may also be able to simplify the processing and production matter through the development of a protocol. The protocol is an agreement between the parties describing exactly how the processing and production will be conducted. So, the protocol can be analogized to the contract that the homeowner enters with its home builder.

The protocol can be very detailed. In fact, like the engineered drawing analogy, the protocol can go a long way towards streamlining the overall discovery process because the parties discuss and agree to the attributes in advance. The advance agreement can streamline the process and eliminate unnecessary efforts by incorporating the processes discussed previously to gain efficiency like multi-stage discovery as well as others suggested by the expert.

Testimony

The reality is that a lot of lawyers are not well versed in computer issues and really do not know how to thoroughly examine an expert's work. This even applies to the retaining counsel who may view the selection of experts as only another piece of evidence. Thus, their concern is simply whether the expert's opinion supports the needs of the case.

To a certain extent, the fact that an expert's opinion supports the needs of the case would seem obvious; yet, the shortcoming is that counsel may not have fully revealed what the needs of the case actually are to the expert. Had retaining counsel explained the case more fully the expert might have still been able to provide the opinion but at the same time recognized that the precise manner envisioned by counsel was not persuasive nor meaningful.

For example, litigators may want to make a point about how files were deleted from the media after a certain date. The evidence may well support that files were deleted after a certain date. If retaining counsel has not taken the time to examine the issue and explain the case with the expert it will not be until opposing counsel cross examines the expert that the retaining

counsel learns that the files were all deleted as part of routine system maintenance and not done by a deliberate user action, which is where client counsel was wanting to go.

If litigation is like chess then testimony is like the end game. One will never get a chance to play the end game if one has a weak opening and middle game and picks an expert that is not really competent in the disciplines described elsewhere. Similarly, the advantages gained by a great opening and middle game can be squandered with a weak end game. Thus, an expert's testimony skills can be an important consideration.

There are two attributes that should be considered when evaluating an expert's testifying skills. One is whether the expert has testified before. The other is the sophistication of the examination to which he has been subjected by opposing counsel.

In regard to the first, has the expert testified before, the interests are twofold. One is where has he testified. Ideally it is best that he has testified in courts similar to the one in which the case will be decided. The other is that his opinions have not been rejected for some reason and he was prevented from even testifying. Clearly, satisfying both of these criteria will help smooth the qualification process.

In regards to the second, there are actually several considerations. One is whether the expert has been subjected to stiff interrogation during deposition and cross examination at trial or some motion hearing. In other words, how well can the expert handle the fastball and did it affect any of his other performance when opposing counsel tried the equivalent of the brush back.

Of course, it is not just an expert's performance against a power pitcher that should be considered. The other involves the finesse pitcher that may try to neutralize an expert by mischaracterizing his opinion or restate his findings. If opposing counsel is somewhat successful, even without the expert realizing the significance of what opposing counsel was trying to accomplish because the retaining counsel had not taken adequate time to prepare the expert or allow him to review letters, deposition transcripts or motions so that he could be aware of opposing counsel's "theories", then the expert's opinions could be successfully neutralized. In such a case, retaining counsel is not likely to undo the damage on redirect because it might be a subject that he has never discussed with the expert. In such a case, retaining counsel is likely to follow the old adage that one should not ask questions when one does not already know the answer. Consequently, in that case, retaining counsel is likely to sit quietly even though there could have been ample means to "toss the grenade" back at the enemy before it actually exploded.

Of course, it is probably not practical to prepare the expert for every conceivable tactic that opposing counsel could try. Consequently, when selecting an expert, it is important to realize that in more cases than not the expert is on his own when defending his opinions against opposing counsel. It is good to know that the expert not only has the technical skills to defend his opinions against the so called "power pitcher" that will make a direct assault but also has the experience to recognize and defend his opinions against the "finesse pitcher" that is happy to work the "corners", so to speak.

Clearly, the fact that a computer expert has previously survived testimony in depositions or trial may not be that comforting. Thus, it is important to understand just what kind of opposition he has experienced.

In order to evaluate the expert's testifying experience, the litigator probably needs to learn the cases in which the expert has testified and then evaluate the attorneys that he opposed. Of course, the litigator may be able to shortcut this exercise by questioning the expert about his experiences and to what degree he believed they had been challenging and why and whether the expert considered the opposition a "power pitcher" or a "finesse pitcher" and the ultimate outcome.

When evaluating the expert's testifying ability, it could also be useful to discuss how he could assist in the examination of the opposition's witnesses such as their 30(b)(6) technology person, key personnel and how they used their computer hardware or software and, of course, the opposing expert. Using an expert is all of these situation is particularly important, since counsel if all too often unable to differentiate a good story from just a well prepared story.

Industry Specifics

Industry specific background is not essential for expert qualification, although it could result in knowledge not familiar to the trier of fact. Also, industry specific background can be helpful for the computer forensic expert. Activities, systems or artifacts that might otherwise go unnoticed could be recognized by the expert familiar with that industry.

For example, they may already be familiar with certain applications and know how to interpret their data. In the preservation phase they may know that participants in that industry typically have certain systems or data that should be included in the preservation. Also, experts familiar with an industry may be able to recognize omissions in preservation or production as a result of their knowledge. So, industry specific knowledge could be a real cost saver.

Presentation Skills

While there is no expressed qualification requirement for presentation skills, there often is a requirement that the expert be useful to the trier of fact. Typically, one interprets usefulness in technical terms but technical competence may not be the only consideration.

Indeed, an expert that communicates as technically as his expertise may not be of any use to anybody. Thus, a good characteristic of an expert is one that can “translate” the technical aspects of his expertise into something understood by his listeners. In addition, there may be several languages or dialects in which he needs to communicate.

When communicating with jurors and even the client he may need to explain his findings in everyday terms and analogies. When communicating with the legal team, he may need to explain his findings using concepts they would easily understand, although sometimes the computer expertise of the legal team is not that advanced either.

An expert's presentation skills are not just important while testifying at trial. Indeed, they are important throughout the entire litigation lifecycle that can include briefings with the legal team and the client as well as formulation of tests and procedures for advancing the case.

Interestingly, advancing the case is not just about sifting and interpreting evidence. It can include using his expertise to counter the obstacles devised by opposing counsel to stifle discovery. In this regard, there are two ways that the expert can help. The first is uncovering the flaws in the opposing side's claims that requests are overly burdensome or assisting counsel in devising techniques for overcoming their objections or their requests for overly burdensome discovery. The second is devising techniques for sifting data efficiently when opposing counsel has delivered "quicksand".

So, the expert must fill many roles. It is not enough that he find interesting artifacts. He must also be a teacher and a strategist. The expert must be able to educate client and counsel about differing ways to obtain relevant evidence that is important to the case as well as the significance of his findings. At the same time, he must help them understand how those artifacts and the media or devices on which they reside will affect case strategy for better or worse.

While the technical skills of the computer forensic expert can be quite significant to the case from an efficiency and effectiveness perspective, the evidential value of the expert is his opinion and its aid to the trier of fact. While those opinions will actually be delivered as testimony, the manner in which they are initially articulated through the discovery process is a report. Of course, other vehicles could also be possible such as Affidavits or Declarations but the most likely method will be through a report. Thus, a significant consideration about an expert's presentation style can be his report writing capability.

Many of the forensic tools used by experts possess report writing tools. While these tools can be useful for experts, who already understand all of the attributes they contain, they are not typically good for anyone else. The reporting tools contained within forensic analysis tools provide little more than a means to accumulate the more significant data that has been analyzed in a central medium that simply facilitates locating the items that have been tagged as more significant. Thus, these reports are often no more than raw data dumps of items that the expert wants to be able to find again easily. Furthermore, they do not provide a means to summarize the raw data into something that makes its significance more obvious and is well suited as an exhibit for trial or deposition.

An expert's writing style and ability to communicate in writing can be important. The subject matter is often very technical but the findings must be comprehended by many with far less understanding than the expert. Thus, communicating that knowledge and presenting it in an easily comprehensible fashion such that its significance to the case is easily understood is very important.

While important, the expert's writing style is not all that matters. The report should contain sufficient evidential matter to support the expert's opinions. After all, if the opinion is to survive and advance case, there must be some comprehendible basis for the opinion.

A good way to assess the expert's presentation and communication skills would be to share some case specifics with the expert and let him explain how well his experience fits with

the specifics in this case. Such an approach not only provides a means to assess how well he communicates but it can help confirm the litigator's assessment of the expert's relevant experience. In the process, the expert may be able to recognize that what the litigator thinks is needed may not actually be a good idea. In that case, this could be a good opportunity to put things back on track.

Counsel may also want to inquire about the expert's experience writing reports including the style he uses for writing reports. While counsel may already have an idea what he needs for the case, he also needs something that will be useful to the trier of fact and something that will seem like a bunch of disjointed, mind numbing data points.

Educational Background

While the expert should have knowledge "not familiar in everyday life" or "in possession of the jurors", a formal education is not a requirement for qualification. Besides, the issue at hand is not likely a problem in a text book and the mere fact that he made a passing grade on some test does not mean that he will even be useful to the trier of fact.

Evaluating a computer forensic expert's educational background is not like evaluating those of a licensed engineer, medical doctor or accountant. By comparison to these other professions, the entire computer industry is relatively new. Someone with twenty years experience dates to a time when there was not even an abundance of degreed offerings, if any.

While there are more generalist degree programs today such as computer science, information systems, software engineering and the like, even they are not designed with the skills that computer forensic experts are likely to use. So, there may be no real advantage to experts having such credentials. So, an educational degree may be nothing more than a means to separate candidates.

In more recent times, there are degree programs in computer forensics that are starting to appear in college curriculum. While these are likely to provide a good foundation to those having them, again they are only a foundation. If anything, their usefulness may signal the seriousness at which the holder, pursues his career. On the other hand, in some esoteric areas it is unlikely that a worthy expert would have need of generalist designations.

Training

Training is another area that the litigator can use to distinguish computer forensic candidates. In this regard there are a number of training directions that the litigator may find of interest. Essentially there are the general training classes and there are the tool specific training classes.

The general training classes can involve fundamental issues such as file systems, operating systems, and software applications such as e-mail, application databases, and software applications in general. Such classes would reveal how these subjects work, how to interpret their meta data. and how to extract and handle their artifacts.

As an example, consider the situation where the computers to be examined are Microsoft Windows based machines versus Apple Mac machines. The file systems that accompany these two different devices behave differently and leave different kinds of artifacts. Knowing about these artifacts, where they reside and how to interpret them can not only affect the expert's opinion but influence the budget required to interpret them.

The other area where training can be influential is on the tools used by the expert to develop his own opinions as well as refute those of the opposing side. These days there are a number of forensic tools and no single tool will perform all evaluations. So, in order to perform a comprehensive examination,n the expert will likely need to have several tools in his toolbox and needs to be familiar with them whether through self training and seasoned use or formal training.

The need for tool familiarity is not limited to the performance of the expert's own work. Rather, he will also likely need this familiarity to understand and evaluate the work of the opposing expert, if there is one.

Licensing and Certifications

Licenses are typically issued by governing bodies like state or local governments and usually attest to the owner having accomplished a certain level of competency. Certifications are typically issued by groups like professional organizations, trade associations, product manufacturers, etc. and also are supposed to represent a certain level of competency.

Licenses and certification are usually not required for expert qualification. At the federal level it is black letter law that licenses and certification go to credibility and not qualification. At the state level things can be different, however. The state can require licensing or certification as part of expert qualification, although most states follow the federal rules where licensing and certifications go to credibility. One would have to check with their individual state law—both evidence and occupational licensing statutes. The following sections further discuss the significance of licensing and certifications when selecting a computer forensic experts.

Licensing

In federal court state licensing boards have no say in the qualification of an expert. As mentioned earlier, it is black letter law that licensing goes to credibility. Moreover, there is a long line of case precedent where State licensing boards have been rejected where they are in conflict with federal rules and regulation.

In state court, several states have imposed licensing requirements of experts in civil malpractice situations and medical testimony in their evidence statutes. The lack of other licensing requirements appearing in the evidence statutes tends to undermine any argument that the occupational licensing statutes should even be considered.

With respect to computer forensic experts there has been a movement by the private detective industry to claim that territory for itself. These efforts have largely been accomplished through pronouncements by the regulating boards claiming dominion over that territory. They

seem to make these pronouncements without consideration of the evidence statutes, their actual authority or the intent of the legislature.

An evaluation of all states is beyond the scope of this writing; however, the subject is addressed further in another Appendix to this manual. Although the article examines the issue from numerous angles, it considers decisions in several states to support its general conclusion that a state's evidence statutes tend to trump a state's professional licensing statutes and that the pronouncements by many state licensing boards are beyond their actual authority.

If it turns out that a license is required then one should look for experts having the requisite license. If a license is not required then one may still prefer experts having relevant licensing for credibility reasons.

With regard to the PI license requirement for computer forensic experts, the PI license issue is quite misleading. As mentioned above, licenses tend to indicate that the holder has some kind of proficiency in the skill covered by the license. This is not the case for the PI license, however. The PI profession does not teach its members computer forensics and computer forensic proficiency is not even tested on its exams. Thus, when examining an expert with a PI license one should realize is that what those license holders have been tested on is surveillance, weapons handling, funeral escorts and a number of other traditional law enforcement tradecraft. In fact, many have highlighted that PI literature often directs its members to retain an expert when their cases involve computer forensic issues. Clearly, there is no comfort to be had or basis for selecting a computer forensic expert based on the possession of a PI license.

With respect computer forensic certifications, there are several, although like educational degrees, professional certifications in computer forensics are rather a recent commodity. So, it could be likely that computer forensic experts will not have forensic certifications. Of course depending on the nature of the case a forensic certification may not be necessary.

Certifications

Computer forensic certifications generally deal with media files systems, operating systems, and interpretation of their artifacts. In some scenarios such as network or software functionality the classic computer forensic skill set may not be needed. Rather, more traditional computer system operation is all that is necessary.

So, litigators should realize that with respect to computer forensic certification there are relatively few and most of those are tools specific. Examples of tools specific certifications are the Guidance Software, the makers of EnCase, EnCE [EnCase Certified Examiner] and Access Data's, the makers of the Forensic Toolkit, ACE [Access Data Certified Examiner]. Of course there are still others but these two examples are probably the best known.

Examples of the non-tool specific certifications are the Certified Forensic Computer Examiner (CFCE) that is offered to law enforcement personnel only by IACIS. Another generalist certification is the Certified Computer Examiner (CCE) offered to anyone by the International Society of Forensic Computer Examiners (ISFCE).

Beyond these classical forensic certifications are numerous operational certifications. Some of these include those offered by vendors like Microsoft such as the Microsoft Certified System Engineer (MCSE) and Microsoft Certified Professional (MCP) to name a few of the Microsoft certifications. Many other vendors offer their own certifications as well such as Cisco Systems with their Cisco Certified Network Administrator (CCNA).

There are also generic certifications offered by industry associations such as the Computer Technology Industry Association (CompTIA).

Criminal versus Civil

One might consider using an expert with a law enforcement background. These individuals tend to make great witnesses for juries because of their instant credibility.

If the case is a civil matter, however, there are other things to consider. After all, the differences between criminal and civil cases are more than the law. Indeed, the capabilities of the experts are shaped by the procedural differences as well as the cultures spawned by those procedures.

In criminal cases the bar is higher than in a civil matter. In addition, prosecutors can have larger case loads than their civilian counterparts. Both of these factors can pressure them and their experts to focus on the low hanging fruit. The net result is that an expert grounded in criminal cases involving child pornography may be more accustom to finding the sure thing than going the extra mile to pursue issues that require research, testing, extensive analysis or marshaling complicated fact patterns.

Another difference is that in a civil case the opposing side often has considerably more notice of the impending production than a criminal defendant served with a search warrant. As such, in a civil matter it can be more important for the computer forensic expert to know how to find traces of what had been on the computer than finding the files themselves.

Also, criminal experts may not be accustomed to the discovery that occurs in civil proceedings. Thus, they may not be proficient in report writing, giving depositions and revealing and supporting their evidence and opinions prior to testifying at trial.

Forensic Tools

The specific tools used by the expert can affect the qualification of a testifying expert. In that case, therefore, they should be accepted, reliable and reliably used. It is helpful if the expert has been trained in their use, although that is not absolutely essential if he has adequate experience and knowledge about their use. After all, having attended a training class may not actually be a guarantee of anything.

As a result of the tool's significance in qualification, the litigator will want to know something about the tools used by the expert. While the litigator may not recognize tool names

provided by the expert, the litigator should have them revealed and discuss their acceptance with the expert.

The number of tools that are available is also much greater than in years past and the number continues to grow. Some of the tools are freeware while some are quite expensive. Although there is no definitive correlation between tool price and adequacy, the litigator will still likely want to inquire.

While there are some very good freeware tools, they may not be as feature rich as the ones with a price. In that case, the less feature rich tool could require more labor hours for the expert to accomplish the same result as the one where the work is included in automated features. So, free may not always be good.

The specific tools used by experts will depend on where in the litigation lifecycle they are being used. Typically, preservation is different from analysis which is different from processing and production.

Preservation

There are a variety of preservation tools that create forensic images. Forensic images are different from the images created by a client's technology personnel in that forensic images capture the entire media. Thus, they capture the active data, the deleted data and they even capture areas of the drive where user data would never be stored. The images typically created by normal technology personnel focus on the active data only.

While the forensic tools are often capable of collecting some smaller segment of a storage media, like the active data, those kinds of images are generally specifically identified as logical images, for example, or some other restrictive container name.

The kinds of tools that an expert will need can vary based on the type of equipment being imaged. The differences tend to be the interface that the storage devices use to transfer their data. For example, internal hard drives use one kind of interface while external devices like flash drives tend to use a different interface. So, the expert needs to have the kind of equipment capable of handling these different interfaces.

The expert is also expected to preserve the data without altering the original evidence. Typically the only concern for alteration is system meta data. It is unlikely that any preservation or collection method would change the data contained within the files themselves.

In any event, the protection of the original evidence is done with write blockers that prevent the collection system from altering the original media but in some cases the imaging method itself may be capable of collecting the data without altering anything even without a write blocker.

Additional considerations to the preservation mechanics themselves involve verification and redundancy. The verification confirms that after the imaging is completed that the image the original media. Calculating the verification typically means reading the data twice—once when the image was created and then again after creation.

When creating images it is best to create redundant copies. It is not likely that the device on which the image resides will fail but it does happen. In that event, it is best to have second copy of the image.

While the approach and technology used by an expert for preservation is one thing to consider, another is the preservation capacity that the expert could deploy. It is not unusual for preservations to involve many devices and their media. In addition, the preservation window is typically narrow. So, the expert needs to have adequate capacity to get the job done within the time constraints.

Analysis

There are no specific tools required for qualification of the expert, although whether one has knowledge about the tools can be important to determining whether the expert has knowledge useful to the trier of fact. Clearly the expert should have knowledge about his own tools but how about those used by the opposition? Actually, it is good that the expert has expertise in many different tools and the mainstream tools in particular.

When considering the tools used by the expert there are actually several considerations. These considerations are the kinds of tools, the variety of tools, the number of tools and how long have they been using them.

With respect to the kinds of tools, the litigator may want to determine whether the expert has invested in mainstream forensic tools or whether he is using freeware and other low priced alternatives. While it is nice to avoid needless markups, the lower priced tools are also commonly less feature rich and will require more labor hours to obtain the same results that might be automated in the higher priced tools.

Again understanding the specific tools owned and used by the examiner can be useful. Some tools are stronger in certain functions than others. So, again, it becomes important for the forensic expert to have diverse resources from which he can draw depending on the requirements of the case.

Forensic analysis tools are not the only kind of tool in the expert's arsenal. In large complex cases it is also the ability to manage the data and marshal the facts. While spreadsheets, as an example, provide robust analysis capability they are size constrained. So, in large cases spreadsheets lack adequate horsepower. In large cases, database applications can become much more essential.

So, in large case the litigator may want to assess how well equipped is the expert to manage large volumes of data and analyze them. Even the forensic tools can have practical size limits such that the data must be piece mealed from those applications and placed in other, more capable data management systems.

Another issue could be the number of licenses of its tools a forensic examiner owns. In large cases, throughput can be essential and multiple licenses a must.

Another category of tools are those that the litigator can use to provide data to the litigator. If the data are comprised of lists then spreadsheets are litigator friendly. But what happens when the lists exceed the capacity of the litigator's spreadsheets. How about different data types such as e-mails. Should those be provided as PSTs, HTML, or MSG type documents? Indeed, there are many questions about how the expert can support the litigator's needs in the kinds of tools that the litigator is capable.

Summary

Despite the increasing availability of computer forensic experts, selecting them is becoming more difficult. It is not that there are fewer of them. Quite the opposite is true. There is much more to choose from and as such the search can be more complicated and time consuming. In addition, as digital data and digital evidence permeate society and the law, the encounters have more variability.

Furthermore, computer forensics is not some kind of single subject discipline. While most people may think of computer forensics as hard drive examiners, the field is much more diverse than that. Also, as computers continue to permeate more and more of our society and legal system, the number of specialties and nuances increase accordingly.

Unlike other experts, the computer forensic expert can contribute to every phase of the litigation lifecycle. Also, the contributions of a computer forensic expert are not just evidential in nature. Indeed, there are also procedural and economic contributions that can be made by the computer expert. So, it is not just about case decisions. Rather, it is also technological and how the technology can be used to litigate faster, cheaper and better.

Clearly, there is much to consider when selecting the right computer forensic expert. One size does not fit all. Making the correct choice can involve a multitude of considerations involving the particular phase in the litigation lifecycle where the expert will be used as well as the technology involved. So, picking the right computer expert is a case where the answer clearly depends.

APPENDIX 2 - Do Computer Forensic Experts Need a PI License?

Introduction

It has become a common claim these days that computer forensic experts must have a Private Investigator (PI) License. The definition of PIs in most State occupational statutes is very amorphous. In fact, if followed literally few would ever escape the requirement to have a PI license before doing anything and the PI Boards have been abusing the definition to gain membership by claiming that a requirement exists for computer forensic experts.

Some theorize that what is really happening is that anyone with a credit card and access to the internet can perform a background check. Thus, the PI profession may be going the way of the elevator operator and the various State licensing boards are battling against progress.

While licensing requirements are often raised in hopes of neutralizing a damaging expert, these arguments tend to fail. When they do succeed, it is likely due to the ambush value of such a tactic when it catches counsel in unfamiliar waters and unprepared for the undertow.

What is really amazing is the number of computer forensic practitioners that parrot and play along with the ruse and the phony claims by many State PI Boards. For many, the attraction could be the barrier to entry that protects their turf from competition or a sales gimmick about a problem that only they can solve as a result of their licensed status.

Some also think that licensing improves the profession and keeps out the riff-raff, although how that is accomplished is somewhat of a mystery, since the various State PI licensing exams do not test or even teach computer forensic proficiency. For others it is just a means to avoid trouble with a licensing Board abusing its power under Color of Law. Still others think that it will protect clients from needless expense and argument; however, those experts are mistaken if they think that bullet proofing a client from an opposing counsel is achieved through appeasement, or even worse, compromising a client's case with someone whose contribution is a passing grade on an irrelevant exam.

The reality is that experts do not need a license in Federal court. In fact, State licensing boards have no say in the matter when the venue is Federal court.

Where State licensing boards could have an effect is in State court but most States model their evidence Statutes after the FRE and never mention a license or at least severely restrict when a license is required. For example, these days it is popular for States to require experts in malpractice cases to have had a license in the professional field about which they will be opining.

The following sections examine the PI licensing issue in particular and expert licensing in general for both Federal and State Courts.

Professional Licensing in Federal Courts

Admissibility of forensic experts in Federal cases is controlled by Rule 702 of the Federal Rules of Evidence (FRE). Rule 702 prescribes several conditions for admissibility but none of them involves a license issued by any State Occupational Board much less a State's PI Board. Indeed, under the FRE a license goes simply to credibility. *Dickerson v Cushman*, Inc., 909 F.Supp. 1467, M.D. Ala. S.Div (1995).

While licensing advocates often argue that to permit unlicensed experts to testify would be sanctioning a violation of the law, Federal courts have rejected those arguments. *Calvetti v Antcliff*, 346 F.Supp.2d 92 (2004) at 112. In fact, the Supreme Court has assigned to "trial judges the task of ensuring that the expert's testimony rests on reliable foundation and is relevant to the task at hand." *Daubert v. Merrell Dow Pharm. Inc.,* 509 U.S. 579, (1993) Thus, State licensing boards simply have no say in the matter when the venue is Federal Court.

Not only is a license not required for forensic experts in Federal courts, States may not impose additional requirements not contemplated by Congress. *Sperry v Florida,* 373 U.S. 379 (1963). The specific issue of a State's PI licensing requirements has even been considered, at least in the context of federal contractors performing background investigations. In that case, after considering numerous Federal decisions involving State licensing issues including the Supreme Court decision in *Sperry*, it was decided that Virginia could not frustrate federal laws by giving itself the power of review by way of a licensing requirement. *United States v Commonwealth of Virginia*, 139 F.3d 984 (1998)

Professional Licensing in State Courts

Whether or not licensing of forensic experts is required in State courts is a different analysis. The requirements of forensic experts are typically addressed in a State's evidence statute while a State's professional licensing requirements are addressed in its occupational statutes. Determining which statutes control the licensing of forensic experts typically involves statutory construction analysis to determine the intent of the State's Legislature.

In the case of *Thompson v Gordon*, 221 Ill.2d 414 (2006), the Illinois Supreme Court considered the Illinois Legislature's separate standards for expert witnesses under its evidence

statutes versus licensing under its occupational statutes. In addition, the court considered the fact that the Legislature had expressly imposed licensing requirements in malpractice situations but not in other situations under its evidence statutes. Thus, the Illinois Supreme court decided in favor of the evidence statutes over the occupational statutes.

The *Thompson v Gordon* decision is important to the PI licensing issue because it overruled the prior Illinois precedent in *People v West*, 264 Ill. App.3d 176 (1994) to the extent that it held that a license was a prerequisite to expert admissibility. The fact that that part of *People v West* has been overruled is quite significant, since it is often cited by PI advocates as the basis for their dominion over forensic experts.

In the recent case of *Susan Lukjan v. Commonwealth of Kentucky*, No. 2010-CA-001509-MR (2012), the Kentucky Court of Appeals reversed and remanded a lower court decision where the defendant's forensic expert was excluded because the expert was not a licensed PI. In *Lukjan* the Appeals court did similar statutory construction analysis and decided that, "**Providing testimony in a court proceeding is not the equivalent of selling the public one's services as a private detective . . . Kentucky's statutes governing the practice of private investigating are simply not meant to have any evidentiary effect.**" (emphasis added)

The *Lukjan* case is also instructive about the unintended consequence of a license requirement. In *Lukjan*, the license requirement was used by the prosecution at the trial court to suppress exculpatory evidence which was an act characterized by the Appeals court as "not harmless".

Often times a Court's statutory construction analysis is determined simply in favor of a detailed statute over a general statute. In *Donegal Mutual Insurance Company v White Consolidated Industries*, 121 Ohio Misc.2d 14 (2002) the Ohio Court of Common Pleas for Darke County also addressed the specific issue of whether a forensic expert required a private investigator license and held that a witnesses' failure to obtain a private investigators license from the state did not preclude them from testifying. In other words, the detailed statute, the evidence statute in this case, prevails over the more general statute, the occupation statute.

One of the oldest cases to consider the PI licensing question is *Kennard v Rosenberg*, 127 Cal.App.2d 340 (1954). In that case the Appeals Court also saw a difference between offering services to the public and testifying in court as an expert. As a result, the Court decided that, "Where statute is susceptible of two constructions, one leading inevitably to mischief or absurdity, and the other consistent with justice, sound sense and wise policy, the former should be rejected and latter adopted."

Although there are countless State court decisions involving licensing of forensic experts and finding in favor of the evidence statutes, there are two Alabama decisions that are particularly instructive when examining the licensing issue in State courts. The first is *Wood v State*, 891 So.2d 398 (2003). Besides finding in favor of the evidence statutes, the decision is very useful because it examines decisions in many other states like Georgia, Virginia, Alaska, New York, Tennessee, Iowa, Pennsylvania, Louisiana, and Arkansas to name a few, where courts in those states had also grappled with the applicability of professional licensing to

forensic experts and generally found that the occupational statutes have no effect on the evidence statutes.

One of the more persuasive and amusing decisions mentioned and considered in *Wood* involved a Rhode Island case, *Owens v Payless Cashways, Inc.*, 670 A.2d 1240 (R.I.1996). In that case the issue involved whether rules governing licensing of engineers supplanted judicial discretion regarding the qualification of experts under Rhode Island evidence rules.

In making its decision, the *Owens* Court reasoned that the professional licensing and evidence statutes were not in conflict and that the qualification of expert witnesses and the matters about which they may testify are within sound discretion of trial justice. The Court further explained that the expert is there to assist the trier of fact and that persons of great learning, like Archimedes or Wernher Von Braun, should not be barred from courts simply because they had not been licensed.

The second Alabama case that is particularly instructive is *Arthur v Bolen*, 41 So.3d 745 (2010). In that case, the Supreme Court of Alabama also considered whether forensic engineers must be licensed. This case is distinguishable from the previously mentioned decision in *Wood* in two respects. First, the *Arthur* decision involved engineers rather than psychologists like in *Wood*. Second, Alabama's occupational statute for engineers had previously contemplated expert testimony while Alabama's occupational statute for psychologists had not.

The story in *Arthur* begins in 1997 when the Alabama Legislature made changes to the engineering occupational statute and expressly included expert testimony as part of the definition of engineering. It was not until 2006, however, when the issue appeared in the case of *Board of the City of Mobile v Hunter*, 956 So.2d 403 (2006) that the Alabama Supreme Court decided that by including expert testimony in the occupational definition of engineering that the Legislature had superimposed the licensing requirement onto the evidence statutes, specifically Rule 702 of the Alabama Rules of Evidence. Consequently, in *Hunter* a license was required for an engineer to testify as an expert.

Interestingly, in the next legislative session following the *Hunter* decision, the Alabama Legislature again changed the definition of engineering and omitted expert testimony from the definition in the occupational statute but left the licensing requirement in malpractice cases in the evidence statutes, which apparently was its intent in the first place. As a result, when the Alabama Supreme Court addressed the issue again in *Arthur v Bolen* it permitted the testimony of an unlicensed engineer about the attachment of a staircase, since his opinion did not involve the design of the staircase.

What the *Hunter* decision helps to cement is that when the occupational statute has included expert testimony in the definition of the occupational license then the licensing Board could well be within its authority to claim that forensic experts must also be licensed. On the other hand, where the occupational statute has not been constructed to expressly include expert testimony then a license is not required unless the licensing requirement appears in the evidence statute.

Testifying Versus Other Work Performed by Forensic Experts

Hardcore PI advocates will review the various court decisions where a license requirement for forensic experts was rejected and claim that while experts can testify without having a license they would still be breaking the law by performing any other work. This kind of logic is also doomed, however.

Usually under the various rules of evidence forensic experts must base their opinions on a reliable foundation. This often means making their own tests and taking their own measurements. They simply cannot rely on opinions provided by others unless they have at least taken steps to perform or review the work themselves and form an opinion. *In re Polypropylene Carpet Antitrust Litigation,* 93 F.Supp.2d 1348 (2000) and also *Williamson v. Harvey Smith, Inc.*, 246 Ga. App. 745 (2000)

The significance of the evidence statutes, particularly those involving experts, has broad based application to litigation matters. Essentially, anyone can be called to testify whether they actually testify or not. Consequently, actual testimony should not be the determining criteria. Rather, the fact that one could be called to testify as an expert for any number of reasons should be sufficient to trigger the rules of evidence and its related criteria when litigators are preparing their case.

Under rules of evidence, matters involving scientific, technical or specialized knowledge are generally reserved for experts. What actually constitutes scientific, technical or specialized knowledge can be a low bar, since the determining factor is whether or not the information is "familiar in everyday life" and "in possession of the jurors". *US v Wilson*, 408 Fed.Appx. 798, 2010 WL 4608797 (C.A.5 (La.)) (2010), and *US v Johnson*, 617 F.3d 286, C.A.5, (2010)

Courts have even analogized the interpretation of computer forensic reports to specialized medical tests and interpretation by police officers of slang and code words used by drug dealers, which they have deemed specialized knowledge of an expert. *US v Ganier*, 468 F.3d 920, C.A.6 (2006)

Constitutional Challenges to Professional Licensing Requirements

If one finds themselves in a situation where professional licensing of forensic experts is required and they are contemplating a Constitutional challenge, one should review the above referenced decision in *Hunter*. In that case, the Hunters challenged the Alabama engineering licensing law on various Constitutional grounds and lost. So, the case is instructive of the obstacles that must be overcome.

With regard to the PI licensing issue, however, the matter is likely much simpler and does not pose a Constitutional question. Typically, the PI license issue is not one that is consistent with legislative intent and requirements clearly articulated in statutory language. Rather, it is just a licensing Board improperly applying its amorphous definition of Private Investigator/ Detective to forensic experts. Administrative agencies, like licensing boards, are usually only authorized to implement the laws passed by the Legislature. *North Fulton Medical Center v Stephenson, et al, Northside Hospital et al v Stephenson, et al*, 269 Ga. 540 (1998)

Professional Licensing in Georgia Courts

In Georgia, the requirements for the admissibility of expert opinion are described in the evidence statutes in Title 24 of Georgia's code. The admissibility of expert opinion in criminal cases is described at OCGA 24-7-707 (previously OCGA 24-9-67) and at OCGA 24-7-702 (previously 24-9-67.1) for civil cases.

In criminal cases under OCGA 24-7-707, "The opinions of experts on any question of science, skill, trade, or like questions shall always be admissible; and such opinions may be given on the facts as proved by other witnesses." Clearly, the admissibility of forensic experts in criminal matters does not require a license, since their opinions "shall always be admissible". In fact, nowhere is the error of the PI Board's opinion more obvious than in criminal matters.

In civil cases under OCGA 24-7-702 the requirements for expert opinion are more complicated and subject to several requirements. First, the expert must be qualified by "knowledge, skill, experience, training, or education". Second, the expert's testimony must be based on a reliable foundation comprised of,

- Sufficient facts or data which are or will be admitted into evidence at the hearing or trial;
- The product of reliable principles and methods; and
- The application of the principles and methods reliably to the facts of the case.

Third, the expert's scientific, technical, or other specialized knowledge will, "Assist the trier of fact . . . to understand the evidence or to determine a fact in issue."

There are two interesting facets of Georgia's basic statutory requirements for the admissibility of expert testimony. First, in criminal cases the admissibility requirements for expert opinion are not nearly as stringent as in civil cases, since expert opinion in always admissible in criminal cases. Second, the requirements for qualification of experts in civil cases do not include a licensing requirement for admissibility of the expert's testimony.

In 2005 the requirements for experts in civil cases were supplemented with two additional requirements, however. First, paragraph (c) of OCGA 24-7-702 imposed a licensing requirement on experts when testifying about professional negligence and an actual experience requirements when testifying about medical malpractice. With respect to the license, the expert must have been licensed by the state in which he was practicing or teaching at the time the act or omission occurred. With respect to the experience requirement in medical malpractice cases the expert must have had actual experience or practice in the area or specialty in which the opinion is being given.

Second, paragraph (f) of OCGA 24-7-702 was added that authorizes Georgia courts to draw from decisions by the US Supreme Court and other Federal Courts interpreting and applying the standards of *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993) and its progeny.

So, while the basic criteria for expert admissibility in civil cases do not require a license, those criteria were supplemented in 2005 in subsequent paragraphs with a professional

licensing requirement in malpractice cases. Licenses are not required in other civil matters, however.

With respect to the Daubert criteria or other Federal Court decisions that were added in 2005 authorized for consideration in paragraph (f), the requirements for expert qualification under rule 702 of the Federal Rules of Evidence are similar to Georgia's. Under Rule 702, "A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

- the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
- the testimony is based on sufficient facts or data;
- the testimony is the product of reliable principles and methods; and
- the expert has reliably applied the principles and methods to the facts of the case."

As a result, the federal cases do not contemplate any limitation on expert witnesses as a result of state licensing boards even though licensing could affect a witness' credibility. In *Dickerson v Cushman*, Inc., 909 F.Supp. 1467, M.D. Ala. S.Div (1995), the court explained that, "Federal courts have allowed persons to testify as expert witnesses even though they did not possess certificates of training or education, memberships in professional organizations, and may not have been the most outstanding practitioners in their fields. *See United States v. Barker,* 553 F.2d 1013, 1024 (6th Cir.1977). In general, the fact that an expert does not have a degree or license in his or her professed specialty goes to the weight of his or her testimony rather than its admissibility. *United States v. Bilson,* 648 F.2d 1238, 1239 (9th Cir.1981). "

Clearly, Georgia's evidence statutes do not require expert witnesses to have a license of any kind except in civil malpractice cases. Nonetheless, the question about whether the professional licensing statutes are relevant to the qualification of experts and admissibility of their testimony has been argued many times over many years.

The Georgia courts have followed similar reasoning as the federal courts when confronted with the question about professional licensing of expert witnesses. (see *Williamson v Harvey Smith Inc.*, 246 Ga. App. 745, 542S.E.2d 151 (2000) citing *Dayoub v Yates-Astro Termite Pest Control Co.*, 239 Ga. App. 578, 521 S.E.2d 600, 99 FCDR 3085 (1999), "The possession of a license in Georgia does not go to qualification as an expert witness but may go to the weight and credibility that a jury gives to such expert's opinion." See also, *Ashley v State*, 728 S.E.2d 706, (2012), "The possession of a license in Georgia does not go to qualification as an expert witness but may go to the weight and credibility that a jury gives to such expert's opinion." citing *In the Interest of C.W.D.,* 232 Ga.App. 200, 206–207(3)(a), 501 S.E.2d 232 (1998)).

In fact, the requirements in Georgia are minimal and a license is not required. (see *Dayoub v Yates-Astro Termite Pest Control Co.*, 239 Ga. App. 578, 521 S.E.2d 600, 99 FCDR 3085 (1999). "The requirements for qualification as an expert witness are minimal; generally, nothing more is required to qualify an expert than evidence that the person has been educated in a particular trade, science, or profession.")

While there is no precedent on computer forensic licensing, other efforts to exclude unlicensed experts in Georgia have failed. In *Dayoub* for example, the Appeals court concluded

that, “Such license requirement is arbitrary and capricious and imposed a standard of qualification greater than that required by law,” citing OCGA 24-9-67. In *Nelson v State*, 279 Ga. App. 859, 632 S.E.2d 749 (2006), the Appeals court characterized a criminal defendant’s arguments against the testimony of an unlicensed psychologist as “meritless” explaining that, “This Court has repeatedly held that it is a matter within the sound discretion of the trial judge as to whether a witness has such learning and experience in a particular profession as to entitle him to be deemed prima facie an expert.”

Furthermore, the court in *Dayoub* also said that, "The question of whether a witness is qualified to render an opinion as an expert is a legal determination for the trial court and will not be disturbed absent a manifest abuse of discretion," citing OCGA § 24-9-67 and *Bales v. Shelton,* 197 Ga. App. 522, 525(3), 399 S.E.2d 78 (1990). So clearly, at least in Georgia, it is the courts and not the licensing Boards that are the gatekeepers for determining who is or is not an expert witness. Moreover, the consequence of this fact in any e-discovery or traditional computer forensic situation is far reaching considering recent Federal decisions in cases like *Victor Stanley Inc. v Creative Pipe Inc.*, 250 F.R.D. 251, 70 Fed.R.Serv.3d 1052, (2008), "Indeed, it is risky for a trial judge to attempt to resolve issues involving technical areas without the aid of expert assistance."

The idea advanced by licensing advocates that testifying experts can simply offer opinions based on the work performed by licensed professionals is also doomed, since both the federal and Georgia cases as well as their respective rules of evidence require that experts base their work on a reliable foundation, which often means making their own tests, taking their own measurements, or at least reviewing and confirming the work done by others. (see, *In re Polypropylene Carpet Antitrust Litigation*, 2000, 93 F.Supp.2d 1348, motion to amend denied 2000 WL 863456, "Expert may not simply repeat or adopt findings of another expert without attempting to assess validity of opinions relied upon." See also, *Williamson v. Harvey Smith, Inc.*, 246 Ga. App. 745, 542 S.E.2d 151, "Home inspector testifying as an expert witness could base his testimony on report that had been prepared by someone else in his office; inspector testified that he went back to property and verified report's contents.")

Any notion that the Board’s claim reflects legislative intent as manifested in the far ranging definition of a private detective business is misguided as evidenced by the wording in OCGA 24-7-702(f) mentioned above holding just the opposite. Furthermore, OCGA 24-7-702(c) does require licensing of experts in malpractice cases. Thus, the absence of a licensing requirement in other matters further evidences the absence of legislative intent with respect to PI licensing. The absence of an exemption for expert witnesses in the private security statute should not be interpreted as expanding its coverage to expert testimony, since the legislature omitted exemptions in the statutes of other professions as well.

When examining the question about whether computer forensic experts should have a PI license, there is no doubt that the Private Investigator licensing statutes are not relevant to the qualification of expert witnesses and admissibility of their opinion. In fact, the lack of legislative intent for a PI licensing requirements for experts is apparent from the recent history of this issue, which begins in March 2006 when HB 1259 cleared the General Assembly and went to Governor Perdue for signature.

HB 1259 made only a few changes to the existing Private Investigator (PI) statute. The most significant was that it upgraded the penalty for an unlicensed private detective business from a misdemeanor to a felony.

The change was widely touted by PI types as a stealth move directed at computer forensic practitioners. Because the definition of private detective business is so broad, the change brought outcry from numerous other professions who feared ensnarement as well.

On May 5, 2006, Gov. Perdue vetoed the bill explaining that the felony provisions could result in unintended consequences as a result of the overly broad definition of private detective business and the lack of exemption for expert witnesses. So clearly, at least the PI licensing statutes were not intended to govern expert witnesses.

Nonetheless, In 2007 PI lobbyists resumed their efforts with a new bill, HB 504. Interestingly, one of the PI lobbyist in the HB 504 effort was related to the then Board Chair, who also operates a private detective and security firm.

The new bill updated the definition of a private detective business to expressly include "any type of digital or electronic information". It also expressly exempted the application of the private detective statute to other licensed professionals performing within the scope of their profession.

Clearly, the new bill was trying to overcome its prior shortcomings. Furthermore, this second attempt evidences that the definition of a private detective business must not have included computer forensics or electronic information; otherwise, why need to modify it?

At the same time, the new bill would have made a PI license a kind of super license, since all analytical professionals would be covered by the PI license requirement unless covered by an exemption or some other professional license.

Despite that licensed accountants, engineers and medical personnel, for example, were exempted from coverage, the new bill still lacked an exemption for expert witnesses as mentioned in Governor Perdue's veto explanation and the expressed intent of the legislature reflected in OCGA 24-9-67.1(f).

Unsurprisingly, HB 504 disappeared into committee and was never heard of again. So, it never passed the legislature and never made it to the governor's desk for signature. Indeed, all that remains is the Board’s April 2007 opinion that was issued in the face of legislative failure.

The bottom line is that qualification of expert witnesses and the admissibility of their testimony is controlled by the evidence statutes in Title 24 of Georgia's code. The professional licensing statutes in Title 43 of Georgia's code, in general and PI licensing in particular, have no role to play in the qualification or admissibility of forensic experts and their opinions.

Summary

The question of whether computer forensic experts require a PI license is currently a hot topic in American Jurisprudence. Numerous groups and individuals have invested considerable time in answering the question for those who are interested. Unfortunately, the work by most of these researchers is usually limited to the various State PI licensing statutes and opinions by the PI Boards. Thus, they never consider applicability of the evidence statutes, controlling precedent or any analysis of Legislative intent.

The reality is that a PI license is not required in Federal Courts. The answer is more complicated for State courts and requires some amount of statutory construction analysis on a State by State basis. Generally, however, a State's evidence statutes tend to trump that State's occupational statutes when forensic experts are the subject of the analysis.

Also, the impotence of the licensing statutes is not limited to an expert's actual testimony. Indeed, the supremacy of the evidence statutes will extend to the work performed by the forensic expert in developing his opinion, since it must be based on a "reliable foundation".

APPENDIX 3 – Sample Protocol for Forensic Analysis and Production of ESI

This sample protocol has been developed based on the guidance and suggestions described in the chapter titled, “Designing Plans and Protocols – A Systems Engineering Approach to Cyber Litigation”. To better understand the rationale used in developing this sample protocol, consult the guidance and suggestions contained in that chapter.

TABLE OF CONTENTS

1) Purpose

This protocol is being put in place in the matter of _____ to govern the preservation, analysis, and production of ESI.

All matters involving the preservation, processing, production, and review of ESI related to the Devices are incorporated in this protocol. In the event of a dispute, the parties agree to use the dispute provisions of this protocol to resolve same.

2) Definitions

a) EDEA – Electronic Discovery Escrow Agent. The EDEA is the entity responsible for providing expert technical services under this protocol. The EDEA may be called by either party to testify about the work performed under this protocol. The parties may also call other experts to support or refute the EDEA's opinions. Except as specifically set forth below, there shall be no *ex parte* communication between the parties, the parties' counsel, their respective retained experts, and the EDEA.

b) Electronic Storage Device – Any item that can be used by a person for storing and retrieving digital data and contains both the storage media and the means for storing and retrieving data to its media even though it may need to be connected to some other piece of equipment for the data to be interpreted by a person. Examples of Electronic Storage Devices are computer workstations, laptops, servers, cellphones, Personal Data Assistants (PDA), flash drives, thumbdrives, hard drives, etc.

c) Electronic Storage Media – Any item that can be used by a person for storing and retrieving digital data but relies on another device to write or read the data to the media. Examples of Electronic Storage Media are tapes, diskettes, CDs, DVDs, zip disks, etc.

d) Entropy test – A method frequently used to identify encrypted files. Entropy tests may not always identify protected files, since it is essentially a test of randomness. Files having both random and non-random components may not fail the test.

e) ESI – Electronically Stored Information

f) Event Logs – A windows system log that captures various machine operation activities such as logon and logoff, network connection or disconnect, etc.

g) File Slack – See the definition for Slack Space

h) File System – The file system of a storage media is the equivalent of the "card catalog" in a library. It is what electronic systems use to know the names and locations of files and folders on the storage media along with other attributes like date stamps and active or deleted status.

i) Forensic Data Copy - A Forensic Data Copy (FDC) is a method of securing or "petrifying" data files into a protective container that prevents future alteration of the collected data. This method is focused at capturing selected data files from a storage media and not the entire contents of the storage media itself.

j) Forensic Grade Copy – A Forensic Grade Copy (FGC) is a method of copying data from an electronic storage media in a way that captures the data available to the copying method. Typically, this method is used with cellphones where the data captured may not be everything on the device but is everything that the device manufacturer allows to be captured from the device through whatever interfaces the device manufacturer has designed for such purposes. The data is then stored in a container to protect the copied data from future alteration of the collected data.

k) Forensic Grade Image – A Forensic Grade Image (FGI) is a special kind of copy of an electronic storage media that captures the entire contents of the media including active data as well as deleted data or free space as well as those areas of the media that are

typically not available to the media users such as boot sectors and unpartitioned space. The copy is typically made using special protection measures to ensure that none of the media's data is altered during the process.

l) Free space – The area of a storage media available to store new data. Free space can contain deleted data, since the act of deletion usually only changes the status of the storage area containing a file from "in use" to "available for use". Free space is sometimes referred to as unallocated space since it is not currently allocated to storing active files.

m) Hashing – The act of computing a mathematical score of a data stream for use in subsequent validation or identification. The most common hashes used in this project shall be the MD5 or SHA1 hash.

n) Hibernation file – The hibernation file is a feature of many computer operating systems where the contents of RAM are written to non-volatile storage such as a hard disk, as a file or on a separate partition, before powering off the computer. When the computer is restarted it reloads the content of memory and is restored to the state it was in when hibernation was invoked.

o) INFO/INFO2 File – A windows system file used by the Recycle Bin to track deleted files

p) Internet Cache – Files used by web browsing software that tracks internet history data as well as local file access data.

q) Jump Lists – A collection of Windows based file activity records containing information about files that have been opened and viewed similar to what is contained in a Link File.

r) Link File – A windows system file that is created whenever a file is opened. Link files contain numerous metadata attributes about the file that was opened such as the location of the file, its file system date stamps, and the type of storage media on which the file resided.

s) Metadata – Metadata is data about data. Metadata may generally be viewed as either System Metadata or Application Metadata. System Metadata is data that is automatically generated by a computer system and relates to other data files or activities of the system. For example, System Metadata often includes file system information such as date and time stamps, file path (location on the media), attributes such as read-only or other system generated information such as pointers, and activity or operation logs. Application Metadata is data within a file and relates to that particular file. Application Metadata is divided into two types, Substantive Metadata and Embedded Metadata. Substantive Metadata is data that reflects the substantive changes made to the document by the user. For example, it may include the text of actual changes to a document. Embedded metadata includes other data embedded in the document by the system or software application such as author or creator, organization, and various date stamps. While no generalization is universally applicable, System Metadata and embedded metadata is less likely to involve issues of work product and/or privilege.

t) MSG – MSG is the format of a container (file) used to hold individual e-mail messages and their attachments in a Microsoft Outlook/Exchange mail system.

u) Native File(s) – ESI in the electronic format of the application in which such ESI is normally created, viewed and/or modified. Native Files are a subset of ESI.

v) NSRL – National Software Reference Library is a list published by the National Institute of Standards Technology of known file hashes, specifically MD5 and SHA1, for published software. The library is updated quarterly to reflect revisions and new releases. The library is typically used to identify and remove from further consideration files contained in standard software applications that, while matching files types of interest like spreadsheets or text documents, shall have no significance to this litigation.

w) OCR – Optical Character Recognition is the process of converting image based textual characters into textual data that, in the context of this project, can be searched with other electronic means.

x) PDF – Portable Document Format is an image file format commonly used for document management in litigation. The conversion from native format to PDF shall eliminate metadata contained within the native format document, although the PDF format shall contain the searchable text of the remaining image.

y) PST – PST is the format of a container (file) used to hold an individual's e-mail messages and attachments in a Microsoft Outlook/Exchange mail system. In a metaphorical sense the PST container is the equivalent of an individual mailbox containing letters (e-mail messages).

z) Registry – A file used by the Windows Operating System to store data attributes used by the operating system for machine operation. The Registry is composed of several files. The attributes they contain include installed hardware and software, security data, configuration data, user data, etc.

aa) RTF – RTF (Rich Text Format) is a text based file format developed by Microsoft for use with Microsoft products like Outlook and Word and for cross platform document interchange.

bb) Security Identifier (SID) – A security identifier is an intelligently coded value used on Windows NT class machines that uniquely identifies the machine or domain and the user associated with certain data or functions. The machine or domain portion is a set of 3 ten character strings separated by dashes. The user portion is a 3 or more character suffix added to the machine or domain identifier. The user portion uniquely identifies the user for that machine or within that domain. User identifiers of 1000 or less are system level users, including built-in users like the machine or domain administrator, while identifiers of 1001 or more are other users.

cc) SetupAPI.Log – A Windows system log found on Windows systems prior to Vista that captures information related to installation of hardware devices.

dd) SetupAPIDev.Log - A Windows system log found on Windows systems Vista and later that captures information related to installation of hardware devices.

ee) Slack space – Electronic media is typically divided into smaller storage segments. Slack space is the area from the end of an actively stored file to the end of the storage segment containing the active file.

ff) Static Image(s) -- A representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. In the absence of agreement of the parties or order of Court, a Static Image should be provided in either Tagged Image File Format (TIFF, or .TIF files) or Portable Document Format (PDF).

gg) SWAP file -- A swap file (or swap space or a pagefile) is a space on a hard disk used as the virtual memory extension of a computer's RAM (Random Access Memory). The swap file allows a computer's operating system to pretend that it has more RAM than it actually does. The least recently used files in RAM are "swapped out" to the hard disk until they are needed later.

hh) TIFF – Tagged Image File Format is a graphical image file format commonly used for document management in litigation. The conversion from native format to TIFF shall eliminate metadata contained within the native format document. A TIFF image is not searchable without first having its text based characters converted to searchable text.

ii) TXT – TXT is a text only file format usually based on the standard ASCII (American Standard Character for Information Interchange) character sets.

jj) UTC – Universal Time Coordinated. Many computer system file dates are stored internally in UTC format and then converted to local time, when presented, based on the computer's time zone settings. In a general sense, UTC is similar to Greenwich Mean Time (GMT). Consequently, when converting UTC times to local East Coast United States time, for example, users would subtract either 4 or 5 hours from the UTC time, depending on the existence of daylight savings time, to convert to local time.

3) ESI Identification and Preservation:

kk) The parties shall work with the EDEA to develop a data map of all devices, media, and/or accounts that should be preserved.

ll) The parties shall provide the EDEA with any images and copies of any data that they have already preserved. The EDEA will examine the images and copies to confirm that they are suitable forensic grade images or copies for the purposes of this analysis. If the EDEA determines that the previously prepared images or copies are defective or otherwise unsuitable, the EDEA shall proceed with whatever images or copies are acceptable while the parties determine how to address the issues associated with the problem images or copies including a re-imaging or copying and the use of both versions for the analysis described herein.

mm) The parties shall cooperate with the EDEA to preserve as quickly as possible any devices, media or accounts that have not already been preserved but identified for preservation.

i) The EDEA shall prepare Forensic Grade Images (FGI) for any computing devices like laptops, desktops, servers, flash drives, and/or external hard drives.

ii) The EDEA shall prepare Forensic Grade Copies (FGC) of any cellphones.

iii) The EDEA shall download the data from any cloud based web mail, social media, or data storage location and create Forensic Data Container (FDC) similar to an Access Data, AD1 image.

a. The EDEA shall prepare a tabular report of all devices, storage media and accounts for which it has been supplied a preservation image and/or has collected and preserved data. The report shall identity at a minimum the:

i. Custodian,

ii. Device, media or account type,

iii. Device, media or account manufacturer or provider,

iv. Device or media serial number including any internal firmware serial number,

v. Device or media volume serial number,

vi. Device or media volume label,

vii. Collection or preservation date,

viii. Confirm whether a valid image exists for work under this protocol.

4) Processing and Production

The sections contained in this part prepare the preserved data that has been selected for assessment of its contents as well as production of those contents that are desired. If the parties choose, they may pursue a staged approach where preserved items of lesser interest are processed later, if at all. The work to be performed by the EDEA and the parties in reviewing, clearing and producing the data is described below.

4(a). Preproduction Processing & Preparation

The EDEA shall perform the following tasks to prepare the selected media and its data for reporting and searching as described in subsections 4(b) and 4(c) below:

i) Parse the media's active file system to identify active and deleted files as well as their attributes.

ii) Search the media's free space to locate prior instances of the media's files system, parse their contents and attributes, and incorporate the results into the file system catalog.

iii) Parse any Windows Volume Shadow Copy (VSC) data if it exists.

iv) Explode any instances of compound files like compressed archives and/or e-mail containers. Compound documents like databases or XML files or Office documents

shall not be exploded into their individual components. Rather, they shall remain as single documents.

v) Recover deleted documents from free space as well as those found in the system swap and hibernation files. At this time, this effort shall be limited to automated recovery efforts only and to those results that can be recovered intact. The process shall be performed using:

(1) Data carving methods that identify recoverable files based on file signature patterns of file headers and file footers, and

(2) The types of documents that should be recovered using data carving techniques are link files as well as any other file type listed in Exhibit 6.

(3) The results of any data carving processes should be added back to the file system list of file and should be identified by something like a file name of "carved" suffixed with a unique value.

vi) Recover deleted e-mail messages from their containers using database record recovery techniques

vii) Calculate MD5 hashes of each individual file on the device or media for use in subsequent deduplication and volume reduction efforts. In the event of compound documents like e-mail and compressed archives, the hashes shall be computed for the parent document (e-mail and compressed archive) as well as each individual child document.

viii) Perform signature analysis to confirm that document types match their file extension so that subsequent document selection or volume reduction efforts based on file extension are reliable.

ix) Perform entropy tests to identify encrypted documents requiring passwords or other access credential prior to searching or other subsequent processing, production or review efforts.

x) The EDEA shall recover active and deleted instances of Windows Recycler files such as INFO/INFO2 and $R and $I. The EDEA shall then parse these recovered files to reveal the original file names, original paths and deleted dates of deleted data.

4(b). Post Processing Reports

The EDEA shall prepare several different reports with respect to the preserved data for which it has processed in order to assist the parties in analyzing the contents thereof:

4(b)(i) File System Reports

(1) Catalog the file system contents in a tabular report format (Excel spreadsheet or equivalent).

(2) The reports will be segmented between at least text messages, e-mail and then loose files. If the text messages, e-mail or loose file segments contain more rows

than can be presented in the report, the individual lists shall be further segmented in order to produce a complete listing.

(3) The file lists shall include:

(a) Both currently active and deleted text messages, e-mail or loose files appearing in the current file system,

(b) Any text messages, e-mail or loose files obtained from file system remnants,

(c) When compound documents are included the list shall preserve and identify the parent child relationship such as through identification a parent and child identifying value.

(4) The file list shall follow the specification provided in the Exhibit 1 for loose files (F), e-mail (E) and text messages (T).

4(b)(ii) File Activity Reports

(1) Recover and parse both active and deleted link files and jump lists from preserved Windows based devices or media containing these Windows based artifacts using TZ Works Link Parser and Jump List Parser or equivalent and prepare a tabular report containing both their file system metadata, to the extent it still exists, as well as their internal metadata pertaining to the files to which the link files and jump lists are pointing.

(a) The EDEA's link file and jump list report shall include all data elements provided by the parsing tool but shall, at a minimum, include the following data attributes.

(i) Name and extension of the file to which they point.

(ii) Full path of the file to which they point.

(iii) File system date stamps (Create, Modified, and Last Accessed) of the file to which they point.

(iv) File system date stamps (Create, Modified, and Last Accessed) of the link file or jump list item itself.

(v) Size of the file to which it points.

(vi) Volume serial number and volume label for the media on which the file to which it points is stored.

(vii) Drive type for the media on which the file to which it points is stored.

(2) The EDEA shall parse browser history using Digital Detectives Net Analysis or Magnet Forensics Internet Evidence Finder or equivalent from both active and free space of the storage devices for Windows Internet Explorer as well as any other browser used on the device like Google Chrome or Safari, and prepare and produce tabular reports.

(a) For any instances of file activity retrieved from Windows Internet Explorer, the produced report shall include, at a minimum, the user, date and time stamp for the file activity, full file path, number of visits and the browser record type.

(b) For any instances of web page activity from any browser, the produced reports shall include, at a minimum, the user, date and time stamp for the browser activity, data type (like File, HTTP, HTTPs, etc), host or domain, file name, path or URL, number of visits, any internet searches and their results, the browser record type.

(c) For any instances of text messaging discovered in the browsing history, the EDEA shall recover and decrypt text messages using Magnet Forensics, Internet Evidence Finder (IEF) or equivalent.

4(b)(iii) Device System Reports

(1) The EDEA shall parse and prepare text based reports of the following Windows registry hives from devices having them using the latest version of RegRipper.

(a) System

(b) Software

(c) Security

(d) SAM

(e) NTUser.Dat for relevant user profiles

(f) UsrClass.Dat for relevant user profiles

(2) The EDEA shall convert the Windows SetupAPI.log or SetupAPIDev.log into a text based report from devices having them.

(3) The EDEA shall parse the following Windows Event Logs using Event Log Explorer or equivalent and prepare tabular reports.

(a) System

(b) Security

(c) Application

(4) The tabular reports of the Windows event logs shall include all available event log fields including but not limited to the record number, date/time stamp, event type, event user, and a description of the event ID.

(5) For Apple machines the EDEA shall parse and prepare text based reports of the System log as well as any archived version.

(6) For cellphones the EDEA shall prepare a tabular report that merges call log activity with text message activity in order to provide a comprehensive view of device communication activity.

4(b)(iv) Attached Device Reports

(1) The EDEA shall prepare tabular reports of attached devices for any Windows or Apple based systems.

1) The Windows based machines shall compile information from the System, Software, and NTUser registry hives for each relevant user as well as the SetupAPI.log or SetupAPIDev.log

2) The Apple based machines shall compile information from the current System log file as well as any archived System log files.

3) The reports shall identify the host machine and include the name of the

a) attached device manufacturer,

b) attached device model,

c) device type (such as camera card, flash drive, external hard drive, internal hard drive, etc.)

d) serial number,

e) friendly name if any,

f) the first date the storage device was attached,

g) the most recent date it was attached as well as the following other attributes:

1. SetupAPI install date for a Windows based machine,
2. Volume GUID for a Windows based machine
3. Volume Label,
4. Volume Serial Number in both hex and decimal formats,
5. Device Classes date on a Windows based machine,
6. USBSTOR Explicit Property values for install date, last arrival date and last removal date for a Windows based machine,
7. NTUser Mountpoints2 UserID and Attach date values for a Windows based machine,

4) The report shall identify the particular data source from where it obtained each of the above report attributes.

4(b)(v) Windows Shellbag Reports

5) The NTUser report shall be a textual based report produced by Reg Ripper 2.8 or later or equivalent.

6) The UsrClass report shall be a tabular report produced by Shell Bag Explorer 7 or later or equivalent of folder activity of all devices accessed under the user profile.

4(c). Document Search

The EDEA shall search the contents of the preserved data using keyword search, hash search, file name and security identifiers. The keyword search engine shall be an index based search engine like DTSearch or equivalent. The specific search criteria for these methods, the keyword search terms, MD5 values, file names and security identifiers are provided in Exhibits 2 through 5 of this protocol.

4(c)(i) Search Preparations

Prior to conducting the searches, the data from the various storage devices and data sources shall be prepared as described below.

1. Non-searchable image file formats like PDF, JPEG, TIFF, etc. shall be converted to text searchable form.
2. Encrypted documents shall be identified and a list provided to the parties to identify which encrypted files should be decrypted so that they can be searched.
3. All text searchable formats including the converted text files shall be indexed for subsequent keyword searching.

4(c)(ii) Search Terms

The parties shall cooperate in the development of search terms designed to facilitate the identification of relevant documents in the most economical manner possible.

The parties may update the search terms for revisions to existing terms or even for entirely new terms as a result of actual performance of the search effort. Such revisions must be agreed to or resolved through the dispute resolution provision of this Protocol before being executed by the EDEA.

The producing party may include search terms that are designed to facilitate the identification and review of privileged documents that should be withheld or documents containing confidential information that should be protected.

4(c)(iii) Search Reports

For any files meeting the various search criteria for keywords, MD5 hash values, file name or security identifiers, the EDEA shall prepare a tabular style report listing the files and various attributes meeting those search criteria.

(1) The EDEA shall prepare a separate list of matching files for each search methodology.

(2) To the extent possible the lists shall contain the elements shown in the file list specification shown in Exhibit 1 to this protocol.

(3) The EDEA shall use the Label field of the file list to identify whether files in the list contained content related keywords or metadata keywords or both. The EDEA should use one type of semaphore code to represent content related keywords and a different semaphore code to represent metadata keywords.

(4) If the EDEA's search engine is unable to process all of the content related keywords or the metadata related keyword search terms in a single list the EDEA shall use unique semaphore codes for each keyword search list subset. The EDEA shall provide a schedule of its semaphore codes and the keyword search terms it represents.

(5) In addition to the file list, keyword search results shall also be reported in a contextual based report that in addition to identifying the file containing a hit and the exact search term, it will provide at least 100 characters either side of the search term in order to provide context about how the keyword was being used and determine whether the context is consistent with the document being sought.

4(d). Selection of ESI for Production

The parties will use the results from preprocessing reports and the various search reports set forth in subsections 4(b) and 4(c) to determine what data will be produced. The actual data production procedures are described in the next section.

4(e). Production of Analytical Reports and ESI

The following data formats and production steps shall be used for the production of any of the EDEA's output such as analytical reports or ESI from preserved devices, media or, accounts and selected for production.

4(e)(i) Produced Data Format

(a) Analytical and tabular reports like file lists, attached device lists, Windows event logs, browser history, Windows Shellbags, Windows Link files and jump lists, search hit lists shall be produced in Excel spreadsheets;

(b) Windows Registry reports and Apple System logs shall be produced in text format;

(c) Documents other than e-mail shall be produced in their original native format;

(d) E-mail messages shall be produced in single message format like MSG;

(e) Individual text messages shall be produced in PDF format;

(f) Compound documents like text messages and e-mails shall be produced with all parts (messages and attachments included; however, if an email message stands on its own the individual elements of the entire email chain do not have to be produced);

(g) Compound documents like compressed archives (zip files) do not need to be produced with all parts; rather, only those parts of interest can be produced by themselves;

(h) If data is produced on a DVD or hard drive the storage device shall be marked or otherwise identified with a unique identifier that can be used for tracking and referencing purposes

4(e)(ii) Production Steps

(i) All reports generated under sections 4(b) and 4(c) shall be provided to the producing party's counsel for review in order to conduct a privilege and confidentiality analysis prior to production to the receiving party's counsel;

(j) Producing party's counsel shall have the following time periods to conduct their review of reports from the EDEA, unless agreed otherwise by the parties.

(k) For Attached device lists, event logs, browser history of web page activity and Windows Shellbag reports set forth the in 4(b) producing party's counsel shall have 3 business days from date of receipt to return redacted reports or advise the EDEA of the redactions to be made to the reports.

(l) For file lists, browser history of file activity, link file and jump list, and registry reports set forth in 4(b) Producing party's counsel shall have 7 business days from the date of receipt to return redacted reports or advise the EDEA of the redactions to be made to the reports.

(m) For keyword search context reports set forth in 4(c) Producing party's counsel shall have 7 business days from date of receipt to return redacted reports or advise the EDEA of the redactions to be made to the reports.

(n) Producing party's counsel may request the EDEA provide the actual files for review to assist with the privilege and confidentiality review. Producing party's counsel shall have at least two business days after receipt of the actual file to provide feedback on the confidential or privileged nature of the document.

(o) Upon clearance by Producing party's counsel, the EDEA shall provide the redacted reports to Receiving party's counsel.

(p) Receiving party's counsel shall then designate which documents from the reports generated under subsection 4(c), document search, it will request for production. Receiving party's counsel will identify the requested documents

by highlighting the corresponding rows of documents from the report provided by the EDEA or by identifying the Item ID of the requested item.

(q) The EDEA shall produce native format versions of the documents requested by the Receiving party's counsel to Producing party's counsel for review as permitted by sections 6 and 7 of this protocol.

(r) Producing party's counsel shall use their best efforts to review, disposition, and produce cleared documents on a rolling basis.

(s) The Producing party's counsel shall advise the EDEA of the documents it is clearing for production through any sensible means such as highlighting the cleared documents on the file list spreadsheet or supplying the EDEA with the item numbers of the cleared documents.

(t) The EDEA shall then produce cleared documents by:

(i) Providing the documents in native file format to both the Producing and Receiving party's counsel along with an inventory file list of the documents being provided;

(ii) The accompanying inventory file list shall be in a delimited file format such as .DAT or Excel CSV.

(iii) The load file shall contain at least the following columnar attributes for each file produced:

1. Produced File Name and extension;
2. Item ID;
3. Original file name;
4. File extension;
5. File path on the original media;
6. Create date;
7. Modified date;
8. Access date;
9. Record date (NTFS file systems only)
10. MD5 Hash;
11. File type description determined from signature/header analysis;
12. Media Custodian name;
13. Any restrictions for privacy or confidentiality;

(iv) If any documents in the list include e-mails and attachments the inventory file list shall also include the following columnar attributes for each file produced:

1. E-mail date;

2. Produced file name in the event that it is different than the original file name as a result of suffixing or other measures designed to accomplish file name uniqueness that is required by the production media;
3. E-mail subject (the subject will be used as the original e-mail name unless another method is chosen);
4. Sender;
5. Message date (Sent date for sent messages and receipt date for received messages);
6. Recipient (large distribution lists of more than 15 recipients can be abbreviated in the inventory list);
7. CC (large distribution lists of more than 15 recipients can be abbreviated in the inventory list);
8. BCC (large distribution lists of more than 15 recipients can be abbreviated in the inventory list);
9. Attachment file name;
10. Message or attachment indicator;
11. E-mail message and attachment grouping indicator;
12. Privilege status; and
13. Restrictions;

(v) The media containing documents cleared for production shall segregate the produced files into folders representing the different media from which they were extracted;

(vi) The finally produced media will also be marked or otherwise identified with an unique identifier that can be used for tracking and referencing purposes; alternatively, the produced media may be sent electronically by the Producing party's counsel directly to Receiving party's counsel.

4(f). Other Processing and Production

The EDEA may not perform any analysis or work beyond what is set out in this protocol, absent explicit written agreement of the parties on the scope of the work and responsibility for costs. Although there is no limitation to what additional analyses could be requested by the parties the following are illustrative examples.

i) Examination of attached devices to determine whether they have been attached to other devices, any identifiers of those other devices like SIDs and whether the data on attached devices was subsequently shared or used after the device was last attached to a machine being examined.

ii) Parsing Windows UsnJrnl or Apple FSEvent logs to obtain additional information about particular file or folder changes.

iii) Analysis of a document's application metadata to determine ownership, history or other attributes.

iv) Analysis of overwritten files to identify the files that have overwritten them and the date and time at which they were overwritten.

v) Reports of files likely copied to attached storage devices based on correlation of file activity dates and times to dates and times when other storage devices were attached.

vi) Reports of files or folder contents on attached devices based on correlation of file list reports to shellbag folder reports of attached storage devices.

vii) Review, analysis and extraction of fragments from free space or slack space containing search hits.

viii) Decoding Windows deleted files paths with $Rxxxxxx folder names to determine the actual deleted folder name in the path.

ix) Analyses to determine the complete attachment history of attached storage devices to a machine being examined.

5) Device Cleaning

After considering any reports or documents produced under this protocol, the Receiving party's counsel shall advise the Producing party's counsel of any additional devices that need to be examined and potentially cleaned.

Producing party's counsel shall have 5 days to review the notification by the Receiving party's counsel of additional devices that need to be examined and potentially cleaned. Any additional work on these devices such as imaging, forensic analysis and data cleaning shall be covered by a different protocol unless the parties choose to amend this one.

The cleaning protocol shall follow the following guidelines:

a. Loose files shall be deleted in their entirety or if more economical their parent folder can be deleted in its entirety.

b. E-mails shall be deleted from their containers entirely (including any attachments) or if more economical e-mails to be saved can be rebuilt into new containers and the old e-mail container deleted in its entirety similar to loose files.

c. All browser cache and temporary internet file cache shall be deleted or "flushed" in its entirety.

d. All Windows Volume Shadow Copy shall be deleted or "flushed" in its entirety.

e. All free space shall be wiped using the following.

i. For Windows machines the Cipher utility, or equivalent, shall be used with the /W switch to wipe free space on a volume, for example where the C: is to be wiped the command line instruction would be "*Cypher /W:C:*"

ii. For Apple machines use the Apple Disk Utility feature or equivalent. After accessing the Apple Disk Utility, select the erase tab, then select the erase free space option.

6) Confidentiality

a) Either party may claim sensitive documents to be confidential and not for public disclosure. In addition, either party may further condition the release and distribution of produced documents to criteria such as attorney eyes only. Any party claiming such condition or restriction shall advise the other(s) of the specific document and their condition or restriction at any time prior to or at the time of production to the other party.

b) The EDEA is to keep all information confidential and is not to disclose any information to any party unless that information has been first cleared for release by the data owner.

c) The EDEA acknowledges that it may have access to confidential information or learn confidential information during the performance of this project. The EDEA agrees (i) to use such information only for the purposes of carrying out its work on this project; (ii) to use due care to prevent disclosure of any such information to any third party; and (iii) to disclose any such information only on a need-to-know basis in order to perform services under this project or as required by a subpoena or other legal action directing such disclosure.

7) Privilege

The parties shall use the following procedures to identify and remove privilege documents from disclosure.

a) The parties may choose to review for privilege those documents selected for production.
   i) Any redactions to lists or reports for privilege shall be limited to content that implicated the privilege and other identifying content shall remain active. The term "REDACTED" shall be substituted for the content deemed privileged.
   ii) The Producing Party's counsel shall advise the EDEA of its redactions to lists or reports. The EDEA shall update the lists and reports for the redactions and produce copies of the redacted lists and reports to both sides as described in the section of this protocol on Production of ESI.

b) If the parties wish to claim privilege for any requested document they shall prepare a privilege log indicating such and the basis for the claim. The Producing Party's counsel shall then provide that list to the Receiving Party's counsel and to the EDEA.
c) In the event of compound documents like e-mails or compressed archive files, only the document identified as privileged shall be excluded for privilege, unless agreed otherwise by the parties or only selected documents were requested for production.

d) If the basis for the claim involves privileged information contained only in substantive metadata which can be redacted, the Producing Party's counsel shall identify those documents accordingly.
e) Native format documents that can be produced with redaction shall be converted to an image format like PDF or TIFF and produced.
f) In the event of an inadvertent production of privileged information, the document should be immediately returned to the Producing Party's counsel and all copies held by the Receiving Party's counsel destroyed. The inadvertent production of privileged information shall not waive privilege.

8) Disputes

a) The parties shall cooperate to resolve all disputes arising from this protocol. In the event of a dispute, the respective parties involved shall arrange for a teleconference within three business days after the complaining party informs the other of a request to address the dispute.

b) The complaining party has the obligation to inform the EDEA of the dispute and confirm that the EDEA has received notification of the dispute. During the pendency of the dispute the EDEA shall continue with those items of the work that are not in dispute. If the EDEA has any questions regarding the items of the work covered by the dispute, he should bring those issues to the attention of the parties and the resolution procedures set forth in this section shall apply.

9) Costs

The cost of the EDEA will be evenly split by the parties unless stated otherwise in particular provisions of this protocol.

10) Completion

a) The EDEA shall retain all data until completion of the litigation. At the completion the EDEA shall destroy all data and provide destruction certificates to each of the parties.

b) The data deletion shall be accomplished by deleting data from active servers, wiping storage media like hard drives and overwriting backup tapes.

c) In addition, the EDEA shall return any equipment that it is holding such as computers, cellphones, etc.

11) Signatures

12. Exhibits

EXHIBIT 1 – File List Specification

F = Loose Files E = E-Mail T = Text Msg

File List Specification		
Field Name	**Description**	**List**
Name	File name	F,E
Item Number	A sequential identifier assigned to items in the "case" at the level of granularity selected for analysis of compound documents like compressed archives (zip files) and e-mail containers. So, if electronic media are processed individually, the item numbers will be unique only to the items on each media. On the other hand, if electronic media is processed in groups then the item number will be unique for all of the media in the group. Item numbers will only be assigned to items at the level of detail selected at the time of processing. For this project the EDEA should choose to process all devices simultaneously at least for the purpose of developing file lists and performing searches.	F,E
Parent ID	The Item # of the parent container. Contents of a zip file would reference the zip file itself. An attachment in an e-mail would reference the message. An e-mail message would reference the e-mail container (i.e. PST file).	F,E
Label	A field reserved for tagging list records	F,E
Extension	File extension	F,E
Bad Extension	T/F whether the file extension matches the file Type / Category in the adjoining column. The determination of whether the file extension is bad is based on an analysis of the file internals using header analysis. This determination is only provided in Level 2 File System Analysis or above.	F,E
File Type / Category	The identification of the file by type or category, such as Excel 2003, based on an evaluation of the file's internals and not just the file's extension.	F,E

File List Specification		
Field Name	**Description**	**List**
File Class	Broad category designation of data types such as file, directory, etc.	F,E
Created	On Windows based systems the create date is when the file was placed on the media. This may or may not equate to the date when the file was actually created. For Apple based systems the create date follows the file from media to media. So, the create date on Apple based systems is a better indicator of the file's actual create date.	F,E
Modified	The date when the file was last changed, although in older applications it can mean the date last saved regardless of whether any changes were made.	F,E
Accessed	The date when the file was last "accessed". Depending on the operating system this could mean opened and viewed or simply highlighted or even touched by an automated system like backup system or virus checker or backup system.	F
Record Date (NTFS)	The date when the file system record was last changed for a NTFS file system (Typically Windows).	F
MFT Record No (NTFS)	The unique identifier of the record on a NTFS file system (typically Windows). Since the MFT Record No is part of the file system for a NTFS formatted media, the MFT Record No is unique for that partition on the media only.	F
Physical Size	Actual size of the file in bytes.	F,E
Logical Size	Size in bytes reserved on the media for holding the file as presented in the file system.	F
Path	Location of the file expressed as the folder route to the file starting from the root folder of the volume. The name given to the media is also included as are the logical segments (partitions) of that media.	F,E
Deleted	T/F whether the item, including e-mails recovered from a container, is deleted or active.	F,E
From Recycle Bin	T/F whether the file was located in the Recycle Bin	F
Recycle Bin Original Name	If the file is currently residing in the Recycle Bin and can be recovered by the user this is the original name of the file before it was deleted and placed in the Recycle Bin.	F
Recycle Original Name	This is the name of the deleted file identified in a $I file.	F
Recycle Date	This is the deletion date of the deleted file identified in a $I file.	F

File List Specification		
Field Name	**Description**	**List**
Start Cluster	Starting cluster of the file on the media.	F
Start Sector	Starting sector of the file on the media.	F
MD5 Hash	A calculated value that is unique to files having those exact contents, at least within probabilities that are in the trillions of trillions of trillions. Thus, files with the same MD5 hash have a very high probability of being identical	F.E
Duplicate	Contains a value representing the instance that a file with its MD5 Hash was found within the collection of media that were subjected to processing.	F,E
From Free Space	T/F if the file is located in Free Space. A deleted file that still exists in free space will not be known unless data carving processes have been. Once the file has been retrieved and added to the file list the From Free Space indicator will be set to TRUE; otherwise, it is set to FALSE.	F
Carved	T/F whether the file has been recovered from free space or file slack based on a search through those areas for file headers.	F
Encrypted	T/F whether the file is likely encrypted or password protected based on an evaluation of the chaos in the file's contents as determined with an entropy test.	F,E
Indexed	T/F whether the file has been indexed and is ready for keyword searching.	F,E
Owner Name	Name of the file's Owner typically Windows systems	F
Owner SID	SID [Security Identifier] of the owner on typically a Windows system. The SID is an intelligently coded value that includes both the Machine or Domain ID as well as the individual user account ID on the Machine or Domain.	F
Actual File	T/F whether item is part of a file whose existence is identified in the media file system.	F
Compressed	T/F whether this item is a compressed archive like a ZIP file	F,E
Resident	T/F. If the file is small enough and can fit entirely within the NTFS file system record then it is "Resident" .	F
Graphic File	T/F whether the file is recognized as a graphical file type like JPEG, TIFF, BMP or others.	F.E
OCR Graphics	T/F whether graphic file has been subjected to Optical Character Recognition	F.E
Opened	T/F whether Internet downloads have been opened	F

File List Specification		
Field Name	**Description**	**List**
Container	T/F whether the file is a container (i.e. a ZIP file in the case of individual files or a PST file in the case of e-mail messages) holding other contents.	F,E
From Email	T/F whether the record is a recognized e-mail container like PST or the contents of a recognized e-mail container.	E
Email File	T/F whether this file is related to an e-mail. It could be the e-mail container such as the PST file or it could be an element within the e-mail container such as a folder or related to the e-mail itself like the message. It does not include attachments. Thus, attachments would have a "F" indicator.	E
Email Message	T/F whether this is the e-mail message.	E
Has Attachment	T/F whether the message has one or more attachments	E
Attachment Count	The number of attachments contained in an e-mail	E
Attachment (Is attachment)	T/F whether this item is an e-mail attachment	E
Missing Attachment	T/F whether the message is missing one or more attachments	E
Submit Time	Date and time when e-mail was submitted for transmission by the e-mail client	E
Delivery Time	If message is outgoing it is the date and time when the e-mail was sent. If message is incoming it is the date and time when e-mail was received.	E
Subject	Subject of e-mail	E
From	E-mail sender	E
To	E-mail recipient	E
CC	E-mail carbon copy recipient	E
BCC	E-mail blind carbon copy recipient	E
Unread	T/F whether the message has been read.	E
Unsent	T/F whether the message was not sent.	E
Internet Message ID	Message ID set in Outlook or Exchange by an e-mail client if configured to do so.	E
Conversation Topic	Typically the subject line of the message in Outlook or Exchange without prefixes for Reply (RE:) or Forward (FW:).	E
Conversation Index	A formatted and encoded hexadecimal string in Outlook or Exchange that can be used for ordering messages having the same conversation topic.	E

File List Specification		
Field Name	**Description**	**List**
Email Thread ID	Related e-mails may have a common thread ID. It is similar to Conversation Index in that it starts with a base value and then increments the suffix with each element in the chain, although this e-mail attribute is a Microsoft unique addition.	E
Author	Application metadata contained within some documents identifying the document's author.	F
Direction	Direction of text message whether incoming or outgoing	T
Deleted	T/F indicator whether the message was active or deleted and recovered from the message container.	T
Read Status	T/F indicator of whether the text had been read	T
Message Type	An indicator of the type of message such as SMS, MMS or iMSG	T
Folder	The folder such as inbox or outbox in which the message was found.	T
Remote Party	Identification by name and number the remote party	T
From	Identification by name and number of the party from whom the text is sent	T
To	Identification by name and number of the party to whom the text is sent	T
Time Stamp	The date and time stamp of the text transmission	T
Text	The content of the text message	T
Read Time	The date and time when the text was read if available	T
Delivered Time	The date and time when the text was delivered if available	T
Description		T
File Offset	The byte offset of the text message within the database file	T
Database Name	The database file in which the text message was found	T
Hash Value	Hash value of an widely used method such as MD5 or SHA-2	T

EXHIBIT 2 – List of File Names

File Name

EXHIBIT 3 – List of MD5 Hash Values

MD5 Hash Values

EXHIBIT 4 – Keyword Search Terms

Search Terms

EXHIBIT 5 – File Security Identifiers

Domain/Machine Identifier portion of Security ID

EXHIBIT 6 – Data Carving File Types

List of file types for data carving

State Bar of Georgia
INSTITUTE OF CONTINUING LEGAL EDUCATION

STATE BAR SERIES

Mediation/Settlement Of The Restrictive Covenant Case . . . An Interactive Panel Discussion

Presented By:

Terrence Lee Croft
JAMS/Croft ADR, Atlanta, GA

Charles A. Hawkins, II
The Hawkins Firm LLC, Atlanta, GA

David N. Schaeffer
Miles Mediation, Atlanta, GA

UNIQUE MEDIATION ISSUES IN RESTRICTIVE COVENANT CASES

David N. Schaeffer
Miles Mediation & Arbitration
6 Concourse Parkway
Atlanta GA 30328
678-320-9118
dschaeffer@milesmediation.com
dschaefferlawfirm@gmail.com

Introduction: There are an extraordinarily large number of moving parts and remedies in restrictive covenant cases and the settlement of such cases. The first issue is always whether injunctive relief is appropriate. That normally depends on whether the covenants are enforceable, which in turn may depend on when they were entered into. If before 2011, they will be subject to the old rules and if after early 2011, they will be subject to the new Restrictive Covenants Act, O.C.G.A § 13-8-1 et seq. ("New Act"), for which there is very little appellate guidance. That first issue is essentially a question of law, but the New Act is anything but clear and leaves open many interpretations. The second issue will always be whether the defendants violated the provisions and whether the defendant competing company induced those violations. That can be a complicated factual issue, especially when it comes to non-solicitation covenants. The third issue will be whether, if violations have occurred, damages can be proved. This is also a complicated issue, as proving lost profits and lost customers can be very difficult unless the customers are willing to participate as witnesses in the case. The mediation may also be quite different depending on whether the restrictive covenants are in conjunction with an individual employee or independent contractor leaving an employer or whether it is in the context of the seller of a business competing in violation of a non-compete provision. Different remedies may be considered depending on the context.

Many of the moving parts depend on when the mediation takes place. Generally, these cases are settled after temporary restraining orders or interlocutory injunctive relief are either granted or denied by the court handling the litigation. If the initial efforts on the part of the plaintiff to obtain injunctive relief fail, generally mediation will focus on contested enforceability of the covenants and any actual damages incurred because of their alleged violations. The plaintiff will have much less leverage if the court has not entered a TRO or interlocutory injunction. If the court orders an interlocutory injunction, the plaintiff has considerable leverage and will be hard pressed to give that up without a substantial payment, which in turn brings damage calculations into the mix.

It is critical for the neutral mediator to understand both the procedural, equitable, legal, and practical business issues involved and to be familiar with not only the New Act, but for older covenants, the old rules set forth by decades of case law. The mediator must also understand the difficulty in assessing and proving damages and the time and expense that doing so entails.

Injunctive Relief: Injunctive relief is the "hammer" in these types of cases. The Motion for TRO or the Motion for Interlocutory Injunction and the hearings and orders on those motions provide the parties with the first indicator of potential success in pursuing or defending the case. The threshold issue is whether the plaintiff is "reasonably likely to prevail on the merits," which depends on whether the Court thinks the underlying covenants are enforceable. Thus, the granting of a TRO or interlocutory injunction generally indicates (but does not necessarily assure) that the Court is inclined to hold that the covenants are enforceable. Likewise, the denial of a TRO or interlocutory injunction may be based on a decision by the Court that the covenants are not clearly enforceable, or the denial may be based on other unrelated factors such as a delay in seeking injunctive relief, laches, unclean hands, the absence of a showing of immediate harm, or other equitable factors. Deciphering the real reason behind the judge's thinking depends on how thorough the judge explains the basis for his or her decision in the order denying relief. But clearly, if an interlocutory injunction is entered, which most of the time will stay in place for the usual one or two-year duration of the restriction while the lawsuit winds its way though discovery, there will be significant incentive for the defendant(s) to settle the case in order to get back to work.

There are many ways to settle a case even if the Court has entered injunctive relief. The defendant may offer to accept a more limited injunction in return for the defendant not contesting the case. The defendant may agree not to compete if he or she is permitted to return to work for the plaintiff under new restrictive covenants. The defendant may offer some sum of money for the plaintiff to lift or modify the injunction and dismiss the case. The defendant may agree not to solicit a limited, concrete list of the customers the plaintiff may be most concerned about or to not try to recruit specific employees in return for the plaintiff not enforcing a broader injunction. Or the defendant may agree to stay out of his or her primary former territory if allowed to compete in less important territories potentially covered by the injunction. Or the defendant's new competing employer may agree to restrict the ex-employee from competing in certain territories or soliciting or handling specific customers' business.

In short, injunctions are a powerful leveraging agent for the plaintiff, but they can be modified by the parties through negotiation and settlement designed to protect the plaintiff from the most egregious damage while allowing the defendant to continue to earn a living. Because of the expense of discovery and pursuing the cases all the way to a jury trial on damages, there is almost always some flexibility on the part of the plaintiff even if it has been successful in obtaining injunctive relief.

Enforceability of the Covenants: This is always going to be an issue in the mediation even if the Court has issued an injunction. The defendant always has the threat of an appeal to overturn the injunctive relief or may be successful in convincing the Court to allow it to file a counterclaim for wrongful injunction, thereby exposing the plaintiff to possible damages if it were to lose on appeal. The defendant will almost always argue that it expects to win the case at the summary judgment phase with some combination of the covenants not being enforceable, the covenants not being violated even if enforceable, or there being no provable damages.

The mediator will need to be familiar enough about the New Act to understand the possible open issues that may affect the enforceability of the covenants. Are the covenants reasonable in time, geographic area,a nd scope of prohibited activities as required by O.C.G.A. § 13-8-53? Is the defendant one of the persons to whom post-employment non-competes now apply under O.C.G.A. § 13-8-53, i.e. is the person a sales person, a key employee, a professional, as defined in the statute (See O.C.G.A. § 13-8-51(5),(8) and (14)? Are the definitions too vague to come to any definitive conclusion on that issue? What constitutes "material contact" for purposes of non-solicitation clauses? Are specific geographic restrictions still required for non-solicitation covenants? Are the covenants, if overly broad, able to be blue-penciled or otherwise modified by the Court under O.C.G.A. § 13-8-54 (b)? What about "economic hardship" as a defense to the restrictive covenant under O.C.G.A. § 13-8-58(d)? Should that play a role in the mediation? What evidence would constitute "economic hardship"?

The biggest problem here is that even after seven years, there are almost no appellate decisions to provide guidance on these issues. However, that lack of clarity is a primary motivator for the parties to settle in mediation. With uncertainty comes flexibility and compromise. The experienced mediator will always use uncertainty as an essential tool to move the parties towards each other to reach a solution with which both sides can live.

Disputes Over Whether The Covenants Have Been Violated: Generally, if the restriction is a non-compete covenant with a clear territorial limitation or a specific list of customers with whom the ex-employee may not compete, proof of a violation can be definitively proved by paper discovery, even though actually getting that discovery is often delayed by requests for protective orders and evasive responses or objections to interrogatories and document requests. Sometimes the defendant may do things indirectly and hide the paper trail by paving the way for other persons to deal with the customer in the territory and thus not being the official salesperson on the defendant competing company's records. However, with patience and, if necessary, motions to compel, proof can be obtained.

If the covenant is a non-solicitation clause, proof is much harder. Did the defendant solicit or just accept business from the customer? Who solicited whom? Did the customer leave the plaintiff for other reasons unrelated to the defendant? If the customer's representative or agent who was solicited by the defendant is willing to testify and be involved, then proof is obtainable. However, plaintiffs are usually reluctant to involve the customers for fear that they will just take their business elsewhere. In some instances, the customers may not like being restricted from choosing the salesperson with whom they have placed their trust for many years and may not want to support enforcement of the restrictive covenant.

E-discovery is essential in these cases to nail down what contact information the defendant took on cell phones or other digital platforms, who the defendant called and when, whether there were any prior calls initiated from the customer, etc. Once again, that type of discovery is expensive and time-consuming and may not be available when the parties want to mediate the case.

The mediator will need to be attuned to these issues and the discovery disputes that may arise in order to seek or block this proof. If the negotiations depend on fully knowing the results of this type of discovery, then the mediation may need to be postponed and resumed at a later time following the completion of discovery.

Damages: Once again, the New Act is vague on damages as a remedy. It merely says that: "A court shall enforce a restrictive covenant by any appropriate and effective remedy available at law or at equity, including, but not limited to, temporary and permanent injunctions." O.C.G.A. § 13-8-58(c). Presumably, that would include lost profits from sales or customers taken by the competing conduct. But would it also include disgorgement of revenues or profits received by the violator of the covenants or the company he or she now works for? Disgorgement is a remedy recognized under Georgia law in other contexts such as trade secret misappropriation or usurpation of business by a disloyal servant, so under the broad language of O.C.G.A. § 13-8-58(c), such a remedy would seem to be allowed. But there are no appellate decisions to guide us.

Proof of damages is difficult in these cases. There are many variables which could affect the level of business from a customer or in a geographical area which may not be related to the violation of the restrictive covenants. It is easier to show the business obtained by the defendant for a competitor than it is to show that the plaintiff has lost its business from that customer, especially if the customer has not entirely switched all its business to the competitor who has hired the former employee. If the only covenant is a non-solicitation of customers provision, then in addition to losing the business, the plaintiff has to prove solicitation by the ex-employee caused that loss of business, as opposed to the customer merely switching the business for other reasons or through its own decision without solicitation from the former employee. Effective e-discovery may help with this proof, and, in some cases, I have found direct evidence of solicitation through emails and texts, to bolster the circumstantial evidence based solely on the timing to the switched business.

However, if large sums are demanded in mediation, the plaintiff should be prepared to provide definitive proof of the amount of damages for each customer affected or taken entirely and lost profits as to the ex-employee's specific territory. Otherwise, the damages will be speculative and a persuasive argument for a large recovery or settlement will be missing from the negotiations. In my experience, this is a huge problem where the parties attempt an early mediation shortly after the initial injunction hearings. The discovery necessary to prove the damages has not been done, would be expensive to do if it were to be done, and may or may not provide the evidence sought without taking the risk of involving the actual customers.

Settlement will always be easier if the competing company who has induced the breaches is included in the litigation. Most of the time, unless the individual defendant is a professional with substantial resources, the defendant will plead poverty and inability to pay any significant amount of damages. However, payment plans can sometimes be worked out, usually in combination with some specific restrictions as to specific territories or customers.

Conclusion: Because to the uncertainties regarding enforcement of the restrictive covenants under the New Act and the difficulty in proving damages without a large expenditure of time and e-discovery costs, mediation of these cases frequently defaults to an evaluation of the costs of litigation and the business disruption caused by the litigation and discovery process. If violations are clear, defendant competitors who have hired an ex-employee and placed them in the restricted territory, may essentially buy their peace for a reasonable sum, or agree to keep that employee out of that territory for a certain period in order to settle the suit and avoid litigation costs. Plaintiffs must also factor in the uncertainties of a result, the speculative nature of their damages, the risk of involving customers in the litigation and therefore the risk of losing the customers completely, and then make a business decision as to how far to push the injunctive relief and the damages demands. Sometimes, just the fact that the Plaintiff has filed suit, obtained injunctive relief, and the defendant ex-employee has suffered a restriction on his or her ability to make a living for many months or up to two years, can work as a serious disincentive for other employees to leave and compete in the future. Such a chilling of similar conduct by other employees may be the best remedy of all for the future of the business. A seasoned mediator with knowledge of all these factors can help the parties think through all the possibilities and risks and hopefully come to a solution that both parties can accept.

Appendix

ICLE BOARD

Name	Position	Term Expires
Carol V. Clark	Member	2019
Harold T. Daniel, Jr.	Member	2019
Laverne Lewis Gaskins	Member	2021
Allegra J. Lawrence	Member	2019
C. James McCallar, Jr.	Member	2021
Jennifer Campbell Mock	Member	2020
Brian DeVoe Rogers	Member	2019
Kenneth L. Shigley	Member	2020
A. James Elliott	Emory University	2019
Buddy M. Mears	John Marshall	2019
Daisy Hurst Floyd	Mercer University	2019
Cassady Vaughn Brewer	Georgia State University	2019
Carol Ellis Morgan	University of Georgia	2019
Hon. John J. Ellington	Liaison	2019
Jeffrey Reese Davis	Staff Liaison	2019
Tangela Sarita King	Staff Liaison	2019

GEORGIA MANDATORY CLE FACT SHEET

Every "active" attorney in Georgia must attend 12 "approved" CLE hours of instruction annually, with one of the CLE hours being in the area of legal ethics and one of the CLE hours being in the area of professionalism. Furthermore, any attorney who appears as sole or lead counsel in the Superior or State Courts of Georgia in any contested civil case or in the trial of a criminal case in 1990 or in any subsequent calendar year, must complete for such year a minimum of three hours of continuing legal education activity in the area of trial practice. These trial practice hours are included in, and not in addition to, the 12 hour requirement. ICLE is an "accredited" provider of "approved" CLE instruction.

Excess creditable CLE hours (i.e., over 12) earned in one CY may be carried over into the next succeeding CY. Excess ethics and professionalism credits may be carried over for two years. Excess trial practice hours may be carried over for one year.

A portion of your ICLE name tag is your **ATTENDANCE CONFIRMATION** which indicates the program name, date, amount paid, CLE hours (including ethics, professionalism and trial practice, if any) and should be retained for your personal CLE and tax records. **DO NOT SEND THIS CARD TO THE COMMISSION!**

ICLE will electronically transmit computerized CLE attendance records directly into the Official State Bar Membership computer records for recording on the attendee's Bar record. **Attendees at ICLE programs need do nothing more as their attendance will be recorded in their Bar record.**

Should you need CLE credit in a state other than Georgia, please inquire as to the procedure at the registration desk. ICLE does not guarantee credit in any state other than Georgia.

If you have any questions concerning attendance credit at ICLE seminars, please call:
678-529-6688

State Bar of Georgia

INSTITUTE OF CONTINUING LEGAL EDUCATION

/ICLEGA

#ICLEGA
#TUESAT2

/ICLELINKEDIN

ICLEGA.ORG