ELECTRONIC PAYMENT SYSTEMS AND THE ISSUES THEY GENERATE

D.M. Studler
Ronald G. Mund

I. INTRODUCTION

In the past, fidelity bond claims usually involved the theft of money or other assets by physical means. Now and in the future, crime claims will often involve theft by electronic transfers in various forms, including those involving Automated Clearing House[1] transfers, wire transfers, or payroll loaded cards. Money and paper checks are being replaced with an electronic medium of exchange. This article will provide an overview of such transactions and a helpful resource regarding electronic funds transfers systems and the regulations and laws governing them. This article discusses electronic fund transfers by plastic cards, wire transfers, and ACH Networks, including ACH history, concepts, and participants. It will also address the legal framework and regulatory rules governing fund transfers by electronic means with a view toward assessing their impact on fidelity and crime insurance coverage. The intent of this article is to provide the reader with a better understanding of electronic funds transfer systems and to serve as a resource for fidelity professionals.

II. THE HISTORY OF ACH TRANSACTIONS

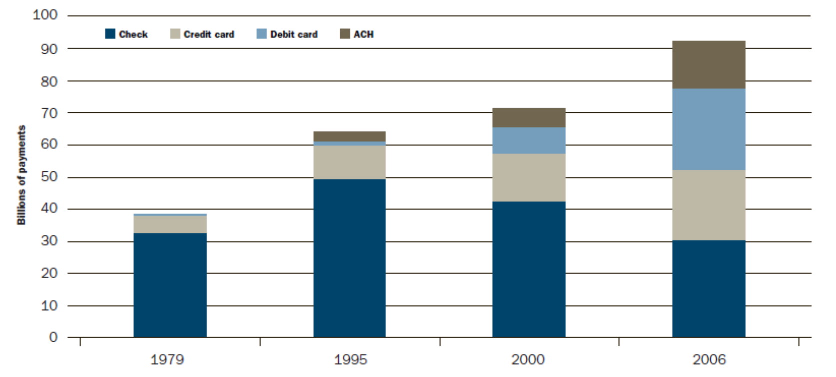
ACH-type transactions are derived from the need for a system based upon the distribution and settlement of credits and debits.

[1] Hereinafter ACH.

D.M. Studler, Member SDC CPAs, LLC in Aurora, Illinois. Ronald G. Mund, Director Financial Institution Bond and Crime Claims Travelers Bond and Financial Products Claims in Naperville, Illinois.

In the 1970s in response to the ever increasing volume of checks that threatened to overwhelm the traditional check clearing system, the ACH system was created.[2] ACH is "a nationwide electronic funds transfer (EFT) system that provides for the inter-bank clearing of credit and debit transactions and for the exchange of information among participating financial institutions.[3] Direct paycheck deposits is an example of EFTs that go through the ACH system. The ACH network, as we know it today, was born from a response to the overwhelming growth of check payments. The volume of checks written in the United States grew steadily throughout the 20th century and peaked in 1995 at 49.5 billion. Due to the rise in alternative payment forms, this number had decreased to 33 billion by 2006. Only cash (including debit cards) was used more often. The following chart from the Federal Reserve Bank of Atlanta illustrates U.S. retail payments and shows that ACH credit card, and debit card payments have increased steadily since 1995.[4]

Composition of U.S. retail payments by number of payments, selected years



Note: Check figures for 2006 do not include the estimated 2.6 billion checks that were converted to ACH transactions.
Sources: Gerdes and Walton (2002); Board of Governors (2007b)

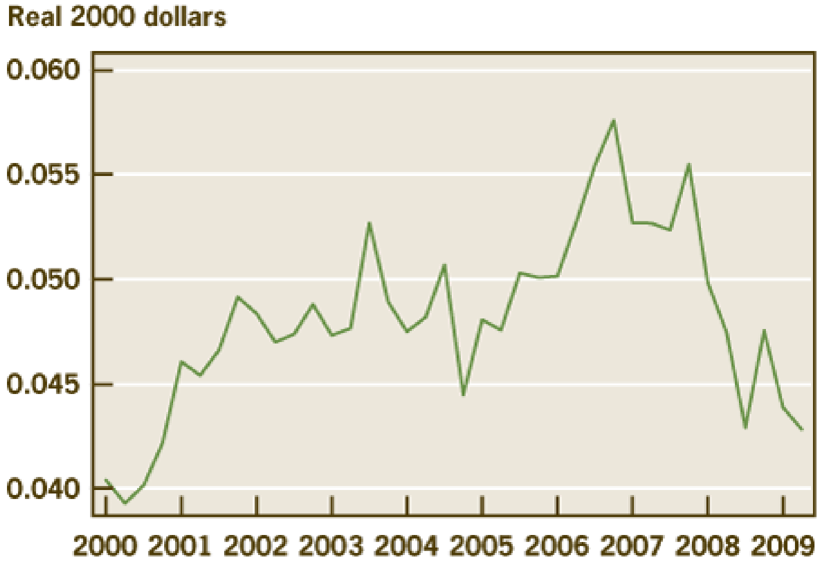
The convenience offered by checks has led to increased risks. Check losses increased by approximately five percent since the 1990s,

[2] What is ACH?, http://www.ach.com/What-is-ACH-.aspx (last visited Oct. 4, 2012).

[3] *Id.*

[4] Stephen Quinn & William Roberds, *The Evolution of the Check as a Means of Payment: A Historical Survey*, 93 ECON. REV. no. 4, at 23 (2008).

even though the aggregate value and number of checks written during that time declined.[5]



The demands of customer protection, financial institution risk management, and inefficient and costly check processing in a period of declining technology costs and increased technology volume and advances provided an opportunity for an efficient, less expensive and electronic alternative to checks. Innovation has increased the sophistication of the ACH system. The traditional distinction between checks and other non-cash payments, such as cards and ACH, is becoming obfuscated.[6]

The ACH transaction has no geographic or language restraint or restriction. "ACH transactions and networks are governed by operating rules and guidelines developed by the actual users of the ACH system

[5] Report to the Congress on the Check Clearing for the 21st Century Act of 2003, Board of Governors of the Federal Reserve System, at 2 (April 2007).

[6] Report, *supra* note 8.

and are administered through a series of agreements among financial institutions, customers, trading partners and ACH operators."[7]

III.
THE NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION

The National Automated Clearing House Association[8] was formed in 1974 to coordinate the United States ACH movement. A clearing house is a financial institution that provides clearing and settlement services for the financial and security industry. The purpose of clearing houses and NACHA is to ensure participants in the exchange honor their trade settlement obligations. Clearing houses are active in options, futures, payments, securities, and derivatives. Clearing houses can be private companies or the Federal Reserve Bank.

As a not-for-profit trade association, NACHA develops rules and business practices for the ACH network. NACHA's activities and initiatives facilitate the adoption of electronic payments for internet commerce, electronic bill payment and presentments, financial electronic data interchange, international payments, electronic checks, and electronic benefits transfer. NACHA also promotes the use of electronic payment products and services, such as direct deposit and direct payments.

NACHA brings together system stakeholder organizations through industry councils to encourage the efficient and effective utilization of the ACH network and to develop new ways to use the network to benefit stakeholders. While NACHA serves over 10,000 financial institutions, it does not service all institutions.

Through efforts of NACHA and the Federal Reserve Bank, local ACHs were electronically linked in 1978, which increased volume, improved efficiency, and reduced transaction costs.

[7] Quinn & Roberds, *supra* note 6, at 28.

[8] Hereinafter NACHA.

As of July 1, 2012, there are two ACH operators: the Federal Reserve and Electronic Payments Network.[9] In 2011, NACHA and Federal Reserve processed $33.91 trillion[10] and fifty-two percent of the commercial interbank ACH transactions. The Electronic Payments Network, the only private sector ACH operator, processed the remaining forty-eight percent.[11] Credit card payments are handled by separate networks. MasterCard and Visa serve as mandatory clearing houses for transactions on their networks.

ACH Network Operations is a store and forward batch processing system. Transactions received by financial institutions are gathered throughout various time periods, batched, and sorted by destination for transmission. The transmissions often occur at a predetermined time period. ACH provides economy of scale, unlike wire transfer, which we discuss later. The economy of scale with ACH transactions is one of the reasons for the cost differential between ACH transactions and wire transfers.

As depicted in the ACH Rules Handbook, participants in the ACH Network Operations include:[12]

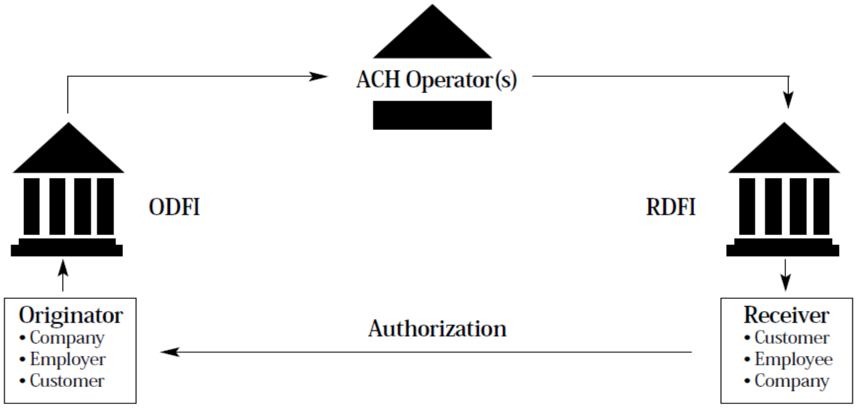
[9] Hereinafter EPN.

[10] *ACH Payment Volume Exceeds 20.2 Billion in 2011*, NACHA – The Electronic Payments Association (April 12, 2012).

[11] THE ELECTRONIC PAYMENTS NETWORK, http://www.epaymentnetwork.com/home php (last visited July 10, 2012).

[12] NACHA, ACH OPERATING RULES & GUIDELINES 1, Figure 1 (2010).

ACH Participants



In understanding the ACH network, one should be familiar with the following terms: (1) Originator: Any individual or Organization that initiates ACH debit or credit entries according to authorization from a Receiver; (2) Originating Depository Financial Institution:[13] A participating depository financial institution that receives ACH entries from Originators or Third-Party Senders and delivers ACH entries directly (or indirectly through a Third-Party Service Provider) to the ACH Operator; (3) Automated Clearing House Operator: ACH Operators are central clearing facilities through which financial institutions transmit or receive ACH entries;[14] (4) Receiver: An individual, corporation or other entity that has authorized an Originator to initiate a credit or debit entry to a transaction account held at an RDFI; (5) Third-Party Service Providers: A Third-Party Service Provider is an entity other than an Originator, ODFI or RDFI that performs any function on behalf of the Originator, ODFI or RDFI with respect to processing ACH entries; and (6) Third-Party Sender: A Third-Party Sender is a type of Third-Party Service Provider, which Originators or ODFIs use for outsourcing their payment services. The ODFI has an agreement with the Third-Party Sender, but does not have any direct agreements with the originators behind the Third-Party Sender. The

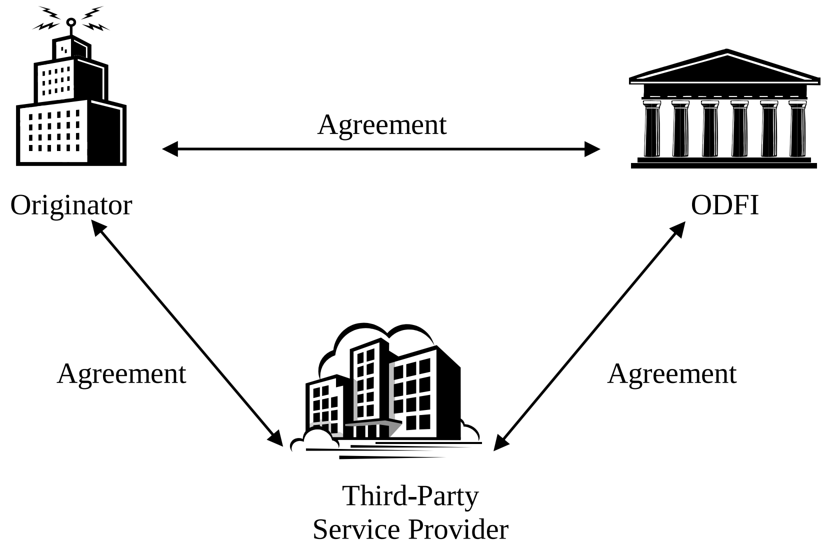
[13] Hereinafter ODFI.

[14] NACHA, ACH Risk Management Handbook 14 (5th ed. 2010).

Third-Party Sender is an intermediary between the Originator and the ODFI.[15]

The following two clients as depicted in the ACH Risk Management Handbook illustrate the differences between a Third-Party Service Provider Model and a Third-Party Sender Model:[16]

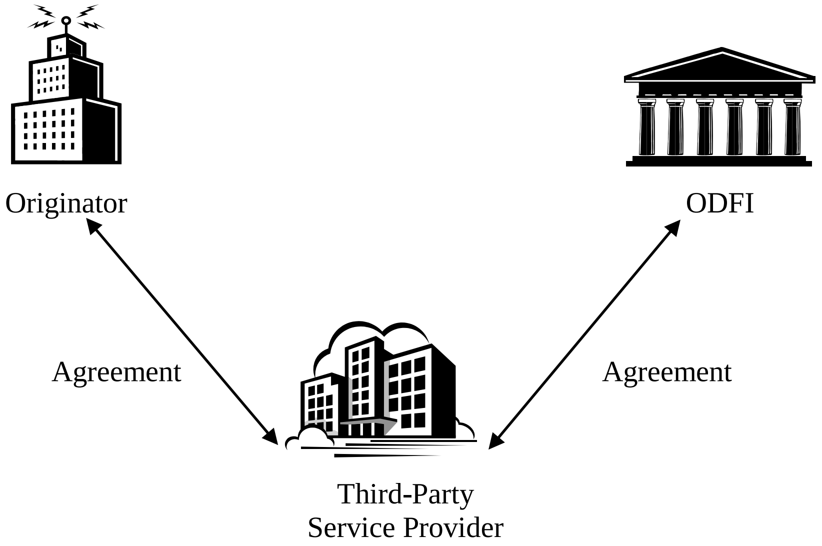
Third-Party Service Provider Model



In the Third-Party Service Provider Model, one Third-Party Service Provider is involved in the ACH origination process. The Originator has an agreement with the ODFI and the Third-Party Service Provider. The ODFI also has an agreement with the Third-Party Service Provider."[17]

[15] *Id.* at 15.
[16] *Id* at 15-16.
[17] *Id*.

Third-Party Sender Model



The Third-Party Sender Model also involves one Third-Party Service Provider in the ACH origination process. And, like the other model, the Originator has an agreement with the Third-Party Sender and the Third-Party Sender has an agreement with the ODFI. But in the Third-Party Sender Model, the Originator and the ODFI do not have an agreement.[18]

IV.
OTHER PAYMENT SYSTEMS

There are a myriad of reasons why people and businesses choose one payment instrument over another, including convenience, usage costs, familiarity, and access. All else being equal, check usage remains widespread because checks retain the properties that made them popular in the past. In addition, accepting a check does not require as much start-up infrastructure for a business as does accepting credit cards or debit

[18] *Id.*

cards.[19] Some experts believe the truncation of hard copies of checks and replacing them with digital images has extended the life of the check.[20] The trend in non-cash payments in the United States (payment by check, ACH, debit, credit and electronic benefits transfer)[21] increased from 81 billion to 93 billion from 2003 to 2006.[22] In 2009, the number increased to 109 billion payments with a value of $72.2 trillion.[23]

According to the Federal Reserve, electronic payments make up over 75% of all noncash payments by number and more than 50% of the value, broken down as follows:[24]

	Number	Value
Checks	22%	44%
ACH	18%	51%
Credit Card	20%	3%
Debit Card	35%	2%
Prepaid	5%	<1%

Wire transfers are different than ACH payments. There are two wholesale services: Fedwire Funds Service and Fedwire Securities Service. Fedwire Funds Service is for interbank funds transfers. Fedwire Securities Service is for the issuance, transfer maintenance and safekeeping of book-entry securities issued by the U.S. Treasury, Federal government agencies and certain international organizations. Fedwire Funds Service is a payment system, whereas Fedwire Securities Service

[19] Daniel Littman & Paul Bauer, *Are Consumers Cashing Out?*, Federal Reserve Bank of Cleveland (Oct. 1, 2007), *available at* http://www.clevelandfed.org/research/Commentary/2007/100107.cfm.

[20] Barkley Clark & Barbara Clark, *Federal Reserve Publishes Final Regulation Implementing Durbin Interchange Fee Limits*, 4 CLARKS' BANK DEPOSITS & PAYMENTS MONTHLY 7 (July 2011).

[21] Hereinafter EBT.

[22] Gerdes, *supra* note 9 at A77.

[23] FEDERAL RESERVE SYSTEM, THE 2010 FEDERAL RESERVE PAYMENTS STUDY 4 (Dec. 2010).

[24] FEDERAL RESERVE SYSTEM, THE 2010 FEDERAL RESERVE PAYMENTS STUDY - NONCASH PAYMENT TRENDS IN THE UNITED STATES: 2006-2009 14 (Apr. 2011).

is a delivery system that exchanges securities simultaneously for an agreed upon payment.

Wire transfers are processed:

1. Individually, not by batch.

2. In real-time, not held.

SWIFT is the Society for Worldwide Interbank Financial Telecommunications. SWIFT is a member-owned cooperative used by over 10,000 financial institutions and corporations in 212 countries.[25] SWIFT is a messaging infrastructure, not a payment system. The actual fund movements are completed through correspondent bank relationships, Fedwire, or CHIPS.

CHIPS stands for Clearing House Interbank Payment System and is an interbank payment system related to international trade used for the transfer of international monies. CHIPS is used by SWIFT or Fedwire.

There are many wire services, including: CHAPS and BOSNET and CHIPS. Money transfer services include, but are not limited to: Western Union, MoneyGram, Sterling Draft, and Kotok. Often these systems are considered the "legal" and "known." However, like Hawalas, risks exist because identifications and safewords are often fraudulent.

Card payments are increasing in usage. The number of payments made by debit card or EBT card grew by 12.8 billion from 2003 to 2006, reaching 48.1 billion.[26] Cards may be issued in the form of credit cards, charge cards, debit and prepaid debit cards and may offer an endless variety of incentives.

[25] SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATIONS, Company Information *at* http://www.swift.com/about_swift/company_information/index.page? (last visited July 4, 2012).

[26] Gerdes, *supra* note 9, at A81.

Charge cards and credit cards are not payment instruments, as there is no direct transfer of funds. Charge payment cards require settlement of entire funds at the end of the month or period, such as the widely known American Express Green card. Charge payment cards charge the merchants a fee for the use of a card. Credit cards also charge merchants fees for use. Credit cards are different than Charge cards, as the cardholder is granted a loan from the issuing financial institution, such as Visa and MasterCard.

Debit cards differ from charge cards and credit cards in the following ways. Debit cards fall into two categories—ATM only cards and ATM payment (open) cards. The holder of an ATM only debit card is limited to obtaining cash from an ATM. The holder of an ATM payment (open) card can obtain cash from an ATM and also use the ATM payment (open) card to make purchases directly from a merchant. Debit cards are exclusively issued by commercial banks and credit unions. Debit cards are linked to business bank accounts or personal bank accounts so that use of the debit card results in an immediate debit to the holder's bank account. Debit cards usually require a personal identification number for "online" debit.

Prepaid debit cards can be open or closed looped cards. Open loop prepaid debit cards are often also known as EBT. Large employers are using prepaid cards for issuing payroll to unbanked employees, literally putting net payroll values on "open" debit cards for employees to spend if they have no bank accounts. An open loop allows the prepaid debit card to be used anywhere. Another example of EBT cards are child support and unemployment disbursements by state benefit programs.

A closed loop card can only be used for purchases at the "private" sponsoring merchant. Examples include a prepaid debit card at Starbucks or for a municipality's transportation system. The cards can be "reloaded" and reused an unlimited number of times.

Who knows, but perhaps before long, consumers might be able to blink their eyes or provide fingerprints and pay their our obligations with the ever-changing technology of "electronic payments."

V.
RULES/REGULATIONS APPLICABLE TO PAYMENT SYSTEMS

The payments systems and processes operate through a series of legal agreements. Before any transaction is initiated, the originator and ODFI execute an agreement to use the ACH to originate payments. The agreement should bind the originating company to the NACHA Operating Rules, define the parameters of the relationship between the parties, identify processing requirements for specific application(s), and establish liability and accountability for procedures related to various applications.

While NACHA Operating Rules is the primary document addressing rules and regulations for the ACH network, Federal government ACH payments are controlled by provisions of Title 31 Code of Federal Regulations Part 21.[27] Other laws having a bearing on ACH operations include the Uniform Commercial Code[28] Article 4 that governs check transactions, Article 4A that governs credit funds transfers, and the Electronic Funds Transfer Act as implemented by Regulation E. Certain other activities related to ACH payments are affected by The Right to Financial Privacy Act,[29] Regulation D regarding reserve requirements, Regulation CC regarding funds availability, and the Dodd-Frank Act regarding remittances to foreign countries. Appendix A contains a table reflecting the various electronic payment systems and applicable laws and regulations in a summary format for quick reference.

VI.
FUNDS TRANSFERS UNDER ARTICLE 4A UNIFORM COMMERCIAL CODE

A. Application of Article 4A

A credit funds transfer is one in which the originator initiates a transfer to move funds from the originator's account into the receiver's

[27] 31 C.F.R. §§ 21.100 – 21.605 (2012).

[28] Hereinafter UCC.

[29] 12 U.S.C. §§ 3401 *et seq.* (2012).

account.[30] In simpler terms, this can be referred to as a "push transfer" the originator is pushing funds from the originator's account to the receiver's account. Electronic payroll deposits are one example of a credit funds transfer.

A debit funds transfer is one in which the originator initiates a transfer to move funds from the receiver's account to the originator's account.[31] In simpler terms, this can be described as a "pull transfer;" the originator is pulling funds from the receiver's account causing the receiver's account to be debited. A preauthorized withdrawal of funds by a utility company from a customer's account is one example of a debit funds transfer.

Article 4A of the UCC applies to credit funds transfers[32] made through a funds transfer system[33] except for funds transfers governed by the Electronic Funds Transfer Act of 1978[34] and Regulation E[35] issued by the Board of Governors of the Federal Reserve System pursuant thereto.[36] The primary purpose of Regulation E is to protect individual consumers engaging in electronic fund transfers,[37] which only includes natural persons.[38] But U.C.C. Article 4A is limited to credit funds

[30] NACHA, UNDERSTANDING THE ACH NETWORK: AN ACH PRIMER 3 (2008).

[31] *Id.* at 4.

[32] U.C.C. § 4A-104 (2011) ("'Funds transfer' means the series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator's bank or an intermediary bank intended to carry out the originator's payment order. A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order.").

[33] *Id.* § 4A-105(5) ("'Funds-transfer system' means a wire transfer network, automated clearing house, or other communication system of a clearing house or other association of banks through which a payment order by a bank may be transmitted to the bank to which the order is addressed.").

[34] Electronic Fund Transfer Act of 1978, Pub. L. No. 95-630, § 902, 92 Stat. 3728 (1978).

[35] 12 C.F.R. §§ 205.1 – 205.20.

[36] U.C.C. § 4A-108.

[37] 12 C.F.R. § 205.1(b).

[38] *Id.* at § 205.1.

transfers made through a funds transfer system by businesses. Simply because a funds transfer made through a funds transfer system involves an account in the name of a natural person or persons, does not necessarily mean that Article 4A is inapplicable. If the transaction's purpose is commercial or based on a profit motive, it will not be considered to be a consumer transaction.

Article 4A does not apply to debit funds transfers.[39] The comments in the UCC explain the limitations on the applicability of Article 4A to particular transactions.

> The Electronic Fund Transfer Act of 1978 is a federal statute that covers a wide variety of electronic funds transfers involving consumers. The types of transfers covered by the federal statute are essentially different from the wholesale wire transfers that are the primary focus of Article 4A. Section 4A-108 excludes a funds transfer from Article 4A if any part of the transfer is covered by the federal law. Existing procedures designed to comply with federal law will not be affected by Article 4A. The effect of Section 4A-108 is to make Article 4A and EFTA mutually exclusive. For example, if a funds transfer is to a consumer account in the beneficiary's bank and the funds transfer is made in part by use of Fedwire and in part by means of an automated clearing house, EFTA applies to the ACH part of the transfer but not to the Fedwire part. Under Section 4A-108, Article 4A does not apply to any part of the transfer. However, in the absence of any law to govern the part of the funds transfer that is not subject to EFTA, a court might apply appropriate principles form Article 4A by analogy.[40]

Effective in 2013, Section 1073 of Dodd-Frank Wall Street Reform and Consumer Protection Act[41] amends the EFTA by adding

[39] U.C.C. § 4A-104 cmt.4.

[40] *Id*.

[41] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301).

Section 919 Remittance Transfers. A Remittance Transfer "means the electronic (as defined in section 106(2) of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. § 7006(2)) transfer of funds requested by a sender located in any State to a designated recipient that is initiated by a remittance transfer provider, whether or not the sender holds an account with the remittance transfer provider or whether or not the remittance transfer is also an electronic fund transfer, as defined in section 1693a of this title."[42] Because a Remittance Transfer will now be governed under the EFTA, it will no longer be governed under Article 4A.

The Permanent Editorial Board has proposed changing Article 4A to more clearly specify this effect:

> Sec. 4A-108. Relationship to Electronic Fund Transfer Act.
>
> (a) Except as provided in subsection (b), this Article does not apply to a funds transfer any part of which is governed by the Electronic Funds Transfer Act of 1978 (Title XX, Public Law 95-630, 92 STAT. 3728,15 U.S.C. Sec. 1693 et seq.) as amended from time to time.
>
> (b) This Article applies to a fund transfer that is a remittance transfer as defined in the Electronic Fund Transfer Act (15 U.S.C. Sec. 1693o-1) as amended from time to time, unless the remittance transfer is an electronic funds transfer as defined in the Electronic Fund Transfer Act 15 U.S.C. Sec 1693a as amended from time to time.
>
> (c) In a funds transfer to which this Article applies, in the event of an inconsistency between an applicable provision of this Article and an applicable provision of the Electronic Fund Transfer Act, the provision of the Electronic Fund Transfer Act governs to the extent of the inconsistency.

[42] 15 U.S.C. § 1693o-1(g)(2).

B. Authorized Payment Orders

Under Article 4A, a payment order[43] initiating a credit funds transfer is authorized if the person identified as the sender is the person who authorized the payment order. A payment order initiating a credit funds transfer is also authorized if the sender is bound by the law of agency.[44] In simple terms, if the customer is the person who initiated the payment order, or if a person authorized by the customer to initiate payment orders initiated the payment order, it is an authorized payment order.

C. Effective Payment Orders

A payment order initiating a credit funds transfer is effective as the order of the bank's customer, whether or not authorized, if:

- The bank and the customer have agreed that the authenticity of a payment order initiating a credit funds transfer will be verified pursuant a security procedure;[45]

[43] U.C.C. § 4A-103 ("'Payment order' means an instruction of a sender to a receiving bank, transmitted orally, electronically, or in writing, to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary if: (i) the instruction does not state a condition to payment to the beneficiary other than time of payment; (ii) the receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender; and (iii) the instruction is transmitted by the sender directly to the receiving bank or to an agent, funds-transfer system, or communication system for transmittal to the receiving bank.").

[44] *Id*. § 4A-202(a).

[45] *Id*. § 4A-201 ("'Security procedure' means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.").

- The security procedure is a commercially reasonable method of providing security against unauthorized payment orders; and

- The bank proves it accepted the payment order in good faith and in compliance with the security procedure; and any written agreement or instruction of the customer restricting acceptance of payment orders in the name of the customer.[46]

Whether a security procedure is commercially reasonable is a question of law determined by considering: (1) the wishes of the customer expressed to the bank; (2) the circumstances of the customer known to the bank, including size, type, and frequency of payment orders normally issued by the customer; and (3) the security procedures in general use by customers and receiving banks similarly situated. A security procedure will be deemed to be commercially reasonable if: (1) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (2) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in the customer's name and accepted by the bank in compliance with the security procedure chosen by the customer.[47]

D. Exception To Enforcement Of Effective Payment Orders

A receiving bank is not entitled to enforce or retain payment of a payment order that is effective as the payment order of the customer if the customer proves the payment order initiating the credit funds transfer was not caused, directly or indirectly: (1) by person entrusted at any time with the duties to act for the customer with respect to payment orders or the security procedure, or (2) by a person who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank,

[46] *Id.* § 4A-202(b).

[47] *Id.* § 4A-202 (c).

information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault.[48]

E. Liability Of Financial Institution

1. Liability Under Article 4A-202(a)

A bank is not liable to return funds to its customer for a payment order initiating a credit funds transfer if the payment order is an authorized payment order under Section 4A-202(a). The issues of authorization was addressed in *Skyline International Development v Citibank F.S.B.*[49] In that case, Eric Chang, a principal in Skyline, gave Citibank instructions to wire transfer $16,000 to the Beijing Peace Hotel's account at Bank of China. After Citibank issued the wire transfer, Citibank requested Chang sign the wire transfer form. Chang then made a telephone call on his cell phone to confirm the information on the wire transfer form. He then told Citibank he had made a mistake and needed to change the beneficiary on the wire transfer from the account of Beijing Peace Hotel to the account of Jin Liu at Bank of China. Citibank advised him that the wire transfer had already been sent but it would be cancelled or recalled. Chang then instructed Citibank to wire transfer $16,000 to the account of Jin Liu at Bank of China and signed the wire transfer form authorizing that wire transfer. Citibank then completed a wire transfer recall form for the first wire transfer and faxed it to Citibank's central wire transfer processing facility.[50] Approximately one month later, Citibank notified Skyline its account would be debited for the $16,000 wire transfer to the Beijing Peace Hotel at the Bank of China.

Skyline filed suit against Citibank asserting a claim for an unauthorized wire transfer. The Illinois Appellate Court reversed the trial court's grant of summary judgment to Skyline on the unauthorized wire transfer claim because it found Section 4A-202(a) refers to identity authorization and Chang was authorized to act on behalf of Skyline.[51] So according to the *Skyline* court, the controlling issue under 4A-202(a)

[48] *Id.* § 4A-203 (a).
[49] 706 N.E.2d 942 (Ill. App. Ct. 1998).
[50] *Id* at 944.
[51] *Id* at 947.

is not whether the actual transfer was authorized, but merely whether the person initiating the transfer had the authority to do so.

2. Liability Under Article 4A-202(b)

Whether a bank is liable to return funds to its customer for a payment order initiating a credit funds transfer if the payment order is effective as the payment order of its customer depends on whether the requirements of UCC 4A-202(b) have been met. Under UCC 4A § 202(b), the customer bears the risk of loss if it: (1) agreed to a security procedure; (2) the security procedure was commercially reasonable; and (3) the bank accepted the payment orders in good faith and in compliance with the security procedure and any relevant written agreement or instruction from the customer.

a. Commercially Reasonable Security Procedure

In *Regatos v. North Fork Bank*,[52] the court found that a security procedure involving a comparison of a signature and a confirming telephone call from the customer was commercially reasonable:

> The default rule of the UCC is that the bank will bear the loss of any unauthorized funds transfer. That rule is subject to a broad exception when the bank and its customer agree on a "security procedure" to ensure that payment orders received by the bank are authorized and error free. Specifically, if such a security procedure is in place, the loss from an unauthorized funds transfer will be shifted to the customer where the security procedure is commercially reasonable, and the bank accepted the payment order (i) in good faith and (ii) in compliance with the security procedure. "[R]ights and obligations arising under this section may not be varied by agreement," except in certain ways that are not at issue here.

[52] 257 F. Supp. 2d 632 (S.D.N.Y. 2003), *aff'd*, 431 F.3d 394 (2d Cir. 2005).

> The general liability rules of section 4-A-202 may be varied by agreement in two ways. First, a bank is not required to accept a payment order that violates a written agreement. For example, the bank and its customer may have agreed that a funds transfer that creates an overdraft will not be accepted, or that the customer may only send funds transfers to certain listed beneficiaries. Second, a bank can be relieved of using a commercially reasonable security procedure without shouldering any loss if (a) the bank offered but the customer rejected a commercially reasonable security procedure, and (b) the customer agreed in writing to be bound by unauthorized or erroneous funds transfers.
>
> A payment order accepted in good faith pursuant to a commercially reasonable security procedure is said to be "effective" as the order of the customer because it can be properly verified. Such an order is effective even if it is actually unauthorized, as in the case of a perfect forgery.
>
> Section 4A-203 provides two instances, however, where a customer will not be obliged to bear the loss of an unauthorized yet effective funds transfer: (1) where the parties specifically so agree; and (2) when the payment order was (i) not issued by the account holder or her agent; and (ii) not issued by someone who gained knowledge of the security procedure from the account holder or her agent. The customer has the burden of proving that the second instance applies. When it does, however, Article 4A places the risk of so-called "interloper fraud" on the bank, rather than the customer.
>
> But where a payment order is not effective—or where a payment order is unauthorized and there is no security procedure in place—the bank has an invariable duty to refund the lost funds . . . .[53]

[53] *Id.* at 640-41 (citations omitted).

In *Brago Filho v. Interaudi Bank*,[54] the court was asked to decide whether the parties agreed to a security procedure for validating wire transfers and whether the security procedure was commercially reasonable under section 4A-202(2) of the New York UCC. The plaintiffs, citizens of Brazil, opened an account at defendant's headquarters in New York City. When the account was opened, the plaintiffs signed a "Telecommunications Instructions Authorization/ Indemnification Agreement" that provided that the Bank was authorized: "to accept and immediately act upon instructions from [the customer] via telephone, telegram, telefacsimile, untested telex, electronic mail, or any other means of telecommunications."[55] The agreement further provided that the defendant would, "select security procedures for accepting instructions that are commercially reasonable for [the Bank]."[56] The plaintiffs gave the defendant their home telephone number and an unidentified cell phone number that may have been the plaintiffs' former work number. In addition, the plaintiffs signed an agreement authorizing the defendant to hold their mail which meant the plaintiffs received their bank statements by mail.[57]

The defendant's internal document titled "Funds Transfer Policy and Procedures" provided that the signature on the written request for all transfer requests had to be verified by comparison to the signature card on file, and for a fax transfer request, the request had to be confirmed by a call to or a call from the customer.[58] The customer had provided answers to questions including, but not limited to, mother's maiden name, identification number and last deposit made.[59] The plaintiffs were paid approximately $1.7 million dollars in cash for work as a sales representative. The plaintiffs delivered the cash to Hajjar and Nicholas. Hajjar deposited the cash into his account at the defendant and then transferred it to the plaintiffs' account. Between February 13, 2001, and August 6, 2001, seventeen wire transfers totaling $950,924.00 were

[54] No. 03 Civ. 4795 (SAS), 2008 U.S. Dist. LEXIS 31443 (S.D.N.Y. Apr. 16, 2008).

[55] *Id.* at 2.

[56] *Id.*

[57] *Id.* at 5.

[58] *Id.* at 16

[59] *Id.*

initiated by facsimiles received by the Defendant.[60] Citing *Regatos v. North Fork Bank*,[61] the Court held the defendant's procedures were commercially reasonable even though the plaintiff's argument that a requirement that the bank initiate the confirmation call and require a password would have increased security.[62]

b. Acceptance in Good Faith

Regatos and *Brago Filho* shed some light on what constitutes a commercially reasonable security procedure which is only one element of the section 4A-202 test that a bank must satisfy to escape liability for an unauthorized transfer. Section 4A-202 also requires that the transfer request be accepted in good faith. The court addressed this issue in *Experi-Metal, Inc. v. Comerica Bank*.[63] Before addressing the issue of good faith, the court first examined whether plaintiff had proved that Comerica Bank's security procedures were commercially reasonable. The court rejected Experi-Metal's expert testimony as to what would meet industry or commercial standards for accepting the payment orders as follows, indicating the difficulty a plaintiff may have in proving this point:

> Mr. James testified that industry standards required Comerica to engage in fraud scoring and fraud screening, which would have immediately stopped the wire transfers based on certain variables and risk factors. These variables and risk factors include, but are not limited to, the following: the limited prior wire transfer activity in Experi-Metal's accounts (only two transfers initiated in prior years, both in 2007); the length of Experi-Metal's prior online sessions compared to the criminal's session on January 22, 2009; the pace at which the payment orders were entered on January 22, 2009; the destinations of the wire transfers (Moscow,

[60] *Id.* at 8.

[61] 257 F. Supp. 2d 632 (S.D.N.Y. 2003), *aff'd*, 431 F.3d 394 (2d Cir. 2005).

[62] *Id.* at 646.

[63] No. 09-14890, 2011 U.S. Dist. LEXIS 62677 (E.D. Mich. June 13, 2011).

> Estonia, and China); and the identities of the beneficiaries (individuals, many with Russian-sounding names). According to Mr. James, a "[m]ajority of the banks" have implemented monitoring systems to detect fraudulent activity.
>
> Even Paul Carrubba, Comerica's expert witness, acknowledged that "some banks" were moving to fraud monitoring systems as of January 2009.
>
> Mr. James failed to convince this Court, however, that on January 22, 2009, a bank had to provide fraud monitoring with respect to its commercial customers to comport with "reasonable commercial standards of fair dealing." While the evidence suggests that the Federal Financial Institution Examination Council's Handbook provides guidance to banks with respect to its commercial customers, express security mechanisms outlined in the handbook are not mandatory for those customers. Mr. James was not specific as to which banks have adopted fraud monitoring. He identified by name only a few banks that have done so. However, and perhaps most importantly, he failed to inform the Court as to when a "majority of the banks" or even the few banks he named implemented fraud monitoring systems. No evidence was presented to the Court from which it can conclude that banks comparable in size to Comerica utilized fraud screening and fraud scoring as of the date of the incident at issue in this lawsuit.[64]

Nonetheless, the court found that Comerica had not accepted $1.7 million in wire transfer payment orders in good faith:

> Over the next several hours, the criminal initiated 97 wire transfer payment orders from Experi-Metal's Sweep Account, totaling more than $1.9 million. There are a number of considerations relevant to whether Comerica acted in good faith with respect to this

[64] *Id.* at 32-33.

> incident: the volume and frequency of the payment orders and the book transfers that enabled the criminal to fund those orders; the $5 million overdraft created by those book transfers in what is regularly a zero balance account; Experi-Metal's limited prior wire activity; the destinations and beneficiaries of the funds; and Comerica's knowledge of prior and the current phishing attempts. This trier of fact is inclined to find that a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier. Comerica fails to present evidence from which this Court could find otherwise.[65]

Thus, according to this court, a bank cannot accept payments in good faith where it has ignored obvious red flats of unauthorized transfers.

In *Skyline International Development v. Citibank*,[66] the Illinois Appellate Court held that Skyline could not recover under section 4A-202(b) because, although Citibank acknowledged it had not followed its own internal security procedure when it made the wire transfer, that did not give rise to its liability because a security procedure is defined to be an agreement between the customer and a bank, not a unilateral practice followed by the bank. As noted by the court:

> The official comment to section 4A-201, states that "[t]he definition of security procedure limits the term to a procedure 'established by agreement of a customer and a receiving bank.' The term does not apply to procedures that the receiving bank may follow unilaterally in processing payment orders."[67]

A discussion of commercially reasonable security procedure would be remiss without referring to the Recommended Decision On Cross Motions For Summary Judgment of the United States Magistrate

[65] *Id.* at 37-38.
[66] 706 N.E.2d 942 (Ill. App. Ct. 1998).
[67] *Id.* at 945.

Judge in *Patco Construction Company v. Peoples United Bank*,[68] which was affirmed by the United States District Court but recently reversed by the First Circuit Court of Appeals. The forty-seven page Recommended Decision contains an extensive discussion of security procedures and recommended summary judgment in favor of Peoples Bank. The Bank utilized an authentication system provided by a third-party vendor that offered a basic product and a premium product. The Bank chose the more costly premium product with, among others, the following features: (1) both a company ID and password and an individual user ID and password were required to access the online banking system; (2) users were required to select three challenge questions and responses for use during login which would be triggered for various reasons; (3) risk profiling which built a risk profile for each customer based on the IP address used to log in, a device cookie placed on the customer's computers which identified the computer the customer customarily used to log in, Geo location to show the location from which the customer logged in; (4) recording of transaction activity (when, how often, and what the user did when logged in); (5) a dollar threshold set by the Bank that would trigger the challenge questions even if the user ID, password, and device cookie were valid; and (6) a subscription to eFraud Network which compared characteristics of the transaction, including the IP address of user seeking access, with those of known instances of fraud. Some of these features operated in the background unseen by the customer.[69]

An unknown party initiated a series of ACH transfers over the course of several days from Patco's account resulting in a loss of $345,445. The court explained the fraud and the bank's response:

> The perpetrators logged in from a device unrecognized by [Bank's] system, and from an IP address that Patco had never before used. The risk-scoring engine generated a risk score of 790 for [first transaction]. The risk-scoring engine reported the following contributors to the risk score for that transaction: (i) "'Very high risk non-authenticated device'; (ii) 'High risk transaction

[68] No. 2:09-cv-503-DBH, 2011 U.S. Dist. LEXIS 58112 (D. Me. May 27, 2011).

[69] *Id.* at 39.

> amount'; (iii) 'IP anomaly; and (iv) 'Risk score distributor per cookie age.'"[70]

Patco brought suit seeking to recover the loss asserting six Counts: (I) U.C.C. § 4A-201 *et seq*.; (II) negligence; (III) breach of contract; (IV) unjust enrichment; (V) and (VI) conversion. The UCC claims appear to be based on the claim that the Bank's security procedures were not commercially reasonable under Article 4A-202(b) since it was not a true multifactor authentication procedure and that Patco had not agreed to the security procedure.

The Recommended Decision discusses the guidance issued in October 2005, by the Federal Financial Institutions Examination Counsel which is entitled "Authentication in an Internet Banking Environment" as follows:

> The Guidance does not endorse any particular technology for compliance with the Guidance. The Guidance states that "financial institutions should periodically . . . [a]djust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information[.]" The Guidance also provides that "'where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multi factor authentication, layered security, or other controls reasonably calculated to mitigate those risks."
>
> The Guidance explains that existing authentication methodologies involve three basic "factors": (i) "[s]omething the user *knows* (e.g., password, PIN); (ii) [s]omething the user *has* (e.g., ATM card, smart card); and (iii) [s]omething the user *is* (e.g., biometric characteristic, such as a fingerprint)."
>
> It states:

[70] *Id.* at 72 (citations omitted).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out-of-band" controls for risk mitigation.

"Out-of-band generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction." FFIEC Guidance at 3 n. 5. "Callback (voice) verification, e-mail approval or notification, and cell-phone based challenge/response processes are some examples."

The Guidance also states:

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties . . . . Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Financial institutions further are advised to "[a]djust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of [their] customer information, and internal or external

> threat to information" and to "implement appropriate risk mitigation strategies."[71]

Patco did not assert that the bank failed to act in good faith. It asserted that the security procedure was not commercially reasonable or, in the alternative, it did not agree to it or the security procedures to which it agreed alone were not commercially reasonable. The magistrate judge found that Patco had agreed to the security procedures because it expressly agreed to the use of security passcodes and "it agreed by course of performance to the use of challenge questions, having cooperated in setting up answers to such questions and having answered them in the course of conducting eBanking . . . ." Although some aspects of the security system were invisible and unknown to Patco, such as device authentication, IP Geo location, transaction monitoring, and a risk-profiling engine, the court found that "Patco can be fairly said to have agreed to the use of the Premium Product security system in *toto*," because the unknown features were "integrated with, and largely operated in the service of the visible portions of systems." The court also found it important that Patco had effectively agreed to the "Modified eBanking Agreement" even though it claimed it had never seen the agreement because "the Bank reserve the right in the original eBanking Agreement to modify the terms and conditions of that agreement at any time effective upon publication," and the modified agreement had been posted online.[72]

The court also rejected Patco's argument that the security procedures were not commercially reasonable:

> Patco asserted that the security procedure was not commercially reasonable because the Bank has set the set the dollar threshold at which the challenge questions were asked at $1.00 thereby reducing the security system to a single factor security system because that meant the challenge question had to be answered for every transaction making them far more susceptible to being uncovered by key tracking malware. In other words,

[71] *Id.* at 25-28 (citations omitted; emphasis added).
[72] *Id* at 104-106.

> Patco asserted the security procedure was not commercially reasonable because it was not a multifactor system.
>
> It further asserted that since, ". . . the Bank's invisible device ID (the asserted second factor) and the profiling engine (the asserted third factor) acted only as triggers for the challenge questions (part of the first factor) rather than, for example, denying access to the system."[73]
>
> . . . .
>
> It is apparent, in the light of hindsight, that the Bank's security procedures in May 2009 were not optimal. The Bank would have more effectively harnessed the power of its risk-profiling system if it had conducted manual reviews in response to red flag information instead of merely causing the system to trigger challenge questions. Indeed, it commenced manual reviews in the wake of the transactions at issue here.[74]
>
> . . . .
>
> A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard.[75]

On July 3, 2012, the First Circuit Court of Appeals entered a forty-three page order[76] reversing the grant of summary judgment in

[73] *Id.* at 116.

[74] *Id* at 133.

[75] *Id.* at 111.

[76] *Patco Constr. Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012).

favor of the bank, affirmed the denial of Patco's summary judgment motion and remanded for further proceedings stating: "On remand the parties may wish to consider whether it would be wiser to invest their resources in resolving this matter by agreement."[77] The Order left open the questions of what, if any, obligations or responsibilities, Patco had under Article 4A and reinstated Patco's claims.[78]

c. ***Liability Generally***

(i) **Debit Transfers**

The court in *Grabowski v. Bank of Boston*[79] addressed liability for debit transfers. *Grabowski* involved funds transfers from accounts of investors at Bank of Boston by Norman Epstein pursuant to a power of attorney from each investor to accounts under his control at other banks. Bank of Boston contended the funds transfers were debit transfers because they were initiated by the beneficiary of the transfer. However, the court found that Article 4A of the UCC does not apply to "debit transfers."[80]

(ii) **Notice/Statute of Limitations**

Article 4A-505 requires that the customer give notice of the customer's objection to payment to the financial institution within one year after the notification of the payment was received by the customer.[81] However, in *Grabowski* the court held that this was only a notice

[77] *Id.* at 216.

[78] *Id.*

[79] 997 F. Supp. 111 (D. Mass. 1997).

[80] *Id.* at 121-22.

[81] U.C.C. § 4A-505 ("If a receiving bank has received payment from its customer with respect to a payment order issued in the name of the customer as sender and accepted by the bank, and the customer received notification reasonably identifying the order, the customer is precluded from asserting that the bank is not entitled to retain the payment unless the customer notifies the bank of the customer's objection to the payment within one year after the notification was received by the customer.").

deadline condition precedent to recovery, not a statute of limitations for purposes of filing suit.[82]

(iii) Modification of Article 4A

Bank of Boston also argued in *Grabowski* that it was not liable to certain plaintiffs because the Commercial Deposit Account Agreement contained a provision that relieved the bank from liability for unauthorized transfers. However, the court found this provision unenforceable under Article 4A, stating:

> Under section 202(a) of article 4A, a bank is liable for unauthorized funds transfers. However, under section 4A-202(b) this default rule is subject to variation by agreement if a bank and its customer agree on a security procedure for verification of the authenticity of a payment order. Such an agreement places the risk of loss on the customer for unauthorized payment orders if an unauthorized payment order is accepted by a receiving bank after verification by the bank in compliance in good faith with a commercially reasonable security procedure. However, except to the extent just stated, rights and obligations relating to authorized and verified payment orders "may *not* be varied by agreement."[83]

(iv) Liability of Intermediary Bank

In *Grain Traders, Inc. v. Citibank, N.A.,*[84] the Second Circuit Court of Appeals ruled that Article 4A precluded an action against an intermediary bank in an electronic funds transfer. In brief, Grain Traders issued a payment order to Banco de Credito Nacional[85] to debit its account in the amount of $310,000.00 and transfer the funds to the account of Banque Du Credit Et Investissement, LTD[86] Beneficiary Claudio Godianich Kramers—under fax advise To Banco Extrader.

[82] 997 F. Supp. at 119-20.
[83] *Id.* at 120 (citations omitted).
[84] 160 F.3d 97 (2d Cir. 1998).
[85] Hereinafter BCN.
[86] Hereinafter BCIL.

Upon receipt of the payment order, Citibank, operating as an intermediary bank, debited BCN's account at Citibank and credited the amount to BCIL's account at Citibank. Pursuant to the payment order, Citibank then issued a payment order to BCIL for the further transfer to the beneficiary. Both BCIL and Banco Extrader became insolvent. Grain Traders then requested that BCN request cancellation of the payment order. After several attempts to contact BCIL, Citibank received a message from BCIL that authorized the debit of BCIL's account. However, by then Citibank had determined that BCIL had exceeded its credit limit and placed a "debit-no post" status on BCIL's account.[87] The Second Circuit upheld the district court's finding that Article 4A established a cause of action only by a sender against the sender's receiving bank, stating:

> In reaching its conclusion, the district court relied on the plain language of Section 402(4) as well as other provisions of Article 4-A. It found that the language of Section 402(4) establishes a right of refund only between a sender and the receiving bank it paid. BCN, not Grain Traders, was the sender that issued the payment order to Citibank and paid Citibank by having its account debited in the amount of $310,000. Grain Traders argues that the fact that Section 402(4) does not use the words "receiving bank" but instead refers to "the bank receiving payment" means that the sender can sue any bank in the chain that received payment. We agree with Citibank that because the words "receiving bank" are defined as the bank that receives a payment order, Section 402(4)'s use of the words "bank receiving payment" simply clarifies that the right to a refund arises only after the sender has satisfied its obligation to pay the receiving bank.

[87] *Id.* at 98-99.

(v) Exclusivity of Article 4A

The district court in *Grain Traders*[88] also dismissed the common law claims of conversion and money had and received against Citibank on the grounds that Grain Traders could not establish essential elements of those claims. While the Second Circuit of Appeals upheld the dismissal of Grain Traders' common law claims, it did so on the grounds that they were barred by Article 4A stating:

> Article 4-A was enacted to correct the perceived inadequacy of 'attempt[ing] to define rights and obligations in funds transfers by general principles [of common law] or by analogy to rights and obligations in negotiable instruments law or the law of check collection.' The Official Comment to Section 4-A-102 states that the provisions of Article 4-A represent a careful and delicate balancing of [competing] interests and are intended to be the exclusive means of determining the rights, duties, and liabilities of the affected parties in any situation covered by particular provisions of the Article. Consequently, resort to principles of law or equity outside of Article 4A is not appropriate to create rights, duties and liabilities inconsistent with those stated in this Article.
>
> We agree with those courts that have interpreted the above language to preclude common law claims when such claims would impose liability inconsistent with the rights and liabilities expressly created by Article 4-A.[89]

Three years earlier in *Sheerbonnet v. American Express Bank*,[90] the same court found that Article 4A did not preclude a common law cause of action under the unique circumstances of the transaction. Sheerbonnet, Ltd. sold troop carriers to Hady Establishment, a Saudi Arabian company. For payment, Hady obtained an irrevocable letter of credit from Banque Scandanave. Upon completing the contract,

[88] *Id*.
[89] *Id.* at 102-03 (citations omitted).
[90] 951 F. Supp. 403 (S.D.N.Y. 1995).

Sheerbonnet requested payment be made in U.S. Dollars by funds transfer to its account at Bank of Credit and Commerce[91] in London. Banque Scandanave initiated payment on July 3rd, instructing its correspondent bank in New York (Northern Trust) to transfer $12.4 million to American Express Bank for credit to BCCI's account at American Express Bank in New York. Prior to the transfer, regulators in England & Luxembourg suspended the operations of BCCI and the United States Federal Reserve Board advised American Express Bank of the suspension of BCCI accounts worldwide, including seizure of BCCI's New York operations. Upon receipt of the transfer from Northern Trust, American Express Bank, while knowing the accounts of BCCI has been frozen, credited the funds to BCCI's account at American Express Bank. Because of the freezing of BCCI's assets, the funds remained were not transferred to Sheerbonnet's account at BCCI in London and American Express Bank asserted a right to set off the funds in the account against debts owed to it by BCCI.[92]

First, the court concluded that "the exclusivity of Article 4-A is deliberately restricted to 'any situation covered by particular provisions of the Article.' Conversely, situations not covered are not the exclusive province of the Article."[93] Second, the court determined that Sheerbonnet's common law causes of action were not inconsistent with Article 4 A and thus not barred by Article 4 A. The Court appeared to focus on the fact that American Express Bank transferred the funds knowing that it would offset the funds for its own benefit with knowledge that the accounts of BCCI had been frozen.

> Sheerbonnet does not complain of an erroneous instruction or execution in the processing of Northern Trusts payment order, causing it to be credited to the wrong party, or in the wrong amount, or at the wrong time. Ironically, we are here now because AEB apparently followed its instructions to the letter. Sheerbonnet argues that in light of the unprecedented and superseding seizure of BCCI, AEB's decision to credit the BCCI London Account, knowing that it was

[91] Hereinafter BCCI.

[92] *Id.* at 405.

[93] *Id.* at 407-08.

> frozen and knowing that AEB would use these very funds as a $12.4 million set-off against BCCI's debt to AEB, was an exercise in self-serving, tortuous tunnel vision. AEB did not ask either the originator or the beneficiary how they would like to proceed in light of the seizure, nor did it confer with the Superintendent of Banks.[94]

In *Hedged Investment Partners, L.P., v. Norwest Bank Minnesota, N.A.*,[95] the court held the exclusivity of Article 4A is limited to particular situations governed by the Article:

> Drawing from the comments and the developing case law, we conclude that the exclusivity of Article 4A is restricted to situations that are covered by particular provisions of the Article and that principles of law and equity may be applied to disputes relating to funds transfers so long as those principles do not create rights, duties, or liabilities inconsistent with those stated in the Article. The Agency Agreement between HIP and Norwest covers specific fiduciary responsibilities that go well beyond the scope of wire transfer services. These contractual responsibilities do not create rights, duties, or liabilities inconsistent with Article 4A, but in addition to it. Consequently, we conclude that the contractual responsibilities are not excluded by Article 4A.[96]

VII.
CASES ANALYZING COVERAGE FOR UNAUTHORIZED ELECTRONIC FUNDS TRANSFERS

Although numerous cases, such as these described above, address a financial institution's liability for unauthorized electronic funds transfers, the authors have not located any case involving litigation by a financial institution against its insurer seeking coverage for a loss resulting directly from an unauthorized electronic funds transfer. There

[94] *Id.* at 412-13.
[95] 578 N.W.2d 765 (Minn. Ct. App 1998).
[96] *Id.* at 771.

are, however, a number of these cases under commercial crime policies. For example, the insured in *Brightpoint, Inc. v. Zurich American Insurance Co,.*[97] sought coverage under Zurich's Form F-Computer Fraud/Wire Transfer policy, which defined Computer Fraud as follows:

> b. 'Computer Fraud' means 'theft' of property following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the .. 'premises' or 'banking premises' to a person (other than a 'messenger') outside those 'premises' or to a place outside those 'premises'. The means by which a fraudulent transfer is initiated includes: written, telephonic, telegraphic, telefacsimile, electronic, cable, or teletype instructions.[98] (Emphasis by underlining added)

Brightpoint's subsidiary in the Philippines served as a wholesaler of prepared telephone cards it purchased from a telecom company. Brightpoint required a large volume customer to make payment by post-dated check with a bank guarantee certifying that there were sufficient funds in the customer's account to cover the post-dated check and committing the bank to pay the post-dated check when presented. The customer would transmit a purchase order and copies of the post-dated check and bank guarantee by facsimile to Brightpoint. An employee of Brightpoint would then go to the telecom company, purchase the prepaid telephone cards, and deliver them directly to the customer. Following this procedure, Brightpoint purchased and delivered prepaid phone cards with a value of approximately $1.5 million. Approximately one week later, the customer met with Brightpoint and advised that it had not submitted the purchase order.[99]

The court granted summary judgment for Zurich because the facsimile of the post-dated check and bank guarantees did not fraudulently cause the transfer of the prepaid telephone cards stating as follows:

[97] No. 1:04-CV-2085-SEB-JPG, 2006 U.S. Dist. LEXIS 26018 (S.D. Ind. Mar. 10, 2006).

[98] *Id.* at 3-4.

[99] *Id.* at 7-8.

> Similarly, we are convinced that the final defense advanced by the insurer has merit. We do not view the faxed post-dated checks and bank guaranties to have "fraudulently cause[d] a transfer" of the phone cards, as required under the policy definition of "Computer Fraud." By Brightpoint's own admission, the facsimile simply alerted the company to the fact that Genato, or perhaps in this case some other person mimicking his methods, wished to place an order. Only after Brightpoint received the physical documents would they release the phone cards and, based on established practices of Brightpoint, the cards would not have been turned over simply on the basis of the facsimile. The fraud in this instance occurred through the use of the unauthorized checks and guaranties, not the manipulation of numbers or events through the use of a computer, facsimile machine or other similar device. The facsimile transmission caused Brightpoint to purchase the cards from its supplier, not to transfer them to its purchaser, and the use of the fax thus cannot be viewed as having directly or proximately caused the theft.[100]

Milwaukee Area Technical College v. Frontier Adjusters of Milwaukee[101] is another case in which an insured sought coverage under a computer fraud insuring agreement. The College entered into a contract with Frontier to process workers' compensation claims. Frontier evaluated the workers' compensation claims and purportedly paid those that were approved. The checks were never sent to the healthcare providers, but Frontier sent photocopies of checks and a false check ledger to the College.[102] Frontier stole a total of $1.6 million as a result of its scheme. The Court did not address whether the loss resulted directly from computer fraud because it determined that the policy excluded liability for any fraudulent or dishonest act committed by any

[100] *Id.* at 19-20.
[101] 752 N.W.2d 396 (Wis. Ct. App. 2008).
[102] *Id.* at 399.

of the College's authorized representatives and that Frontier and its owner were the authorized representatives of the College.[103]

Methodist Health System Foundation v. Hartford Fire Insurance Co.[104] is a computer fraud case in which the court addressed the issue of whether the loss resulted directly from the use of a computer. Methodist Health invested in funds in Meridian Diversified Funds, a mutual fund that invested in hedge funds. Meridian invested a portion of its assets in Tremont Hedge Fund, which in turn invested a portion of its holdings in Bernard L. Madoff Investment Securities, Inc.[105] When the Madoff Ponzi scheme unraveled, Methodist sought coverage from Hartford contending that Madoff used a computer to prepare documents leading investors to believe that Bernard L. Madoff Investment Securities, Inc. was a legitimate investment vehicle.

The court granted summary judgment on the ground, among others, that the loss was not a direct loss:

> The Louisiana Supreme Court has held that '[t]he word 'direct' as used in a contract insuring against direct loss or damages means immediate or proximate as distinguished from remote." . . . .
>
> Here, while the Madoff Ponzi scheme was a contributing factor in Plaintiff's sustained losses, this Court finds that the Madoff Ponzi scheme was not a direct cause of Plaintiff's losses.[106]

Similarly, in *Pinnacle Processing v. Hartford Casualty Insurance Company*,[107] The plaintiff was in the business of processing credit card transactions. It contracted with Merrick Bank to market credit card processing services to merchants. If a merchant contracted with Pinnacle, it could accept credit cards to pay for goods. At the end

[103] *Id.* at 402.

[104] 834 F. Supp. 2d 493 (E.D. La. 2011).

[105] *Id.*

[106] *Id.* at 496 (citations omitted).

[107] No. C10-1126-RSM, 2011 U.S. Dist. LEXIS 128203 (W.D. Wash. Nov. 4, 2011).

of each day, Merrick deposited an amount into its merchant's bank account equal to the amount of credit card transactions that day. Merrick was to be reimbursed by the banks that issued the credit cards, and the issuing banks would in turn debit their customers' accounts for the amount of the purchases. Pinnacle was required to maintain a $250,000.00 reserve account at Merrick to cover chargebacks. Pinnacle incurred $360,823.56 in chargeback losses due to fraudulent credit card transactions by various merchants which it could not recover from the merchants' bank accounts.[108]

The court granted Hartford's motion for summary judgment based on its finding that the loss was not a direct loss due to computer fraud:

> Direct means without any intervening agency or step: without any intruding or diverting factor. Here, PPG's loss was not direct. PPG did not suffer a loss until (1) Merrick Bank was unable to recover the chargeback funds from the merchant banks; (2) Merrick Bank deducted funds from PPG's Reserve Account; and, finally, (3) PPG fulfilled its contractual obligation to replace those deducted funds. To interpret the term "directly" as potentially applying to such an attenuated chain of events would be to "create ambiguity where none exists." Moreover, such an interpretation would render the use of the word "directly" in the insurance policy superfluous: there would be no difference between the phrase "resulting from computer fraud," and "resulting directly from computer fraud."[109]

VIII.
INVESTIGATING THE LOSS

When investigating a claim involving any electronic or mobile payments under a fidelity bond, the investigation should consider at least the following steps:

[108] *Id.* at 4-5.

[109] *Id.* at 12-13 (citations omitted).

- Request the insured to keep the involved hardware in safe custody and not to "scrub" the hard disc on any computer involved. If the Insured is a financial institution, then request the insured to ask its customer to not "scrub" the hard disc on any computer involved. An examination of the hard disc will often determine if the computer has been infected with malware enabling the perpetrator to determine the necessary information to gain access and use an online banking system.

- Request the insured to provide copies of all agreements it has with its customer authorizing the insured to make electronic funds transfers.

- Request the insured's risk manager and IT department personnel to write a memo or retain a diary memorializing all investigative tools and resources employed to determine the source of the computer breach.

- Request the insured to preserve all connection logs and records of user activities.

- Use a forensic computer expert to review any questionable emails, URLs and malware.

- Request the insured to prepare a memo detailing conversations with third parties regarding the discovery of the unauthorized electronic funds transfer.

- Contact local authorities, the FBI, and the Secret Service.

- Inquire as to other victims.

- Obtain an understanding as to whether the ODFI or RDFI are involved.

When necessary, and possible, obtain third party verifications, expert opinions, and supporting documentation as to all understandings when the need arises for policy interpretation and pursuing recoveries.

Another tool to utilize is to map a timeline of incidents, when possible, from facts and information gathered from the investigation. The timeline helps to visualize and interpret the reasonableness of the facts and information presented.

In addition to the above, an investigation under a commercial crime policy for non-financial institutions involves determining a number of factors, including:

- What is a loss? Is it Property, monies and securities?
- What tools, hardware or software are involved?
- Is a "transfer account" involved? If so, whose "transfer account" is involved?
- Is a fraudulent instruction involved? Review definitions and determine if the policy has limitations as to who purports to have transmitted the fraudulent instruction.
- Understand how the use of the computer causes a direct loss. Does the policy have limitations or restrictions as to "whose" computer is used to cause the direct loss?

The commercial crime coverages for computer fraud and funds transfer fraud are intended to be first-party policies and coverages.

Cyber coverages are intended to be first-party policies addressing losses by the insured and third parties due to a breach of the insured's data and information. Cyber liability covers expenses for the insured and liability issues involving third parties. When investigating third parties, the same and similar steps of data protection and reduction of first-party to third-party liabilities, computer experts and accounting experts will help span the gap between the contentions and coverage for adjusters and attorneys.

IX.
SUMMARY

Funds transfers through intermediaries have existed for at least ten centuries, and are continuing to evolve to accommodate the volume of transactions, the technology available, security needs, and user preferences. With each new funds transfer method comes new rules, regulations, statutes, and court decisions to address the questions that have remained constant from the beginning of funds transfers through an intermediary, to the present, and into the future—who bears the risk of loss if the funds transfer is fraudulent? To answer that question, one needs an understanding of what rules and regulations apply to each funds transfer method and court decisions interpreting those rules and regulations. One must also determine if the rules and regulations are exclusive of common law causes of action and whether the parties can modify the applicable rules and regulations by agreement. And if course, one must understand what insurance coverage is available to the party bearing the loss for the fraudulent funds transfer.

APPENDIX A

Transaction Type	Definitions	Laws / Regulations	Accountholder Liability	Return Rights	Potential Fidelity Bond Coverages
Check	Electronic Check Presentiment “Agreement for electronic Presentment” means an agreement, clearing-house rule, or Federal Reserve regulation or operating circular, providing that presentment of an item may be made by transmission of an image of an item or other information describing the item (“presentment notice”) rather than delivery of the item itself. The agreement may provide for procedures governing retention, presentment, payment, dishonor, and other matters concerning items subject to the agreement.” Currently, this transmission, which enables funds to be held prior to arrival of a paper check, is routinely followed by delivery of the paper check from the collecting to the paying bank.	UCC Article 4 §4-110 UCC Article 3 UCC Article 4 Regulation CC, Subpart C, large item notification $2,500 or more[110]	Account agreement UCC	Midnight deadline Claims against depositary FI for breach of transfer and presentment warranties	Forgery or Alteration Securities / Counterfeit
	Substitute Check—A paper reproduction of an original check, containing an image of the original paper check. Also called an Image Replacement Document.	Check 21 Act[111] Regulation CC, Subpart D, substitute checks[112]			

[110] 12 C.F.R. § 229.33.

[111] Check Clearing For The 21st Century Act, Public Law 108-100, October 28, 2003, 12 U.S.C. § 5002(16).

[112] 12 C.F.R. §§ 229.51 – 229.60.

Transaction Type	Definitions	Laws / Regulations	Accountholder Liability	Return Rights	Potential Fidelity Bond Coverages
Wire Transfer	FedWire—The Federal Reserve's wire transfer system FedLine—The computer system (terminals) used for FedWires and other transactions (cash ordering, ACH, etc.) through the Federal Reserve CHIPS—(Clearing House Interbank Payments System)—another system used by New York banks SWIFT—(Society for Worldwide Interbank Financial Telecommunications)—for foreign wire transfers	Regulation J (for wire transfers through Federal Reserve, includes UCC 4A as appendix B)[113] UCC Article 4A (broader coverage of Fund Transfers)	Account agreement. UCC Article 4A. Accountholder has 1 year timeframe to provide notice of unauthorized transactions.	Not applicable. Settlement is final.	Computer Systems Fraud Fraudulent Transfer Instructions Voice Initiated Transfer Fraud Telefacsimile Transfer Fraud
ACH Debit	NACHA—The National Automated Clearing House Association, rule setting organization for ACH payments. Electronic check conversion—a category of the standard entry class codes where ACH transactions are created from checks, such as POP, ARC, BOC, and RCK entries. Electronic check—In ACH terminology, this refers to standard entry class codes where ACH transactions are created from checks, such as POP, ARC, BOC, and RCK entries. Prearranged Payment and Deposit Entry (PPD)—Recurring consumer transactions (payroll, bill payments, etc.).	Regulation E for consumer accounts Account agreements for commercial accounts NACHA Rules (given authority by the Federal Reserve ACH Operating Circular, for non-government items) The Green Book for government payments	No liability for transactions reported within 60 days of statement availability Potential liability for subsequent recurring transactions if notification not received within 60 days of statement availability	Under NACHA rules. Generally 60 days (after settlement) for unauthorized consumer transactions Return reason R10: Customer advises not authorized (Most other returns are required within 2 days)	Computer Systems Fraud? Funds Transfer for credit unions No forged instruments are received by the financial institution

[113] *Id.* §§ 210.25 – 210.32.

Transaction Type	Definitions	Laws / Regulations	Accountholder Liability	Return Rights	Potential Fidelity Bond Coverages
ACH Debit (cont.)	Point-of-purchase (POP) and Back Office Conversion (BOC)—Converting a paper check to an electronic ACH payment by merchants. Accounts Receivable Entry (ARC)—Converting a paper check to ACH for items received via mail or drop box. Phone authorization (TEL)—A consumer initiated debit to their account, authorized by phone. Internet authorization (WEB)—A consumer initiated debit to their account, authorized over the Internet.				
	Re-presented Check (RCK)—Converting a paper check to ACH by merchants or collectors to collect on a consumer check that has been returned non-sufficient funds (NSF) or uncollected funds.	(RCK—these are the only consumer ACHs NOT covered by Reg. E)		RCK—R10 not allowable, Use R51: Notice not provided, signature not genuine, etc	
Remotely Created Check	Remotely created check—also referred to as "demand draft," "preauthorized draft," or "telephone check"—is generally issued by the payee on the authority given by the owner of the checking account on which the remotely created check is drawn. In place of a drawer's signature, the remotely created check generally bears a statement in the signature block that the accountholder authorized the check or bears the customer's printed or typed name.	Regulation CC, Subpart C, section 229.34(d) A regulation change in 2006 shifted responsibility for payment of fraudulent checks from the FI it is drawn on to the FI that accepts it as a deposit	Per account agreement.	Adjustment requests for a warranty claim within 90 days of the cash letter in which the remotely created check was charged. After that, pursue a claim directly with the depositary bank (or in the courts) up to one year.	No coverage (not a forgery) (not a counterfeit)

Transaction Type	Definitions	Laws / Regulations	Accountholder Liability	Return Rights	Potential Fidelity Bond Coverages
Remotely Created Check (cont.)	Remotely created checks are similar to traditional checks except that a remotely created check does not contain the accountholder's wet signature. Another difference is the payee, not the accountholder, creates the remotely created check. Regulation CC definition: means a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn. For purposes of this definition, "account" means an account as defined in paragraph (a) of this section as well as a credit or other arrangement that allows a person to draw checks that are payable by, though, or at a bank.				
ATM Card		Regulation E[114]	Per Regulation E timeframes	Not applicable	Plastic Card for credit unions
Debit Card		Regulation E[115] Card Association Rules	Per Regulation E timeframes for consumer Per agreement (if one exists) for commercial Visa and MasterCard zero liability policies	Card association chargeback rules, if applicable	Plastic Card for credit unions

[114] *Id*. §§ 205.1 – 205.20.

[115] *Id*.

Transaction Type	Definitions	Laws / Regulations	Accountholder Liability	Return Rights	Potential Fidelity Bond Coverages
Credit Card		Regulation Z[116] Card Association Rules	Per Regulation Z timeframes for consumer, and commercial if <10 cards Per agreement (if one exists) for commercial if 10 or more cards Visa and MasterCard zero liability policies	Card association chargeback rules, if applicable	Plastic Card for credit unions

[116] 12 C.F.R. §§ 226.1 – 226.59.