INTERNET THEFT FROM BUSINESS BANK ACCOUNTS — WHO BEARS THE RISK?

Thomas J. Bondurant, Jr.*
Michael J. Finney*

I. Introduction

Perhaps no movie scene is more familiar than a bank heist. In recent years, films such as THE TOWN and THE DARK KNIGHT featured iconic bank robberies. And art still imitates life. In 2010 alone, theft from brick-and-mortar banks in the United States totaled approximately $43 million.[1]

But what of on-line thefts? Not from a bank's general till or safe with the threat of violence, but directly from the accounts of its Internet customers with mere keystrokes? With respect to small and midsize businesses and their commercial bank accounts, current aggregate estimates range as high as a staggering *$1 billion per year*.[2]

Internet fraud and theft is not a new phenomenon, but the scale of this particular problem has exploded in the last two to three years. As business customers increasingly have the ability to send money on-line, opportunity has grown for organized criminal groups. Employees are inundated with Trojans, phishing campaigns, and other types of malware to gain access to businesses' bank accounts. Small to midsize companies are a particularly inviting target. They generally have higher balances and more transaction activity than individuals (making it easier to hide fraudulent activity), and their internal controls are typically less sophisticated than those of larger companies. In addition, there is at least the perception that the smaller banks often used by these businesses may employ less stringent forms of on-line security.

Assuming that the criminals cannot be found and the funds cannot be recovered, who bears the risk for an on-line theft: the bank or the business? This is not a simple question to answer. It is clear that businesses do not have the same

* Mr. Bondurant is a partner at the Roanoke firm of Gentry Locke Rakes & Moore, LLP. Mr. Finney is an associate at Gentry Locke and a member of the Virginia Association of Defense Attorneys.

[1] Greg Farrell & Michael Riley, *Banks to Small Business: If You're Hacked, Tough Luck*, EOS Worldwide, Sept. 16, 2011, http://eosworldwide.com/3941/entrepreneurs/businessweek-small-biz/banks-to-small-business-online-theft-tough-luck/?doing_wp_cron

[2] *Id*.

legal protections as individual banking customers.[3] The governing legal framework is simultaneously archaic and evolving. It is also highly fact-specific.

After briefly detailing the scale and scope of the problem, this article will focus on exploring the legal framework. It begins with the Uniform Commercial Code ("UCC"), developed for the non-Internet age with standards such as "commercial reasonableness" and "good faith." Agency "guidance" informs commercial reasonableness for security procedures in an on-line environment, guidance that has been updated and supplemented twice over the last decade, including as recently as the summer of 2011. As thefts work their way through the judicial system, the first courts are putting their interpretative stamp on these issues. Finally, the article will summarize the current state of the law and describe steps that banks and businesses can take to mitigate the risk of theft, as well as their legal exposure.

II. The Nature of the Problem

Thefts from small to midsize business bank accounts—as well as those belonging to court systems, school districts, and other public institutions—began to rise in the latter half of 2008.[4] As of mid-2009, the FBI's estimate was that criminals had attempted to steal more than $85 million and successfully made off with more than $40 million.[5]

The spike in Internet thefts from smaller businesses led to a number of specific alerts by governmental agencies in the latter half of 2009.

For example, on August 24, 2009, the FBI, Financial Services-Information Sharing and Analysis Center ("FS-ISAC"),[6] and NACHA-The Electronic Payments Association ("NACHA"), jointly issued an alert entitled "Account Hijacking of Corporate Customers Recommendations for Customer Education."[7] This alert warned:

> There has been a shift in the online criminal world from primarily targeting of individuals to increased targeting of corporations. In the past 6 months financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in

[3] Federal law—specifically Regulation E of Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq.*—provides many protections for individual banking customers from fraud and theft. In fact, the UCC section on electronic funds transfers explicitly does not apply to a funds transfer governed by the Electronic Funds Transfer Act. *See* Va. Code § 8.4A-108.

[4] Security Fix: Brian Krebs on Computer Security, *FBI: Cyber crooks stole $40M from U.S. small, mid-sized firms*, The Washington Post, Oct. 26, 2009, http://voices.washingtonpost.com/securityfix/2009/10/fbi_cyber_gangs_stole_40mi.html

[5] *Id.*

[6] FS-ISAC is an industry forum for collaboration on critical security threats facing the financial services sector that was created by a presidential directive. http://www.fsisac.com/about/

[7] https://admin.nacha.org/userfiles/File/Risk_and_Compliance/FS-ISAC%20CAT%20WHITE%20082409.pdf

> funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses.[8]

The alert explained that the business customer was typically compromised by a targeted "spear phishing" campaign. The attack often starts with an

> e-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Website. The e-mail recipient is generally a person within a company who can initiate funds transfers or payments on behalf of the business. Once the user opens the attachment, or clicks the link to open the Web site, malware is installed on the user's computer which usually consists of a Trojan keystroke logger, which harvests the user's corporate online banking credentials.
>
> ***
>
> The customer's online credentials are either uploaded to a website from where the fraudster can later download them, or, if the bank and customer are using two factor authentication system, the Trojan keystroke logger may detect this and immediately send an instant message to the fraudster alerting them of the secure web activity. The fraudster then accesses the financial institution through use of the captured username and password or through hijacking the secure web session.
>
> The fraud is carried out when the fraudster creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through wire or ACH that are directed to the bank accounts of willing or unwitting individuals. Often within a couple days, or even hours of recruiting money mules and opening accounts, money is deposited and the mule is directed to immediately forward a portion of the money to subjects in Eastern Europe by various means.[9]

The FDIC followed with alerts on August 26, 2009,[10] and October 29, 2009.[11] On November 3, 2009, the FBI issued another alert, "Fraudulent Automated Clearing House (ACH) Transfers Connected to Malware and Work-at-Home Scams."[12] It stated that "[w]thin the last several months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking

[8] *Id.*

[9] *Id.*

[10] http://www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html

[11] http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html

[12] http://www.fbi.gov/news/pressrel/press-releases/fraudulent-automated-clearing-house-ach-transfers-connected-to-malware-and-work-at-home-scams

credentials belonging to small and medium businesses, municipal governments, and school districts."[13]

The November 3, 2009, FBI alert directed readers to a "detailed analysis of this scam,"[14] in the form of a November 3, 2009, Internet Crime Complaint Center ("IC3")[15] Intelligence Note, "Compromise of User's Online Banking Credentials Targets Commercial Bank Accounts."[16] In this Intelligence Note, the FBI reasoned that small and midsized businesses, as well as small public entities, may be inviting targets because their contact information and organizational charts are often posted on-line. These postings "may provide the perpetrators with information on who handles the financial transactions for that business or agency."[17] The FBI also noted 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 . . . . The lack of defense-in-depth at the smaller institution/service provider level has created a threat to the ACH system."[18]

As the current $1 billion estimate suggests, the threat has only grown in the past two years. For example, on October 1, 2010, the FBI announced that major members of an international bank fraud ring had been arrested.[19] Based in the Ukraine, this ring alone is thought to have stolen $70 million from 390 small to midsized businesses in the United States over the preceding 18 months.[20]

And the malicious software used by Internet thieves is becoming increasingly sophisticated. In September 2011, security firm Symantec reported a "deluge of malicious email-borne malware," and stated that roughly "72% of all email-borne malware in September could be characterized as aggressive strains of generic polymorphic malware."[21] "Polymorphic malware" means "malicious software that constantly changes its appearance to evade security software,"[22] so that it can "exploit[ ] the weaknesses of more traditional security countermeasures."[23]

[13] *Id.*

[14] *Id.*

[15] The IC3 is a partnership between the FBI, the National White Collar Crime Center, and the Bureau of Justice Assistance. http://www.ic3.gov/default.aspx

[16] http://www.ic3.gov/media/2009/091103-1.aspx

[17] *Id.*

[18] *Id.*

[19] http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud

[20] Krebs on Security, *Ukraine Detains 5 Individuals Tied to $70 Million in U.S. eBanking Heists*, Oct. 2, 2010, http://krebsonsecurity.com/2010/10/ukraine-detains-5-individuals-tied-to-70-million-in-ebanking-heists/

[21] Symantec Intelligence Report: September 2011, at 1, http://www.symanteccloud.com/mlireport/SYMCINT_2011_09_September_FINAL-en.pdf

[22] Krebs on Security, *Monster Spam Campaigns Lead to Cyberheists*, Oct. 3, 2011, http://krebsonsecurity.com/2011/10/monster-spam-campaigns-lead-to-cyberheists/

[23] Symantec Intelligence Report: Sept. 2011, at 1, http://www.symanteccloud.com/mlireport/SYMCINT_2011_09_September_FINAL-en.pdf

III. UCC Provisions Governing Bank Security Measures

UCC Article 4A—as adopted by Virginia Code §§ 8.4A-101 *et seq*.—governs electronic funds transfers between a bank and its business customers, including ACH and wire transfers. In relevant part, § 8.4A-202(b) states:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure,[24] a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.[25]

Thus, if the bank and its business customer have agreed to a security procedure to verify the authenticity of an electronic funds transfer request, then, irrespective of whether the customer actually authorized it, there are two key inquiries:[26] (1) whether the security procedure is a "commercially reasonable" method of protecting against unauthorized transfer requests; and (2) whether the bank accepted the transfer request pursuant to the security procedure "in good faith" and pursuant to any additional restrictions on acceptance that the business customer directs. If the answer to both questions is in the affirmative, then the bank has no liability for the funds transfer.[27] If the answer to either is in the negative, then the bank does face liability.[28]

[24] A security procedure is defined as

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

Va. Code § 8.4A-201.

[25] Va. Code § 8.4A-202(b).

[26] This framing assumes that the breach of the security procedure that enabled the fraudulent transfer request occurred on the business customer's side, not the bank's. If the breach was the bank's fault (*e.g.*, theft committed by a bank employee), then the bank would be liable. *See* Official Comment #5, Va. Code § 8.4A-203.

[27] Va. Code § 8.4A-204(a). A bank, however, may also agree to accept the risk of loss even if it complied with all of its obligations under § 8.4A-202(b). *See* Va. Code § 8.4A-203(a)(1); Official Comment #6, Va. Code § 8.4A-203.

[28] Va. Code § 8.4A-204(a).

Commercial reasonableness is a question of law.[29] This is "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."[30] Still, commercial reasonableness is a fact-specific and fact-intensive inquiry and should be determined according to the following considerations:

> the wishes of the customer expressed to the bank, 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, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.[31]

In addition, a security procedure will be "deemed to be commercially reasonable" so long as two criteria are met:

> (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.[32]

Outside the exception above, which allows a customer to choose and be bound by a security procedure that is not commercially reasonable under delineated circumstances, the requirement of commercial reasonableness "may not be varied by agreement" between the bank and business customer.[33]

As the above definition indicates, commercial reasonableness is a flexible inquiry.[34] It seeks to determine "whether the procedure is reasonable for the particular customer and the particular bank."[35] "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

[29] *See* Official Comment #4, VA. CODE § 8.4A-203 ("The issue of whether a particular security procedure is commercially reasonable is a question of law. Whether the receiving bank complied with the procedure is a question of fact.").

[30] *Id.*

[31] VA. CODE § 8.4A-202(c). The UCC Official Comments provide additional color on the key variables. *See* Official Comment #4, Va Code § 8.4A-203.

[32] VA. CODE § 8.4A-202(c).

[33] VA. CODE § 8.4A-202(f).

[34] *See* Official Comment #4, Va Code § 8.4A-203 ("The concept of what is commercially reasonable in a given case is flexible.").

[35] *Id.*

stringent procedure."[36] In all instances, however, "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."[37]

The standard of good faith is defined as "honesty in fact and the observance of reasonable commercial standards of fair dealing."[38] While the customer can impose additional restrictions (beyond the security procedure) for a bank's acceptance of a payment order in its name,[39] the bank's obligation to have accepted the payment order in good faith and in compliance with the agreed security procedure cannot be varied by agreement.[40]

This statutory scheme "is designed to protect both the customer and the receiving bank."[41] It "is based on the assumption that losses due to fraudulent payment orders can best be avoided by the use of commercially reasonable security procedures, and that the use of such procedures should be encouraged."[42] Banks have "[t]he burden of making available commercially reasonable security procedures . . . because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of the procedures offered to customers to combat fraud."[43] "If a commercially reasonable security procedure is not made available to the customer[,] . . . [then] the bank acts at its peril in accepting a payment order that may be unauthorized."[44] For its part, a business customer has "[t]he burden . . . 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."[45]

IV. Evolution of the FFIEC Standards

With limited case authority interpreting the above UCC framework in the Internet age, the key objective signposts over the past decade have been the authentication standards promulgated by the Federal Financial Institutions Ex-

[36] *Id*.

[37] *Id*.

[38] Va. Code § 8.4A-105(a)(6). Commentary elsewhere in the UCC explains that this definition of good faith was deliberately expanded to include an objective standard of commercial reasonableness, in addition to subjective honesty. Official Comment #20, Va. Code § 8.1A-201.

[39] *See* Official Comment # 3, Va. Code § 8.4A-203 ("A customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank. For example, 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.").

[40] Va. Code § 8.4A-202(f).

[41] Official Comment #3, Va. Code § 8.4A-203.

[42] *Id.*

[43] *Id*.

[44] *Id*.

[45] *Id*.

amination Council ("FFIEC").[46] The FFIEC issued its first guidance applicable to Internet transactions in 2001, which was updated in 2005 and supplemented again in 2011. None of these standards has the force of law, but given the numerous governmental agencies that comprise the FFIEC, they carry significant weight in any legal analysis.

Historically, the FFIEC materials have recommended flexible approaches to meet the evolving nature of on-line fraud. A consistent point of emphasis has been for banks to stay abreast of current technology and threats, adjusting their security measures accordingly. Although the FFIEC's earlier statements offered little concrete guidance for banks, the spate of recent attacks on small businesses has resulted in the inclusion of definitive statements about the kind of security measures that are now inadequate, as well as the measures recommended by the FFIEC. A brief summary of the major FFIEC publications over the last decade follows.

A. 2001 GUIDANCE

On August 8, 2001, the FFIEC published "Authentication in an Electronic Banking Environment,"[47] an "interagency guidance focuse[d] on the risks and risk management controls related to authentication in an electronic banking environment" ("2001 Guidance").[48]

The 2001 Guidance described how authentication methodologies can involve three basic factors:

- something the user knows (*e.g.*, password, PIN);
- something the user has (*e.g.,* ATM card, smart card, token); and
- something the user is (*e.g.*, biometric characteristic, such as a fingerprint or retinal pattern).[49]

[46] The FFIEC

> is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

http://www.ffiec.gov/

[47] http://www.ffiec.gov/pdf/pr080801.pdf

[48] 2001 Guidance at 1.

[49] *Id*. at 2.

As of 2001, the FFIEC had determined that "[a]uthentication methods that depend on more than one factor typically are more difficult to compromise than single factor systems," meaning that "properly designed and implemented multi-factor authentication methods are more reliable indicators of authentication and stronger fraud deterrents."[50] "In general, multi-factor authentication methods should be used on higher risk systems."[51] Moreover, the FFIEC explicitly "caution[ed] financial institutions that single factor authentication alone may not be commercially reasonable or adequate for high risk applications and transactions. Instead, multi-factor techniques may be necessary."[52]

In addition to discussing when to employ single-factor or multifactor authentication procedures, the 2001 Guidance also stated "that a single factor system may be 'tiered' to enhance security without implementing a two-factor system. A tiered single factor authentication system would include the use of multiple levels of a single factor."[53]

The FFIEC also discussed the importance of monitoring systems, which "can detect unauthorized access to computer systems and customer accounts."[54] It stated that "[a] sound authentication system should include audit features that can assist in the detection of fraud, unusual activities (e.g., money laundering), compromised passwords or other unauthorized activities."[55]

Monitoring systems can constitute additional "layers of controls to prevent fraud and safeguard customer information," layers that are not directly based on authentication procedures.[56] For example,

> a financial institution could analyze the typical transactional activity of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits for large items that require manual intervention to exceed the preset limit. In addition, financial institutions can monitor Internet Protocol (IP) addresses and other information to identify suspicious activity.[57]

The FFIEC also emphasized continuous risk assessment for banks.[58] It stated that "[t]he method of authentication used in a specific electronic application should be appropriate and 'commercially reasonable' in light of the reasonably

[50] *Id*.

[51] *Id*.

[52] *Id*. at 3.

[53] *Id*.

[54] *Id*. at 5.

[55] *Id*.

[56] *Id*.

[57] *Id*.

[58] *Id*. at 2-3.

foreseeable risks in that application."[59] However, "[b]ecause the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and service providers should periodically review authentication technology and ensure appropriate changes are implemented."[60]

B. 2005 GUIDANCE

On October 12, 2005, the FFIEC replaced the 2001 Guidance by publishing "Authentication in an Internet Banking Environment" ("2005 Guidance").[61] The FFIEC believed that a comprehensive update was necessary because "[s]ince 2001, there have been significant legal and technological changes with respect to the protection of customer information; increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies."[62] The 2005 Guidance "specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services."[63]

The 2005 Guidance stated that there were numerous technologies and methods that banks can use for customer authentication, including "customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of 'tokens,' transaction profile scripts, biometric identification, and others."[64]

The particular authentication employed "should depend upon the results of the financial institution's risk assessment process."[65] As "the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and technology service providers should develop an ongoing process to review authentication technology and ensure appropriate changes are implemented."[66]

Risks "should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions."[67] "The method of

[59] *Id*. at 3.

[60] *Id*.

[61] http://www.ffiec.gov/pdf/authentication_guidance.pdf

[62] 2005 Guidance at 1.

[63] *Id*.

[64] 2005 Guidance at 2. *See also* Appendix to 2005 Guidance.

[65] 2005 Guidance at 2.

[66] *Id*. at 4.

[67] *Id*. at 3.

authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application."[68] In short, as the risks increase, so should the level of authentication procedures.

While the 2005 Guidance did "not endorse any particular technology" for authentication measures,[69] a "key point" was that the FFIEC had determined "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."[70] For this, and other situations "[w]here 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."[71] As part of a multifactor approach, the FFIEC stated that "out-of-band"[72] controls may be used.[73]

As in 2001, the 2005 Guidance again emphasized monitoring and reporting systems.[74] More specifically, it counseled that banks

> 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. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit.[75]

The 2005 Guidance also included a section on customer awareness.[76] It stated that "[f]inancial institutions have made, and should continue to make, efforts to educate their customers,"[77] as "customer awareness is a key defense against fraud and identity theft."[78] It indicated that these efforts should be monitored for their effectiveness and increased when necessary.[79]

[68] *Id*. at 4.

[69] *Id*. at 1.

[70] *Id*.

[71] *Id*. at 1-2.

[72] By "out-of-band," at this time the FFIEC meant "additional steps or actions taken beyond the technology boundaries of a typical transaction. Callback (voice) verification, e-mail approval or notification, and cellphone based challenge/response processes are some examples." *Id*. at 3 n.5.

[73] *Id*. at 3.

[74] *Id*. at 5.

[75] *Id*.

[76] *Id*. at 5-6.

[77] *Id*. at 5.

[78] *Id*. at 5-6

[79] *Id*. at 6.

C. 2006 FAQS

On August, 15, 2006, the FFIEC member agencies published a set of "frequently asked questions" (and answers),[80] in order "to assist financial institutions and their technology service providers in understanding the [2005 Guidance]" (the "2006 FAQs").[81] The 2006 FAQs repeated much of the information in the 2005 Guidance, but also clarified a few issues.

For one thing, the 2006 FAQs confirmed that the 2005 Guidance "does not call for the use of multifactor authentication."[82] Instead, "[t]he use of multifactor authentication is one of several methods that can be used to mitigate risk," and the 2005 Guidance "identifies circumstances under which the Agencies would view the use of single-factor authentication as the only control mechanism as inadequate and conclude that additional risk mitigation is warranted."[83] In other words, the FFIEC was not necessarily recommending multifactor authentication over layered security or other controls.[84]

The 2006 FAQs also explained that "[b]y definition[,] true multifactor authentication requires the use of solutions from two or more of the three categories of factors."[85] Thus, while "[u]sing multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach," this "would not constitute multifactor authentication."[86]

As for risk assessment, the 2006 FAQs emphasized that even if a bank had "not experienced financial fraud or identity theft originating from its online banking system," it should nonetheless "consider appropriate risk-mitigation steps for both current and future risks."[87] The 2006 FAQs reaffirmed that a bank's "risk assessment [should] specifically consider the risks of phishing, pharming, and malware."[88] The 2006 FAQs also stated the FFIEC's expectation that banks would complete the risk assessment called for in the 2005 Guidance by year-end 2006.[89] With respect to how often the risks must be reevaluated, however, the 2006 FAQs stated that this review did not have to occur on a yearly basis, but just "as appropriate."[90]

[80] http://www.ffiec.gov/pdf/authentication_faq.pdf

[81] 2006 FAQs at 1.

[82] *Id*. at 2.

[83] *Id*.

[84] *Id*. at 3. *See also id*. at 4-5 (defining *layered security* to "include[ ] other risk-mitigating controls that would not strictly be considered multifactor authentication," and "other controls" to "include[ ] other mitigating controls that exist today or that may be introduced in the future").

[85] *Id*. at 6.

[86] *Id*.

[87] *Id*. at 3.

[88] *Id*. at 5.

[89] *Id*. at 4.

[90] *Id*. at 5.

According to the 2006 FAQs, if a bank that "permit[ed] high-risk transactions through a system that relies on single-factor authentication as its only control mechanism" then decided to "ma[ke] customers whole" by "reimburs[ing] customers for any losses associated with Internet fraud," this would not meet the expectations of the 2005 Guidance.[91] Similarly, the FFIEC "believe[s] that permitting customers to opt-out is not an effective risk mitigation strategy and would undermine the effectiveness of the control."[92]

D. 2011 SUPPLEMENT

On June 28, 2011, the FFIEC supplemented the 2005 Guidance by publishing the "Supplement to Authentication in an Internet Banking Environment" (the "2011 Supplement").[93]

The stated purpose of the 2011 Supplement "is to reinforce the [2005] Guidance's risk management framework and update the Agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment,"[94] as well as the 2005 Guidance's expectations on bank risk assessments.[95] The FFIEC was "concerned that customer authentication methods and controls implemented in conformance with the [2005] Guidance several years ago have become less effective."[96] In addition, the 2011 Supplement "establishes minimum control expectations for certain online banking activities[,] identifies controls that are less effective in the current environment," and "identifies certain specific minimum elements that should be part of an institution's customer awareness and education program."[97]

With respect to risk assessments, the 2011 Supplement states that banks "should perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats to customers' online ac-

[91] *Id*. at 4.

[92] *Id*. at 6. This means that the FFIEC would not allow banks to provide a commercially unreasonable security measure at the customer's request, even if the bank otherwise complied with Virginia Code § 8.4A-202(c).

[93] http://www.ffiec.gov/pdf/Auth-ITS-Final%xxx-xx-11%20(FFIEC%20Formated).pdf

[94] *Id*. at 1. By way of background, the 2011 Supplement stated that

> [s]ince 2005, there have been significant changes in the threat landscape. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits, increasing availability and permitting their use by less experienced fraudsters. Rootkit-based malware surreptitiously installed on a personal computer (PC) can monitor a customer's activities and facilitate the theft and misuse of their login credentials. Such malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication.

Id. at 2.

[95] *Id*. at 1.

[96] *Id*. at 2.

[97] *Id*. at 1.

counts."[98] These risk assessments should now be performed: (1) as new information about threats becomes available; (2) before implementing any new on-line services; or (3) in any event, at least once a year.[99]

As for customer authentication, the 2011 Supplement emphasizes that "financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security."[100] In the 2011 Supplement, "[l]ayered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control."[101]

The 2011 Supplement states that, at a minimum, banks' layered security programs should contain two elements.[102] First, they should have monitoring processes designed to detect anomalies and effectively respond to such suspicious activity.[103] These should cover not only a customer's initial log-in but also the "initiation of electronic transactions involving the transfer of funds to other parties."[104] Second, the security programs should have enhanced controls for system administrators who have privileges to set up or change system configurations.[105] "For example, a preventive control could include requiring an additional authentication routine or a transaction verification routine prior to final implementation of the access or application changes."[106]

In addition to these two required components, the 2011 Supplement provided a number of examples of "[e]ffective controls that may be included in a layered security program":[107]

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of out-of-band verification for transactions;[108]

[98] *Id*. at 3.

[99] *Id*.

[100] *Id*. at 2.

[101] *Id*. at 4.

[102] *Id*. at 5.

[103] *Id*.

[104] *Id*. The 2011 Supplement commented that based upon the recent incidents reviewed by the FFIEC, "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." *Id*.

[105] *Id*.

[106] *Id*. The FFIEC also commented that based on the incidents it has reviewed, "enhanced controls over administrative access and functions can effectively reduce money transfer fraud." *Id*. at 6.

[107] *Id*. at 4.

[108] The Appendix to the 2011 Supplement clarified what the FFIEC means by "out-of-band" authentication:

- the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
- enhanced controls over account activities[,] such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (*e.g.*, days and times);
- internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;
- enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.[109]

In addition to layered security, the FFIEC for the first time unequivocally "recommend[s] that institutions offer multifactor authentication to their business customers."[110]

The 2011 Supplement also specifically comments on the effectiveness (or lack thereof) of two authentication techniques: (1) device identification and (2) challenge questions.[111] It states that simple device authentication—consisting of static cookies that can be copied or Internet protocol address matching—is no longer effective as a primary control; instead, device authentication should be "complex," meaning it creates a "digital 'fingerprint' by looking at a number of characteristics."[112] Likewise, simple challenge questions that rely on publicly available information are no longer effective as a primary control; instead, challenge questions controls would ideally rely on private information, include "red

> Out-of-band authentication means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. . . . Out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised.

Id. at 11.

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

[110] *Id*. at 4.

[111] *Id*. at 6.

[112] *Id*.

herring" questions, and use multiple challenge questions without exposing all questions in a single session.[113]

Finally, the 2011 Supplement states that banks should employ targeted awareness and educational efforts for their business customers.[114] The education should include information about the lack of "Regulation E" protections.[115] Another aspect is to explain when, if ever, the bank may contact the customer to obtain its electronic banking credentials.[116] Banks should also suggest that their business customers periodically evaluate the risks on their side, as well as their control measures.[117]

V. Recent Case Law

While many suits have been filed in response to the exploding on-line theft from business bank accounts, only a few have resulted in substantive court decisions about whether the bank or business customer bears the risk of the particular loss. And no decision involves events that took place after the FFIEC promulgated the 2011 Supplement, which will likely be the industry benchmark for years to come. With those caveats in mind, below are brief summaries of recent court cases.

A. *Shames-Yeakel v. Citizens Financial Bank*[118]

This case involved a February 2007 theft from the Shames-Yeakels' home equity credit line. "[A]n unknown person with an IP address different from that of Plaintiffs gained access to Plaintiffs' online Citizens accounts by using Ms. Shames-Yeakel's username and password," stealing $26,500.[119] The plaintiffs asserted a number of claims, including one for negligence. Citizens Financial Bank moved for summary judgment.

The evidence showed that "Citizens protected access to Plaintiffs' online accounts simply by means of a user name and password, or 'single-factor identification'" instead of multifactor authentication.[120] The plaintiffs argued that Citizens should have provided them with a "token," which "is an object possessed by a user, either as a digital object saved to the user's computer or as a physical device carried by the user."[121] On the day of the theft, "Citizens was in the process of issuing physical tokens to its users, in the form of small devices

[113] *Id*. at 6-7.

[114] *Id*. at 7.

[115] *Id*.

[116] *Id*.

[117] *Id*.

[118] Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994 (N.D. Ill. 2009).

[119] *Id*. at 998.

[120] *Id*. at 1000.

[121] *Id*.

that would fit on a key chain and were to generate ever-changing eight-digit pass codes."[122]

Citizens' expert testified that the authentication measures in place "were reasonable and not the cause of the unauthorized transfer."[123] To counter this, the plaintiffs submitted the FFIEC's 2005 Guidance. The court seized upon the 2005 Guidance's statement that the FFIEC "consider[s] 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."[124] Based on this and Citizens' admission that only single-factor authentication was in place at the time of the theft, the court denied the motion for summary judgment.[125]

It must be emphasized that the *Shames-Yeakel* ruling was in the context of a negligence claim, rather than pursuant to the UCC's "commercially reasonable" standard, and involved individual rather than business customers.[126] On the other hand, the flexible nature of the commercial reasonableness inquiry is akin to negligence; thus this decision could still have persuasive force.

B. *PATCO CONSTRUCTION CO. INC. V. PEOPLES UNITED BANK D/B/A OCEAN BANK*[127]

In May 2009, Internet criminals stole more than $200,000 from Patco's account with Ocean Bank, through multiple fraudulent ACH transfers.[128] The withdrawals totaled $588,851, but Ocean Bank was able to block $243,406 of the transfers.[129] Patco brought a claim against Ocean Bank pursuant to UCC § 4A-201 *et seq*., as well as a number of common-law causes of action.[130] The crux of Patco's UCC claim was whether the security procedure offered by Ocean Bank was commercially reasonable or not.[131]

[122] *Id*. at 1000-1001 (internal citations omitted). Together with the username and password that Citizens already required (something the user knows), the token would have constituted multifactor authentication (something the user has).

[123] *Id*. at 1000 (quotation omitted).

[124] *Id*. at 1001.

[125] *Id*. at 1007-1009. *See also id*. at 1009 ("In light of Citizens' apparent delay in complying with FFIEC security standards, a reasonable finder of fact could conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access.").

[126] The UCC also preempts all common-law causes of action that present a "situation covered by the particular provisions" of Virginia Code § 8.4A-201 *et seq*. *See* Schlegel v. Bank of Am., 271 Va. 542, 553-55, 628 S.E.2d 362, 368 (2006); Official Comment, VA. CODE § 8.4A-102 ("The rules that emerged represent a careful and delicate balancing of those interests and are intended to be the *exclusive means* of determining the rights, duties and liabilities of the affected parties in any situation covered by particular provisions of the Article.") (emphasis added).

[127] Case No. 2:09cv503, United States District Court of Maine.

[128] Patco Constr. Co. Inc. v. Peoples United Bank d/b/a Ocean Bank, No. 2:09cv503, 2011 U.S. Dist. LEXIS 58112, at *10 (D. Me. May 27, 2011).

[129] *Id*. at *10-11.

[130] *Id*. at *95-96

[131] *Id*. at *102.

In 2004, Ocean Bank hired a vendor to provide its on-line banking platform.[132] After issuance of the FFIEC's 2005 Guidance, the vendor created two security products designed to meet its requirements, both of which purported to offer multifactor authentication.[133] Ocean Bank selected the more expensive Premium Product, which was implemented in January 2007.[134]

The Premium Product offered the following features:

1) *Passwords and IDs*: For both the company and individual user.

2) *Challenge questions*: Each user was required to select three challenge questions when they first logged in. These challenge questions could be triggered for various reasons, such as an attempted transaction with a "risk score" that exceeded a certain threshold.

3) *Risk Profiling*: Each attempted log-in and transaction created a risk score based on "a multitude of data, including but not limited to IP, device cookie ID, Geo location, and transaction activity."

4) *Device Cookies*: A cookie was placed on customers' computers to identify them. If the cookie changed or was new, this would negatively impact the risk score.

5) *Dollar Amount Rule*: The bank could "set a dollar threshold amount above which a transaction would trigger the challenge questions even if the user ID, password, and device cookie were all valid."

6) *Subscription to eFraud Network*: This network "compared characteristics of the transaction (such as the IP address of the user seeking access to the Bank's system) with those of known instances of fraud." If there were any indicia of fraud associated with the transaction, then it was immediately blocked.

7) *Reports to Financial Institutions*: Banks would be provided standard reports and be allowed to create custom reports.[135]

Along with the Premium Product, Ocean Bank offered a few additional security measures to its business customers. For one, the customers could choose to have e-mail alerts issued. Ocean Bank subscribed to three anti-phishing services and posted phishing and fraud notices to its customers. It also used secure socket layer encryption. Finally, Ocean Bank contractually required customers to monitor their accounts daily and report any anomalies.[136]

There were also security measures available at the time of the theft that Ocean Bank chose to not employ. It did not offer an "out-of-band" authentica-

[132] *Id*. at *23.

[133] *Id*. at *25-32.

[134] *Id*. at *33.

[135] *Id*. at *33-39.

[136] *Id*. at *17-18, *57-64, *107.

tion, a service its vender did provide. Ocean Bank personnel did not monitor the risk-scoring reports described above that were part of the Premium Product, "nor did the Bank conduct any other regular review of transactions that generated high risk scores." Ocean Bank offered neither tokens to its business customers nor a user-selected picture that was available through its vendor.[137]

In June 2008, Ocean Bank set the Dollar Amount Rule to one dollar. This meant that for every transaction involving at least one dollar (effectively, all transactions), Patco was prompted to answer challenge questions in order to access its account. The vendor had defaulted the Dollar Amount Rule to $1000, and Ocean Bank had previously placed the threshold at $100,000, so as to not inconvenience its customers.[138]

Ocean Bank argued that setting the Dollar Amount Rule to one dollar was a means to enhance security, and that it did in fact enhance security by adding an additional layer.[139] For its part, Patco submitted expert testimony "that setting challenge questions to be asked on every transaction greatly increases the risk that a fraudster equipped with a keylogger will be able to compromise the answers to a customer's challenge questions because it increases the frequency with which such information is entered through a user's keyboard."[140]

Patco also argued that the Premium Product did not offer true multifactor authentication. Although device identification was "something the user has,"[141] a negative response prompted the challenge questions, not an inability to log-in to the account. At bottom then, Patco reasoned that logging in to its account and transferring money required only information from the "something the user knows" factor, that is, user names, passwords, and challenge-question answers.[142]

Ocean Bank responded that under the 2005 Guidance, multifactor authentication required only the use of multiple factors in the authentication process, not any particular response if one of the factors detected an anomaly.[143]

More broadly, Ocean Bank argued that the 2005 Guidance did not require multifactor authentication for high-risk transactions, and that it instead stated

[137] *Id*. at *64-69.

[138] *Id*. at *43-53. The vendor believed that a bank could set the Dollar Amount Rule at any amount and the system would still operate effectively. *Id*. at *46.

[139] *Id*. at *48-51.

[140] *Id*. at *52-53, *112-18. Because "Patco did not isolate its computers or forensically preserve the hard drives," it was impossible to be certain how its credentials were compromised. *Id*. at *82-85. Still, for purposes of its decision, the court assumed that the criminals obtained Patco's user names, passwords, and challenge question answers through the use of key-logging malware.

[141] Ocean Bank also argued that its behavioral monitoring tools constituted "something the user is." *Id*. at *54. Patco responded that this factor referred to something physical (*i.e*., biometrics), not behavioral. *Id*. at *54-55. In any event, a negative response on the behavioral monitoring would simply prompt the challenge questions. *Id*. at *55.

[142] *Id*. at *53-57, *116-17, *125-26. The only exception would be if the transaction was flagged by the eFraud Network; in such an event, the transaction was closed down. *Id*. at *38.

[143] *Id*. at *55.

merely that single-factor authentication as the only control was inadequate. Thus, Ocean Bank contended that "layered" security using "something you know" multiple times, and/or in conjunction with the "other controls" it offered, constituted a commercially reasonable security system that complied with the 2005 Guidance.[144]

Each fraudulent transaction in May 2009 generated much higher risk scores than normal under the Premium Product. Still, because the criminals submitted the correct passwords and answers to the challenge questions (and did so every single time they were prompted), they were allowed to continue the transactions.[145]

Ocean Bank moved for summary judgment as to all claims. Patco cross-moved for summary judgment as to the UCC claim.[146]

In a very detailed opinion, the magistrate judge commented that "[t]his is a hard-fought and well-presented case bearing on a discrete but nuanced issue."[147] While crediting the facial appeal of Pacto's argument that by "setting the Dollar Amount Rule threshold at $1, the Bank ill-advisedly neutralized critical aspects of the seemingly high-quality security system it chose to implement in the wake of the issuance of the FFIEC Guidance," he concluded that Ocean Bank "has the better argument and has demonstrated that the security measures that it had in place as of May 2009 were commercially reasonable."[148] The magistrate judge emphasized that commercial reasonableness was a lower standard than the best security procedures available at the time.[149] His decision also found that the Premium Product constituted both multifactor and multilayer authentication.[150]

Accordingly, the magistrate judge recommended that summary judgment be granted to Ocean Bank on all claims.[151] This recommendation was adopted by

[144] *Id.* at *55-57.

[145] *Id.* at *72-79.

[146] *Id.* at *95-96.

[147] *Id.* at *127.

[148] *Id.* at *127-28.

[149] *Id.* at *133-35. For this reason, the deficiencies against the specific key-logging threat that compromised Patco's credentials did not shift the risk of loss to Ocean Bank:

> It is apparent, in the light of hindsight, that the Bank's security procedures in May 2009 were not optimal. The Bank would have more effectively harnessed the power of its risk-profiling system if it had conducted manual reviews in response to red flag information instead of merely causing the system to trigger challenge questions. Indeed, it commenced manual reviews in the wake of the transactions at issue here. The use of other systems, such as tokens and out-of-band authentication, also would have improved the security of the Bank's system and might have minimized the loss that occurred in May 2009 . . . .

Id. at *133.

[150] *Id.* at *128-29.

[151] *Id.* at *135-39. The magistrate judge determined that the common-law claims were either preempted or hinged on the success of Patco's UCC claim. Ruling in Ocean Bank's favor on the UCC claim thus resolved the entire case. *Id.*

the district court without substantive additional discussion.[152] Patco has appealed this decision to the First Circuit.

C. *EXPERI-METAL, INC. V. COMERICA BANK*[153]

On January 22, 2009, a phishing e-mail was forwarded to a user authorized for Experi-Metal's Comerica Bank account. By clicking on the e-mail and entering information into a fraudulent web site, the user gave thieves immediate access to Experi-Metal's bank accounts. Between 7:30 a.m. and 2:02 p.m. that day, 93 fraudulent wire transfer payment orders totaling $1,901,269 were executed. In addition, to facilitate the fraud, the criminal executed twenty "book transfers" between Experi-Metal accounts and related family accounts totaling more than $5.6 million, which resulted in a $5 million overdraft on one account that had zero funds in it at the start of the day. Comerica recovered all but $561,399 of these amounts.[154]

This case resulted in two substantive opinions. First, on July 8, 2010, the court held on summary judgment that the security procedures offered by Comerica were commercially reasonable.[155] The court, however, found that whether Comerica had accepted the wire transfers in "good faith" was a fact question for trial.[156] Second, after a bench trial, on June 13, 2011, the court found that Comerica failed to meet its burden of proving that it had accepted the wire transfers in good faith.[157] It subsequently entered judgment in Experi-Metal's favor for $561,399.[158]

Although the court found on summary judgment that the security measures were commercially reasonable, it did not independently analyze the measures according to the UCC standards, the 2005 Guidance, or any other benchmark. Instead, the court applied basic contract principles and found that Experi-Metal had contractually agreed that the security measures Comerica employed were commercially reasonable.[159] It characterized Experi-Metal's expert opinion to the contrary as "parol evidence" that was "not effective to contradict the plain language of the Service Agreement and Master Agreement."[160]

[152] Patco Constr. Co. Inc. v. Peoples United Bank d/b/a Ocean Bank, No. 2:09cv503, 2011 U.S. Dist. LEXIS 86169 (D. Me. Aug. 4, 2011).

[153] Case No. 09-14890, United States District Court for the Eastern District of Michigan.

[154] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2011 U.S. Dist. LEXIS 62677, at *16-23 (E.D. Mich. June 13, 2011).

[155] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2010 U.S. Dist. LEXIS 68149, at *16-17 (E.D. Mich. July 8, 2010).

[156] *Id*. at *18-23. The court also found that whether the compromised Experi-Metal user was authorized to initiate wire transfer orders presented a genuine issue of fact. *Id*. at *17-18. The court ultimately determined that she was authorized. *Experi-Metal*, 2011 U.S. Dist. LEXIS 62677, at *23-28.

[157] *Experi-Metal*, 2011 U.S. Dist. LEXIS 62677, at *28-38.

[158] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, Dkt. No. 70 (E.D. Mich. July 7, 2011).

[159] *Experi-Metal*, 2010 U.S. Dist. LEXIS 68149, at *11-12, *15-17.

[160] *Id.* at *17.

The court also found that genuine issues of fact remained on the question of good faith. It stated that good faith contained both subjective ("honesty in fact") and objective ("observance of reasonable commercial standards of fair dealing") prongs[161] and that Comerica had the burden of proving that it met these standards when it accepted the wire transfer orders.[162]

In its bench opinion analysis, the court first stated that under the UCC, "[w]hat conduct is required of a bank to comply with the 'good faith' requirement cannot be varied by the parties' agreement(s)."[163] As there was no suggestion that Comerica had acted dishonestly when accepting the wire transfer orders, the dispositive issue was whether Comerica had observed reasonable commercial standards of fair dealing.[164]

The court found that Comerica had not met its burden. The sole evidence on whether Comerica had reasonably acted to shut down the fraudulent wire activity was the testimony of its expert, but the court found that he was unqualified to give the opinion in question.[165] While the expert was qualified to opine on the overdraft standards for Experi-Metal's accounts, neither his testimony nor any other evidence

> informed the court of whether a bank engages in fair dealing when it allows overdrafts totally $5 *million* from a single account that usually has a zero balance, particularly where the ten transactions causing the overdrafts were entered repetitively (many in less than a minute of each other) and during one online session.[166]

In short, the court 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," and Comerica presented no admissible evidence from which the court could find otherwise.[167]

VI. Summary of the Legal Landscape

Although recent opinions have grappled with the issues surrounding third-party Internet theft, it is still quite unclear whether a bank or its business customer will be responsible. There are several reasons for this uncertainty.

First, the two cases described above that were decided under the UCC (*Patco* and *Experi-Metal*) still present questions. The *Patco* decision was exceptionally detailed, but the court itself acknowledged how close the decision was, a decision that is now on appeal. And setting aside the issue of whether the bank was

[161] *Id*. at *18

[162] *Id*. at *21.

[163] *Experi-Metal*, 2011 U.S. Dist. Lexis 62677, at *28.

[164] *Id*. at *30-31.

[165] *Id*. at *35.

[166] *Id*. at *36 (emphasis in original).

[167] *Id*. at *38.

required to provide additional measures, the court's logic in holding that the bank used true multifactor authentication appears shaky. At bottom, a user was required to supply information only from a single factor, "something you know," in order to access the account and initiate a transaction. This fact would also seem to undercut the efficacy of most other "controls" used by the bank as additional "layers" of security.

As for *Experi-Metal*, the court appears to have erred in its summary judgment opinion. It found that the security procedure was commercially reasonable, simply because Experi-Metal had contractually agreed that it was. But the UCC is clear that a bank must use a commercially reasonable security measure—unless it first offers a customer such a measure and the customer opts for, in writing, a commercially unreasonable security measure. Just like the requirement of good faith, the commercial reasonableness obligation—save the above exception—cannot be varied by agreement.[168]

This makes sense, as illustrated by the Official Comments to the UCC. The statutory scheme "is based on the assumption that losses due to fraudulent payment orders can best be avoided by the use of commercially reasonable security procedures, and that the use of such procedures should be encouraged."[169] A bank has "[t]he burden of making available commercially reasonable security procedures," and if it does not, "the bank acts at its peril in accepting a payment order that may be unauthorized."[170]

With respect to the *Experi-Metal* court's good faith decision, it may have limited persuasive value going forward, as it hinged largely on the bank's inability to present admissible evidence. In addition, some of the court's analysis seems to blur good faith with the commercial reasonableness of the chosen security procedure. If the good-faith obligation is as broad as the court suggests, then many commercial reasonableness questions of law may morph into good faith questions of fact.

Second, *Experi-Metal*, *Patco*, and *Shames-Yeakel* involved thefts that occurred in the beginning of 2009 or earlier. This was when the threat to banks and their small and midsize business customers had begun to accelerate, so many of the standards that were commercially reasonable then under the 2005 Guidance may not be reasonable now under the same 2005 Guidance.

Third, the 2011 Supplement—not the 2005 Guidance—is the current FFIEC standard. The 2011 Supplement is much more specific in what is required and what is unacceptable for banks, and some of its mandates appear specifically drawn from the security flaws that were exposed by these cases. For example, simple challenge questions—such as those at the crux of the matter in *Patco*—are now insufficient. Likewise, account monitoring is now required by the FFIEC, a feature that was not used by the bank in *Patco*.

[168] *See supra* at III.

[169] Official Comment #3, VA. CODE § 8.4A-203.

[170] *Id*.

Fourth, commercial reasonableness and good faith are flexible, fact-intensive inquiries. What is reasonable changes in response to the nature of the threat and the technology available, and the 2011 Supplement mandates that banks must undertake risk assessments on a regular basis.

For all of these reasons, cases evaluating thefts that occurred just two years ago may be of limited value in determining what is commercially reasonable today and in the days to come.

VII. Conclusion

There is no simple answer to the question of whether a bank or its business customer will bear the loss of an on-line theft. As the tools used by criminals evolve and become more sophisticated, so, too, must reasonable security measures to thwart the threat. In *Patco,* the bank's apparent compliance with 2005 Guidance did not meet the evolving threat presented by key-logging malware. Now, the 2011 Supplement addresses the state of the "current" threat, but it, too, will likely become outdated before long.

Education and prevention thus must be a focus, so that neither a bank nor a customer will be forced to rely merely on legal positions in this cloud of uncertainty. Banks should follow the 2011 Supplement's instructions and conduct regular risk assessments as new information about threats becomes available and before implementing any new on-line services. In any event, risk assessment should take place at least once a year.

Banks can also initiate customer awareness programs, or businesses can take steps to prevent or mitigate theft on their own, adopting practices such as:

- Logging in to bank accounts only from the bank web site, never directly from an e-mail link (unless in possession of specific and verified instructions from the bank);
- Being suspicious of all e-mails, calls, and text messages from a bank or a bank affiliate;
- Using a dedicated computer for all on-line bank transactions, and for no other purposes;
- Refraining from using a wireless network for on-line transactions;
- Monitoring account balances on a daily basis and reporting any anomalies immediately to your bank;
- Becoming familiar with the specific look and appearance of the bank's web site, and not entering confidential log-in information if something appears amiss;
- Selecting authorized user(s) who cannot be easily identified and contacted from the business's web site;

- Cautioning authorized user(s) to refrain from posting personal information about themselves on-line (like their high school or date of birth) that could be used to answer challenge questions;
- Installing security software and keeping it up-to-date, as well as any hardware or software patches.

In addition to these preventive steps, businesses should discuss the threat with their banks and understand exactly the security measures that are offered. If a bank fails to offer a particular security feature, the business can certainly shop around. Businesses and banks are also advised to check with their insurance carriers to see if these types of Internet thefts are insured losses under their present policies. If not, they should inquire about a cyberinsurance policy.

On the legal merits, the flexible nature of the key questions, the evolving threat, the new FFIEC standards, and the limited case law create an unsettled landscape. At a minimum, banks should study the FFIEC's 2011 Supplement and make sure that they are in strict compliance with its terms. Banks should also be on the lookout for further FFIEC updates.

Finally, for lawyers, there is ample space for skilled advocacy in the event a theft occurs. Lawyers can and should also proactively raise these issues with both their banking and business clients.