MALWARE AND FRAUDULENT ELECTRONIC FUNDS TRANSFERS: WHO BEARS THE LOSS?

Robert W. Ludwig, Jr.
Salvatore Scanio
Joseph S. Szary

I. INTRODUCTION

After federal banking regulators[1] implemented stronger customer authorization controls in the mid-2000s, electronic bank fraud affecting consumers declined significantly.[2] By 2009, the criminals adapted, and the rate of electronic bank fraud has been on the rise ever since, with business accounts as the new target.[3] According to the FDIC, fraud involving electronic funds transfers[4] by businesses resulted in more than

[1] The five federal banking agencies: the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, comprise the Federal Financial Institutions Examination Council [hereinafter FFIEC], which issues regulatory guidelines applicable to the five agencies and their respectively regulated financial institutions.

[2] FDIC, Spyware: Guidance on Mitigating Risks from Spyware, FDIC Fin'l Institution Letter 66-2005 (July 22, 2005), with Informational Supplement: Best Practices on Spyware Prevention and Detection; FFIEC, Authentication in an Internet Banking Environment (Oct. 12, 2005); FFIEC, Information Security, IT Examination Handbook (July 2006); FFIEC, Frequently Asked Questions on FFIEC Authentication in an Internet Banking Environment (Aug. 15, 2006).

[3] Rob Garver, *The Cost of Inaction*, U.S. BANKER (July 2010).

[4] Hereinafter EFTs.

Robert W. Ludwig, Jr. and Salvatore Scanio are partners with Ludwig & Robinson, PLLC, in Washington, D.C. Joseph S. Szary is an Assistant Vice President and Senior Home Office Examiner with Chubb & Son, a division of Federal Insurance Company, in Warren, New Jersey. The authors acknowledge the assistance of Carl F. Lettow, II, of Ludwig & Robinson, PLLC.

$120 million in losses in the third quarter of 2009, up from $85 million lost during the same period in 2007.[5] As a result, the FDIC issued a special alert on fraudulent EFTs—Automated Clearing House[6] transfers and wire transfers:[7]

> Web-based commercial EFT origination applications are being targeted by malicious software, including Trojan horse programs, key loggers and other spoofing techniques, designed to circumvent online authentication methods. Illicitly obtained credentials can be used to initiate fraudulent ACH transactions and wire transfers, and take over commercial accounts. These types of malicious code, or 'crimeware,' can infect business customers' computers when the customer is visiting a Web site or opening an e-mail attachment. Some types of crimeware are difficult to detect because of how they are installed and because they can lie dormant until the target online banking session login is initiated. These attacks could result in monetary losses to financial institutions and their business customers if not detected quickly.[8]

Two months later, the FDIC issued a special alert warning of schemes that recruit individuals to receive and transmit fraudulent EFTs to international accounts.[9] These funds transfer agents, known as "money mules," are typically solicited on the Internet and involve work-

[5] Robert McMillian, *FDIC: Hackers Took More Than $120M In Three Months*, http://news.techworld.com/security/3214661/fdic-hackers-stole-120m-in-three-months-of-online-bank-fraud/ (last visited Sept. 29, 2010); Marcia Savage, *FDIC: ACH Fraud Losses Climb Despite Drop In Overall Cyberfraud Losses*, SearchFinancialSecurity.com, http://searchfinancialsecurity.techtarget.com/news/article/ 0,289142,sid185_gci1411123,00.html (last visited Sept. 29, 2010).

[6] Hereinafter ACH.

[7] FDIC Special Alert, SA-147-2009, Fraudulent Electronic Funds Transfers (Aug. 26, 2009).

[8] *Id.*

[9] FDIC Special Alert, SA-185-2009, *Fraudulent Work-at-Home Funds Transfer Agent Scheme*, http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html (last visited Sept. 29, 2010).

at-home schemes, advance-fee scams, or social networking sites. Criminals originate unauthorized EFTs, transfer the funds to a "money mule," and convince the money mule to quickly withdraw and wire the funds overseas (after deducting the mule's "commission").[10]

In November 2009, the FBI acknowledged the problem in a press release, disclosing that it "has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium businesses, municipal governments, and school districts."[11] The FBI described the typical scenario as a targeted entity receiving a "phishing" e-mail which contains an infected attachment or directs the recipient to an infected website, resulting in malware being installed on the target's computer. The malware will harvest the corporate bank account login information via a key logger.[12] The FBI recognized the role of money mules in carrying out the scheme.[13] The FBI also reported that in most cases the affected business accounts are held at local community banks and credit unions.[14]

II. THE EVOLUTION OF BANKING MALWARE

Malicious software, commonly known as malware, is a general term for software "inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners."[15] "Malware can gain remote access to an information system, record and send data from that system to a third

[10] *Id.*

[11] FBI Press Release, *Fraudulent Automated Clearing House (ACH) Transfers Connected to Malware and Work-at-Home Scams*, http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm (last visited Sept. 29, 2010).

[12] *Id.*

[13] *Id.*

[14] FBI Intelligence Note, Internet Crime Complaint Center, *Compromise of User's Online Banking Credentials Targets Commercial Bank Accounts*, http://www.ic3.gov/media/2009/091103-1.aspx (last visited Sept. 29, 2010); Riva Richmond, *Wanted: Defense Against Online Bank Fraud*, WALL ST. J. (Feb. 8, 2010).

[15] *See* Organization for Economic Co-operation and Development, Malicious Software (Malware): *A Security Threat to the Internet Economy*, http://www.oecd.org/dataoecd/53/34/40724457.pdf (last visited Sept. 29, 2010).

party without the user's permission or knowledge, conceal that the information system has been compromised, disable security measures, [or otherwise] damage the information system . . . ."[16] There are different types of malware, such as viruses, worms, Trojan horses, backdoors, keystroke loggers, rootkits, or spyware, which correspond to the functionality and behavior of the malware.[17] A malware-infected computer that a criminal can remotely control and turn into a "robot" or zombie machine, is known as a "bot," or "botnet" in the case of a network of such computers.[18]

Malware deployed by criminals to take over commercial banking accounts has become more sophisticated in recent years. Three years ago, Silentbanker was employed as a phishing site, where criminals used a fake banking site to install malware on users' computers, and took screen shots of bank accounts, among other things.[19] The current generation of banking malware has evolved to defeat certain security measures. The Trojan horse Zeus (also known as Prg Banking Trojan and Zbot), for example, targets commercial banking systems by waiting until a user logs into the bank's system, and then intercepts the login and password information directly from online forms, as the user completes them.[20] Zeus Clampi, another Trojan horse, works similarly, but employs a "man-in-the-middle" approach, hijacking the banking session after the user has logged in by displaying a website maintenance or other error message.[21]

Clampi and similar variations alert hackers to complete the unauthorized transaction, and are effective even against sophisticated security measures (such as token password generators). For example, a recent virus is capable of installing instant messaging code on computers and thus, when a user enters his digital token code, the malware sends a message to the criminal who logs in while the virus delays the legitimate

[16] *Id*.

[17] *Id*.

[18] *Id*. at 22 n.61.

[19] Robert Vamosi, *New Banking Trojan Horses Gain Polish*, PCWORLD MAG. (Jan. 2010).

[20] *Id*.

[21] *Id*.

login.[22] Even though the password generated by a security token is only valid until the next password is generated (sometimes as often as every 30-60 seconds), "man-in-the-middle" malware can capture those passwords when entered by the user, to permit immediate unauthorized transfers.[23] Other variations, such as Bugat, will modify a bank's login page to extract further information from the customer, and can browse and transmit information stored directly on the user's computer.[24] Another variant, URLZone, is sophisticated enough to be preset to take a specific percentage from an account, in order to avoid tripping the bank's automatic anti-fraud alerts.[25]

Criminals also continue to adapt to evolving software uses and fads. For example, the malware program Koobface "masquerades on Facebook as email from friends."[26] Once accessed, the program downloads to the user's computer, and functions like other Trojan horses, including keystroke capture to obtain password and other security information.[27] Thus, both consumers and business employees, who access Facebook from the same terminal used to process EFTs, risk exposing security information simply by opening a "friend's" email.

III. THE LEGAL FRAMEWORK FOR ALLOCATING COMMERCIAL ACCOUNT LOSSES ARISING FROM FRAUDULENT EFTS

Commercial bank customers utilize two primary types of electronic funds transfers: traditional wire transfers and Automated Clearing House transactions.[28] "The wire transfer is a credit-driven mechanism, handling the transmission of each payment order

[22] Asher Hawkins, *Is Your Online Bank Account Safe?* FORBES (Nov. 16, 2009).

[23] Byron Acohido, *Cybercrooks Stalk Small Businesses That Bank Online*, USA TODAY (Jan. 13, 2010).

[24] Angela Moscaritolo, *New "Bugat" Trojan Harvesting Banking Credentials*, SC MAG. (Feb. 2010).

[25] Vamosi, *supra* note 19, at 41.

[26] The Kiplinger Letter, Vol. 87, No. 30 (July 23, 2010).

[27] *Id*.

[28] As discussed herein, the term EFTs refers to both wire transfers and ACH transfers.

individually, to accommodate particularly large-value payments."[29] Most wire transfers in the United States are conducted via Fedwire, a system operated by the Federal Reserve Banks.[30] CHIPS, a New York-based wire system is operated by the New York Clearing House Association, via the Federal Reserve Bank of New York.[31] International wire transfers are typically conducted via telex or SWIFT messages.[32]

The ACH system, an electronic counterpart to the check system, "is a batch-processing time-delayed payment mechanism where settlement occurs one or two days after data input. It supports both debit and credit transfers."[33] Businesses typically use the ACH system to make payroll and vendor payments.[34]

Whether characterized as a wire transfer or nonconsumer ACH transaction, the allocation of loss involving EFTs is primarily governed by Article 4A of the Uniform Commercial Code,[35] the Operating Rules of the National Automated Clearing House Association,[36] and Federal Reserve Regulation J, which incorporates UCC Article 4A.[37]

UCC Article 4A was first approved by the National Conference of Commissioners on Uniform State Laws and the American Law Institute in 1989.[38] Prior thereto, there was "no comprehensive body of law that defined the rights and obligations that arise from wire transfers." Article 4A was "intended to provide" that "comprehensive body."[39] As with the other UCC Articles, Article 4A incorporates Article 1, and is

[29] BENJAMIN GEVA, THE LAW OF ELECTRONIC FUNDS, § 1.04[3] (Dec. 2009).

[30] *Id*.

[31] *Id*.

[32] *Id*. SWIFT is the Society for Worldwide Interbank Financial Telecommunication.

[33] *Id*.

[34] *Id*.

[35] Hereinafter UCC.

[36] Hereinafter NACHA.

[37] *See* 12 C.F.R. § 210.25(b)(1) (2010). The NACHA Rules apply to ACH transactions. Regulation J applies to Fedwire transfers.

[38] By 1996, Article 4A was adopted by all the states and the District of Columbia. GEVA, *supra* note 29, at § 1.05[2].

[39] UCC Article 4A, Prefatory Note.

potentially subject to the 2001 amendments to Article 1, depending on whether a jurisdiction has adopted the amendments.[40]

UCC Article 4A has its own terminology, as detailed in relevant respects in sections 4A-103 (Payment Order—Definitions) and 4A-104 (Funds Transfer—Definitions). A "Payment Order" is the instruction to the receiving bank to pay a fixed or determinable amount of money.[41] A "Funds Transfer" is the series of transactions which result in payment to the beneficiary.[42] The "Sender" is the person or entity making the payment order or instruction to pay,[43] while an "Originator" is the sender of the first payment order in a funds transfer (if in a chain of transfers).[44] The "Beneficiary" is the person to be paid under the payment order.[45] Banks also are given their own nomenclature: a "Receiving Bank" is the bank receiving the payment order;[46] the "Beneficiary's Bank" is the bank identified in the payment order, to credit the beneficiary's account, or otherwise make payment to the beneficiary;[47] and an "Intermediary Bank" is a receiving bank other than the originator's or beneficiary's bank, again, if the transfer involves series of transactions.[48]

One important body of law that does not apply to EFTs by commercial customers is the Electronic Funds Transfer Act.[49] The EFTA generally provides a limit of $50 on the loss that can be allocated to an account holder for any "unauthorized electronic fund transfer."[50] The EFTA, however, excludes business accounts, as it applies only to transfers of funds involving accounts "established primarily for personal, family, or household purposes,"[51] and is thus inapplicable here.

[40] ***See*** UCC Article 1 App I (2009).

[41] UCC § 4A-103(a)(1).

[42] UCC § 4A-104(a).

[43] UCC § 4A-103(a)(5).

[44] UCC § 4A-104(c).

[45] UCC § 4A-103(a)(2).

[46] UCC § 4A-103(a)(4).

[47] UCC § 4A-103(a)(3).

[48] UCC § 4A-104(b).

[49] Hereinafter EFTA.

[50] 15 U.S.C. § 1693g.

[51] 15 U.S.C. § 1693a(2). For a recent case involving a determination of whether accounts involved in fraudulent EFTs were primarily business or

A. Article 4A's General Rules for Allocating Losses

UCC §§ 4A-202 and 203 allocate loss involving unauthorized[52] EFTs between the bank and its customer. In general, UCC § 4A-204 imposes liability for unauthorized transfers on a receiving bank. It requires a receiving bank to refund any funds (plus interest) from a payment order that was: (1) not authorized by the customer under UCC § 4A-202; or (2) is not enforceable against the customer under UCC § 4A-203 because the payment order was not caused by (a) an authorized employee or (b) a person who obtained access to the customer's transmitting facilities, or otherwise obtained transmittal information from the customer.

Section 4A-202(b) permits the receiving bank to escape liability, even though the customer did not authorize the payment order, if the bank proves that: (1) the bank and customer agreed that the authenticity of a payment order would be verified pursuant to a "security procedure;" (2) the security procedure that has been agreed upon by the bank and customer is "commercially reasonable;" (3) the bank processed the payment orders in "compliance" with the security procedure; (4) the bank processed the order in compliance with any written agreement or instruction of the customer; and (5) the bank accepted the payment order in "good faith."[53]

If these five elements are not met, the bank is strictly liable for an unauthorized EFT.[54] If these conditions are met, the bank will still bear the risk of loss if "the person committing the fraud did not obtain

consumer accounts, see Shames-Yeakel v. Citizens Fin Bank, 677 F. Supp. 2d 994, 1002-07 (N.D. Ill. 2009) (applying Truth in Lending Act and EFTA).

[52] Under UCC § 4A-202(a), a payment order is authorized if the person identified as the sender authorized the order or is otherwise bound under the law of agency.

[53] UCC § 4A-202(b). This section specifies that the bank must prove the last three elements. It is silent as to the burden of proof on the first two elements, but inasmuch as the bank would be asserting this provision as a defense to avoid liability by making an otherwise unauthorized order "effective," the burden should fall on the bank. Section 4A-202(b) also uses the term "accept" rather than "process." As defined in UCC § 4A-209(a), a receiving bank "accepts a payment order when it executes the order."

[54] UCC § 4A-204(a).

the confidential information [facilitating the breach of the security procedure] from an agent or former agent of the customer or from a source controlled by the customer. . . ."[55]

1. An Agreed Verification "Security Procedure"

A "security procedure" is a "procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order . . . is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication."[56] A "security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices."[57]

A "security procedure" does not cover "procedures that the receiving bank may follow unilaterally in processing payment orders."[58] In *Skyline International Development v. Citibank, F.S.B.*,[59] the bank admitted that it failed to follow its internal procedure for obtaining authorization for wire transfers, but argued that the violation was not a violation of a "security procedure," because the customer had not agreed that wire transfers would be verified under the bank's internal procedure. The court agreed, and found that the customer failed to show that the wire transfer was unauthorized.[60] Accordingly, a bank's internal procedures relating to EFTs, which are not contained in the customer agreement, do not constitute relevant "security procedures" under Article 4A.[61]

[55] UCC § 4A-203 cmt. 5.

[56] UCC § 4A-201.

[57] UCC § 4A-201.

[58] UCC § 4A-201 cmt.

[59] 706 N.E. 2d 942 (Ill. App. 1998).

[60] *Id*. at 945.

[61] By the same token, this provision should mean that a bank cannot point to internal procedures not contained in the customer agreement to bolster its "security procedure" as being "commercially reasonable," discussed *infra*. Similarly, a bank's internal fraud procedures that are not incorporated in the customer agreement, such as verifying new payees, applying daily or item limits, or fraud profile screening, would not be relevant in determining whether

In *Experi-Metal, Inc. v. Comerica Bank*,[62] the agreed security procedure required the customer to input its user identification, four-digit PIN, and a six-digit code from a secure token (a randomly generated number that changed every 60 seconds).[63] The customer received a "phishing" email, prompting the customer to login to renew its digital certificates. The customer clicked on the link, and was diverted to a fake website that appeared to be the bank's legitimate site. The customer entered its login and confidential codes, being instantly subject to a "man-in-the-middle" phishing attack. The criminal immediately used the customer's confidential information to connect to the bank, and generated 93 fraudulent wire transfer orders, totaling $1.9 million, to various accounts around the world.[64] The bank contended that it offered the customer the ability to require two individuals to approve wire transfers as an additional security procedure, but the customer had refused the offer.[65] The court concluded that "requiring confirmation by additional users simply is an option or element within a security procedure. The 'security procedure' is the secure token technology."[66]

2. Commercially Reasonable Security Procedures

a. ***Legal Standards***

The UCC's drafters recognized that a principal issue likely to arise in litigation involving fraudulent EFTs is whether the security procedure in effect was commercially reasonable.[67] Unlike UCC Articles 3 and 4, the issue of "commercial reasonableness of a security

there was "compliance" with the "security procedure" in processing the wire or ACH transfers, as also discussed below.

[62] No. 09-14890, 2010 U.S. Dist. LEXIS 68149 (E.D. Mich. July 8, 2010).

[63] *Id*. at *11-14.

[64] *Id*. at *7-9; Response to Amended Motion for Summary Judgment, Exhibit 2, Declaration of Lance James, Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2010 U.S. Dist. LEXIS 68149 (E.D. Mich. July 8, 2010) (hereinafter James Declaration).

[65] 2010 U.S. Dist. LEXIS 68149, at *11-14.

[66] *Id*. at *14.

[67] UCC § 4A-203 cmt. 4.

procedure is a question of law" under Article 4A.[68] The Official Comments note that: "[i]t is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers."[69] Whether the bank complied with the security procedures is a question of fact.[70]

The reasonableness of a security procedure is subject to two tests and the satisfaction of either test is sufficient. First, a "security procedure" is deemed reasonable if:

> (i) 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 (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.[71]

This test focuses on the content of the customer agreement. If

> an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper[,] . . . the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank. But this result follows only if the customer expressly agrees in writing to assume that risk.[72]

[68] UCC § 4A-202(c); *cf.* UCC § 3-103(a)(9) (reasonable commercial standards applicable to claims under UCC Articles 3 and 4).

[69] UCC § 4A-203 cmt. 4.

[70] *Id*.

[71] UCC § 4A-202(c).

[72] UCC §4A-203 cmt. 4.

Indeed, many businesses reportedly have complained about or rejected additional security measures offered by their banks, as inconvenient, or not worth the cost-benefit analysis.[73] In these cases, the customer will bear the risk of loss, and not be able to complain that, by acceding to its wishes, the bank acted "in bad faith by so doing so long as the customer is made aware of the risk."[74]

In the event "a commercially reasonable security procedure is not made available to the customer, subsection [4A-202](b) does not apply. . . . The bank acts at its peril in accepting a payment order that may be unauthorized."[75] Article 4A recognizes that prudent banking practices require that security procedures should be utilized in all EFTs, and "[t]he burden of making available commercially reasonable security procedures is imposed on receiving banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud."[76]

Second, a security procedure is commercially reasonable if it satisfies four principal factors:

> (1) "the wishes of the customer expressed to the bank;"
>
> (2) "the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank;"
>
> (3) "alternative security procedures offered to the customer;" and
>
> (4) "security procedures in general use by customers and receiving banks similarly situated."[77]

[73] Garver, *supra* note 3, at 11.
[74] UCC §4A-203 cmt. 4.
[75] UCC 4A-203 cmt. 3.
[76] *Id*.
[77] UCC § 4A-202(c).

In applying these factors, the "additional guidance" offered by the Official Comments may make a court's determination even more complex. To begin with, the Comments state: "the concept of what is commercially reasonable in a given case is flexible[,]" a pronouncement seemingly at odds with the purported goal of having the issue decided as a matter of law to create a uniform standard.[78] The Comments, much like legislative history, contain conflicting policy statements that can be cited by both the bank and customer:

> The purpose of subsection (b) is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. 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. On the other hand, a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable.[79]

The Comments also introduce additional or amplifying factors. The first is a cost-benefit analysis:

> Verification entails labor and equipment costs that can vary greatly depending upon the degree of security that is sought. A customer that transmits very large numbers of payment orders in very large amounts may desire and may reasonably expect to be provided with state-of-the-art procedures that provide maximum security. But the expense involved may make use of a state-of-the-art procedure infeasible for a customer that normally

[78] UCC § 4A-203 cmt. 4.

[79] *Id*.

> transmits payment orders infrequently or in relatively low amounts.[80]

The second additional factor is: "the type of receiving bank. It is reasonable to require large money center banks to make available state-of-the-art security procedures. On the other hand, the same requirement may not be reasonable for a small country bank."[81] Indeed, many community bank and their service providers are unable to provide the same level of security features offered by large banks.[82] Some software firms, however, claim that cost-effective solutions are available for small banks, such as employing fraud-detection software that triggers a telephone call to the customer requiring additional verification when new payees are added to a customer's EFT order.[83] A third consideration is that the bank may offer different security procedures to different customers: "A receiving bank might have several security procedures that are designed to meet the varying needs of different customers."[84]

The Comments also distinguish between wire transfers and ACH transactions in determining the reasonableness of the security procedure applied:

> in a wholesale wire transfer, each payment order is normally transmitted electronically and individually. A testing procedure will be individually applied to each payment order. In funds transfers to be made by means of an automated clearing house many payment orders are incorporated into an electronic device such as a magnetic tape that is physically delivered. Testing of the individual payment orders is not feasible. Thus, a

[80] *Id.*

[81] *Id.*

[82] Garver, *supra* note 3, at 11.

[83] *See, e.g.*, *Authentify Releases EFT Verifier to Thwart Unauthorized Electronic Fund Transfers by Criminal Employing ZeuS Malware*, BUS. WIRE (Apr. 7, 2010).

[84] UCC § 4A-203 cmt. 4.

> different kind of security procedure must be adopted to take into account the different mode of transmission.[85]

While numerous lawsuits recently have been filed relating to fraudulent EFTs arising from malware attacks, few have addressed this issue, and no court has yet applied the multiple-factor test in UCC § 4A-203(c).[86] In *Transamerica Logistic, Inc. v. JPMorgan Chase Bank, N.A.*,[87] the court found as a matter of law that the bank's security procedures were commercially reasonable where the customer agreement contained a stipulation that the customer "acknowledge[d] and agree[d] that the security procedures described [in the agreement] are commercially reasonable," and the customer offered no "contradictory evidence or argument."

In *Experi-Metal,*[88] the court similarly held that the bank's security procedure was commercially reasonable based on the customer agreement. The customer offered expert testimony, explaining why the secure-token technology was not a commercially reasonable security procedure, including: (1) the technology was known to fail, including against "man-in-the-middle" phishing attacks; (2) the procedure did not verify the identify of the computer sending the instructions to the bank; (3) the procedure was not applied to each wire transfer transaction

[85] *Id*.

[86] A representative pending case is Patco Constr. Co., Inc. v. People's United Bank, No. 2:09-CV-00503-DBH (D. Me. Oct. 9, 2009). The customer's second amended complaint ("SAC") (filed Apr. 23, 2010) contends that the bank's security procedure was not commercially reasonable where it consisted solely of a password and challenge questions for transactions over $1,000. As almost every transaction was over $1,000, challenge answers were frequently used, thus subjecting both passwords and challenge answers to malware attacks. The SAC, among other things, alleges: that the $750,000 ACH daily limit was too high; that security tokens, dual control, or callbacks were not offered; and that the bank did not offer the ability to block transfers from unauthorized IP addresses or email alerts regarding suspicious activity, even though the bank had the capability. Two recently settled cases include: PlainsCapital Bank v. Hillary Mach., Inc., No. 4:09-CV-00653 (E.D. Tex. Dec. 31, 2009); First Cmty. Bank, N.A. v. Tornow & Kangur, L.L.P., No. 1:10CV0008 (W.D. Va. Jan. 8, 2010).

[87] No. 4:07-CV-01678, 2008 U.S. Dist. LEXIS 112708, *3 & n.1 (S.D. Tex. July 21, 2008).

[88] No. 09-14890, 2010 U.S. Dist. LEXIS 68149 at *16-17.

individually; and (4) the bank actually lowered its security standard by going from digital certificate SSL technology to secure token technology.[89] The court, however, rejected that testimony as inadmissible parol evidence.[90]

While the result in *Transamerica* is not surprising given the absence of dispute by the customer, the court's application of exculpatory language in the adhesionary customer agreement, whereby the customer "agrees" that the security procedure is commercially reasonable, is an abdication of the court's responsibility under section 4A-202(c). As discussed above, a court may deem a security procedure commercially reasonable only if two conditions are met: (1) the customer rejects a different security procedure that was commercially reasonable; and (2) the customer agreed to be bound by the chosen security procedure.[91] *Experi-Metal* made no finding that the customer rejected a different security procedure and found that the only security procedure was the secure token.[92] Thus, the court's sole reliance on the customer agreement seems misplaced where the first element was not established. In determining whether the bank's security procedure was commercially reasonable, the court in *Experi-Metal* should have considered the multiple factors set forth in section 4A-202(c), including an evaluation of the customer's expert's opinion as applied to those factors.

b. ***<u>Banking Regulatory Guidelines Relevant to Commercially Reasonable Security Procedures</u>***

The Interagency Guideline Establishing Information Security Standards promulgated by the five federal banking agencies require financial institutions to implement a comprehensive written security program. Among other objectives, the security program shall be designed to "protect against unauthorized access to or use of [customer]

[89] James Declaration, *supra* note 64, at 4.

[90] 2010 U.S. Dist. LEXIS 68149 at *17.

[91] UCC § 4A-202(c).

[92] 2010 U.S. Dist. LEXIS, 68149 at *14.

information that could result in substantial harm or inconvenience to any customer."[93] These guidelines require:

> an institution's information security program be monitored, evaluated, and adjusted as appropriate in light of changes in technology, the sensitivity of customer information, internal and external threats to information, the institution's changing business arrangements, and changes to customer information systems. These same criteria apply to re-evaluating the institution's Internet banking controls.[94]

The federal banking agencies issued specific guidance to banks for adopting security measures to avoid fraudulent EFTs in their October 2005 publication, Authentication in an Internet Banking Environment.[95] The Authentication Guidelines address the process of verifying the identity of a person or entity. Customers are authenticated by having them present one or more factors to prove their identity. The Guidelines outline the three basic "factors" in existing authentication methodologies:

> (1) *Something a person knows*—(*e.g.*, a password, PIN, or shared secret). If the customer types in the correct password, PIN, and/or correctly responds to a challenge question (shared secret), access is granted.
>
> (2) *Something a person has*—(*e.g.* password-generating token or USB token). Tokens are physical devices. A password-generating token produces a new, unique pass code every 30-60 seconds. A USB token is plugged into the customer's computer when accessing the bank's site.

[93] FFIEC, Interagency Guideline Establishing Information Security Standards (Mar. 29, 2005), at Sec. II, B. 3 (codified at 12 C.F.R. pt. 364, App. B (FDIC)); *see also* FFIEC, Interagency Guideline Establishing Information Security, Small-Entity Compliance Guide (Dec. 14, 2005).

[94] FFIEC, Frequently Asked Questions on FFIEC Authentication in an Internet Banking Environment, at 5 (Aug. 15, 2006).

[95] FFIEC, Authentication in an Internet Banking Environment (Oct. 12, 2005) [hereinafter the Authentication Guidelines].

> (3) *Something a person is*—(*e.g.*, biometric characteristic, such as fingerprint, voice pattern, eyes). A customer uses the fingerprint scanner attached to a computer to verify his identity.[96]

The federal banking 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."[97] The agencies state that "[a]ccount fraud and identity theft are frequently the result of single-factor (*e.g.*, ID/password) authentication exploitation."[98] Therefore,

> financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks, such as phishing, pharming, malware, and the evolving sophistication of compromise techniques. 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.[99]

The Authentication Guidelines outline additional control features that banks may employ as part of a multifactor authentication strategy. The first is "out-of-band" authentication which includes "any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction."[100] Examples of "out-of-band" procedures include callback verification to the same or another person at the customer, email approval or notification, or text message-based challenge/response processes.[101]

[96] *Id*. at 2, 7-11.
[97] *Id*. at 1.
[98] *Id*.
[99] *Id*. at 4 (footnotes omitted).
[100] *Id*. at 11.
[101] *Id*. at 3, 11-12.

A second category involves verification of internet protocol address[102] location and geo-location.[103] Each computer on the Internet is assigned an IPA. When a customer accesses the bank's site, a profile is created identifying the IPA used. If a new IPA is identified that does not match the customer's IPA profile, access to the bank's site will be denied. Geo-location is another technique to limit Internet users by determining where they are located to identify whether the distance is considered reasonable in relation to the bank.[104]

A third category is mutual authentication, whereby "customer identity is authenticated and the [bank's web] site is authenticated to the customer."[105] One method is "[t]he use of digital certificates coupled with encrypted communication (e.g. Secure Socket Layer, or SSL). . . ."[106]

Finally, the Authentication Guidelines advise: "Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. Much of this control is not based directly upon authentication. For example, a financial institution can analyze the activities of its customers to identify suspicious patterns[,]"[107] a common fraud detection technique long used by banks.

[102] Hereinafter IPA.

[103] *Id*. at 12.

[104] *Id*. at 12-13.

[105] *Id*. at 13.

[106] *Id*.

[107] *Id*. at 5. The Bank Secrecy Act ("BSA") requires banks to have BSA/anti-money laundering compliance programs and appropriate policies, procedures, and processes in place to monitor account activity and identify unusual activity, such as transactions that are inconsistent with the nature of the customer's business, or any other suspicious activity. *See generally* FFIEC, Bank Secrecy Act/Anti-Money Laundering Examination Manual (2010). The federal banking agencies view electronic banking as a "potentially higher-risk area" of banking, requiring commensurate anti-fraud policies, procedures, and processes. *See id*. at 208-33 (addressing electronic banking, funds transfers, and ACH transactions). Recently, the federal banking agencies implemented Identity Theft Red Flags Rules and Guidelines, requiring banks to have policies and procedures to identify patterns, practices, or activities that indicate the possible existence of identity theft. These rules apply to consumer accounts and other accounts for which there is a foreseeable risk of identity theft, such as

Further, "[f]inancial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit."[108]

As noted above, courts have not yet applied the multiple factor test in UCC § 4A-203(c) in determining whether a bank's security procedure was commercially reasonable, but one court has held that a reasonable finder of fact could find a breach of a duty of care by failure to adhere to the Authentication Guidelines.[109] Specifically, the court noted that the Authentication Guidelines "described single-factor identification (username/password) as 'inadequate' to secure online transactions of financial institutions."[110] While the bank had begun to implement additional measures by employing security tokens after the fraudulent EFTs at issue were effected, only a single-factor identification protected the customer's account.[111]

3. "Compliance" with Security Procedures and Written Instructions

Under the third element, the bank must prove that it complied with the security procedure in processing the payment order: "If the fraud was not detected because the bank's employee did not perform the acts required by the security procedure, the bank has not complied."[112]

Under the fourth element, the bank must similarly prove that it complied with "any written agreement or instruction of the customer restricting acceptance of payment orders . . . ."[113] The Comments recognize that "[a] customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank. . . .

small business and sole proprietorship accounts. *See, e.g.*, 12 C.F.R. § 334.90 (FDIC); 72 Fed. Reg. 63,718, at 63,721 (Nov. 9, 2007); FDIC Press Release, FDIC-PR-88-2009, Agencies Issues Frequently Asked Questions on Identity Theft Rules (June 11, 2009).

[108] *Id.*

[109] *Shames-Yeakel*, 677 F. Supp. 2d at 1008-09 (involving duty to protect customer information).

[110] *Id.*

[111] *Id.*

[112] UCC § 4A-203 cmt. 3.

[113] UCC § 4A-202(b).

Such limitations may be incorporated into the security procedure itself or they may be covered by a separate agreement or instruction."[114] The Comments provide several examples of the limitations customers may impose:

> the customer may prohibit the bank from accepting a payment order that is not payable from an authorized account, that exceeds the credit balance in specified accounts of the customer, or that exceeds some other amount. Another limitation may relate to the beneficiary. The customer may provide the bank with a list of authorized beneficiaries and prohibit acceptance of any payment order to a beneficiary not appearing on the list.[115]

4. Bank Must Prove it Acted in "Good Faith"

As the fifth and final element, the receiving bank must prove that it processed the payment order in good faith.[116] Under Article 4A, "good faith" is defined as "honesty in fact and the observance of reasonable commercial standards of fair dealing."[117] This definition includes the subjective element of good faith and objective element of the observance of reasonable commercial standards of fair dealing. "Although 'fair dealing' is a broad term that must be considered in context," the definition focuses on the "fairness" of the bank's conduct (not the care with which the act was performed).[118] "Honesty in fact" is measured by a subjective standard, and the court must examine the facts surrounding the transaction.[119] The bank's "observance of reasonable commercial standards of fair dealing" is evaluated by an objective measurement of the fairness of the party's action in light of prevailing commercial

[114] UCC § 4A-203 cmt. 3.

[115] ***Id***.

[116] UCC § 4A-202(b).

[117] UCC § 4A-105(d) (incorporating definitions in Article 1); UCC § 1-201(20).

[118] UCC § 1-201 cmt. 20.

[119] UCC 1-201 cmt. 20; Maine Family Credit Union v. Sun Life Assurance Co. of Canada, 727 A.2d 335, 340-42 (Me. 1999).

standards.[120] "Both components must be proved in order to establish good faith, and whether that has been done in a particular case presents a question that ordinarily must be resolved by the fact finder."[121] Under the old standard of "honesty in fact," a bank has been held unable to meet its burden of showing good faith if it acted with knowledge and disregard of suspicious circumstances.[122]

In *Experi-Metal, Inc.*, discussed above, the customer also argued that the bank failed to act in good faith. On January 22, 2009, criminals had hacked into the customer's account, and begun transmitting numerous wire transfer orders to the bank. Between 7:30 a.m. and 10:50 a.m., the bank processed 47 transfers from the customer's account to various accounts in Russia, Estonia, Scotland, Finland, and China, as well as domestic accounts. Between 10:53 a.m. and 2:02 p.m., the bank processed another 46 wire transfers. In total, the bank transferred $1.9 million out of the customer's account.[123]

In two prior years, the customer had only made two wire transfers, both in 2007.[124] The customer contended that the bank's failure to question the wire transfers in these circumstances constituted a lack of good faith.[125] The court agreed, finding a genuine issue of fact existed whether the bank acted in good faith in view of the customer's prior wire activity, the number of sudden wire transfers, and the destinations of the payments.[126]

[120] UCC 1-201 cmt. 20; *Maine Family Credit Union*, 727 A.2d at 340-42.

[121] San Tan Irrigation Dist. v. Wells Fargo Bank, 3 P.3d 1113, 1117 (Ariz. 2000).

[122] Savings Bank Trust Co. v. FRB of New York, 738 F.2d 573, 574 (2d Cir. 1984); *see also* John Hancock Fin. Services, Inc. v. Old Kent Bank, 185 F. Supp. 2d 771, 779 (E.D. Mich. 2002), *aff'd*, 346 F.3d 727 (6th Cir. 2003) (applying revised "good faith" definition).

[123] 2010 U.S. Dist. LEXIS 68149, *6-9.

[124] *Id*. at *19-20.

[125] *Id*. at *21.

[126] *Id*. at *18-19, 21-23 (*citing* In re Jersey Tractor Trailer Training, Inc., 580 F.3d 146 (3d Cir. 2009); *Maine Family Credit Union*, 727 A.2d 335).

B. When the Customer is the Not the Source of the Security Leak

An important exception exists to Article 4A's allocation of liability to the customer: under section 4A-203(a)(2) a customer will not bear the loss where the customer can prove the payment order was not issued by (a) the customer or its agent, or (b) someone who gained knowledge of the security procedure (***e.g.***, user ID, password, etc.) from the account holder or its agent.[127] This provision specifically eliminates negligence of the customer; the issue is whether the customer was the source, "regardless of how the information was obtained or whether the customer was at fault."[128] The exception functions like an affirmative defense in litigation, for which the customer bears the burden of proof under section 4A-203(a)(2).[129] As the Official Comments note, while the "burden of making available commercially reasonable security procedures is imposed on receiving banks," the corresponding "burden on the customer is to supervise its employees to assure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached."[130]

The purpose behind this exception is pragmatic, and based on the reality that criminals have two avenues of attack, against either the bank or the customer:

> Breach of a commercially reasonable security procedure requires that the person committing the fraud have knowledge of how the procedure works and knowledge of codes, identifying devices, and the like . . . [t]his confidential information must be obtained either from a source controlled by the customer or . . . by the receiving bank.[131]

[127] UCC § 4A-203(a)(2).
[128] *Id*.
[129] *Id*.
[130] UCC 4A-203 cmt. 3.
[131] UCC § 4A-203 cmt. 5.

As for evidence as to which party "leaked" the security information, the drafters note that internal investigations by the bank, the criminal authorities, and even bank examiners are the likeliest sources of proof: "Because a funds transfer fraud usually will involve a very large amount of money, both the criminal investigation and the internal investigation are likely to be thorough."[132]

For example, the FBI in late 2009 was conducting an investigation into the theft of tens of millions of dollars from Citibank, apparently caused by attacks on Citibank's systems by Russia-based hackers.[133] While the criminal investigation was ongoing, at least one theft (which may not be related to the larger attack) was discovered by Citibank investigators to be caused by malware residing on the customer's computers.[134] This might indicate the customer cannot meet its burden of proof under section 4A-203(a)(2), as the malware recorded his keystrokes directly from the computer.[135]

Most cases of electronic payment fraud involving commercial accounts originate with the customer; very few have been shown to involve hacking into the bank's system.[136] A recent FBI report, however, suggests that bank computer systems may be vulnerable to hacker incursions. The FBI reported that:

> FBI interviews revealed that the threat stems not only from the malware involved in these cases, but the vulnerabilities presented by the lack of controls at the financial institution or third-party provider level. For instance, in several cases banks did not have proper firewalls installed, nor anti-virus software on their servers or their desktop computers.[137]

[132] *Id*.

[133] Siobhan Gorman & Evan Perez, *FBI Probes Hack at Citibank*, WALL ST. J. (Dec. 22, 2009).

[134] *Id*. at A16.

[135] *Id*.

[136] Garver, *supra* note 3, at 11.

[137] FBI Intelligence Note, *supra* note 14.

Banks therefore should be wary that, even though their EFT security procedures may be commercially reasonable, their own computers systems do not expose them to liability for a loss, should those systems prove to be the source of a security information "leak."

Customers should also take advantage of steps to reduce exposure to loss from malware attacks, including such basic procedures as keeping firewall or anti-virus software current.[138] Both the American Bankers Association and the FBI advise that small and midsize businesses, as the targets of recent attacks, dedicate a separate computer for EFTs.[139] Experts also recommend using a less-common web browser such as Opera, or operating system, such as Ubuntu, "because attackers rarely create malware for them . . . ."[140] Further, customers should ask their bank to set up "dual controls" over accounts, which requires two employees' approval for transactions, as well as limits on the daily amounts of transfers.[141]

C. Article 4A's One-Year Notice Bar

Unless the customer objects to the fraudulent EFTs within one-year, its claims against the bank are subject to UCC Article 4A's one-year statute of repose.[142] UCC § 4A-505 provides:

> 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.

[138] Vamosi, *supra* note 19, at 41.
[139] Acohido, *supra* note 23.
[140] Richmond, *supra* note 14, at R4.
[141] *Id*.
[142] UCC § 4A-505 cmt.

As a statute of repose, section 4A-505 does not provide an "affirmative defense . . . often subject to tolling principles . . . [but] extinguishes a plaintiff's cause of action after the passage of a fixed period of time," here, one year.[143]

The duty of the customer to give notice to the bank is triggered by "recei[pt of] notification reasonably identifying the order . . . ."[144] Article 4A does not define "reasonably identify," so the courts have looked to other UCC provisions for assistance. The Second Circuit approved the trial court's use of the "objectively determinable" standard from UCC § 9-108, and held that monthly statements that provided the dollar amount, date, and identification number of wire transfers, as well as the account's balance, and monthly totals of wire transfers, provided sufficient information from which the customer could identify, and object to, any particular transfer.[145]

Upon receipt of this notification, the customer must notify the bank "of the customer's objection to the payment."[146] This notice must "identify which, if any, specific payments were disputed[,]" and "vague communication regarding suspicious activity cannot meet this requirement."[147] The Supreme Court of California found that the "purpose of the notification requirement is to inform the bank reasonably promptly that the customer believes it is liable for the loss."[148] To satisfy this purpose, the court applied an objective reasonableness test:

> We think the test should be whether, under all of the relevant circumstances, a reasonable bank would understand from the customer's communication that the customer was objecting to what the bank had done in

[143] Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 597 F.3d 84, 88 n.4 (2d Cir. 2010).

[144] UCC § 4A-505.

[145] *Ma*, 597 F.3d at 91.

[146] UCC § 4A-505.

[147] ReAmerica, S.A. v. Wells Fargo Bank Int'l, No. 04-5233, 2008 U.S. Dist. LEXIS 30614, *18-19 (S.D.N.Y. Mar. 18, 2008), *aff'd,* 577 F.3d 102 (2d Cir. 2009) (customer's communication that it might dispute payments insufficient under § 4A-505).

[148] Zengen, Inc. v. Comerica Bank, 158 P.3d 800, 811 (Cal. 2007).

> accepting the payment orders or otherwise considered the bank liable for the loss.[149]

Accordingly, the customer must notify the bank not only which specific payments are questioned, but must also actually dispute the payments (or even indicate the bank is liable for the loss) in order to satisfy UCC § 4A-505.

D. Common Law Claims

In seeking to recover losses for fraudulent EFTs due to malware, bank customers have asserted various common law claims, including breach of contract, negligence, gross negligence, negligent misrepresentation, fraud, breach of fiduciary duty, and breach of duty to protect customer's confidential information against identity theft, as well as claims under unfair trade practices statutes. Generally, common law claims will be displaced if they overlap with Article 4A or are "inconsistent" with Article 4A.

As its Prefatory Note indicates, Article 4A was intended to be comprehensive: "There is no consensus about the juridical nature of a wire transfer and consequently of the rights and obligations that are created. Article 4A is intended to provide the comprehensive body of law that we do not have today."[150] As a result of this careful, comprehensive balancing of interests, "resort to principles of law or equity outside of Article 4A is not appropriate to create right, duties, and liabilities inconsistent with those stated in this Article."[151]

The courts have interpreted these statements to preclude some, but not all, common law claims. For example, the Second Circuit has held that "Article 4A precludes customers from bringing common law claims inconsistent with the statute . . . ."[152] The court examined Article 4A's scope, noting it controlled "how electronic funds transfers are conducted and specifies certain rights and duties related to the execution

[149] *Id*. at 812.

[150] UCC Article 4A Prefatory Note.

[151] UCC § 4A-102 cmt.

[152] *Ma,* 597 F.3d at 89.

of such transactions."[153] Next, the court compared the allegations in the complaint, finding the "various claims concern alleged misconduct by Merrill Lynch with respect to its execution of electronic transfers."[154] Accordingly, the court held that common law claims for breach of contract, breach of fiduciary duty, and negligence were displaced.

In ***Zengen, Inc.***, the court applied a two-prong test for preclusion: where the common law claim would be inconsistent with Article 4A, and "where the circumstances giving rise to the common law claims are specifically covered by the provision of [Article 4A]."[155] The court then examined the negligence and breach-of-contract claims, finding the "gravamen of each" was that the "bank should not have accepted and executed the fraudulent payment orders."[156] Because the claims were therefore "squarely within the provisions" of Article 4A, they likewise were held displaced.[157]

In *Schlegel v. Bank of America*, [158] the Virginia Supreme Court held that common law claims arising from unauthorized payment orders were displaced, but distinguished those from claims based on the bank's subsequent freezing of funds. As in ***Zengen***, the court found that Article 4A's allocation of liability for unauthorized payment orders displaced the common law claims based on the bank's acceptance of the payment order.[159] The bank's actions, however, in freezing the funds in the account where they had been transferred, and refusing to return them to the customer "[was] not a situation covered by any of the particular provisions of [Article 4A]," and thus the resulting common law claims for conversion and breach of contract were held not displaced.[160]

[153] *Id*.

[154] *Id*. at 90.

[155] 158 P.3d at 808*; see also* Hunter v. Citibank, N.A., No. 09-02079, 2010 U.S. Dist. LEXIS 61912, *19 (N.D. Cal. Feb. 3, 2010) (claims displaced where "gravamen" was violation of transfer agreements between customer and bank).

[156] *Id*.

[157] *Id*. at 809.

[158] 628 S.E.2d 362, 367-68 (Va. 2006).

[159] *Id*. at 368.

[160] *Id*.

Applying this analysis, common law claims based on allegations that a bank accepted funds "when it knew or should have known that the funds were fraudulently obtained" have been held not displaced, because Article 4A is "silent" on the issue.[161] Negligence claims arising out of a beneficiary bank's erroneously informing an originator the transfer had not been received, however, was held displaced, as "[section 4A-404(b)] requires a bank to follow instructions to notify the beneficiary when it accepts a payment order, and provides a remedy if the bank does not do so."[162]

In sum, the question of displacement turns on the relationship between the acts underlying the common law claim and the "rights and obligations" created by Article 4A. The more those acts resemble a situation covered by Article 4A, they are more likely to be displaced.

E. Interbank Liability for Fraudulent Electronic Funds Transfers

The federal banking regulators warn banks to be alert for suspicious electronic deposits: "Money mule activity is essentially electronic money laundering addressed by the Bank Secrecy Act and Anti-Money Laundering Regulations. Strong customer identification, customer due diligence, and high-risk account monitoring procedures are essential for detecting suspicious activity, including money mule accounts."[163] Oftentimes, a bank may be able to recover some portion of fraudulent EFTs, depending on how quickly the bank or its customer discovered the fraud, the cooperation of the bank receiving the stolen funds (the "beneficiary bank" under Article 4A, or receiving depository financial institution[164] for ACH transfers under NACHA's rules), and whether the criminal has already withdrawn the stolen funds. Apart from such voluntary cooperation, a customer and its bank generally have little to no recourse against beneficiary banks or RDFIs.

[161] Regions Bank v. Provident Bank, Inc., 345 F.3d 1267, 1275 (11th Cir. 2003).

[162] Moody Nat'l Bank v. Texas City Dev. Ltd., Co., 46 S.W.3d 373, 378 (Tex. App. 2001).

[163] FDIC Special Alert, SA-185-2009, *supra* note 7.

[164] Hereinafter RDFI.

Under UCC Article 4A, the liability of a beneficiary bank is limited to defined circumstances that are generally unlikely, such as where the beneficiary bank knows that the name and account number on the wire transfer order refer to different persons.[165] As applicable to ACH transfers, under the NACHA Operating Rules, the customer's bank, the originating depository financial institution[166] warrants, "to each RDFI, ACH Operator, and Association" that "each entry transmitted by the ODFI to an ACH Operator is in accordance with proper authorization provided by the Originator and the Receiver."[167] ODFIs may make return requests for erroneous entries under Section 8.2.[168] The period for requesting a return entry on an ACH transaction is two days.[169] In view of the ODFI's warranty, the RDFI is not required to return the ACH transfer, unless it has not yet posted the transfer to the receiver's account.[170]

Unless displaced by Article 4A, as discussed above, a customer or its bank potentially may have common law claims against the beneficiary bank under certain circumstances. For example, in ***Regions Bank v. Provident Bank, Inc***.,[171] the court held:

> Article 4A is silent with regard to claims based on the theory that the beneficiary bank accepted funds when it knew or should have known that the funds were fraudulently obtained. Therefore, a provision of state law that requires a receiving or beneficiary bank to disgorge funds that it knew or should have known were obtained illegality when it accepted a wire transfer is not inconsistent with the goals or provisions of Article 4A.[172]

[165] UCC § 4A-207.

[166] Hereinafter ODFI.

[167] NACHA Operating Rules, §§ 2.2.1 and 2.2.1.1 (2010).

[168] *Id*. at § 8.2.

[169] *Id*. at § 6.1.2 (must be made to the RDFI's ACH Operator in time to "be available to the ODFI no later than the opening of business on the second banking day following the Settlement Date of the original entry"); GEVA, *supra* note 29, § 5.05[4][b] (same two-day deadline in Section 6.1.2 also applies to ODFI return requests).

[170] NACHA Operating Rules, § 6.1.5 (2010).

[171] 345 F.3d 1267 (11th Cir. 2003).

[172] *Id*. at 1276.

IV.
IMPLICATIONS FOR INSURANCE COVERAGE

Some banks, particularly community banks, often reimburse the customer for electronic fraud losses to maintain the business relationship, even though not legally responsible.[173] In that event, if an insured bank has paid a fraudulent EFT claim but failed to assert an applicable defense, the payment may be considered voluntary and thus not a covered loss.[174] When an insured bank is settling or has settled a covered claim, one factor an insurer should evaluate is the extent to which, if any, the proposed or made payment may have been based on factors other than the covered legal liability. An insured may have a strong desire to settle the claim for business reasons, such as maintaining profitable business relationships, avoiding adverse publicity, avoidance of future defense costs, especially with "aggressive" opposing counsel, interruption to the insured's normal business through onerous discovery, and the fear of bad faith damages or other sanctions. As institutions of trust, banks especially want to avoid adverse publicity that would raise questions concerning the safety of depositors' funds. Banks also have a strong desire to maintain the confidentiality of their internal procedures, particularly those related to fraud prevention, that could be lost at a public trial. To the extent a settlement involving fraudulent EFT claims reflects concerns other than the covered liability under applicable law, the loss sustained by the insured may not have been caused by the covered event.[175]

[173] Garver, *supra* note 3, at 11.

[174] ***E.g.***, Aetna Life and Cas. Co. v. Hampton State Bank, 497 S.W.2d 80 (Tex. App. 1973) (coverage denied for payment by depositary to drawee under warranty claim where depositary failed to raise fictitious-payee defense).

[175] ***See*** First Nat'l Bank of Memphis v. Aetna Cas. and Surety Co., 309 F.2d 702, 705 (6th Cir. 1962)("considerations other than legal liability such as attorneys fees, costs and expenses, and the time taken by . . . officers and employees in preparation for and the defense of" litigation "cannot be made the basis for imposing liability . . . for the sums paid out in settlement"), ***cert. denied***, 372 U.S. 953 (1963); ***cf.*** KAMI Kountry Broadcasting Co. v. USF&G Co., 208 N.W.2d 254 (Neb. 1973)(insured radio station's settlement was voluntary where employee forged president's signature on loan note, insured first denied liability, and then paid bank in face of threat to pull advertising).