Surging, Swift and Liable? Cybercrime and Electronic Payments Fraud Involving Commercial Bank Accounts: Who Bears the Loss?

By Salvatore Scanio and Robert W. Ludwig

Bank robbery is down by half over the last decade,[1] check fraud has declined in recent years, and cybercrime is surging.[2] As financial transactions have migrated from cash to checks and other negotiable instruments, and today to electronic transfers, so too have criminals. Not only is that "where the money is" as bank robber Willie Sutton once put it, but to younger and more sophisticated thieves that target banks and their customers online, it is more quickly and easily obtained, in larger amounts, than ever before.

In the late 2000's criminals engaged in online banking fraud began to target business accounts. The typical corporate "account takeover" scenario involved a targeted business receiving a "phishing" email directing the recipient to a phony website or to an infected attachment, resulting in data entry on the phony website or the installation of malware (malicious software) on the target's computer. Either way, thieves then harvest the target's corporate bank account login information, with which they originate unauthorized funds transfers.

Malware and other techniques employed by cybercriminals are constantly evolving, from phishing to "man-in-the-middle" attacks (which hijack a customer's online banking session or intercept security token codes in real-time), to installing malware on personal and business mobile devices to gain access to corporate enterprise systems and accounts through infected or phony apps or text messages ("smishing"), social media scams, interception of telephone lines used for verification, phony bank online chat sessions, and direct attacks on banks and their employees.

THE LEGAL FRAMEWORK FOR ALLOCATING COMMERICAL EFT FRAUD

The legal framework applied today to address cybercrime dates to the 1980s—before online Internet and mobile banking was ever contemplated.[3] That decade marked a shift in banking to electronic funds transfers ("EFTs"), the advent of the personal computer and Internet, and the drafting of Article 4A of the Uniform Commercial Code ("UCC") to address EFTs. By then, the dollar volume of wires and other electronic transfers, over a trillion dollars a day, far exceeded the volume of payments by other means.[4] Unlike checks, governed for decades by Negotiable Instruments Law and currently UCC Articles 3 and 4, there was no comprehensive body of law that defined the rights and obligations that arose from electronic transfers. In 1989, Article 4A was proposed by the National Conference of Commissioners on Uniform State Law to provide that body of law.

The drafters of Article 4A recognized that an electronic transfer is "not comparable to payment of a

Salvatore Scanio and Robert W. Ludwig *are members of the law firm Ludwig & Robinson PLLC in Washington, DC, with a national and international practice in banking, insurance and litigation matters. Mr. Scanio, formerly in-house bank counsel, earned JD, MBA and BA degrees from Tulane University. He may be reached at sscanio@ludwigrobinson.com or 202-289-7605. Mr. Ludwig, with twenty years' experience litigating bank fraud matters, has a JD from Washington and Lee University School of Law. He may be reached at rludwig@ludwigrobinson.com or 202-289-7603.*

check by the drawee bank on the basis of a signature that is forged" or on altered or counterfeit paper, and thus new rules were required.[5] Rather, "the receiving bank relies on a security procedure pursuant to which the authenticity of the [EFT] message can be 'tested' by various devices … designed to provide certainty that the message is that of the sender indentified in the payment order."[6] Because EFTs typically are in large amounts, often multimillion dollar "wholesale wire transfers," completed the same day, between sophisticated business or financial organizations, and intended to be efficient, low-cost substitutes for paper instruments, Article 4A was drafted with those defining characteristics in mind, and establishes governing principles and rules that were intended to provide for concomitant efficient, low-cost allocation of risk of loss.[7]

Commercial bank customers utilize two primary types of EFTs: traditional wire transfers and Automated Clearing House ("ACH") transactions. Most wire transfers in the United States are conducted via Fedwire, a system operated by the Federal Reserve Banks.[8] 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."[9] Businesses typically use the ACH system to make payroll and vendor payments.

Wire transfers and commercial ACH transactions are governed primarily by UCC Article 4A, as adopted by the states.[10] In contrast, consumer ACH transactions are governed by the Electronic Funds Transfer Act ("EFTA"),[11] generally providing a limit of $50 on the loss that can be allocated to an account holder for any "unauthorized electronic fund transfers."[12]

Generally, UCC § 4A-204 imposes liability on a receiving bank[13] for unauthorized transfers by requiring the bank to refund any funds (plus interest) from a payment order[14] that was neither: (1) authorized by the customer under UCC § 4A-202, nor (2) enforceable against the customer under UCC § 4A-203, as not caused by (a) an authorized employee or (b) a person who obtained access to its transmitting facilities, or otherwise obtained transmittal information from the customer. Thus, whether the risk of loss for an unauthorized EFT falls upon the bank or the customer is governed by UCC §§ 4A-202 and 203.

Under subsection 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. Subsection 4A-202(b) further permits the receiving bank to escape liability, even though the customer did not authorize the payment order, if the bank proves: (1) the bank and customer agreed the authenticity of a payment order would be verified through a "security procedure;" (2) the security procedure agreed upon by the bank and customer is "commercially reasonable;" (3) the bank processed the payment order 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."[15]

If these five elements are not met, however, the bank will be strictly liable for any unauthorized EFT.[16] Moreover, even if these conditions are met, the risk of loss will still shift to the bank if "the person committing the fraud did not obtain the confidential information [facilitating breach of the security procedure] from an agent or former agent of the customer or from a source controlled by the customer. …"[17]

"SECURITY PROCEDURE" DEFENSE

As will be shown below, in assessing whether a bank or its customer should bear the loss for a fraudulent EFT, the key determination is whether the bank's security procedures were commercially reasonable under the UCC and newly developing case law. This determination focuses on: (a) the terms of bank-customer agreements; (b) whether the bank's security procedures complied with banking agency guidelines; (c) whether the bank's security procedures were designed to meet the circumstances of the customer, as opposed to a one-size-fits-all approach; and (d) whether the bank implemented and followed readily available security procedures in connection with the transactions at issue.

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."[18] A "security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices."[19]

In *Experi-Metal, Inc. v. Comerica Bank*,[20] 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).[21] In an effort to avoid liability under UCC § 4A-202(c), discussed *infra*, the bank contended it offered the customer the ability to require two individuals to approve wire transfers as an additional security procedure, but the customer refused that procedure.[22] The U.S. District Court for the Eastern District of Michigan rejected this argument, concluding that "requiring confirmation by additional users simply is an option or element within a security procedure. The 'security procedure' is the secure token technology."[23] As discussed *infra*, the court found this security procedure to be commercially reasonable.

A "security procedure," however, does not include "procedures that the receiving bank may follow unilaterally in processing payment orders,"[24] such as its internal policies and procedures. Thus, a bank cannot point to its internal procedures which are not contained in the customer agreement to bolster its "security procedure" as being "commercially reasonable." In *Chavez v. Mercantil Commercebank, N.A.*,[25] the U.S. Court of Appeals for Eleventh Circuit recently rejected a bank's attempt to use a catch-all clause in its customer agreement that the bank "may use … any other means to verify any Payment Order or related instruction" to show additional internal procedures were part of its "security procedures" where the agreement provided a specific security procedure. 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 to whether there was "compliance" with the "security procedure" in processing the wire or ACH transfers. By the same token, a bank's failure to follow its internal procedure for processing EFTs should be not be considered a failure to follow an agreed upon "security procedure."[26]

A specific "security procedure" does not need to be identified in the customer agreement if it simply provides that the bank will select security procedures that are commercially reasonable, according to the U.S. District Court for the Southern District of New York in *Brago Filho v. Interaudi Bank*,[27] where the court reasoned:

> By signing the [customer agreement] plaintiffs agreed to the Bank's security procedures, so long as they are found to be commercially reasonable. It does not matter that plaintiffs did not know what the Bank's security procedures were because [UCC Article 4A] compels banks to use commercially reasonable procedures. Indeed, a bank that chooses unreasonable procedures does so at its peril.[28]

COMMERCIALLY REASONABLE SECURITY PROCEDURES

Legal Standards. The UCC's drafters recognized that a principal issue likely to arise in litigation involving fraudulent EFTs is whether any security procedure in effect was commercially reasonable.[29] To promote uniformity the drafters provided, unlike in UCC Articles 3 and 4, that the issue of "commercial reasonableness of a security procedure is a question of law" under Article 4A.[30] As explained in the Article 4A Official Comments ("Comments"): "It 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."[31] Whether the bank complied with the security procedures, however, remains a question of fact.[32]

A court may find a security procedure to be commercially reasonable in one of two ways. Under the first method, 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.[33]

The focus in this provision is 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.[34]

In cases where a customer rejects security measures offered by the bank, the customer will bear the risk of loss, and not be able to complain that the bank acted "in bad faith by so doing so long as the customer is made aware of the risk."[35]

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."[36] Article 4A recognizes that prudent banking practices require that security procedures should be utilized for all EFTs, and that "[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."[37]

The second method is more complex. Whether a security procedure is commercially reasonable is determined by considering primarily four 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."[38]

The application of these factors is not a simple task. According to the Comments, "the concept of what is commercially reasonable in a given case is flexible," a pronouncement at odds with Article 4A's policy goal of creating a uniform standard by having the issue decided as a matter of law.[39] The Comments also contain other conflicting guidance:

> 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.[40]

In addition, the Comments introduce other 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 transmits payment orders infrequently or in relatively low amounts.[41]

The second "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."[42] A third 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."[43]

Numerous lawsuits have been filed in recent years by customers seeking recovery from their banks for fraudulent EFTs arising from malware attacks, presenting the issue of whether the bank's security procedures were commercially reasonable. Most of these cases have settled, and only a few have resulted in judicial decisions.

In *Patco Constr. Co., Inc. v. People's United Bank*,[44] the U.S. Court of Appeals for the First Circuit, reversing a district court in Maine,[45] held that the bank's security procedures were not commercially reasonable. In *Patco*, a customer's computer had been infected by the Zeus/Zbot malware allowing cybercriminals to steal Patco's login credentials and fraudulently withdraw $588,851 through a series of large ACH transfers over several days in May 2009.[46] Patco had used online banking to make ACH transfers for weekly payroll payments involving recurrent characteristics: they were always made on Fridays; were initiated from computers in Patco's office in Sanford, Maine; originated from a single static Internet Protocol ("IP") address; were accompanied by tax witholdings and 401(k) contributions; and were modest amounts, the largest being $36,634.[47] The security procedure utilized by the bank consisted of: (1) user IDs and passwords; (2) invisible device authentication, which placed "device cookies" to identify computers used to access online banking; (3) risk profiling, consisting of a profile for each customer based on its online banking usage, to compare the transaction at issue; and (4) challenge questions and answers based on a dollar threshold for certain transactions.[48] The bank originally set the challenge question procedure to transactions over $100,000 for all customers, and subsequently lowered the threshold to $1.[49] As the First Circuit noted, "[t]here were several additional security measures that were available to [the bank] that [it] chose not to implement," including (1) Out-of-Band Authentication, such as notification to the customer via telephone or other means; (2) User-Selected Picture; (3) Password-generating Security Tokens; and (4) Monitoring of Risk-Scoring Reports (with the latter two procedures adopted by the bank after the fraud occurred).[50] The fraudulent withdrawals were directed to new payees, originated from computers not recognized by the bank, and from an IP address that Patco had never used before, resulting in high risk scores of 790, 785, 720, and 563, a "significant departure" from Patco's usual risk scores of 10 to 214, but the bank did not have any procedure in place to monitor high risk scores or to notify the customer.[51]

The First Circuit concluded that the bank's collective failures rendered its security procedures commercially unreasonable:

> In our view, Ocean Bank did substantially increase the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and high dollar transfers [because frequent answers were more exposed to capture by malware]. Then, when it had warning that such fraud was likely occurring in a given transaction, Ocean Bank neither monitored the transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable.[52]

The First Circuit emphasized that the bank's adoption of a "one-size-fits-all" $1 threshold for all customers, to target universally low-dollar fraud, violated "Article 4A's instruction to take the customer's circumstances into account."[53] The court also based its conclusion on the fact that the bank did not utilize other security measures "not uncommon" in the industry, including manual reviews of high risk transactions and the use of password-generating security tokens.[54]

In two other recent cases, however, the courts focused on the content of bank-customer contracts in finding that the bank's security procedures were commercially reasonable. In *Experi-Metal*,[55] the district court held the security procedure to be commercially reasonable, finding that under the "plain and unambiguous terms of the [deposit agreements, the bank's] secure token technology was reasonable" because the customer so agreed in its contract with the bank.[56] The court rejected as parole evidence the customer's expert's opinion that secure token technology was not a commercially reasonable security procedure.[57] In *All American Siding & Windows, Inc. v. Bank of America, N.A.*,[58] a Texas court similarly relied on online banking agreements in which the customer "agreed that the authenticity of ACH transactions were to be

verified using an ID, passcode, and digital certificate verification."[59] Based on those agreements and the bank's affidavit that it "follow[ed] the guidelines of the Federal Financial Institution Examination Counsel and requires multifactor authentication for its online banking customers," the court concluded that the security procedures were commercially reasonable, entitling the bank to summary judgment.[60]

Banking Regulatory Agency Guidelines. As recognized by the First Circuit in *Patco*, the guidelines issued by the Federal Financial Institutions Examination Council ("FFIEC") establish relevant guideposts for evaluating whether banks security procedures are commercially reasonable.[61] To begin with, financial institutions are required to have a comprehensive written information security program. Among other objectives, the security program shall be designed to "protect against unauthorized access to or use of [customer] information that could result in substantial harm or inconvenience to any customer."[62] 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.[63]

FFIEC, and the federal banking agencies in turn, issued specific guidance to banks for adopting security measures to avoid fraudulent EFTs in its October 2005 publication, *Authentication in an Internet Banking Environment* (the "FFIEC 2005 Guidelines").[64] At that time, the agencies "consider[ed] 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."[65] The agencies stated that "[a]ccount fraud and identity theft are frequently the result of single-factor (*e.g.*, ID/password) authentication exploitation."[66] Thus, "financial institutions should implement multifactor authentication, layered security, or other controls … in light of new or changing risks, such as phishing, pharming, malware, and the evolving sophistication of compromise techniques."[67]

The FFIEC 2005 Guidelines outlined 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."[68] 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.[69] A second category involves verification of internet protocol address ("IPA") location and geo-location.[70] 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.[71] A third category is mutual authentication, whereby "customer identity is authenticated and the [bank's web] site is authenticated to the customer."[72] One method is "[t]he use of digital certificates coupled with encrypted communication (*e.g.*, Secure Socket Layer, or SSL)…."[73]

Finally, the FFIEC 2005 Guidelines advised: "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[,]"[74] a common fraud detection technique long used by banks. 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."[75]

In June 2011, FFIEC issued a *Supplement to Authentication in an Internet Banking Environment* ("FFIEC 2011 Supplement"), recommending that banks use a layered security framework, covering five core areas: (1) fraud detection and monitoring; (2) multifactor authentication; (3) Internet protocol and device analysis; (4) transaction limits and controls; and (5) customer education.[76] FFIEC observed that "manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers

being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior."[77] Therefore, as part of a bank's layered security program, the following two elements are now mandated. First, a bank's program must have "processes to detect anomalies and effectively respond to suspicious or anomalous activity related to:" (a) customer login and authentication; and (b) online funds transfers.[78] Second, the program should include enhanced controls for customer administrators who have authority to set up or change system configurations.[79] The agencies also point out that "[l]ayered security controls do not have to be complex. For example, implementing time of day restrictions on the customer's authority to execute funds transfers or using restricted funds transfer recipient lists, in addition to robust logon authentication, can help to reduce the possibility of fraud."[80]

Because most banks rely on third-party technology service providers for their Internet banking platform, FFIEC has recently re-emphasized that banks have ultimate responsibility for such outsourced activities. In October 2012, FFIEC issued two manuals in this area: the *Supervision of Technology Service Providers*, part of its *IT Examination Handbook*; and new *Administrative Guidelines for the Implementation of the Interagency Program for the Supervision of Technology Service Providers*.

In January 2013, FFIEC proposed guidelines to address activities conducted via social media by banks. As "[s]ocial media is one of several platforms vulnerable to account takeover and the distribution of malware," FFIEC and the federal banking agencies advise that banks "should ensure that the controls it implements to protect its systems and safeguard customer information from malicious software adequately address social media usage. Financial institutions' incident response protocol regarding a security event, such as a data breach or account takeover, should include social media, as appropriate."[81]

"COMPLIANCE" WITH SECURITY PROCEDURES AND WRITTEN INSTRUCTIONS

Under the third element of UCC subsection 4A-202(b), 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."[82]

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 . . . ."[83] The Comments recognize that a customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank . . . . Such limitations may be incorporated into the security procedure itself or they may be covered by a separate agreement or instruction."[84] The Comments provide several examples of the limitations customers may impose:

> [T]he 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.[85]

As discussed, the banking agencies recognize these types of limitations as an appropriate part of a bank's layered security control program.

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.[86] Under Article 4A, "good faith" is defined as "honesty in fact and the observance of reasonable commercial standards of fair dealing."[87] "Honesty in fact" is measured by a subjective standard, requiring a court to examine the facts surrounding the transaction.[88] The bank's "observance of reasonable commercial standards of fair dealing," however, is evaluated by an objective measurement of the fairness of the party's action in light of prevailing commercial standards.[89] "Although 'fair dealing' is a broad term that must be defined in context, it is clear that it is concerned with the fairness of conduct rather than the care with which an act is performed."[90]

In *Experi-Metal*, having concluded that the security procedure was commercially reasonable, the court then addressed the further issue whether the bank handled the wires at issue in good faith. On January 22, 2009, criminals had hacked into the customer's account, and between 7:30 a.m. and 10:50 a.m., the bank processed 47 wire transfers to accounts in Russia, Estonia, Scotland, Finland, China, and the United States. Between 10:53 a.m. and 2:02 p.m., the bank processed another 46 wires. Altogether the bank transferred $1.9 million from the customer's account.[91] In two previous years, the customer had made only two wire transfers, both in 2007.[92] In view of prior wire activity, the number of sudden wire transfers, and the destinations of the payments, the court found a genuine issue of fact existed whether the bank acted in good faith.[93] At a bench trial, the court ruled in favor of the customer. The bank presented evidence only on the subjective element of good faith, failing to "present evidence from which this Court could determine what the 'reasonable commercial standards of fair dealing' are for a bank responding to a phishing incident such as the one at issue and thus whether" the bank satisfied "the objective prong of the 'good faith' requirement."[94] As a result, the court as "trier of fact [was] 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."[95]

CUSTOMER RESPONSIBILITY WHEN BANK FAILS TO USE COMMERICALLY REASONABLE SECURITY PROCEDURE

In *Patco*, after finding the bank's security procedure to be commercially unreasonable, the First Circuit affirmed the denial of Patco's cross-motion for summary judgment and remanded the case. Raising an issue not reached or briefed below, the appeals court noted that "[i]t is unclear … what, if any, obligations a commercial customer has when a bank's security system is found to be commercially unreasonable."[96] While seemingly broad, the issue as framed by the First Circuit narrowly addressed the remaining loss-allocation rule of Article 4A, section 4A-204.[97] That section provides, *inter alia*, that where no commercially reasonable security procedure is in effect, the bank shall refund any unauthorized payments, and further, pay interest unless "the customer fails to exercise ordinary care to determine that the order was not authorized … and to notify the bank … within a reasonable period of time not exceeding 90 days … ."[98] This customer obligation of ordinary care pertains only to whether it may recover interest, otherwise "the bank takes the risk of loss with respect to an unauthorized payment order. … "[99] On remand, the parties settled without briefing the issue, with the bank agreeing to pay Patco's unrecovered loss in full, plus interest,[100] in a case where the losses occurred over a matter of days, well within the 90-day limit of subsection 4A-204(a) or other "reasonable time" within which Patco could have reasonably become aware of the fraud.

LIABILITY WHEN THE CUSTOMER IS 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 be obligated to bear the loss where it can prove the payment order was not issued by (a) it or its agent, or (b) someone who gained knowledge of the security procedure (*e.g.*, user ID, password, etc.) from it or its agent.[101] 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."[102] The exception functions like an affirmative defense in litigation, for which the customer bears the burden of proof under section 4A-203(a)(2).[103] As the 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."[104] 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.[105]

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.[106] Recent FBI reports, however, suggest that bank computer systems may be vulnerable to hacker incursions. In one report, the FBI noted:

> 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.[107]

In another report, the FBI described a "new trend" in which bank employees credentials have been stolen to generate fraudulent customer wire transfers. Specifically, the cyber criminals used spam, phishing e-mails, keystroke loggers, remote access Trojans ("RATs") and variants of Zeus malware to steal bank employee credentials providing the thieves with access to the bank's networks. The stolen credentials were used to initiate fraudulent wire transfers overseas in amounts varying between $400,000 and $900,000. In some of the incidents, the bank also suffered a distributed denial of service ("DDoS") attack against its internet banking system, thereby preventing bank personnel from identifying and stopping the fraudulent transactions.[108] In December 2012, the Comptroller of the Currency ("OCC") issued an alert concerning DDoS attacks and their relation to customer account fraud. The OCC reiterated its "expectations that banks should have risk management programs to identify and appropriately consider new and evolving threats to online accounts and to adjust their customer authentication, layered security, and other controls as appropriate in response to changing levels of risk."[109] Banks should therefore 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 losses from malware attacks, including such basic procedures as keeping firewall or anti-virus software current. 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.[110] Experts also recommend using a Live CD approach for online banking,[111] or less-common web browser (such as Opera) or operating system (such as Ubuntu) "because attackers rarely create malware for them. . . ."[112] Further, customers may ask their bank to set up "dual controls" over accounts, requiring two employees' approval for transactions, establish limits on the amounts of transfers, and implement restricted funds transfer recipient lists.[113]

NOTES

1. Jack Nicas, *Crime That No Longer Pays, Bank Robberies on the Decline as Criminals See Greater Rewards in Online Theft*, Wall Street Journal (Feb. 5, 2013), at A3.
2. *See generally*, Internet Crime Complaint Center, 2011 *Internet Crime Report*.
3. *See generally*, Mary J. Cronin (ed.), Banking and Finance on the Internet (1997).
4. UCC Art. 4A, Prefatory Note.
5. UCC § 4A-203, cmt. 1.
6. *Id.*
7. *Id.*
8. Benjamin Geva, The Law of Electronic Funds, § 1.04[3] (Dec. 2009).
9. *Id.* at § 1.04[4].
10. Wire transfers conducted over the FedWire system are subject to Federal Reserve Regulation J, which incorporates UCC Article 4A. *See* 12 C.F.R. § 210.25(b)(1); Utility Supply Co. v. AVB Bank, 2010 U.S. Dist. LEXIS 126948, *9-14 (N.D. Okla. Nov. 30, 2010) (wire transfers conducted over FedWire are governed by Regulation J, incorporating UCC Article 4A as Appendix B to 12 C.F.R. part 210, thereby presenting a federal question). By 1996, Article 4A was adopted by all the states and the District of Columbia. Geva, *supra* note 8, at § 1.05[2]. ACH transactions are also subject to the Operating Rules of the National Automated Clearing House Association ("NACHA").
11. UCC § 4A-108 ("This Article does not apply to a funds transfer any part of which is governed by the [EFTA]"). The EFTA applies to transfers of funds involving accounts "established primarily for personal, family, or household purposes." 15 U.S.C. § 1693a(2). For a case involving a determination of whether accounts involved in fraudulent EFTs were primarily business or consumer accounts, *see* Shames-Yeakel v. Citizens Fin'l Bank, 677 F. Supp. 2d 994, 1002-03, 1006-07 (N.D. Ill. 2009) (applying Truth in Lending Act and EFTA).
12. 15 U.S.C. § 1693g.
13. A "receiving bank" is the bank receiving the payment order; typically, the customer's bank. UCC § 4A-103(a)(4).
14. A "payment order" is the instruction to the receiving bank to pay a fixed or determinable amount of money. UCC § 4A-103(a)(1).
15. UCC § 4A-202(b).
16. UCC § 4A-204(a).
17. UCC § 4A-203 cmt. 5.
18. UCC § 4A-201.
19. *Id.*
20. 2010 U.S. Dist. LEXIS 68149 (E.D. Mich. July 8, 2010).

21. *Id.* at *11-14.
22. *Id.* at *11-14.
23. *Id.* at *14.
24. UCC § 4A-201 cmt.
25. 2012 U.S. App. LEXIS 24358, at *15-22 (11th Cir. Nov. 27, 2012).
26. *See* Skyline Int'l Development v. Citibank, F.S.B., 706 N.E.2d 942, 945 (Ill. App. 1998) (bank's admission of failure to follow internal procedure for obtaining authorization for wire transfers was not relevant to whether bank followed agreed "security procedure").
27. 2008 U.S. Dist. LEXIS 31443 (S.D.N.Y. Apr. 16, 2008).
28. *Id.* at *15.
29. UCC § 4A-203 cmt. 4.
30. UCC § 4A-202(c); *compare* UCC § 3-103(a)(9)(reasonable commercial standards applicable to claims under UCC Articles 3 and 4).
31. UCC § 4A-203 cmt. 4.
32. *Id.*
33. UCC § 4A-202(c).
34. UCC § 4A-203 cmt. 4.
35. UCC §4A-203 cmt. 4.
36. UCC § 4A-203 cmt. 3.
37. *Id.*
38. UCC § 4A-202(c).
39. UCC § 4A-203 cmt. 4.
40. *Id.*
41. *Id.*
42. *Id.*
43. UCC § 4A-203 cmt. 4.
44. 684 F.3d 197 (1st Cir. 2012).
45. 2011 U.S. Dist. LEXIS 58112 (D. Me. May 27, 2011), *adopted by*, 2011 U.S. Dist. LEXIS 86169 (D. Me. Aug. 4, 2011).
46. 684 F.3d at 204-06.
47. *Id.* at 200.
48. *Id.* at 202-03.
49. *Id.* at 203.
50. *Id.* at 203-04.
51. *Id.* at 204-05.
52. *Id.* at 211.
53. *Id.* at 212.
54. *Id.* at 212-13.
55. 2010 U.S. Dist. LEXIS 68149 at *16-17.
56. *See also* Transamerica Logistic, Inc. v. JPMorgan Chase Bank, N.A., 2008 U.S. Dist. LEXIS 112708, at *3 & n.1 (S.D. Tex. July 21, 2008) (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 did not offer any "contradictory evidence or argument").
57. *Id.*
58. 367 S.W.3d 490 (Tex. App. 2012).
59. *Id.* at 500-501.
60. *Id.* at 500-502.
61. 684 F.3d at 201-04.
62. FFIEC, *Interagency Guidelines 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 Guidelines Establishing Information Security, Small-Entity Compliance Guide* (Dec. 14, 2005); FFIEC, *Information Security, IT Examination Handbook* (July 2006).
63. FFIEC, *Frequently Asked Questions on FFIEC Authentication in an Internet Banking Environment*, at 5 (Aug. 15, 2006).
64. FFIEC, *Authentication in an Internet Banking Environment* (Oct. 12, 2005).
65. *Id.* at 1.
66. *Id.*
67. *Id.* at 4 (footnotes omitted).
68. *Id.* at 11.
69. *Id.* at 3, n.5, 11-12.
70. *Id.* at 12.
71. *Id.* at 12-13.
72. *Id.* at 13.
73. *Id.*
74. *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). FFIEC views 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). The federal banking agencies have also 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 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* (Jun. 11, 2009).
75. *Id.*
76. FFIEC, *Supplemental to Authentication in an Internet Banking Environment* (June 28, 2011), at 3-8.
77. *Id.* at 5.
78. *Id.*
79. *Id.*
80. *Id.* at 11-12.
81. FFIEC, *Social Media: Consumer Compliance Risk Management Guidance* (Jan. 17, 2013), at 30.
82. UCC § 4A-203 cmt. 3.
83. UCC § 4A-202(b).
84. UCC § 4A-203 cmt. 3.
85. *Id.*
86. UCC § 4A-202(b).
87. UCC § 4A-105(d) (incorporating definitions in Article 1); UCC § 1-201(20).
88. UCC 1-201 cmt. 20; Maine Family Fed. Credit Union v. Sun Life Assurance Co. of Canada, 727 A.2d 335, 340-42 (Me. 1999).
89. UCC 1-201 cmt. 20; Maine Family Fed. Credit Union, 727 A.2d at 340-42.
90. UCC § 1-201 cmt. 20
91. 2010 U.S. Dist. LEXIS 68149, *6-9.

92. *Id.* at *19-20.
93. *Id.* at *18-19, 21-23 (citing *In re* Jersey Tractor Trailer Training, Inc., 580 F.3d 147 (3d Cir. 2009) and Maine Family Fed. Credit Union, 727 A.2d 335).
94. Experi-Metal, Inc. v. Comerica Bank, 2011 U.S. Dist. LEXIS 62677, *35 (E.D. Mich. June 13, 2011).
95. *Id.* at *38.
96. *Id.* at 214-15.
97. *Id.* at 214. The First Circuit also acknowledged the Comment to section 4A-102, which states: "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."
98. UCC § 4A-204(a) & cmt. 1. What is a reasonable time depends on the facts of the particular case. For example, as explained in the Comment: "If a payment order for $1,000,000 is wholly unauthorized, the customer should normally discover it in far less than 90 days." *Id.*, cmt. 1.
99. UCC § 4A-204(a) cmt. 1.
100. Pamela Ryckman, *A Win for Small Businesses in a Bank Fraud Case*, New York Times, (Dec. 12, 2012), available at *http://boss.blogs.nytimes.com/2012/12/12/a-win-for-small-businesses-in-bank-fraud-case/* (last visited Feb. 4, 2013). The bank did not pay Patco's attorney's fees, which approximated the $350,000 loss, while incurring an estimated $1 million in fees itself. *Id.*
101. UCC § 4A-203(a)(2).
102. *Id.*
103. *Id.*
104. UCC 4A-203 cmt. 3.
105. UCC § 4A-203 cmt. 5.
106. Rob Garver, *The Cost of Inaction*, U.S. Banker (July 2010), at 11.
107. FBI Intelligence Note, *Internet Crime Complaint Center, Compromise of User's Online Banking Credentials Targets Commercial Bank Accounts* (Nov. 3, 2009), available at *http://www.ic3.gov/media/2009/091103-1.aspx* (last visited Feb. 4, 2013).
108. FBI, Financial Services Information Sharing and Analysis Center, and the Internet Crime Complaint Center, *Fraud Alert—Cyber Criminal Targeting Financial Employee Credentials to Conduct Wire Transfer Fraud* (Sept. 17, 2012), available at *http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf* (last visited Feb. 4, 2013).
109. OCC, Alert 2012-16, Information Security: Distributed Denial of Service Attacks and Customer Account Fraud (Dec. 21, 2012).
110. Byron Acohido, *Cybercrooks Stalk Small Businesses That Bank Online*, USA Today, Jan. 13, 2010, available at *http://www.usatoday.com/tech/news/computersecurity/2009-12-30-cybercrime-small-business-online-banking_N.htm* (last visited Feb. 4, 2013).
111. Krebs On Security, *Banking on a Live CD* (July 12, 2012), available at *http://krebsonsecurity.com/2012/07/banking-on-a-live-cd/* (last visited Feb. 4, 2013).
112. Riva Richmond, *Wanted: Defense Against Online Bank Fraud*, The Wall Street Journal (Feb. 8, 2010), at R4.
113. FFIEC, *supra* note 76, at 11-12.