Who's There? What to Do When the Government Is Knocking on Your Door —

An Employer's Guide to Handling Government Visits and Information Requests

2007–2008

Philip L. Gordon
James E. Hart
Kerry L. Middleton
Ronald A. Peters
John C. Kloosterman
Bonnie K. Gibson
Steven R. McCown
Alison J. Gates
Katherine Dix
Jason M. Gerrol
Lisa A. Cottle

LITTLER MENDELSON, P.C.
THE NATIONAL EMPLOYMENT & LABOR LAW FIRM®

IMPORTANT NOTICE

This publication is not a do-it-yourself guide to resolving employment disputes or handling employment litigation. Nonetheless, employers involved in ongoing disputes and litigation will find the information extremely useful in understanding the issues raised and their legal context. This Littler Report is not a substitute for experienced legal counsel and does not provide legal advice or attempt to address the numerous factual issues that inevitably arise in any employment-related dispute.

Copyright © 2007 Littler Mendelson, P.C.
All material contained within this publication
is protected by copyright law and may not
be reproduced without the express written
consent of Littler Mendelson.

Table of Contents

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

Who's There? What to Do When the Government Is Knocking on Your Door — An Employer's Guide to Handling Government Visits and Information Requests

I. Introduction: What to Do When Law Enforcement Is Investigating a Crime at Your Workplace*

A. Introduction[1]

Requests for information from law enforcement can place a corporation in a delicate situation, requiring it to consider and balance several interests — interests that are sometimes competing. A corporation may potentially need to consider and safeguard its own interests as well as the interests of the employee in question, other employees, its customers and the public. Consider the following examples:

- Police knock on the door of a limousine service company and want to obtain electronic data about a company car that was involved in a fatal accident, as well as work schedules of the driver.
- A door-to-door salesman is accused of assaulting a potential customer, and the police contact the company and want to obtain a pre-employment criminal background check conducted by the company, work schedules of the employee, and phone records of the employee's company-issued phone.
- An individual is accused of "date rape" while the individual is off-duty and police contact the individual's employer and ask for his emails sent over the company server for the past three months.

Depending on the facts, the first two scenarios could potentially expose the company to criminal[2] or civil liability for the underlying act of its employee. The second and third scenarios could alert the company that one of its employees poses a risk to fellow employees or customers. The third situation could implicate privacy interests of the employee in question, other employees, customers as well as trade secret or similar issues.

A company must be ready to respond quickly if necessary. The focus of this Report is to provide employers with information as to what to do when different governmental or law enforcement agencies approach the employer for information, documents and/or cooperation with an investigation or when law enforcement appears to be investigating the company for potential illegal acts. The following are some steps that can assist a company in preparing for such a situation. The remainder of this Report will focus on various specific situations that may arise and provide detailed responses for use by the employer in similar situations.

B. What an Employer Can Do Now: Implement Safeguards Before the Situation Arises

Implement Applicable Policies.

An employer would be prudent to devise and implement policies before an issue arises. If police are ever to arrive at a company's door, there may be little if any time to respond. The potential for making a bad decision will dramatically increase if decisions have to be made on the spot. With that in mind, policies and procedures should be well-established before hand.

A company may potentially subject itself to criminal or civil liability from law enforcement and employees depending on the action it takes. On the one hand, a company has the duty to protect the private information of its employees.[3] Improperly turning over personal documents of its employees can — under certain circumstances — subject companies to various civil claims, such as invasion of privacy, defamation,[4] or negligence. On the other hand, law enforcement agencies encourage and expect

---

* This section of the Littler Report was prepared by Jim Hart, a shareholder in Littler Mendelson's Orange County, California office. Prior to joining Littler, Mr. Hart practiced criminal law as a Deputy Attorney General in the California Attorney General's Office.

1 **Cautionary note** — This Report focuses on actions that should be taken by *private* employers in response to an inquiry by law enforcement. The duties of public employers and the rights that must be afforded to a public employee by public employers may vary from the duties of private employers. See *O'Connor v. Ortego*, 480 U.S. 709 (1987). Similarly, this Report focuses on responses to *violent* crimes, which may entail different considerations than for nonviolent crimes. Different agencies such as the law enforcement division of the Securities and Exchange Commission (SEC) will operate pursuant to different policies that may require a different level of cooperation from employers. For further information on investigations by the SEC, see section IV of this Report. *See also* Marvin Pickholz and Jason Pickholz, *Investigations Put Employees In Tough Spot*, 236 N.Y.L.J. 15 (July 24, 2006) (noting that the SEC asks companies to waive attorney-client privileges to take advantage of cooperation credit).

2 According to the Department of Justice's memorandum on bringing claims against corporations:

> Corporations are "legal persons," capable of suing and being sued, and capable of committing crimes. Under the doctrine of *respondeat superior*, a corporation may be held criminally liable for the illegal acts of its directors, officers, employees, and agents. To be held liable for these actions, the government must establish that the corporate agent's actions (i) were within the scope of his duties; and (ii) were intended, at least in part, to benefit the corporation. In all cases involving wrongdoing by corporate agents, prosecutors should consider the corporation, as well as the responsible individuals, as potential criminal targets. Memorandum, Dep't of Justice, *Bringing Criminal Charges Against Corporations* (June 16, 1999), *available at* http://www.usdoj.gov/criminal/fraud/policy/Chargingcorps.html.

3 *See*, *e.g.*, CAL. CONST., art. 1, § 1.

4 *Starr v. Peale Vision, Inc.*, 54 F.3d 1548, 1555-58 (10th Cir. 1995) (while slanderous statements about criminal activity did not support employer defamation liability under Oklahoma law, forwarding such comments to outsiders could support a defamation claim). Please also note that although defamation claims are a legitimate concern, there may also be viable defenses to documents handed over in the course of an investigation. See, *e.g.*, CAL. CIVIL CODE § 47 (affording privilege to publication of information in a judicial or other official proceeding).

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

a certain level of cooperation, and if the company is subject to an investigation, cooperation can largely affect a future decision to prosecute and the ultimate legal sanction that is handed down.

As one way to deal with these competing interests, companies may want to implement a policy requiring a search warrant or subpoena before employment records are turned over. This requirement will both help deter law enforcement agencies from conducting a fishing expedition through company records and protect employers from future suits by angry employees. In some states, a subpoena may not only be advisable, but may be mandatory. For example, Connecticut, has strict laws prohibiting the release of personnel files absent an employee's consent, a search warrant or a subpoena.[5] Other jurisdictions, have procedures requiring that documents be reviewed for privacy or privilege issues before they can be disclosed to others. For example, California criminal subpoena rules require that documents be delivered directly to a court, and permit a court to conduct an *in camera* review for privacy issues before the documents are released to the parties.[6] Police may also be looking for information that is afforded special protection under the law. For example, an employee under investigation could argue that a background check gathered pursuant to the Fair Credit Reporting Act (FCRA) only permits an employer to receive such a report, but not to further disclose the report to a third party such as law enforcement.

However, as discussed below, a company should take care to assist law enforcement where possible. Having copies of requested documents ready upon receipt of a subpoena and working with the police on timing and other convenience issues can ease ill feelings with law enforcement. In addition, full and helpful cooperation with agencies such as the Department of Justice, FBI or the federal prosecutors is extremely important as prosecutors will assess the company's degree of cooperation when the time comes to decide whether or not to prosecute the company. The degree of cooperation by a company is also assessed at the sentencing phase or criminal indictment and full cooperation could result in a lesser fine in the criminal sentencing.[7]

Designate & Train Employees Who Will Be Required to Respond to Law Enforcement Requests.

To adequately implement policies, an employer should consider what areas of the business may be affected by law enforcement investigations. Requests for information from police may require the involvement of an on-site person to communicate with the police. Requests for information from police may also require involvement of human resources, legal counsel, security or information technology professionals. The employer should designate specific individuals within each of the potentially targeted business units to serve as a liaison between law enforcement and the members of the organization who will need to help develop a response and collect relevant information. Having a single point of contact will avoid the potential for frustration on the part of law enforcement who may feel as though they are being shunted around an organization or who receive inconsistent responses from different company representatives.

Develop Contacts with Police.

Developing a contact with local law enforcement at the municipal or county, state and federal level also is a good proactive step that can be taken by a company. Corporate participation in local police activities is not only part of being a good corporate citizen but can be very helpful if the company ever has to interact with the police or other law enforcement agencies. Police contacts may be willing to alert the company before documents are officially sought or may be willing to answer questions about a request for company documents.[8]

C. How to Respond

First Gather Facts Necessary to Make an Informed Decision.

A decision is only as good as the information that informs it. Time permitting, the person tasked with working with the law enforcement agency should be prepared to gather information that will be necessary to make informed decisions on how best to proceed. Basic questions can get this job done: who, what, when, where and why.

Who —

Who is knocking at the door? Ask for identification. There are various law enforcement agencies that may be involved. Is it the sheriff, a local police officer, the district attorney's office, the city attorney's office, the FBI, U.S. Marshall, the Department of Homeland Security, an Alcohol, Tobacco and Firearms agent or a representative from some other agency? These agencies operate in different geographic areas, enforce different laws, and maintain different internal policies and operating cultures.

---

5 Conn. Gen. Stat. § 31-128f.

6 See, *e.g.*, Cal. Penal Code §§ 1326-1327 ("When a defendant has issued a subpoena to a person or entity that is not a party for the production of books, papers, documents, or records, or copies thereof, the court may order an *in camera* hearing to determine whether or not the defense is entitled to receive the documents.").

7 See Department of Labor, *McNulty Memo*, *available at* http://www.usdoj.gov/dag/speech/2006/mcnulty_memo.pdf and the Federal Sentencing Guidelines, *available at* http://www.ussc.gov/guidelin.htm .

8 Please note that there is a big difference between how state and federal law enforcement agencies operate, and their individual willingness to disclose information about the target of an investigation can vary greatly.

Who is the target of the investigation? Find out who is the target of the investigation: the company, an employee, a client. You may not always be told but it is worth asking. It is also important to know this as there may be competing interests between the company and the individuals being investigated. The retention of more than one attorney may be necessary.

Who is the victim? If the victim is an employee or customer, the company will want to put certain measures, such as a restraining order, in place to protect the employee or customer from any further harm.

What —

What is the scope of the law enforcement's or agency's authority (*i.e.* does the law enforcement agency have a search warrant or subpoena)? The reaction of a company to an inquiry will be different depending on whether or not the law enforcement agency is armed with a search warrant, an arrest warrant, or a subpoena. If the police have a search warrant, then the company will have little choice but to provide access to the area to be searched. If the company is served with a subpoena *duces tecum*,[9] the employer may be required to send the documents directly to court and may face potential liability for handing the information over to police or some other agency.

What is the stage of the investigation? How a company reacts will depend in large part on the stage of the investigation. If the investigation is pursuant to a charge filed against an employee, the employer may need to respond to the police and decide on how to deal with the employee. By contrast, if there is no case and police are simply following up before closing an investigation, then a different posture towards an employee may be warranted.

When -

When must the company comply? If the law enforcement agency is armed with a search warrant, a company will likely have to comply with the demand immediately. Similarly if the situation is an emergency — where the threat of physical harm or immediate destruction of evidence is involved — the law enforcement agency may be justified in conducting an immediate search of an employer's premises for records without any warrant.

Alternatively, if the police are armed with a subpoena, then the company may have a certain period of time to respond. If the police do not have a subpoena but only a request, then the company may be able to refuse the request absent a search warrant or subpoena, limit the request or negotiate a timeline to comply with the request so as to minimize any disruption to the workplace.

Where -

Where do the police want to search? Whether or not the police need a search warrant or whether or not the company can consent to a search will depend on the location to be searched. Courts have held that police do NOT need any warrant to search trash.[10] As a result, a company may not be able to insist on a warrant if a law enforcement agency is rifling through the trash for certain records. If police want to search a private car, handbag, wallet, etc. contained on company property, the company may not be able to consent on behalf of the employee.[11] In the unlikely event that police want to search for documents contained in portions of the commercial building open to the public, then the police similarly may not need to obtain a warrant.[12]

Where must the company comply? The law enforcement agency may permit the company to copy documents and forward them. As stated, if the law enforcement agency serves a subpoena *duces tecum*, then the employer may only be required to produce certain documents in court and the law enforcement agency may not be permitted to actively search the premises.[13]

Why —

Why are these records necessary? A company may not receive any response to this question. Nevertheless, the question is worth asking.

If There Is a Search Warrant or Subpoena, Read It & Follow It.

If there is a search warrant or subpoena, read it. A company should be cognizant of the limits of the warrant. A company should be aware of which specific areas are subject to search, when the area is subject to a search, which items are subject to seizure and who may conduct the search and seizure. For example, if there is a search warrant for a specific area, the law enforcement agency must confine its search to that area, unless the company consents to a larger search. A search warrant does not mean that employees can be questioned. On the other hand, if the agency has an arrest

9 A *subpoena duces tecum* is a writ directing a person to appear in court and bring documents described in the writ.

10 *California v. Greenwood*, 486 U.S. 35, 39-41 (1988).

11 *Mancusi v. DeForte*, 392 U.S. 364, 369-72 (1968) (subpoena *duces tecum* calling for union to produce books did not permit the warrantless search of private property absent consent); *see also People v. Thompson*, 205 Cal. App. 3d 1503 (1988) (finding that employee had reasonable expectation of privacy in countertop drawer, back storeroom, desk or closet where he or she stores personal property, but did not have any privacy expectation in the floor beneath the counter).

12 *Marshall v. Barlow's Inc.*, 436 U.S. 307, 311 (1978).

13 See *Carlson v. Superior Court*, 58 Cal. App. 3d 13, 22-23 (1976).

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

warrant, that does not mean that the officers can search for documents.[14] If a subpoena *duces tecum* requires that documents be delivered directly to a court, the company should not hand the documents over to a law enforcement agency who may only be charged with serving the document on the company.

A company should not only read the subpoena or warrant to determine how to comply with its terms, but should also review the document for any defects. A search warrant may be defective if the wrong address is listed or if the time within which the warrant could be served has expired. If a search warrant has expired (*i.e.* the time to conduct the search has lapsed), a company representative should alert police of this fact. While the police may insist on executing the warrant regardless of any defect, the company should make a record of its efforts to object.

Safeguard the Materials If Not Immediately Produced.

If there is no warrant, and no immediate search will occur, a company should secure the area that will be subject to a search or the documents subject to production. If, for example, the company insists on a warrant where there is none, the police will have to secure a warrant, which will create lag time between the initial contact and the ultimate search/production. In the meantime, the company should take care to safeguard the information they believe will ultimately be part of the search/production.

Actively destroying documents, or permitting their destruction, can expose the company to criminal charges. Once the company is on notice that the law enforcement agency is seeking information in connection with a criminal investigation, the company can conceivably be subjected to an obstruction of justice charge by intentionally destroying information sought.[15] The case of Arthur Anderson is a high profile example. The company was charged with obstruction of justice after destroying literally tons of Enron documents related to the company's misdeeds. In-house counsel and Human Resources need to direct the parties involved (including all involved employees) not to delete, tamper or remove documents. Communication at this stage is critical. If the organization already has developed a process for implementing a "litigation hold" in response to actual or threatened civil litigation, that process should be similarly followed in connection with a criminal proceeding. If the organization has not yet developed such a process, then the person responsible for the organization should, at a minimum, identify the "key players" (*i.e.*, the employees most likely to possess responsive information), and send those individuals a memorandum describing the categories of documents that need to be preserved and the steps that should be taken to preserve them. The organization may need to involved IT professionals to ensure that electronically stored information is properly preserved.

Minimize Disruption to the Workplace.

When police ask for information, those tasked with managing the process should take care to minimize disruption to the business. A company may want to consider whether it is possible to arrange for a search or transfer of documents to take place after hours or away from employees. If copies of documents can be provided to police rather than original documents, a company should consider this option, especially if the documents are necessary to the smooth operation of the business. However, law enforcement often will be seeking originals, like a hard drive from a laptop and a copy will not suffice for evidentiary purposes (unless the copy is a mirror image created by an expert in computer forensics following approved protocols and using appropriate technology).

Be Courteous and Cooperative Without Becoming an Agent of the Police.

It is important not to be a hindrance to law enforcement's investigation but company personnel should not be so involved in the investigation that they could be considered agents of the police.

D. Determine Whether an Independent Investigation by the Company Is Required & Whether Any Action Is Necessary to Protect Employees.

An employer has a duty to protect its employees. Obtaining knowledge of a police investigation of a violent crime may put a company on notice to take steps to safeguard other employees. One common response to a known physical danger posed to employees is to obtain a restraining order against the person that poses the threat.

Notice of a police investigation may also provide grounds to terminate the employee that is subject to the investigation. A company may not have the luxury of waiting to see the results of a police investigation and may have to commence its own investigation to determine whether employment action is

14 *Steagald v. United States*, 451 U.S. 204, 211-12 (1981).
15 See 18 U.S.C. §§ 1501-1517

warranted. Sometimes this is difficult as the police have taken the evidence, (*e.g.* the laptop's hard drive) and companies must be creative in the investigation without spoiling or losing any documents or property relevant to the police investigation.

At the same time, employers need to take care that their own investigation does not compromise the law enforcement investigation. The employer will need to determine whether to confer with law enforcement before commencing an investigation. If it appears that the internal investigation could "tip off" the target of a criminal investigation, or otherwise interfere with that investigation, the employer may need to postpone its own investigation but could take other steps, such as informing security personnel to be diligent with respect to a particular employee, to protect the organization from liability and other employees from possible harm.

E. Checklist for Responding to Inquiries for Information from Police

The following is a checklist of the steps an employer can take when the police come knocking on the door:

- ❒ **Advanced preparations.**
  - ❒ Devise and implement policies that explain under what circumstances employee records can be released to the law enforcement agencies or investigating governmental agencies.
  - ❒ Designate and train relevant employees who will respond to the law enforcement agencies' inquiries (*e.g.* from the human resources department, the security, the legal department, or IT).
- ❒ **Responding to the Inquiry.**
  - ❒ Ascertain the identity of the law enforcement agency and confirm that the involved law enforcement officials are authorized to act on the agency's behalf.
  - ❒ Request the purpose of the investigation.
  - ❒ *If there is a search warrant or subpoena* — read the document and comply with its terms. A company may be required to take different action depending on whether the document is a search warrant, an arrest warrant or a subpoena. Pay close attention to:
    - Who is entitled to conduct a search or seizure;
    - When the search can take place;
    - To whom the documents must be delivered (if the document is a subpoena *duces tecum*, a company may be required to deliver documents directly to the court rather than handing documents over to the law enforcement agency);
    - What is subject to search or seizure; and
    - Follow law enforcement or agents conducting the search to monitor what is searched and taken but do not get in the way or unnecessarily interfere.
  - ❒ *If there is no search warrant or subpoena* —
    - Consult company policies on whether to insist on a search warrant or subpoena.
    - If there are no company policies requiring a search warrant or subpoena, consider whether the request implicates company trade secrets, confidential business information or the privacy rights of its employees, customers or other third parties. If so, then courteously request a subpoena or search warrant. If more time is needed to consider these issues attempt to negotiate more time for that purpose.
  - ❒ When possible, cooperate with the law enforcement agency on convenience issues.
  - ❒ When possible, minimize the interruption to the workplace by, for example, permitting a search to occur before or after working hours.
  - ❒ Preserve other relevant information/documents that may be subjected to future requests.
- ❒ **Following up.**
  - ❒ Depending on the nature of the investigation, determine whether an internal investigation is needed, what to do with the subject of the investigation, and what to do to ensure the safety of other employees and customers.
  - ❒ Follow up with the law enforcement agency to see the conclusion of the investigation.

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

II. Police Knock on Your Door Investigating Identity Theft*

The Federal Trade Commission calls identity theft the fastest growing crime in America today. Not only does it cost American businesses and consumers a reported $50 billion a year, it also causes untold headaches for an estimated 10 million U.S. victims annually. Congress and state legislatures have enacted various laws to combat the increasing problems of identity theft. For example, the federal Identity Theft and Assumption Deterrence Act of 1998[16] and the federal Identity Theft Penalty Enhancement Act[17] prescribe criminal penalties for identity theft. Recently enacted state laws impose significant duties on organizations that collect sensitive personal information, such as social security numbers.

These laws place an employer in a precarious situation. Companies must balance various competing interests when it comes to a law enforcement investigation into identity theft. On one hand, the employer has a strong incentive to cooperate with the police who conduct investigations about identity theft, not only to be good corporate citizens but also because the police are the ones who apprehend the identity thieves and protect the employer from being subject to further identity crimes. On the other hand, there are important privacy interests at stake in the workplace. As noted above, statutes and regulations may limit the circumstances under which an employer can lawfully disclose information about an employee to law enforcement and employees enjoy common law protections against malicious prosecution and defamation.

Therefore, improperly turning over personal information of its employees can, under certain circumstances, subject the employer to various civil liabilities. Although there are not many reported cases that have resulted in an employer paying damages to employees victimized by identity theft, the legal underpinnings for such claims already appear to be in place. Claims can be asserted for invasion of privacy, negligent hiring, negligent retention and supervision, negligence, unreasonable disclosure of private facts, and defamation.[18]

A balanced approach can be achieved if the employer is armed with sufficient information about the investigating agency's authority and the potential risks to employees, customers or other third parties. The following discussion focuses on four aspects that will assist the employer in responding to the police's investigations. Section A discusses what is *identity theft* and what constitutes *identity information*. Section B deals with the privacy concerns for the employees when the police seek the employees' information. Finally, Section C suggests how the employer should respond. Lastly, there are additional steps employers need to take to follow up.

A. What Is Identity Theft?

Identity theft occurs when someone uses another person's personal identifying information without permission to commit fraud or other crimes. *Personal identifying information* include: name, social security number, date of birth, driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number, unique biometric data such as fingerprint, voice print, retina or iris image, unique electronic identification number, address, routing code, telecommunicating identifying information or access device, bank account number, and credit card number.[19]

Identity thieves may obtain personally identifying information by various means. They rummage through trash cans in search for a bank statement or a medical bill. They also steal credit cards. Because the employer routinely collects basic identifying information for each employee, the employer's database is under increasing attack from identity thieves. According to a survey conducted by the Federal Trade Commission, 14% of the respondents to the survey stated that they were victims of identity theft perpetrated by a family member or a work-place associate.[20]

B. What Privacy Concerns Are Implicated if the Employer Turns Over Sensitive Employee Documents to Law Enforcement?

Employees may have a reasonable expectation of privacy in certain parts of the workplace, such as bathroom, locker rooms, and offices that can be locked and/or shielded from the view of others, unless the employer has given reasonable notice that no such expectation exists because those areas will be viewed, inspected, or monitored in some way.

---

* This section of the Littler Report was prepared by Jim Hart, a shareholder in Littler Mendelson's Orange County, California office.

16 18 U.S.C. §§ 1028 *et seq.*

17 *Id.*

18 While these claims are legitimate concerns, there may also be viable defenses. For example, for defamation, California Civil Code § 47 provides a defense.

19 18 U.S.C. § 1028.

20 *Identity Theft Survey Report*, Federal Trade Comm'n, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html.

When police seek documents related to identity theft, the employer should be aware that different levels of protection and procedural safeguards can attach depending on the specific type of information sought and the geographic location of the search. Some states have implemented strong protections for all personnel documents. For example, Connecticut state law prohibits the release of personnel files absent a search warrant, a subpoena or an employee's consent.[21]

Because of these privacy concerns, an employer may be required to take different approaches to different pieces of information when documents are sought by the police. For example, an employer may feel comfortable turning over personnel documents of the accused that list his or her date of hire, but may insist on a search warrant before handing over the background check conducted of the employee before his or her hire.

C. What Can Be Done in Advance of an Inquiry?

Devise and Implement Applicable Policies.

Companies should consider issuing policies dictating how it will respond to police inquiries. Written policies will avoid inconsistencies and will give clear direction to employees who are being pressured to hand over certain confidential documents. An employer should consider requiring a subpoena or search warrant before turning over employee or other confidential information, while being cooperative in complying with the subpoena or search warrant.

Consider Designating a Person as the Liaison.

It is prudent for an employer to designate a specific person as the liaison between the police and the employer. This designated liaison should be the first point person the moment the police come knocking on the door. The existence of a liaison helps the police by providing them a contact source and at the same time it allows the employer to have a chance to oversee the turn over of the information to make sure the laws and policies are complied with. It is important to notify employees of the identity of the designated liaison and his/her contact information so employees will know to immediately contact the appropriate person once the police knock or contact the company.

Moreover, the liaison shall be the person who diligently confirms the identity of the police, the validity of any documents the police provide to support their request, and the police's compliance with these documents. If the document is a search warrant, the liaison need to make sure that the police do not venture outside the parameters of the search warrant. As for a subpoena, the liaison needs to ensure that the employer does not unnecessarily turn over information that goes beyond the scope of the subpoena.

Categorize and Separate the Employee Files.

If not already accomplished, it is also prudent to categorize the employee files and maintain them separately. The following is a general categorization of employee files.

- **General Personnel File —** It consists of an employee's job application, offer letter, performance evaluations, discipline records, letters of commendation, etc. Because the definition for identity information is very broad, virtually all of the documents in this file will be considered involving the employee's privacy and the release of such information without a search warrant or a subpoena will entail risk.
- **Medical File —** This includes the employee's medical information, doctor's notes, workers' compensation documents, and any documents related to medical leaves, etc. This is the type of record that absolutely must be kept in a separate file apart from the regular personnel files. The ADA requires that any medical records pertaining to employees be kept in separate confidential medical files. Because of the sensitive nature of a person's medical information, the employer should consult with counsel regarding health and privacy laws when complying with a warrant or subpoena.
- **I-9 Records —** These are the documents that verify an employee's eligibility to work in the United States. Keeping these documents separately serves several purposes. For example, it reduces the employer's exposure to potential claims of invasion of privacy, because the employer can turn over only the I-9 records, and not other files, in response to an immigration audit.
- **Safety Records —** Similar to the I-9 records, these safety records serve a specific purpose, and if the police's

21 Conn. Gen. Stat. § 31-128f.

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

investigation is limited in scope to these records, providing just these records helps reduce the employer's potential liability for claims such as invasion of privacy.

- **Grievance and Investigation Records** — These records often contain embarrassing, confidential, or extremely private information about employees and the release of these records may give rise to various claims such as defamation, invasion of privacy, and even intentional infliction of emotional distress.[22]
- **Documents Generated by the Employee or Pertaining to the Employee** — These are documents that are drafted by the employee or are about the employee. Examples include memoranda written by the employee, emails sent and received by the employee on the employer's server, time cards reflecting the employee's work time, and payroll information. Although there may not be a need to keep all these documents in a centralized place, this information is of the greatest interest to the police investigating identity theft. Knowing where to retrieve such information helps expedite the process of complying with any search warrant or subpoena and thus minimize the interruption to the workplace.

D. How Should the Employer Respond?[23]

How the employer should respond depends on the nature of the inquiry. If there is a search warrant or subpoena, the employer should discover the terms of the legal instrument and should comply with the terms. If the search warrant permits police to search for certain specific information, the employer should limit searches for nonpermitted information. The employer should guard against law enforcement exceeding the terms of the legal instrument. If, for example, the instrument is a subpoena *duces tecum* requiring an employer to bring certain documents to court on a certain day, the employer should guard against any attempt to use the subpoena to conduct an immediate search of the premises. If the law enforcement agency comes armed with an arrest warrant, the warrant will not permit a search of the employer's premises except under limited circumstances. If the warrant is stale (*e.g.*, the time to conduct the search has expired), the employer should raise this fact immediately. There is always the chance that the law enforcement agency will insist on the search despite a defect, and the employer should not physically bar the search under color of law. Nevertheless, the employer will want to make a record of any objection at the earliest convenience.

If there is no search warrant, subpoena or other legal instrument, the employer should follow its policies on how to respond. If the employer has a policy requiring a subpoena or warrant, the employer should insist on the subpoena or warrant while being otherwise cooperative. The employer should work with the police on the terms of compliance by having the documents available, maintaining contact with the police about the status of the warrant or subpoena, and providing access after hours to minimize disruption to the workplace. If the employer does not have a policy or the policy does not require a search warrant or subpoena, the employer should consult with legal counsel regarding the potential liability for turning over specific information and should arrange for a time to turn the information over once a consultation has occurred. The employer may also want to attempt to place restrictions on the voluntary disclosure of such information. This is always balanced against the duty to cooperate and the benefits of full cooperation.

E. How Should the Employer Follow Up?

The police's investigation is a two-way communication channel between the police and the employer. The employer should take this opportunity to know as much as possible from the police about the identity of an accused and victim and the employer need to follow up on this information.

First, if the employer learns enough to know how the alleged identity thief obtains other employees' information, the employer needs to take immediate actions to correct the problems and guard against any future breach. It is important to look at any flaws in the systems that may have allowed for the breach.

Second, if the employer learns that some of its employees might be victims of identity theft, the employer may want to assist these victims in taking actions to control damages and restore their credit worthiness, while recognizing that actions taken may be considered to be admissions by the company. These efforts will not only boost workplace morale but also ease any ill feelings the victims might develop against the employer.

---

22 See *supra* note 4.

23 For further discussions on which specific questions to ask law enforcement and other general discussions about responding to inquiries for records, please see Section I.

Third, if the employer learns that the accused is a current employee, the employer needs to decide whether an independent internal investigation is warranted. An employer has a duty to protect its employees. Obtaining knowledge of a police investigation may put the employer on notice to take steps to safeguard other employees. Notice of a police investigation may also provide grounds to terminate the employee in question. An employer will likely not have the time to wait for a conviction before taking action and will likely have to commence its own investigation to determine whether termination or some other employment action is warranted.

Finally, the employer needs to safeguard related materials in case they are needed later on. If there is no warrant, and no immediate search will occur, an employer should secure the area that will be subject to a search. Actively destroying documents, or permitting their destruction, can expose the employer to criminal charges. As discussed in Section I above, the case of Arthur Anderson is a high profile example. Once the employer is on notice that law enforcement is seeking information in connection with a criminal investigation, the employer can conceivably be subjected to an obstruction of justice charge by intentionally destroying information sought.[24]

The legal and ethical obligation to preserve evidence, especially electronically stored documents and data ("ESI"), has been highlighted by the recent e-discovery amendments to the Federal Rules of Civil Procedure.[25] The ESI may be especially important in investigations of identity theft as more and more identity thieves use the Internet to gain access to people's personal identifying information. Thus, information such as the employer's intranet, security system, log sheet about who accessed what information and when, and the employee's log-in and log-out information will be of crucial significance in the investigations and shall be studiously maintained by the employer.

F. Summary

The employer is in a delicate situation when it comes to employee's confidential information and identity theft. The employer has the duty to safeguard the security of employees' and customers' confidential information, prevent it from being stolen by identity thieves, and refrain from inadvertently and illegal releasing it. At the same time, the employer may need to comply with the law enforcement agencies' requests for information and assist the law enforcement agencies to apprehend the identity thieves before any further damages are inflicted. What information can be released to whom under what circumstances is a very complicated question and the answers vary depending on different facts.

While familiarity with the laws and timely consultation with legal counsel is of crucial importance, the following lists some simple steps that employer can take.

- ❒ **Advanced Preparations.**
  - ❒ Devise and implement appropriate policies. These policies should address not only how the employees' confidential information should be maintained but also the procedures for releasing such information.
  - ❒ Designate a liaison. The employer needs to designate a liaison who will: (1) assist the police in providing the information needed; and (2) oversee the turn-over of the information to ensure the policies and relevant laws are complied with.
  - ❒ Categorize employee's files. There are different categories of employees' information and files that serve different purposes. Keeping these files separately helps limit the employer's potential liabilities and protect against disclosure of some information.
- ❒ **Responding to the Inquiry.**
  - ❒ Determine who the law enforcement agency is and confirm their identity.
  - ❒ Inquire about why the law enforcement agency is doing the investigation.
  - ❒ *If there is a search warrant or subpoena* — read the document and comply with its terms. A company may be required to take different actions depending on whether the document is a search warrant, an arrest warrant or a subpoena. Pay close attention to:
    - Who is entitled to conduct a search or seizure;
    - When the search can take place;
    - To whom the documents must be delivered (if the document

24 See 18 U.S.C.A. §§ 1501-1517

25 Rule 26 of the Federal Rules of Civil Procedure.

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

is a subpoena *duces tecum*, a company may be required to deliver documents directly to the court rather than handing documents over to the law enforcement agency); and

- What is subject to search or seizure.

❒ *If there is no search warrant or subpoena —*

- Consult company policies on whether to insist on a search warrant or subpoena.
- If there are no company policies requiring a search warrant or subpoena, consider whether the request implicates company trade secrets, confidential business information or the privacy rights of its employees, customers or other third parties. If more time is needed to consider these issues, attempt to negotiate more time for that purpose.

❒ When possible, cooperate with the law enforcement agency on convenience issues.

❒ When possible, minimize the interruption to the workplace by, for example, permitting a search to occur before or after working hours.

❒ Preserve the information and documents that are not immediately turned over because they may become relevant later on. The employer should pay special attention to electronically stored data, such as the employee's emails, log-in and log-out documentation, log sheet about the information accessed by the employee, and such payroll information as the employee's direct deposit.

❒ **Following up.**

❒ Depending on the nature of the investigation, determine whether an internal investigation is needed, what to do with the subject of the investigation.

❒ Correct any flaws in the company's systems or security so that the breach does not occur again, if possible.

❒ If necessary, assist victims of identity theft.

❒ Follow up with the law enforcement agency regarding the progress of the investigation.

III. What to Do When the Cops Are at Your Door: Security Breaches Involving Private Employee Information*

Identity theft and other related horror stories about lost or stolen company laptops are in the news more and more frequently these days. Employers should take heed as this is fertile new ground for bad publicity and even legal liability. To date, 35 states and the District of Columbia have passed some type of legislation that requires employers to notify employees of a security breach that involves the disclosure or possible disclosure of their personal information to unauthorized persons. Similar legislation is in the works at the federal level as well. Employers headquartered in states that have not yet passed such a law may still have an obligation to provide notice if their employees reside in one of the jurisdictions that have enacted notice legislation. Putting aside notice obligations, all employers potentially are exposed to legal liability for negligence in preventing or responding to a security breach.

While Section II above, focused on investigations of identity theft by a company employee, this section deals with an employer's obligations and involvement when their internal data, including personnel files or other employee information has been stolen. Personnel files typically contain private employee information that is quite valuable to an identity thief. Therefore, employers must take steps to protect personal information, especially if it is stored electronically. They must also respond appropriately upon discovering a security breach concerning private employee data.

A. Overview of Applicable State Laws

California was the first state to pass a law requiring private employers to notify affected employees in the event of a security breach involving their private information.[26] In the past four years, the following states have passed similar legislation pertaining to private employers:

* This section of the Littler Report was prepared by Kerry Middleton, a shareholder in Littler Mendelson's Minneapolis, Minnesota office.

26 See Cal. Civ. Code §§ 1798.80 *et seq.*

Arizona[27]	Nebraska
Arkansas[28]	Nevada
Colorado[29]	New Hampshire
Connecticut[30]	New Jersey
Delaware[31]	New York
Dist. of Columbia[32]	North Carolina
Florida[33]	North Dakota
Georgia[34]	Ohio
Hawaii[35]	Pennsylvania
Idaho[36]	Rhode Island
Illinois[37]	Tennessee
Indiana[38]	Texas
Kansas[39]	Utah
Louisiana[40]	Vermont
Maine[41]	Washington
Michigan[42]	Wisconsin
Minnesota[43]	Wyoming
Montana[44]	

The statutes vary from state to state and not all impose the same obligations on employers. In addition, some states (*e.g.*, Michigan) require employers to take certain steps to safeguard employee social security numbers. Although each statute is a little different, there are some common themes.

Employers are required to notify employees whose personal information has been disclosed to any unauthorized person. Most statutes do not have specific requirements for the content of the notice and generally allow for written, electronic or telephonic delivery. With regard to timing of the notice, most state laws require that the employees be advised "without unreasonable delay." A few states have a 45-day deadline for notice. Generally, notice may be delayed if it would interfere with a law enforcement investigation. Accordingly, if law enforcement authorities have commenced an investigation, employers should consult with those officials before sending out notices to employees.

The notice statutes do not require that employers notify law enforcement about a security breach. However, such breaches often involve criminal conduct, such as hacking or the theft of a laptop. Employers who suspect criminal conduct should notify local law enforcement authorities and, in certain circumstances, the FBI or the secret service. All notice statutes permit employers to delay notice to individuals if notice would interfere with a law enforcement investigation. Accordingly, if law enforcement authorities have commenced an investigation, employers should consult with those officials before notifying employees to determine whether notice would jeopardize an on-going investigation.

The statutes generally require notice when the employer learns of a security breach or it appears reasonably likely that a breach has occurred. What type of personal information may trigger a notice obligation also varies somewhat from state to state. However, unauthorized disclosure of the following types of information along with employee names will usually require an employer to take action:

- Social Security numbers
- Bank account information
- Credit card information
- Drivers' license numbers

If an employer determines that it must notify employees of a security breach, then the notice should include:

- A short description of how the breach occurred (*e.g.*, lost laptop)
- A description of the type of information disclosed (*e.g.*, social security numbers, bank account numbers)
- Steps taken by the employer to address the breach
- Steps the employees should take (*e.g.*, contact credit bureaus, notify banks)
- Identity of a company contact person who can answer questions and provide further assistance.

Employers should refer to the applicable state law to be sure that the notice meets all legal requirements.

27 Ariz. Rev. Stat. Ann. § 44-7501
28 Ark. Code Ann. §§ 44-110-101 *et seq.*
29 Colo. Rev. Stat. Ann. § 6-1-716
30 Conn. Gen. Stat. Ann. § 36-701b
31 Del. Code Ann. tit. 6, §§ 12B-101 *et seq.*
32 Effective July 1, 2007
33 Fla. Stat. Ann. § 817.5681
34 Ga. Code Ann. §§ 10-1-910 *et seq.*
35 Haw. Rev. Stat. Ann. §§ 487N-1 *et seq.*
36 Idaho Code Ann. §§ 28-51-104 *et seq.*
37 815 Ill. Comp. Stat. Ann. 530/10
38 Ind. Code Ann. §§ 24-4.9-1-1 *et seq.*
39 Kan. Stat. Ann. § 50-7a02
40 La. Rev. Stat. Ann. §§ 51:3071 *et seq.*
41 Me. Rev. Stat. Ann. tit. 10, §§ 1346 *et seq.*
42 Effective July 2, 2007
43 Minn. Stat. § 325E.61
44 Mont. Code Ann. § 30-14-1704

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

B. Employer to Do List

Employers should take steps to minimize the risk of security breaches involving employees' personal information and be prepared to act quickly and effectively should a breach occur. The following preventive measures should be considered:

1. Learn the applicable state law in all states where the company has employees.
2. Develop policies for managing, securing and properly destroying employees' personal information.
3. Identify positions and individuals who have access to sensitive information.
4. Ensure that appropriate staff receive security awareness training.
5. Develop and distribute a clear reporting procedure for suspicious activity.
6. Educate employees about identity theft and defensive steps they can take.
7. Develop and implement an action plan for responding to a security breach.

When an employer learns of a security incident that might trigger an obligation to notify, the employer should investigate to determine the nature and scope of the breach and then consult with counsel to determine whether notice is required by law and, if not, whether notice is advisable as a business decision. If the employer determines that notice should be given, the following steps may be appropriate depending on the situation:

1. Notify and consult with law enforcement officials.
2. Notify affected employees.
3. Notify government agencies as required by law.
4. Notify credit reporting agencies.
5. Consider disciplinary action against employees responsible for the breach.

C. Conclusion

Employers are entrusted with a fair amount of their employees' private, sensitive information. If that information falls into the wrong hands, it is potentially catastrophic for affected employees, and employers could be the subject of negative publicity and may be exposed to significant liability. Employers should take proactive steps to limit their potential liability. In addition to conferring with counsel, there are other reliable resources available, including the Federal Trade Commission's website at www.ftc.gov.

When it comes to avoiding legal liability an employer will be better off if it can demonstrate that it took preventive measures to protect its employees and responded promptly when it learned of a security breach. Therefore, employers should become familiar with statutory requirements, take steps now to avoid a security breach, and develop an action plan to respond quickly if there is a breach.

Nebraska	Neb. Rev. Stat. Ann. §§ 87-801 *et. seq.*
Nevada	Nev. Rev. Stat. Ann. §§ 603A.020 *et. seq.*
New Hampshire	N.H. Rev. Stat. Ann. §§359-C:19-21
New Jersey	N.J. Stat. Ann. § 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat. Ann. § 75-65; 75-61; § 14-113.20(b)
North Dakota	N.D. Cent. Code §§51-30-01 *et seq.*
Ohio	Ohio Rev. Code Ann. §1349.19
Pennsylvania	73 Pa. Cons. Stat. § 2302
Rhode Island	R.I. Gen. Laws § 11-4.2 *et seq.*
Tennessee	Tenn. Code Ann. § 47-18-2107
Texas	Tex. Bus. & Com. Code Ann. § 48.103 and § 48.002
Utah	Utah Code Ann. § 13-44-102 *et seq.*
Vermont	Vt. Stat. Ann. Title 9, § 2430 *et seq.*
Washington	Wash. Rev. Code § 19.255.010
Wisconsin	Wis. Stat. Ann. § 895.507
Wyoming	Effective July 1, 2007

IV. Behind Closed Doors: Child Pornography & What to Do When the Police Arrive: Pertinent Laws and Preventative Strategies*

Employees who use corporate resources to access child pornography over the Internet expose their employer to significant civil and criminal liability. This section discusses the

basic laws governing *child pornography* and its possession, cases that have discussed child pornography in the workplace, and what are the employer's obligations to report child pornography to the authorities.

A. The Illegality of Child Pornography Under Federal & State Laws

Federal and state laws prohibit possessing or accessing child pornography. More specifically, *child pornography* is defined as material that "visually depicts sexual conduct by children" below a specified age.[45] Additionally, federal laws ban interstate commerce in child pornography.[46] Several states have also enacted laws that require information technology technicians to report child pornography if they encounter it in the course of their work.[47] Despite the fact that there are serious penalties attached to viewing, possessing, and producing child pornography, usage statistics continue to soar. In 2002, the U.S. Customs Service estimated that there were more than 100,000 websites offering child pornography, and revenue estimates for the industry range from approximately $200 million to more than $1 billion per year.[48] Although statistics concerning the Internet are prone to change as rapidly as the Internet does, the numbers do consistently indicate that child pornography generates enormous amounts of revenue, it attracts an increasingly large number of viewers, and the children featured on such sites are younger with each passing year.

All of this may be troublesome for employers because knowing possession of child pornography is a crime, even if the employer had no involvement in downloading the child pornography to its information technology systems. The following cases discuss the obligations of an employer who has discovered an employee accessing child pornography in the workplace.

B. Cases Discussing Child Pornography in the Workplace

The legality of an employer voluntarily turning over an employee's hard drive to the FBI was addressed by the Ninth Circuit Court of Appeals in early in 2007. The court determined that child pornography on a workplace computer was admissible evidence even though it was obtained without a search warrant.[49] Although the defendant in the criminal case, Mr. Jeffrey Ziegler, was found to have had an expectation of privacy in his locked office, and his computer inside, his employer had an overriding right to consent to a search of Ziegler's work computer. The court reasoned that because his employer, Frontline Processing, in Bozeman, Montana, told Ziegler at the beginning of his employment that computers were for business use only, the employer could give valid consent to the FBI's search of the hard drive contents of his workplace computer even if Ziegler had placed personal items in the computer.

Notably, in the normal course of business, Frontline monitored employee use of the Internet. The company monitored Ziegler's computer and discovered that Ziegler had searched for "underage girls" and "preteen girls" and that he had stored numerous pornographic images on his work computer. As the internet service provider had already made a report to the FBI and the FBI was ready to proceed with an investigation, two Frontline IT professionals, with the permission of the chief financial officer, made a copy of Ziegler's hard drive. Shortly after this, the company voluntarily turned the computer over to the FBI.

Ziegler was indicted on counts of receipt and possession of child pornography, as well as a count of receipt of obscene material. Ziegler entered a not guilty plea, and moved to suppress the evidence as inadmissible because no warrant had been issued. The trial court disagreed, and noted that Ziegler had no "reasonable privacy in the 'files he accessed on the Internet'" and denied the motion. On appeal, Ziegler's primary argument was that entry into his office to search his workplace violated the Fourth Amendment and the computer evidence on the hard drive must be suppressed. The court of appeals found that Ziegler had a reasonable expectation of privacy in his office, because he kept a lock on his door, and used a password to access his computer.

However, the court went on to hold that Frontline had the ability to consent to the search without its employee's permission because departmental employees had access to all machines, and because the computer was the type of "workplace property that remains within the control of the employer." The court concluded its analysis by holding that although Ziegler retained a legitimate expectation of privacy in his workplace office, Frontline retained

---

* This section of the Littler Report was prepared by Alison Jacobs Gates, an associate in Littler Mendelson's Houston, Texas office.

45 *New York v. Ferber*, 458 U.S. 747, 764 (1982).

46 18 U.S.C. § 2251 (production of child pornography), § 2251A (selling or buying children for sexual exploitation), § 2252 (possession, distribution, and receipt of child pornography), 2252A (possession, distribution, and receipt of child pornography), § 2260 (importation of child pornography).

47 Ark. Code Ann. § 5-27-604 (failure to report computer child pornography); Mich. Comp. Laws § 750.145(c)(9) (obligation of computer technician to report child pornography to law enforcement); Mo. Rev. Stat. § 568.110 (professional's duty to report child pornography found on film, photographs, videotapes); Okla. Stat. tit. 21 § 1021.4 (disclosure of obscene material involving minors); S.C. Code Ann. § 16-3-850 (film processor or computer technician to report film or computer images containing sexually explicit pictures of minors); S.D. Codified Laws Ann. § 22-22-24.18 (computer repair technicians to report suspected violations of child pornography laws).

48 *See* MyKidsBrowser Website, *at* http://www.mykidsbrowser.com/internet-pornography-statistics.php#childporn (last visited Mar. 18, 2007).

49 *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007).

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

the ability to consent to a search of Ziegler's office and his computer. As a result, Ziegler's motion to suppress was denied.

Prior to this case, one other case had discussed child pornography in the workplace. In *Doe v. XYC Corp.*, XYC was aware that one of its employees was viewing *adult* pornography in the workplace.[50] Specifically, a coworker complained that the employee in question minimized his screen when approached, and other company personnel reviewing website visit logs noted that the employee had visited pornographic sites. Although XYC noted that one of the sites related to teenagers, XYC failed to check their content, and the employee was never disciplined for viewing this material at the workplace. The court held that employers have a duty to uncover and stop an employee's use of company Internet resources for the purpose of accessing child pornography once the employer is aware, or should be aware, that an employee is accessing adult pornography. This case is sure to be the first of many to discuss an employer's obligation in dealing with child pornography in the workplace, but it is especially alarming because the employer was held liable for damages done to a child whose images were posted on the Internet by the employee. The court reasoned that the employer should be held responsible for damages caused by an employee's criminal conduct when the employee engages in the conduct on the employer's premises, using the employer's equipment, and the employer has the ability to control the conduct and knows or should know that there is a reason for exercising such control. The court found that the employer was negligent for failing to uncover and stop the employee's activities.

Cases such as *Ziegler* and *Doe* emphasize the importance of communicating electronic resource policies to employees, monitoring employee Internet usage, and reporting child pornography to law enforcement agencies immediately when it is discovered in the workplace. The following provides a brief outline of how to handle an investigation of the workplace by law enforcement agencies, and serves as a guide to developing workplace strategies to eliminate the need for law enforcement visits.

C. Pornography in the Workplace: How to Deal with the Police & Preventative Strategies:

- If police or other law enforcement agencies come to your workplace and intend to search or seize items from your company, they must use a warrant. If they do not have a warrant, you are still considered to be on notice and must ensure that the computers in question are isolated and secured from all other employees. Company testing of the computers should not occur in the interim and no employee should be permitted to access the images "to check whether they really are child porn."
- If any employee witnesses the viewing of child pornography, or has reason to believe that child pornography is being stored on any media, the computer, hard drive, and all backup copies need to be locked and secured, and law enforcement agencies need to be contacted immediately.
- Implement an electronic resource monitoring program, and actively review information to determine whether employees are accessing prohibited websites. If this review suggests that an employee is viewing any type of pornography, investigate further. There is no need to contact the police if the employer can easily determine that the pornography is not child pornography (*e.g.* the URL is www.playboy.com). However, the employee should be promptly questioned about his or her Internet activity and disciplined appropriately. If the investigation provides any reason to believe that the employee did access child pornography, law enforcement should be contacted.
- Strengthen electronic resource policies and employee handbooks so that employee access of objectionable sites is grounds for disciplinary action up to and including dismissal.
- Update your workplace policies to remind employees of the illegal nature of child pornography, and provide them with the company policy on steps to take if they encounter a coworker accessing child pornography.
- Consider using web-filtering products so that employees can only access sites with permissible content.
- Perform random scans of employee computer stations for improper images.

In conclusion, every employer needs to develop an individualized process for dealing with child pornography in the workplace.

---

50 *Doe v. XYC Corp.*, 382 N.J. Super. 122 (2005). For additional analysis of this case see Littler's ASAP, *Prohibiting Porn In Your Workplace Is Not Enough: New Jersey Court of Appeals Imposes New Duties on Employers Who Engage in Electronic Monitoring, available at* http://www.littler.com/presspublications/index.cfm?event=pubitem&pubitemid=13484&childviewid=249

V. The Police Come Looking for a Registered Sex Offender... and He Works for You: What Should an Employer Do?*

Many employees may feel uneasy and even afraid after finding out that one of their coworkers is a registered sex offender. Some employees may even refuse to work with the individual. What are the employer's obligations, if any, in these circumstances? When an employer hears that an employee is a registered sex offender and a coworker refuses to work with him or her, the employer should take three steps:

- Determine whether an employee is truly a registered sex offender. As will be explained below, consultation with counsel is particularly important because employment-related background checks are regulated by fair credit reporting laws and an employer can be exposed to criminal penalties for misusing the Megan's Law website.
- Evaluate the pros and cons of reassigning or terminating the registered sex offender.
- Consider working with the coworker to create an environment where she feels and is safe.

A. Confirming the Conviction

Employers have several lawful options to confirm the presence of a sexually-related conviction, including the use of a background check and, in limited instances, the use of state websites listing registered sex offenders.

Background Checks

Federal and state fair credit reporting laws regulate the process for obtaining an employment-related criminal background check report. This section discusses the federal requirements for obtaining a criminal background check on an employee. An employer should consult experienced counsel to determine whether a background check is lawful and appropriate under state law before proceeding.

Prior to obtaining a criminal background check report, the employer must provide the appropriate notice to the employee and obtain the employee's prior written consent.[51] If the employer determines an adverse employment action is appropriate based, in whole or in part, on the findings contained in the criminal background check report, the employer must notify the employee that a report was requested and permit the employee to promptly identify any mistakes or discrepancies in the report. The employer should provide the employee with a copy of the background check report and a summary of the individual's rights under the fair credit reporting laws.[52] The "pre-adverse action" notice typically, should be mailed to the subject of the background check by a means that creates proof that the notice was received, such as registered or certified mail.

After providing the employee with a sufficient period of time to identify and clarify any mistakes or discrepancies in the report (generally, a minimum of five days is recommended), the employer should notify the employee of the adverse employment action. The notice must inform the employee that the decision was based in whole, or in part, on the information contained in the criminal background check report. Additionally, the employer should provide the employee with: (1) the contact information for the background check company; and (2) a statement that the background check company did not make the adverse employment action decision.[53] As with the pre-adverse action letter, the employer should consider providing the adverse action decision to the employee via mail with a return-receipt requested.

California Department of Justice's Megan's Law Registry and Website

Many states' police departments or departments of justice, including California, post relatively up-to-date information about sexual offenders on their department's website. This section discusses some of the requirements for utilizing the California Department of Justice's Megan's Law Registry and Website. As each state regulates the use of its sexual offender registry differently an employer should contact experienced counsel prior to using a sexual offender registry to make employment decisions.

Megan's Law Website provides information on certain sex offenders residing in California.[54] In appropriate circumstances, this website can be a useful tool for employers seeking to confirm whether an individual is a registered sex offender. However, employers should be cognizant that the California Penal Code section 290.46 prohibits the use of information contained within the website for employment purposes except when the information is used "to protect a person at risk" or as otherwise permitted by law.

---

* This section of the Littler Report was prepared by Katherine Dix, an associate in Littler Mendelson's Denver, Colorado office. Philip Gordon, a shareholder in Littler's Denver office and Rod Fliegel, a shareholder in Littler's San Francisco office also contributed to this section.

51 15 U.S.C. § 1681b.

52 15 U.S.C. §1681b(3).

53 15 U.S.C. § 1681m.

54 The accuracy of the website (as with other similar state websites) is limited. The website does not contain an exhaustive list of all individuals convicted of sex offenses in California because: (1) some individuals convicted of sex offenses are not required to register with the state; and (2) the website only includes individuals who comply with the states' registration requirements.

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

In determining whether other employees or customers qualify as "persons at risk," the employer, in conjunction with experienced counsel, should evaluate:

- the age and gender of coworkers and customers; and
- whether employees and customers will be in unsupervised contact with the sex offender employee.

If an employee does not constitute a threat to "persons at risk" or as otherwise permitted by law, the employer cannot discriminate against (*i.e.* terminate) the employee on the basis of the information found on the website. Arguably, however, an employer could make an adverse employment decision based on information contained both within a background check report and the website.

B. Evaluating How to Best Proceed

Once an employer confirms that an employee is a registered sex offender, the employer faces the difficult choice of determining whether to take an adverse action against the employer. The employer should remember that termination of employment may lead to a discrimination claim by the employee, but continued employment may lead to a negligence lawsuit by a coworker or customer and bad publicity for the company. Hence, the employer and his or her experienced counsel should carefully:

- Review the employee's application materials. Did the employee falsify his or her employment application? If so, termination may be appropriate. Conversely, an employee's upfront and complete disclosure of the conviction and the surrounding events may weigh in favor of continued employment.
- Consider workplace violence issues. Does the employee pose a risk to his or her coworkers or the employer's customers? In making this determination, the employer may wish to consider the nature and gravity of the offense, the time passed since the offense, whether the employee has successfully participated in any rehabilitation programs, and whether the employee has been convicted of any other offenses. The employer also should consider the employee's job responsibilities and whether coworkers will be exposed to the employee in isolated areas or where the coworker may otherwise confront difficulty obtaining assistance in the event the employee misbehaves.

If the employer decides not to terminate the employment of the registered sex offender, the employer should confirm its commitment to providing a safe working environment to the coworker and inform the coworker of the safety measures currently in place to protect employees. If the coworker still refuses to work with the registered sex offender, upon consultation with experienced counsel, the employer may consider transferring one or both employees.

C. Best Practice

The best practice is to avoid this situation by pre-screening job applicants. In conjunction with experienced counsel, an employer should consider:

- Instituting a pre-employment screening policy that the company can apply consistently in a fair and even-handed manner. Developing this policy with experienced counsel is important so as to ensure compliance with both state and federal fair employment laws.
- Posting a prominent notice or otherwise giving notice that all employment applicants will be required to submit to a background check.
- Including a notice on application forms and employee handbooks that applicants who materially falsify or misrepresent information on applications and other pre-employment documents will not be considered for employment or, if discovered during employment, will be discharged.

Upon receiving a completed application, an employer should:

- Review the application form to ensure the applicant fully and accurately completed the form. If a sexually-related conviction is disclosed, the employer should confirm the conviction through a background check and request details from the applicant.
- If a sexually-related conviction is disclosed by a background check report and the employer wishes to disqualify

the applicant on that basis, the employer should notify the applicant of the information in a pre-adverse action letter and give him or her an opportunity to contest the information. After a sufficient period, the employer should notify the applicant of the adverse action that the decision was based on, or based in part, on the background check report. This adverse action letter should include: (1) the contact information for the background check company; and (2) a statement that the background check company did not make the adverse employment action decision. Both letters should be sent via certified mail with return receipt requested.

If the employer wishes to screen applicants based on information contained in the Megan's Law Website, in consultation with experienced counsel, the employer should consider whether the applicant poses a threat to at risk persons. If not, information contained in the website alone should not be the basis for a no-hire decision.

VI. Now Who's Knocking... The SEC: Investigations by the Securities and Exchange Commission — Stock Option Backdating*

Stock option backdating is the white-collar crime *du jour* — every day the news is filled with reports about various companies being investigated over this practice. Option backdating refers to the practice of granting someone (usually an executive) an option that is dated prior to the date the option actually was granted. For example, if the company grants options to executive X on April 1 when the price of stock is $100 but dates the grant January 15 when the price of stock was $60. Thus, the executive can purchase stock at $60 and immediately sell it for a nice profit.

Backdating is not illegal if it is done transparently. Backdating only becomes illegal if it is done in such a way as to mislead stockholders, including filing improper disclosures with the Securities and Exchange Commission (SEC). Most of the companies caught in the initial wave of the backdating scandal were actively concealing the fact that they granted backdated options to executives. Currently, however, the companies being investigated are more likely to have engaged in minor violations; for example, a company whose compensation committee belatedly signed off on an option grant that occurred the prior month and then uses the committee approval date as the grant date in its disclosures.

Despite what is reported in the media, it is unlikely that the SEC, the Department of Justice (DOJ) or any other federal agency will actually turn up on the company's doorstep unless they are merely dropping off a letter or subpoena in person. Accordingly, the first part of this section will focus on what to do when that letter or subpoena is received. The second part will focus on what to do if an agency, usually the FBI, actually comes to your door with a search warrant.

A. Receiving the Target Letter or Subpoena

A company being investigated by the SEC generally will receive a *target letter* (named because it indicates that the company is the target of an investigation). The *target letter* will probably also request that the company provide the SEC with specified documents (probably a lot of specified documents) in a very short period of time and that the company not destroy any documents. If, on the other hand, it is the DOJ who is interested, they will send a *subpoena* demanding that the company provide specified documents (also a lot of documents in a short period of time). It is unlikely, but possible, that the agencies will personally deliver the target letter or subpoena; instead, you are more likely to receive them by mail.

After reading the letter or subpoena, take a deep breath — a lot of work needs to be done in a short period of time. The first 24-72 hours of a government investigation are crucial. The goal is to perform a brief internal investigation and then meet with your Board of Directors as soon as possible. Performing a brief internal investigation allows the company to realistically assess the basis of the government's claims so as to determine whether any remedial action is necessary. It also allows the company to provide the Board with an educated assessment of the issues at hand and how the company should respond to those issues.

The Board needs this assessment in order to best determine how to cooperate with the government. In determining how to proceed after completing their investigation, both the SEC and the DOJ place tremendous weight on the amount of cooperation they receive from the company being investigated. Both

* This section of the Littler Report was prepared by John C. Kloosterman, a shareholder in Littler Mendelson's San Francisco, California office. Special acknowledgments are also extended to Lee H. Rubin, a partner with Mayer Brown Rowe & Maw, L.L.P. specializing in securities and white-collar criminal defense, who was a great resource for this portion of this Littler Report.

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

agencies have issued memoranda outlining what constitutes full cooperation.[55] While each agency's factors are slightly different, they share an overall theme — the government will look favorably upon companies that are proactive and fully cooperate with the investigation. *Proactive* means that the company will perform its own internal investigation, take all appropriate actions (including disclosure of any wrongful conduct and terminating employees who acted improperly) and allow the government full access to the information discovered during the investigation. The internal investigation referred to is usually an independent investigation ordered by the Board of Directors or a Board committee, not the brief investigation needed to perform before meeting with the Board. But this investigation is also proactive and will help determine what additional proactive steps are taken next.

After reviewing the target letter or subpoena, and the relevant agency's memorandum on cooperation, the next step is to deal with the documents requested. For the time being, do not worry about the return date on the target letter or subpoena — this is something your legal counsel can negotiate with the agency. Instead, steps need to be taken to ensure that all relevant documents and records are preserved, including electronic data. At a minimum, a memo needs to be issued to employees regarding document preservation. The IT department should also be involved to ensure that relevant backup tapes and discs are saved. All publicly-available records and data relating to the company should be reviewed — the company should assume that the government has also acquired these records.

Legal counsel who is experienced with securities and/or white-collar crime matters and, ideally, has substantial experience dealing with the investigating agency should be consulted. Involvement of employment counsel is also important at this juncture because a number of employment-related issues likely will arise once interviews with employee witnesses begin.

Those witnesses are the next priority. Based on the contents of the target letter or subpoena, the next step is to identify employees with knowledge of the relevant events. There are a number of potential witness issues to be aware of. First, any of the witnesses identified may be whistleblowers and may have already spoken with the government. Second, these witnesses may need separate legal counsel and the company may be obligated (by contract, corporate by-laws or statute) to provide the employee with separate counsel. Third, it is possible that some of the identified witnesses may turn out to be targets themselves. Fourth, even if none of the witnesses are whistleblowers, it is possible that the government has already talked with some of them or may want to talk with them soon.

Public relations is another important issue to consider. A communications procedure should be established so only one company representative is speaking to the media about the matter. This is an appropriate strategy for all topics addressed in this Report.

Now that many of the preliminary steps have been taken, the focus should turn to the brief investigation mentioned at the outset. Again, the goal of this investigation is to gain information that will allow the company to realistically assess the matter at hand and determine whether any corrective action should be taken prior to the meeting with the Board. If not already done so, review all of the publicly available material that was gathered earlier. Employees identified as potential witnesses should be interviewed. Because of the issues mentioned above, these interviews will need to be conducted very carefully. It should be emphasized to the witnesses that the investigation is confidential, that they have the right to have counsel present and remind them of their Fifth Amendment rights.

If any of the witnesses assert their Fifth Amendment rights, discuss with legal counsel, including employment counsel, whether the employee should be terminated for refusing to cooperate. The interviews may also reveal that some of the witnesses acknowledge their part in wrongdoing and whether to terminate or take some other employment action against these individuals should also be discussed with legal counsel. Before terminating a wrongdoer, the company should assess the risks to the company of terminating versus keeping the employee.

After reviewing documents and interviewing employees, it may be apparent that there is an issue requiring corrective action, such as terminating an employee or amending any SEC filings. If so, the need for immediate action should be discussed with outside counsel.

55 The SEC's is the *Seaboard Report, available at* http://www.sec.gov/litigation/investreport/34-44969.htm. The DOJ's most recent memorandum is the *McNulty Memo, available at* http://www.usdoj.gov/dag/speech/2006/mcnulty_memo.pdf.

Finally, a meeting with Board of Directors should be scheduled to inform them of the target letter or subpoena, the results of the brief investigation and any corrective actions you have taken. Make sure the Board is aware of the relevant agency's memorandum on cooperation and the points outlined in that memorandum.

The Board may determine that an independent investigation is needed. If so, the Board likely will nominate a special litigation committee to oversee the investigation and hire legal counsel to perform the investigation. This counsel should not be the counsel the company has previously retained to assist it with the matter and should be a lawyer or firm that is unconnected to the company. Otherwise the investigation may not be considered sufficiently independent.

B. The FBI Is at the Door

If federal agents turn up on your company's doorstep with a search warrant, it is most likely the FBI and they probably are interested in a specific individual or have reason to believe that the company is destroying evidence. Again, in securities-related matters, it is not normal for federal agents to show up and demand that they be allowed access to your records unless they have a search warrant.

The overall goal is to stay reasonably calm and control the search as much as possible. Having a large number of federal agents barge into the company and begin searching records is disconcerting and is meant to be that way — the more stunned the company is, the more likely it is that the agents will have unfettered access to the company records. So the first priority is to remain as calm and level-headed as possible. Then contact legal counsel.

The following are steps that should be taken when the FBI appears with a warrant for a securities-related investigation:

- Find out who the agent-in-charge is and ask to see the search warrant. The agents are required to provide the company with a copy. Review the warrant to make sure it is signed by a magistrate judge and that the warrant is being executed within the allotted timeframe. You should fax a copy of the warrant to legal counsel.
- Inform the agents that the company wants legal counsel present for the search and ask if the agents will wait. If the agents do not agree to wait, which is likely, tell them that they are refusing the company's reasonable request and ask that they note the request and their refusal.
- Question the agent-in-change about the search — find out which agencies are represented, obtain business cards from all of the agents, ask what the investigation is about, etc.
- Put together a team to manage the search from the company's perspective. The team should consist of someone from senior management who can coordinate the company's efforts and liaise with the agents, one or more individuals from IT (it is likely that portions of the government's search will involve the company's computer system), several note takers and, if possible, legal counsel. The company may also consider sending all of the other employees home. If so, advise them of their right to speak with or not speak with the agents.
- Do not answer specific questions from the agents without legal counsel present. The agents are there to look for specific records, not to interrogate employees. The company can and should respond to questions about whether a specific document is covered by the warrant. But, absent advice from legal counsel, the company should not answer general questions about the company. **This message should also be conveyed to all relevant employees.**
- Shadow the agents as they perform their search. This means following each agent and taking notes on where the agent is searching and what records the agent is taking. Under no circumstances should anyone else get in the agents' way or interfere with their search (except that if the agents begin searching for records outside the parameters of the warrant, then this should be pointed out to them). But at the same time, do not let the agents search through records alone. It is likely that one or more agents will focus on the company's computer system and will ask to use a computer to search through the system. IT professionals should watch these agents carefully.
- After reviewing the warrant and determining what the agents are searching for, analyze whether any of the

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

records sought are privileged. If so, tell the agent where those records are kept, that they are privileged and that the company does not waive the privilege.

At the conclusion of the search, the agent-in-charge is required to catalog the records taken in the presence of a company representative. If it appears that the agent is taking records that the company cannot operate without, ask if a copy can be made. It may be possible to have a copy service make copies while the agents watch. While a company representative must be present while the agents catalog the records, the agents do not have to provide the inventory list to the company. Instead, the agents must provide a copy of the list to the magistrate who signed the warrant. The magistrate will provide the company with a copy of the list if the company asks for a copy.

Finally, after the agents have left, go through the areas where the agents focused their search and determine what was taken. Talk with the employees who work in those areas to see if they can shed any light on why the agents were interested in their documents.

VII. Who's Here Now? It's ICE: Immigration-Related Worksite Investigations & Audits[56]

A. Introduction

A number of government agencies have an interest in enforcing federal immigration laws. But the primary agency that affects employers is Immigration and Customs Enforcement (ICE), which is part of the Department of Homeland Security (DHS).[57]

ICE is the agency responsible for enforcing an employer's obligations to verify, and re-verify, the work authorization of all new employees.[58] ICE may enforce this responsibility through random I-9 compliance audits or through a narrower investigation based on a lead. The lead can be an anonymous tip,[59] or facts that form a reasonable suspicion of an employer's noncompliance.

Most recently, ICE has been concentrating its enforcement efforts on investigations, not random audits. Specifically, these investigations have focused on: (1) worksites related to critical infrastructure and national security (*e.g.*, nuclear power plants, chemical plants, airports, and military/defense facilities); (2) industries viewed as employing a large percentage of unauthorized workers (*e.g.*, the construction industry or agricultural industry); and (3) employers suspected of egregious violations of immigration and labor laws. Investigations of this last category often are a concerted effort between the Department of Labor (DOL), Department of Homeland Security (DHS), and Federal Bureau of Investigation (FBI) and have resulted in criminal prosecutions involving criminal sanctions and charges of harboring illegal aliens, money laundering and/or knowingly hiring illegal aliens.[60] These are the raids frequently shown in the media but they are the least prevalent of ICE's enforcement mechanisms.

B. Notice of an ICE Audit

ICE must provide an employer with three days' notice prior to a worksite inspection. ICE accomplishes this with a Notice of Inspection (NOI). If an NOI is received, look carefully at it to ensure that the designated recipient is accurate. If a subcontractor or other entity is the designated recipient, then immediately identify the appropriate entity/person for receipt.

No subpoena or warrant is required prior to an inspection. But precedent indicates that an employer cannot be penalized for refusing to provide the I-9 forms absent an administrative subpoena or warrant.[61] In addition, precedent supports the assertion that ICE may not inspect an employer's premises,[62] or enter employer premises to speak with employees without a warrant.[63]

An ICE agent may deliver the NOI, but unless the government has already secured a subpoena or a warrant, there is no need to make the requested information immediately available. However, consultation with legal counsel to determine whether to cooperate or mandate a warrant or subpoena prior to inspection is emphatically suggested.

With the assistance of legal counsel, a standard policy addressing what managers should do if an ICE agent makes an

---

56 This section of the Littler Report was prepared by John C. Kloosterman, a shareholder in Littler Mendelson's San Francisco, California office, Lisa A. Cottle, an associate in Littler Mendelson's Cleveland, Ohio office and Bonnie Gibson a shareholder and Jason M. Gerrol an associate of Littler Global located in Phoenix, Arizona.

57 The Department of Citizenship and Immigration Services (CIS), which is part of the DHS, has been known to make unannounced visits to worksites, primarily for the purpose of inquiring into the nonimmigrant visa status of a company's workforce. In addition, the FBI investigates *racketeering activity*, which has been defined by the Racketeer and Corrupt Organization Act (RICO) to include "any act which is indictable under the Immigration and Nationality Act..." *See generally* 18 U.S.C. §§ 1961 *et seq.* Further, DOL regulates certain issues relating to nonimmigrant workers holding H-1B visas. Finally, the Department of Justice's Office of Special Counsel for Immigration-Related Unfair Employment Practices (OSC) will visit workplaces where allegations have been made that the employer is discriminating against employees based on their immigration status. However, the OSC generally visits as part of an investigation and does not show up unannounced.

58 *See generally* MOU, Meissner, Comm. INS and Anderson, Asst. Sec. ESA (Nov. 23, 1998), *reprinted in* 75 No. 47 *Interpreter Releases* 1696, 1711-21 (Dec. 14, 1998).

59 *See U.S. v. Widow Brown's Inn*, 3 OCAHO No. 399 (Jan. 15, 1992).

60 News Releases and Fact Sheets regarding ICE's investigative focus can be found at www.ice.gov.

61 *See generally McLaughlin v. Kings Island*, 849 F.2d 990, 997 (6th Cir. 1988) (finding that an employer may not be penalized for asserting Fourth Amendment rights in response to a request from the Secretary of Labor to inspect documents).

62 *See generally Marshall v. Barlow's Inc.*, 436 U.S. 307, 310 (1978) (finding the Fourth Amendment protects commercial buildings, as well as private homes).

63 *See U.S. v. Widow Brown's Inn*, 3 OCAHO No. 399 (Jan. 15, 1992)

unannounced visit should be developed. In particular, that policy should address: (1) the regulatory requirement that an NOI be issued; (2) the company's policy regarding the potential need for a warrant or subpoena before the ICE agent is allowed to enter the worksite premises; and (3) the need to immediately inform a designated responsible officer about the visit. Having this standard policy in place will ensure that managers know what to do in the event of an ICE visit. and that appropriate company officials are notified of the NOI and the upcoming ICE audit.

C. Preparing for the Audit

The ICE audit will involve the inspection of I-9 forms. In this regard, the best defense is a good offense.[64] The employer should work with legal counsel to prepare and implement a comprehensive I-9 policy. At a minimum, this policy should address: (1) the deadlines by which each section of the I-9 form must be completed; (2) the prohibition on requesting specific documents, or more documents than the law requires; (3) instructions regarding how to determine the retention date of each form; (4) the company's policy on copying the documents called for in Section 2 of the I-9 form; and (5) how to comply with the obligation to reverify work authorization using a tickler system. Additionally, a manager should be designated and trained to be in charge of preparing, maintaining, reverifying, retaining and ultimately purging I-9s in compliance with the I-9 policy.

As noted above, the government is generally required to provide employers with three days' notice of an I-9 audit, although an employer may waive this requirement and allow for immediate access.[65] Accordingly, I-9 forms should be maintained so they can be accessed on short notice. Also immediately contact legal counsel after receiving notice of an I-9 audit.

Consultation with experienced legal counsel is critical in determining how to respond to notice of an I-9 audit and will ensure that the employer's interests are protected every step of the way. Counsel will orchestrate the company's internal review of its I-9s prior to the government's audit. After receiving the I-9 audit notice, quickly perform a self-audit to demonstrate good faith compliance with the law and mitigate any penalties the government may impose. Additionally, take advantage of section 274A(b)(6) of the Immigration and Nationality Act, which affords the opportunity to avoid sanctions for certain "technical or procedural" violations by correcting them within ten days of the government's notice identifying those items considered "technical or procedural."

Before undertaking the self-audit, compile a roster of all employees hired since November 6, 1986, including their hire and termination dates. Then purge all I-9s for employees who were hired more than three years ago or terminated more than one year ago, whichever date is the latest.[66] The remaining I-9s are subjected to the self-audit.

The next step is to assemble an audit team consisting of legal counsel, the manager responsible for I-9 forms and assistants trained in the company's I-9 policy. The audit team will review the forms to confirm that they are consistent with the I-9 policy. If the forms need to be amended, those amendments must be made in a nondestructive manner, such as lining through incorrect information and noting the correct information in the margin, as well as providing an explanation for the new information and a signature and date for the change. Do not destroy or alter the original forms in a manner that renders illegible any original information. Legal counsel should also prepare a memorandum summarizing the findings of the self-audit and action steps that the employer will take to ensure complete I-9 compliance.

Legal counsel also will identify where the government will conduct its audit — should the government be permitted to review the forms on the company's premises, or should the company provide the agents with photocopies of the forms for off-site review. Regardless of where the review will take place, it is critical that the agents not take the original I-9s.

D. Penalties

ICE has discretion to assess a range of money penalties for I-9 violations. The dollar amount imposed will be a factor of the employer's size, demonstrated efforts at good faith compliance and violations committed, as well as any prior history of immigration-related violations.[67] Penalties for errors made on I-9 forms, or "paperwork" violations, can range from $100 to $1,100 per form, depending upon the number of violations on each form and the date when the offense occurred.[68] If the government's audit reveals that the employer knowingly hired or continued to

64 Although the focus of this discussion is I-9 audits, the following practical advice applies equally to preparing for and responding to DOL audits of H-1B Public Access Files.

65 *See* 8 C.F.R. § 274a.2(b)(2)(ii).

66 *See* 8 C.F.R. § 274a.2(b)(2).

67 *See* INA § 274A(e)(5).

68 *See* 8 C.F.R. § 274a.10(b)(2).

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

employ an unauthorized worker, possible fines range from $250 to $11,000 per unauthorized worker depending upon the employer's prior history of similar violations and the circumstances of the particular case.[69] Where ICE finds a "pattern or practice" of immigration violations, it may also impose a criminal penalty of imprisonment for no more than six months.[70]

When ICE concludes its audit, it may serve the company with either a Warning Notice or a Notice of Intent to Fine (NIF). The company also can expect a follow-up from the government regarding specific problem cases identified during the audit. A NIF will specifically set forth the violations alleged and state the penalty imposed. Depending upon the extent of the company's I-9 compliance and its conduct during the audit, a lower-cost settlement may be obtained.

Conclusion

Despite media reports, most ICE enforcement efforts are the result of a targeted investigation, not a raid. Nevertheless, it is important to realize that employers are entitled to receive three days notice prior to an ICE audit. But if an ICE agent knocks on your door, you should immediately contact legal counsel to discuss how to respond.

VIII. What to Do When OSHA Comes Calling?*

The Occupational Safety & Health Act of 1970 ("the Act") became operational on April 28, 1971. In the federal scheme, the Act is implemented by the Occupational Safety and Health Administration (OSHA), which generally has jurisdiction over employers whose business operations affect interstate commerce. For many states, regulation of workplace safety is vested in OSHA. Technically, the Act preempts all state job safety and health legislation. However, Section 18(a) of the Act provides that if the Secretary of Labor determines that a particular state has created standards comparable to OSHA's and has a plan for enforcement that meets the criteria set forth in 18(c) of the Act, jurisdiction may be ceded back to the state.

This section will generally discuss issues and strategies for handling an OSHA inspection as that is defined under the Act. However, employers should consult their legal counsel to determine if their state has its own regulations since state safety laws and enforcement procedures vary in some respects from the federal scheme.

A. When You Might Be Subject to an OSHA Inspection

OSHA prioritizes its inspections into four categories: (1) imminent dangers; (2) fatality and catastrophic investigations; (3) investigation of complaints; and (4) regional programmed investigations.[71]

Imminent Danger

Section 13(a) of the Act defines an *imminent danger* as a danger "which could be reasonably expected to cause death or serious physical harm immediately or before the imminence of such danger can be eliminated through the enforcement procedures otherwise provided by this Act."

Fatality & Catastrophic Investigations

The purpose of a fatality and catastrophic investigation is to determine if noncompliance with OSHA standards contributed to the cause of the workplace injuries. Most such investigations result directly from the obligation of the employer to report to the local OSHA area office any fatality within 8 hours of its occurrence.

Investigation of Complaints

OSHA procedures require that it investigate and inspect in response to any written complaint unless: (1) the persons complaining does not establish a reasonable grounds to believe that a violation threatening physical harm or an imminent danger exists; (2) a recent inspection or other reliable evidence indicates that the danger is not present or has been abated; or (3) the complaint is outside OSHA's jurisdiction. OSHA must respond to all complaints involving imminent danger within 24 hours. For other complaints not involving imminent danger OSHA generally will respond within 30 working days.[72]

Regional Programmed Investigations

OSHA also initiates inspections of certain high risk employers, or those who are either in high risk industries or who have lost workday injury and illness rates substantially above the national average. OSHA's current enforcement procedure for programmed inspections is called the Site-Specific Targeting Program. The

---

69 *See id.* § 274a.10(b)(1)(ii).

70 *See id.* § 274a.10(a).

***** This section of the Littler Report was prepared by Ron Peters, a shareholder in Littler Mendelson's San Jose, California office and Steve McCown of Littler Mendelson's Dallas, Texas office.

71 Occupational Safety & Health Administration, *Field Inspection Reference Manual*, ch. I-B-3-a.

72 *Id.* Occupational Safety & Health Administration, *Field Inspection Reference Manual*, ch. I-C-2.

selections for programmed investigations are based on the yearly Field Operations Program Plan, which is conducted by each Area Office. Targeted employers are selected randomly from a list and placed into an inspection cycle.

B. Advanced Notice of an Inspection

Section 2(b)(10) of the Act contemplates that no advance notice of an inspection will be given and Section 8(a)(1) specifically provides for unannounced inspections in order to promote safe and healthful working conditions. The theory being that if an employer had advanced notice of OSHA inspections, they would only comply with the Act in preparation for a scheduled inspection. In fact Section 17(f) of the Act provides for a criminal penalty against any person who provides unauthorized advance notice of any OSHA inspection. While there are some limited exceptions,[73] employers should assume that they will not have advance notice of an OSHA inspection.

C. Demanding a Warrant Before Inspection

In 1978, the U.S. Supreme Court in *Marshall v. Barlow's, Inc.*,[74] held that requiring that OSHA obtain a warrant prior to inspecting an employer's premises was reasonable. The Court held that the requirement of obtaining a search warrant was not overly burdensome on the inspection system or the courts and that it would provide assurances that the inspections were reasonable under the Constitution. As a practical matter this means that it is a foregone conclusion that OSHA will be able to obtain a warrant to inspect the premises if the employer demands that they do so.

Therefore, an employer should consider carefully whether they want to demand one before letting the investigator proceed with the inspection. While demanding a warrant can buy the employer some additional time to prepare for the inspection, warrants can generally be obtained easily within a few hours, and OSHA may perceive an employer's demand for a warrant as an attempt to thwart their investigation.

D. How To Be Prepared for an OSHA Inspection

Be in Compliance with Safety & Health Rules & Procedures

It may seem obvious, but no where is the phrase "an ounce of prevention is worth a pound of cure" more apt than in the world of workplace safety. The Act and OSHA place a very high priority on worker training and education. An employer should conduct regular self-audits of all facilities and identify any and all dangers. Moreover, employers should also have a system in place for documenting efforts to enforce safety standards and any efforts to abate any identified dangers.

Be in Compliance with Recordkeeping Requirements

All employers covered by the Act are subject to recordkeeping requirements. Section 8(c)(2) provides that employers must keep accurate records of "work related deaths, injuries and illnesses other than minor injuries requiring only first aid treatment and which do no involve medical treatment, loss of consciousness, restrictions of work or motion, or transfer to another job." The Act's recordkeeping system consists of three forms for the recording of work related injuries and illnesses: a log, injury and illness incident reports/Supplementary records, and an annual summary. The Log of Work Related Injuries (OSHA Form 300) is used to classify injury and illness cases and to note the extent and outcome of each. The Injury and Illness Incident Reports (OSHA Form 301) provides greater detail concerning the injury including the details of the injury and extent of harm and treatment received. Both form 300 and 301 must be completed within 7 days of the employers knowledge of the injury and be maintained at the employer's establishment.[75] The Annual Summary (OSHA Form 300A) requires that the employer at the end of each calendar year provide a total of all work related injuries and illnesses for each business location.[76] Employers are also required to keep records of Hazard Communications Programs, company safety programs, programs governing exposure to electricity, and required posters. Employers should also keep records of safety training.

At a minimum the following records should be kept up to date:

1. OSHA 300 Logs
2. OSHA Form 301, Supplementary Records/Incident Records
3. OSHA Form 300A, Annual Summary
4. Hazard Communication Program
5. Company Safety and Health Programs, including safety meeting minutes, records of dissemination and enforcement of program, training, etc.
6. Assured Equipment Grounding Program (if GFCI not used)

73 29 C.F.R. § 1903.6 provides that advance notice may be given: (1) in case of imminent danger, to allow immediate abatement; (2) for inspections after normal business hours; (3) where special arrangements for inspection are needed; and (4) where advance notice is needed to insure the presence of employer and employee representatives.

74 *Marshall v. Barlow's, Inc.*, 436 U.S. 307 (1978).

75 29 C.F.R. § 1904.29(b)(3).

76 *Id.* § 1904.32(a).

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

7. OSHA Posters

E. Investigation Procedure

Presentation of Credentials

Once an investigation is undertaken by OSHA they are required to follow a fairly routine procedure. First, upon arrival at the worksite, the investigator must present his/her credentials. Section 8(a)(1) of the Act conditions the authority of OSHA to act on the presentation of proper credentials. This provision protects against forcible entry and unauthorized access by individuals who may falsely hold themselves out to be OSHA investigators to try and extract penalties and bribes on the spot.[77] Credentials must be presented to an "owner, operator or agent in charge." As a practical matter, any manager will probably qualify as someone authorized to accept the investigator's credentials.[78] After the proper presentation of the credentials, the employer generally cannot place any further preconditions on the inspection.[79] However, if the investigation is being conducted pursuant to a warrant then the investigator cannot expand the scope of the inspection beyond what is indicated in the warrant. If the employer suspects an investigator proceeding without a warrant may expand the scope of the inspection too much, this may be an occasion to demand a warrant before permitting the inspection.

Opening Conference

Following the proper presentation of credentials, the investigator will conduct an opening conference with the employer. If the inspection is being made pursuant to a complaint, the complaint should be shown to the employer. The employer may request the identity of the complainant, but the OSHA investigator will not reveal the identity of the complainant if the complainant has so requested. The opening conference is deliberately brief in order that the investigator can move onto the inspection itself without delay.[80] During this conference the investigator will inform the employer of the general scope of the investigation including what parts of the employer's establishment he or she would like to see. The investigator will also provide a request for records kept by the employer. This will generally include most or all of the records identified above. The employer is advised to inform the investigator of any trade secret issues prior to the inspection and can request that such secrets be kept confidential.[81] During this conference the employer should also inform the investigator of any special conditions related to the inspection and provide the investigator with any protective clothing.

The Inspection

Section 8(e) of the Act provides that an employer has the right to have its representative accompany the investigator on his tour of the employer's establishment. An employer is well advised to never leave the investigator alone during the tour of the establishment.

During the inspection the investigator is entitled to collect evidence and record all relevant information. This may include taking photographs, environmental samples and making diagrams. Since this evidence may be used against the employer, the employer is well advised to simultaneously gather their own evidence. The investigator can also video tape the inspection. OSHA generally has an obligation to honor the employer's right of confidentiality to protect trade secrets.[82] Section 8(a)(2) also provides that during the inspection the OSHA investigator may also interview privately any owner, operator, manager or employee.

Closing Conference

The Closing Conference takes place immediately following the inspection tour. The purpose of the conference is to review the findings of the investigation. The employer will have the opportunity to discuss whether there will likely be any citations issued and the classification and basis for any citation.[83] The investigator will also address any hazards identified and provide guidance on how the employer can abate such hazards.

F. Checklist: Presentation of Credentials/Opening Conference

1. Immediately notify appropriate management personnel and/or legal counsel.
2. Ask for Investigator's credentials.
3. Escort investigator to a private office or other location.
4. Ask the investigator to identify the purpose of the inspection and how it was initiated. (*i.e.* by complaint, programmed inspection etc.).
5. Ask investigator to wait for management personnel

77 *Usery v. Godfrey Brake & Supply Serv., Inc.* 545 F. 2d 52 (8th Cir. 1976)

78 *Tobacco River Lumber Co.*, 3 OSHC 1059, 1974-5 OSHD ¶ 19,565 (1975) (employee designated to "handle matters" in owners' absence deemed to be an agent in charge.")

79 *Id.; Usery*, 545 F.2d at 55.

80 Occupational Safety & Health Administration, *Field Inspection Reference Manual*, ch. II-A-3

81 *Id.* ch. II-A-3-i.

82 *In re Establishment Inspection of Kelly-Springfield Tire Co.* 13 F. 3d 1160 (7th Cir. 1994).

83 Occupational Safety & Health Administration, *Field Inspection Reference Manual*, ch. II-A-5.

to arrive, or ask if he/she will return later when the appropriate person is available. One day is preferable, two days will ordinarily be acceptable.

6. Consider whether to demand a warrant, or inspect the warrant carefully for scope before complying.
7. Inform the investigator of any trade secret issues and request confidentiality to protect such secrets.
8. Record names of all present during inspection; take notes on everything that is said.
9. Obtain a copy of the search warrant if the inspection was initiated by a warrant.
10. If not by warrant, ask the investigator to define clearly what is to be inspected. Do not permit the investigator to exceed the scope without conferring with legal or corporate personnel.
11. Be at all times courteous and cooperative, but do not volunteer unnecessary information.
12. Do not speculate about anything.

G. Checklist: Inspection/Walk Through

1. Designate the person who will accompany the investigator. This person should be someone who is:
   a. familiar with federal or applicable state safety standards;
   b. familiar with the specific work environment and operation subject to inspection; and
   c. familiar with company safety policies.
2. Attitude toward inspection: Be courteous and professional at all times.
3. Strategies during the investigation:
   a. Answer honestly, all factual questions about the company's operation. If you do not know the answer, do not guess.
   b. Make certain the investigator understands the answers.
   c. Do not admit violations, more information can always be obtained and you will not have sufficient information at the time of the inspection to justify an admission, and voluntary admissions can be used by OSHA to prove a violation.
   d. If possible, present the companies position including any mitigating information at the time of the inspection. It is better to avoid a violation by presenting exculpatory or mitigating evidence, such as the absence of risk or of imminent harm, than to have a violation that is defensible with later revealed information.
   e. Do not overreact to the investigator's questions or assertions.
   f. When necessary seek assistance and from safety personnel, foremen or supervisors.
   g. Play an active role in the inspection.
   h. Bring a digital camera and take identical photos to those taken by OSHA.
   i. Never leave the investigator alone.
   j. Avoid performing any demonstration.
   k. Get company approval before permitting OSHA to interview any witnesses.
4. Witness Interviews.
   a. Do not permit interviews in public.
   b. Instruct employees to request a company representative be present during any interviews. OSHA cannot require private interviews with supervisors.
5. Witness Statements.
   a. Supervisors — Should be instructed not to give written statements without company approval, and should request a copy for the company.
   b. Non-supervisors — encourage all employees to request a company representative be present. Train employees to provide clear and accurate statements. Request a copy of any written statement provided by any employee. After the statement is given immediately debrief the employee.

COPYRIGHT ©2007 LITTLER MENDELSON, P.C.

H. Checklist: Closing Conference

1. Make note of all present and what is said, including OSHA, especially the details of any proposed violations.
2. Do not volunteer information.
3. Do not admit any violations.
4. Do not commit to a time frame abatement.

I. Checklist: Abatement

1. If the alleged hazard can be reasonably corrected, go ahead and make the correction, even if you feel you will later challenge the violation.
2. Where the alleged hazard cannot be corrected immediately, be certain to request sufficient time to do so to avoid an additional failure to abate violation.
3. Questions regarding any alleged violations should be directed to corporate or other appropriate management personnel.

J. What to Say & Do When an OSHA Compliance Officer Arrives

The following is also a script as to what should be said and done when an OSHA compliance officer arrives at the job site.

Immediately notify _____.

Ask to see credentials — write down name or get business card.

Escort into office — have OSHA stay in office until decision made how to proceed.

Ask why inspection taking place — obtain copy of complaint if applicable.

Inform OSHA as follows:

"It is our Company policy to have _____ present at all OSHA investigations. I will call _____ now and let you know when _____ will be here. Usually, this will not be too much of a delay."

If OSHA objects and insists on proceeding, inform OSHA as follows:

"I cannot let you proceed until _____ arrives. You may review our OSHA records while you wait if you wish or you can leave and return at approximately _____ when I expect _____to arrive."

If OSHA asks if you are refusing entry to job site to perform inspection, inform OSHA as follows:

"No, I am only asking you to delay your inspection for a reasonable period of time to allow _____ to be here."

If OSHA continues to insist to proceed with inspection, contact _____ immediately to discuss further steps (search warrant request, asking OSHA to leave, etc.)

Notify all appropriate managers, foremen and subcontractors of impending OSHA inspection.

Littler Mendelson Offices

Atlanta, GA
404.233.0330

Boston, MA
617.378.6000

Charlotte, NC
704.972.7000

Chicago, IL
312.372.5520

Cleveland, OH
216.696.7600

Columbia, SC
803.231.2500

Columbus, OH
614.463.4201

Dallas, TX
214.880.8100

Denver, CO
303.629.6200

Fresno, CA
559.244.7500

Houston, TX
713.951.9400

Indianapolis, IN
317.287.3600

Irvine, CA
949.705.3000

Kansas City, MO
816.817.0735

Las Vegas, NV
702.862.8800

Los Angeles, CA
310.553.0308

Melville, NY
631.293.4525

Miami, FL
305.400.7500

Minneapolis, MN
612.630.1000

Mobile, AL
251.432.2477

Newark, NJ
973.848.4700

New Haven, CT
203.234.6344

New York, NY
212.583.9600

Northwest Arkansas
479.442.5134

Philadelphia, PA
267.402.3000

Phoenix, AZ
Littler Mendelson, P.C.
602.474.3600

Phoenix, AZ
Littler Mendelson Global Migration Law Group
602.256.6700

Pittsburgh, PA
412.201.7600

Portland, OR
503.221.0309

Providence, RI
401.454.2903

Reno, NV
775.348.4888

Sacramento, CA
916.830.7200

San Diego, CA
619.232.0441

San Francisco, CA
415.433.1940

San Jose, CA
408.998.4150

Santa Maria, CA
805.934.5770

Seattle, WA
206.623.3300

Stamford, CT
203.564.1449

Stockton, CA
209.472.7944

Tysons Corner, VA
703.442.8425

Walnut Creek, CA
925.932.2468

Washington, D.C.
202.842.3400

LITTLER MENDELSON, P.C.
600 Attorneys + 42 National Offices = One Integrated Solution
www.littler.com

Employment and Class Action Litigation | Unfair Competition and Trade Secrets | Employee Benefits | Labor Management Relations
HR Risk Management and Corporate Compliance | Workplace Safety | Global Migration