2012

Civil Liability Theories for Insufficient Security Authentication in Online Banking

Paul Rice

Civil Liability Theories for Insufficient Security Authentication in Online Banking

Paul Rice[*]

I. Introduction

This Note will discuss the growing number of lawsuits against banks involving customers who seek to recover funds after a theft occurs due to perceived inadequate online authentication. As banking transactions have moved from physical bank locations with vaults to the online world, so have the criminals who threaten them. Most domestic banks offer online banking with a Web browser, providing the same services as a physical bricks and mortar bank branch. As banks move services to an online accessible model, they face additional challenges. With online banking, banks must provide reasonable security to protect customers' funds and accounts. This reasonable security includes the processes and procedures that banks traditionally used to physically protect funds and methodologies to now protect against new threats. If banks fail to implement reasonable online information security controls, losses to criminals will increase and customers will hold banks accountable through the courts.

This Note proceeds in five parts. Part II of the Note concerns first, traditional physical security expectations for banks; second, federal regulations related to online banking; and lastly, online security expectations, particularly those based on federal guidance found in the Graham-Leach-Bliley Act (GLBA)[1] and Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook.[2] Collectively, these areas establish the background operating environment and duty of care for online banking authentication. Part III will then discuss three recent cases: *Shames-Yeakel v.*

[*] Bachelor of Arts, Biology, June 1997, University of Chicago; Juris Doctor, anticipated, May 2013, DePaul University College of Law. CISSP, (ISC)2.

[1] Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.). *See also* Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 Berkeley Tech. L.J. 497 (2002).

[2] Fed. Fin. Inst. Examination Council, Information Technology Examination Handbook: E-Banking, http://ithandbook.ffiec.gov/it-booklets/e-banking.aspx (last visited Feb. 23, 2012).

Citizens Financial Bank,[3] *Patco Construction Company v. People's United Bank*,[4] and *Experi-Metal, Inc. v. Comerica, Inc.*,[5] where the plaintiffs in each case advanced negligence theories in an attempt to recover funds lost after third party cyber crime. Part IV will analyze the claims advanced in these cases and predicts that future plaintiffs will succeed despite possible bank defenses. Part V will conclude that even though the court considered the question of "commercially reasonable security" settled in a contract in *Experi-Metal, Inc.*, other suits will likely succeed because banks must meet or exceed the minimal standard of care for authentication to avoid liability to online banking customers for theft.

II. Background: The Confluence of Online Banking, Federal Banking Regulations, and Customer Expectations

A. *Banking Security Expectations in Physical and Electronic Contexts*

Consumers choose to place money in banks at least in part because of the greater convenience and security that banks provide.[6] Federal regulations indicate the need to encourage routine banking and savings.[7] Banks have had to replicate many of the security procedures, processes, and technologies that protect physical banks for the online world.[8] Traditionally, banks' focused their physical security on protecting real property stored in a vault.[9] Theft and environmental loss posed the greatest threat to stored physical funds.[10] The standard for reasonable security controls developed over time to address these and

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

[4] Patco Constr. Co., Inc. v. People's United Bank, No. 2:09-CV-503-DBH, 2011 WL 2174507 (D. Me. May 27, 2011), *aff'd sub nom* Patco Constr. Co., Inc. v. Peoples United Bank, No 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011); Patco Constr. Co., Inc. v. Peoples United Bank, No. 09-503-P-H, 2010 WL 1403929, at *4 (D. Me. Mar. 31, 2010) (refusing to grant motion for summary judgment).

[5] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2010 WL 2720914 (E.D. Mich. July 8, 2010).

[6] *See* Jon Newberry, *'Anytime, Anywhere, Anyway': Online Banking Offers Greater Convenience and Easier Financial Planning*, 82 A.B.A. J. 94 (1996). *See generally* Jinkook Lee & Julia Marlowe, *How Consumers Choose a Financial Institution: Decision-Making Criteria and Heuristics*, 21 Int'l J. Bank Marketing 53 (2003) (finding that consumers value convenience most when selecting a bank).

[7] *E.g.*, Federal Deposit Insurance Act of 1950, Pub. L. 81-797, 64 Stat. 873 (1950) (codified in sections of 12 U.S.C.).

[8] Eugene M. Katz & Theodore F. Claypoole, *Willie Sutton is on the Internet: Bank Security Strategy in a Shared Risk Environment*, 5 N.C. Banking Inst. 167 (2001).

[9] *Id.* at 171–72.

[10] *E.g.* fires, tornadoes, and hurricanes.

involved perimeter defenses.[11] Perimeter defenses limited access to valuables, protected those valuables from harm, and also served a deterrent function.[12]

A medieval castle represents a classic analogy for a bank's perimeter defenses.[13] A castle's defenses addressed multiple threats including direct attacks by cavalry, indirect attacks by archers, protracted battles where the attackers attempt to starve the inhabitants, and barrage by war machines such as catapults and ballista.[14] Moving from the outside in a castle had large fields, providing it with a 360 degree view of the battlefield, a moat, thick castle walls, large towers, and secure internal chambers.[15] The layered physical defenses of a bank are analogous to a castle. As one progresses from the parking lot of a bank to a safe deposit box in a vault, the bank's defenses increase.[16]

Banks also rely on human interaction to provide authentication to ensure that only legitimate customers access their funds.[17] In a physical bank, the teller can ask the customer to provide a form of state-sponsored identification, the teller can compare the picture to the customer, and verify other characteristics such as handwritten signatures. Other controls include requiring the use of pre-printed checks with the account number, address verification, and using dollar amount thresholds for transfers that require multiple signers.[18] The process of authenticating customers is so routine that most people do not even notice the numerous control points that go into a simple withdrawal of funds from a checking account at a physical bank branch.

Customers comfortable with traditional bank security and human interaction expect the same level of security when banking services move online. This customer expectation helps set the basic features and security controls for online banking. Consumers expect to perform routine banking from anywhere with anytime access via the Internet.[19] Banks must continue to address traditional threats to funds, while also meeting new challenges, especially in the area of authentication.[20] The routine processes and procedures for identifying cus-

[11] *See* Katz & Claypoole, *supra* note 8, at 172–73 (including the use of bank vaults, security guards, and other techniques minimizing theft and maximize detection).

[12] *Id.* at 172 ("Protecting a treasure requires more than just thick walls.").

[13] *Id.* at 171.

[14] *Id.* at 172.

[15] *Id.*

[16] *See* Katz & Claypoole, *supra* note 8, at 172.

[17] *Id.* at 173.

[18] *Id.* at 175.

[19] *Id.* at 177.

[20] *See id.* at 175.

tomers become more complex when many of the physical cues no longer exist. For example, some banks have allowed customers to deposit checks with a camera-equipped cell phone.[21] In this model, the bank no longer has physical possession of the check or the person attempting to cash the check.[22] Instead the bank must find substitutes for traditional verification processes. To address this challenge, the federal regulators have stepped in to provide guidance. In the absence of a market-driven trend, the regulators have helped level the playing field by setting the minimum requirements for online banking, specifically regarding authentication.

B. *An Overview of Online Banking Regulations*

The financial services sector falls under a complex web of federal and state regulations designed to govern operations and customer information protection.[23] At the highest level, the Board of Governors of the Federal Reserve System sets the overall monetary policy for the United States.[24] The activities of a financial services company determine which regulatory body provides oversight.[25] A bank will often fall under several regulatory programs based on the bank's charter and services it offers.[26] Different federal agencies regulate banks offering traditional checking and savings accounts depending on the nature of the bank's charter.[27] Nationally chartered banks fall under the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller for Currency (OCC).[28] Credit unions and state chartered banks fall under the review National Credit Union Administration (NCUA).[29] The FDIC insures deposits held in traditional personal checking and savings accounts.[30]

[21] Method for Remote Check Deposit, U.S. Patent No. 20100082470 (filed Oct. 1, 2008), *available at* 2010 WL 1243574.

[22] *Id.*

[23] AM. BAR ASSOC., INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE FOR GLOBAL EXECUTIVES, LAWYERS AND TECHNOLOGISTS 188–89 (Thomas J. Shaw ed., 2011).

[24] *See* BOARD OF GOVERNORS OF THE FED. RES. SYS., THE FEDERAL RESERVE SYSTEM: PURPOSES & FUNCTIONS, http://www.federalreserve.gov/pf/pf.htm (last updated Aug. 24, 2011).

[25] *Id.* at 4–6.

[26] *See generally* FFIEC, ENFORCEMENT ACTIONS AND ORDERS, http://www.ffiec.gov/enforce ment.htm (last updated Feb. 3. 2012) (discussing the various federal administrative agencies responsible for bank operation oversight).

[27] *See* ABA, *supra* note 23, at 12.

[28] *Id.*

[29] *See generally* National Credit Union Administration, 12 C.F.R. § 701.1–701.39 (2010).

[30] *See generally* Federal Deposit Insurance Act of 1950, Pub. L. 81-797, 64 Stat. 873 (1950) (codified in sections of 12 U.S.C. § 1811).

The Federal Reserve maintains regulations that govern a bank's activities.[31] Federal regulations govern each type of bank account and activities involved with banking transactions, for example, the Electronic Funds Transfer Act,[32] referred to as Regulation E.[33] These regulations, taken as a whole, govern most aspects of a bank falling within the Federal Reserve System.

Of the many types of bank accounts, consumers often begin their banking relationship with a basic checking account. The industry and regulations define "consumer checking accounts" as "demand deposit accounts."[34] Demand deposit accounts represent a category that includes several noninterest-bearing accounts, including traditional checking accounts.[35] "Demand deposit" means "a deposit that is payable on demand, or a deposit issued with an original maturity or required notice period of less than seven days."[36] The parties in the three cases discussed in the next section each had funds in demand deposit accounts with their respective banks.[37]

Regulation E governs online banking, which is the use of a computer to initiate the electronic transfer of funds to or from a consumer demand deposit account.[38] The Board of Governors of the Federal Reserve System stated that

> Regulation E provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments).[39]

Electronic funds transfer (EFT) involves the transfer of funds either between consumer accounts (such as checking and savings accounts)

[31] Board of Governors of the Federal Reserve System, 12 C.F.R. § 201.1(b) (2003).

[32] Electronic Funds Transfer Act, 15 U.S.C. § 1693 (2010).

[33] Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205.1 (2010) (pursuant to the Electronic Funds Transfer Act, 15 U.S.C. § 1693 (2010).

[34] Reserve Requirements of Depository Institutions (Regulation D), 12 C.F.R. § 204.2(b)(1)(i) (2010) (pursuant to authority granted by 12 U.S.C.A. § 3105 (2010).

[35] *Id.* at § 204.2(b)(1).

[36] *Id.*

[37] Of note, only consumer demand deposit accounts are afforded protection under Regulation E. Senators have proposed expanding the consumer protections of Regulation E to business account holders. *See* discussion *infra* Part IV.

[38] Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205.3.

[39] BOARD OF GOVERNORS OF THE FED. RES. SYS., REGULATIONS: COMPLIANCE GUIDE TO SMALL ENTITIES, http://www.federalreserve.gov/bankinforeg/regecg.htm (last updated Oct. 4, 2011) [hereinafter COMPLIANCE GUIDE TO REG. E]; *see also* 12 C.F.R. § 205.3(b).

or to pay bills.[40] If an unauthorized fund transfer occurs, a bank would only make a consumer liable for a maximum of fifty dollars, but the failure to notify the bank in a timely fashion could result in a complete loss.[41] The regulation attempts to strike a balance between the bank's duty of care to protect an account and the customer's responsibility to notice unusual activity. The questions of what constitutes an unauthorized fund transfer and where the balance of responsibility should lie will play a prominent role in the three cases later discussed in Part III.

The preceding regulations set the foundation for the regulatory framework that governs online banking for consumer checking accounts. The regulations establish the standard of care for a bank that offers online services and they also reflect reasonable general expectations for information security. The next section will cover the foundations of reasonable consumer expectations for online banking security.

C. *Federal Guidelines Establish Reasonable Online Banking Security*

Interagency Guidelines Establishing Information Security Standards further refined the Federal Reserve System regulations and established the guidelines for information security for banks falling under the authority of the OCC.[42] These guidelines set minimum standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.[43] Of particular relevance here, each bank must perform an assessment of "access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals" and then implement appropriate controls.[44] The Federal Financial Institutions Examination Council (FFIEC) specifically established guidance for authentication in an online banking environment.

[40] EFT "refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset account." *See* COMPLIANCE GUIDE TO REG. E, *supra* note 39.

[41] *See* Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205.6(b) (2011).

[42] Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30 app. B (2011) ("The Interagency Guidelines Establishing Information Security Standards (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p-1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b) of the Gramm-Leach-Bliley Act.").

[43] *Id.* at (2)(B).

[44] 12 C.F.R. pt. 30 app. B (3)(C)(1)(a).

The FFIEC is an interagency council that assists with uniform principles, standards, and reporting for the examination of financial institutions.[45] The FFIEC InfoBase provides examination guidance to financial institutions in the IT Handbook.[46] The InfoBase contains several booklets on topics including business continuity planning, online banking, auditing, and payment systems.[47] The booklets provide guidance on the expectations of the regulatory agencies that perform on-site reviews of financial services companies.[48] Due to developments in online banking, the FFIEC released guidance on federal regulator expectations for authentication.[49] The FFIEC released a supplement to the 2005 FFIEC Guidance in June of 2011.[50]

The regulators developed the FFIEC Guidance to discuss improvements in authentication technologies that might minimize the increasing incidents of fraud.[51] The recommendations apply equally to consumer and business online banking.[52] As a matter of policy, the agencies represented by the FFIEC no longer consider single factor authentication as the only control mechanism to be adequate for high-risk transactions involving access to customer information or the movement of funds to other parties.[53] This means that the practice of authenticating a customer using only a user name and password no longer represents reasonable access controls when customers request access to their online bank account.[54] Instead, banks should move to the use of multiple factors to authenticate users.[55] According to the Guidance: "Existing authentication methodologies involve three basic 'factors': something the user *knows* (e.g., password, PIN); something

[45] *See* BOARD OF GOVERNORS OF THE FED. RES. SYS., *supra* note 24, at 62.

[46] FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK INFOBASE, http://ithandbook.ffiec.gov/ (last visited Feb. 23, 2012).

[47] FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK INFOBASE: IT BOOKLETS, http://ithandbook.ffiec.gov/it-booklets.aspx (last visited Feb. 20, 2012).

[48] *Id.*

[49] FED. FIN. INST. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (Oct. 12, 2005), http://www.ffiec.gov/pdf/authentication_guidance.pdf [hereinafter FFIEC GUIDANCE].

[50] *See generally* FED. FIN. INST. EXAMINATION COUNCIL, SUPPLEMENT TO AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (June 29, 2011), http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf [hereinafter FFIEC SUPPLEMENT].

[51] FED. FIN. INST. EXAMINATION COUNCIL, FREQUENTLY ASKED QUESTIONS ON FFIEC GUIDANCE ON AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 2 (Aug. 15, 2006), http://www.ffiec.gov/pdf/authentication_faq.pdf; FFIEC Supplement, *supra* note 50, at 2.

[52] FFIEC GUIDANCE, *supra* note 50, at 2.

[53] *Id.*

[54] *Id.*

[55] *Id.* at 2–3.

the user *has* (e.g., ATM card, smart card); and something the user *is* (e.g., biometric characteristic, such as a fingerprint)."[56]

Proper implementation of this Guidance requires the use of a factor from two or more categories.[57] The use of two factors from a single category will not prove sufficient, for example, a bank that requires a customer to submit a username, password, and an answer to a personal question such as the customer's mother's maiden name. The use of these three factors (username, password, and mother's maiden name) from the same category does not satisfy the guidance.[58]

Authentication methods that rely on more than one factor are more difficult to compromise. While thieves might obtain a customer's username and password using any number of techniques,[59] the difficulty of compromising an account goes up when a thief must compromise another factor. For example, a bank that implements a two-factor authentication system might require customers to provide their username, password, and a six-digit number from a previously issued physical token. The six-digit number expires either ten-minutes after the bank issued it or after the customer uses it, whichever occurs first.[60] Thus, a thief would have to obtain all three pieces of information in order to compromise the account.

While increasing security, the FFIEC counsel recognized that the burden attached to implementing a multi-factor authentication program, and that the level of authentication used in a particular application, should be appropriate to the level of risk in that application.[61] This allows for a risk-based determination of particular controls. The FFIEC guidelines acknowledge that the "legal appropriateness of any particular authentication method (or any other security measure) is not determined in the abstract."[62] The FFIEC guidelines also state,

[56] *Id.* at 3.

[57] FFIEC GUIDANCE, *supra* note 49, at 1.

[58] *Id.* at 3.

[59] Techniques may include technical (using keyloggers or other trojan horses) or traditional social engineering (obtaining log on credentials via coercion and deceit).

[60] Jim Bruene, *Bank of America Launches SafePass, but You'd Never Know from Its Website*, NETBANKER (Sept. 12, 2007), http://www.netbanker.com/2007/09/bank_of_america_launches_safepass_but_not_mentioned_on_website.html ("The system . . . sends users a 6-digit code via text message. The code is then entered at BofA's website to authorize larger transfers, new bill-pay merchants, new accounts for funds transfer, or to login from a new computer, not previously 'registered' for online banking.").

[61] FFIEC GUIDANCE, *supra* note 49, at 6.

[62] Thomas J. Smedinghoff, *Where We're Headed: New Developments and Trends in the Law of Information Security*, 3 PRIVACY & DATA SECURITY L.J. 103, 117 (2007) [hereinafter Smedinghoff I], *available at* http://www.edwardswildman.com/files/News/a58aea4d-61c6-4641-83ad-0f73b7320464/Preview/NewsAttachment/64d8c778-753d-4256-9a5d-10e9154d1151/Where_We're_Headed_-_New_Developments_and_Trends_in_the_Law_of_Information_Security%20

"What constitutes legally appropriate authentication may also change over time as new threats arise and better technology is developed to address them."[63]

For example, Google now offers two-factor authentication for its online applications including Google Mail, Google Documents, and Google Reader.[64] Google calls its new authentication scheme two-step verification, making use of two factors: something the user knows and something the user has.[65] Users must supply their username and password (something known), and also provide the verification code that Google sent to the users' registered cell phone in a text message.[66] Once authenticated, users may also establish the computer they used to access Google Apps as trusted or untrusted.[67] The computer then becomes the second, physical element of the authentication process.

With Google offering this advanced feature set to protect e-mail and other online applications, banking customers will increasingly question why their banks do not offer similar protection. By avoiding the time, expense, and difficulty of managing tokens, Google has enhanced the authentication process through common consumer devices such as cell phones capable of receiving text messages via SMS.

Regulators also look to trends in technology when seeking to establish commercial reasonableness.[68] The notion of a reasonable authentication standard will continue to evolve, spurred by the arms race between criminals and businesses. Thieves will think up ever more sophisticated methods of overcoming multi-factor authentication. The definition of reasonable and legally appropriate authentication will also grow to encompass ever more complex processes that may include previously unheard of technology.[69]

(Smedinghoff).pdf. *See also* Thomas J. Smedinghoff, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy & E-Transactions Law*, 16 MICH. ST. J. INT'L L. 1 (2007).

[63] *See* Smedinghoff I, *supra* note 62, at 118.

[64] Eran Feigenbaum, *A More Secure Cloud for Millions of Google Apps Users*, OFFICIAL GOOGLE ENTERPRISE BLOG (Sept. 20, 2010), http://googleenterprise.blogspot.com/2010/09/more-secure-cloud-for-millions-of.html.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *See generally*, FFIEC GUIDANCE, *supra* note 49 (discussing regulatory expectations and notice of trends in commercial authentication technology); FFIEC SUPPLEMENT, *supra* note 50.

[69] FFIEC GUIDANCE, *supra* note 49, at 8; *see* FFIEC SUPPLEMENT, *supra* note 50 (indicating that the FFIEC released new guidance to update the 2005 materials); *see also* Tracy Kitten, *New Authentication Guidance Soon?*, BANK INFO. SECURITY (Jan. 31, 2011), http://www.bankinfosecurity.com/articles.php?art_id=3282 (discussing the historical backdrop and expectations for the FFIEC Supplement.)

D. *Summary of Background on Federal Regulation and Customer Expectations for Online Banking*

Banks must implement reasonable authentication methods that meet or exceed the guidelines present in a variety of federal regulations, and the FFEIC Guidance suggests options. These methods have to not only address the federal regulations, but also meet customers' expectations for the security of their funds stored at banks. The regulations and customer expectations establish the baseline for online authentication and when banks fail to meet this baseline, liability for loss will probably attach.

III. OVERVIEW OF PERSONAL AND COMMERCIAL ONLINE BANKING: CIVIL NEGLIGENCE CASES

Three cases, representing personal and commercial banking clients, have sought civil recovery of lost funds under a tort negligence theory accusing the banks of breaching their fiduciary responsibilities to protect customer accounts.

A plaintiff that files cases under this novel theory of liability generally includes four elements: first, that the bank provided online banking, including Automated Clearing House (ACH) transfers from a checking account; second, a third party somehow gained access to the online banking system and transferred funds out of the plaintiff's account without permission; third, the bank failed to provide notice to the plaintiffs of unusual or suspicious activity; and lastly, the bank's security measures did not prevent the fraudulent transfers.[70]

Liability may attach in either of two situations: first, under strict liability situations where the bank fails to implement controls required by Federal or State statutes; or second, under tort negligence where the bank controls fall short of the "reasonable security" standard and duty of care for online banking.

A. Shames-Yeakel v. Citizens Financial Bank

The plaintiffs in *Shames-Yeakel*, a couple with funds at the bank, alleged that they lost $26,500 due to identity theft from their online bank account.[71] They alleged that the bank violated various statutes and committed negligence in the design, implementation, and opera-

[70] David Navetta, *Online Banking and "Reasonable Security" Under the Law: Breaking New Ground?* (Jan. 14, 2010), http://www.infolawgroup.com/2010/01/articles/reasonable-security/online-banking-and-reasonable-security-under-the-law-breaking-new-ground/.

[71] Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994, 996 (N.D. Ill. 2009).

tion of the online banking site.[72] The Bank moved for summary judgment and the court affirmed in part and denied in part.[73]

The judge dismissed the statutory negligence theory raised by the couple under the Fair Credit Reporting Act (FCRA).[74] The judge ruled that the account in question did not meet the standard of a demand deposit account under Regulation D and thus the FCRA or Regulation E did not apply to the account.[75] This ruling foreclosed the possibility of succeeding on the strict liability claim. If the plaintiffs succeeded on the FCRA claim, they could have pursued a strict liability claim and avoided having to demonstrate the civil tort duty element. Instead, the couple had to proceed with their complaint under a general tort negligence claim.[76]

The judge allowed the general tort negligence claim to proceed and held that a reasonable fact finder might determine that the Bank acted negligently in protecting the couple's account.[77] The court relied in part on the Bank's duty to protect its customers and the Bank's failure to implement the FFIEC Guidelines for Authentication in Internet Banking; holding that the use of a single factor for authentication (username and password) was insufficient and beneath what was commercially reasonable for the time.[78] Perhaps reflecting the sentiment expressed in other FFIEC guidance, the judge noted that "[i]f this duty not to disclose customer information is to have any weight in the age of online banking, then banks must certainly employ sufficient security measures."[79]

B. Patco Construction Company v. People's United Bank

In *Patco*, the plaintiffs alleged that Ocean Bank failed to adequately protect customer funds against theft.[80] The complaint alleged negligence, breach of fiduciary duty, and raised a state statutory negligence claim.[81] Patco alleged that "[t]his action arises out of Ocean Bank's failure to fulfill one of its most basic obligations, namely, to protect its

[72] *Id.* at 996.

[73] *Id.*

[74] *Id.* at 1007.

[75] *Id.* at 1009.

[76] Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d. 994, 1007 (N.D. Ill. 2009).

[77] *Id.* at 1009.

[78] *Id.* at 1008–09.

[79] *Id.* at 1008.

[80] Patco Constr. Co., Inc. v. Peoples United Bank, No. 09-503-P-H, 2010 WL 1403929 (D. Me. Mar. 31, 2010).

[81] *Id.*

customers' funds against theft."[82] Following the same pattern as *Shames-Yeakel*, criminals accessed Patco's account and transferred hundreds of thousands of dollars to numerous bank accounts through ACH.[83] The complaint noted the "sophisticated systems" that Ocean Bank advertised that it employed and also suggested that these systems proved insufficient.[84] The plaintiffs alleged a breach of the Maine's State Statute.[85] Similar to *Shames-Yeakel*, the plaintiffs pursued a strict liability claim.

The next section will further discuss that the plaintiff survived a motion for summary judgment on the indemnification clause of the bank agreement.[86] The bank raised a contract item as a possible defense to the negligence claim.[87] The Bank suggested that the agreement between the parties allowed them to waive a responsibility for the unauthorized transfer of funds.[88] The court later affirmed the magistrate judge's recommendation and granted the Bank's motion for summary judgment: the court found that the record indicated that the Bank's security was adequate.[89]

C. Experi-Metal Inc. v. Comerica, Inc.

In *Experi-Metal Inc.* (EMI), the plaintiffs alleged that Comerica failed to prevent forty-seven fraudulent funds transfers from EMI's commercial account.[90] Similar to the previous cases, the plaintiffs alleged that they did not authorize the funds transfers.[91] This case presented several interesting claims because it is the first to reach trial and address a contractual agreement to determine whether the bank's security was "commercially reasonable."

Comerica implemented token-based authentication where a "a user accesses the Comerica Business Connect website by entering his or her user ID, his or her confidential 4-digit PIN, and a six-digit code

[82] Complaint and Demand for Jury Trial at 1, Patco Constr. Co., Inc. v. People's United Bank, No. 09-CV-00503, 2009 WL 4764707 (D. Me. Oct. 9, 2009).

[83] *Id.*

[84] *Id.*

[85] *Id.* at 5–6 (citing ME. REV. STAT. tit. 11 § 4-1201).

[86] *See* Patco Constr. Co., Inc. v. Peoples United Bank, No. 09-503-P-H, 2010 WL 1403929, (D. Me. Mar. 31, 2010) (People's United Bank raised the indemnification clause as a defense to liability).

[87] *See* Patco Constr. Co., Inc. v. Peoples United Bank, No. 09-503-P-H, 2011 WL 2174507, at * 4-6 (D. Me. May. 27, 2011).

[88] *Id.*

[89] *Id.*

[90] Experi-Metal, Inc. v. Comerica Bank, No. 2:09-cv-14890, 2010 WL 2720914, at *3 (E.D. Mich. July 8, 2010).

[91] *Id.* at *1.

from a secure token."[92] The parties agreed that this secure token technology "would be used to verify the authenticity of payment orders and that this security procedure was commercially reasonable."[93]

According to the governing state statute, "commercial reasonableness" is a question of law that the court should determine by considering what the parties knew about routine banking transactions and whether the parties agreed to the security procedure in writing.[94] As a result, the claims in *EMI* revolved around other negligence theories surrounding the failure to monitor and warn the plaintiffs of suspicious activities that the bank should have noticed.[95]

The court decided the case in June of 2011.[96] The court noted that "the person(s) who committed the fraud against Experi-Metal on January 22, 2009, obtained Experi-Metal's confidential information that enabled the breach from an agent of Experi-Metal and that '[s]ection 440.4702, therefore is determinative of which party is responsible for the loss at issue in this case . . . .' "[97] The court affirmed its earlier dismissal of a motion for summary judgment, stating that the Bank satisfied the criteria under section 440 for consumer-initiated wire transfer orders.[98] The court found "no genuine issue of material fact that Comerica and Experi–Metal agreed that the authenticity of payment orders would be verified pursuant to a security procedure and that Comerica's security procedure was *commercially reasonable*."[99] The court thus did not find occasion to comment on "commercially reasonable security," instead disposing of the case on an analysis of the UCC fair dealing doctrine.[100]

IV. ANALYSIS: ESTABLISHING AN EXPANDED TORT NEGLIGENCE CLAIM AGAINST ONLINE BANKS

Federal regulations and consumer expectations have established the reasonable duty of care that a financial institution must follow for an online authentication system that grants customers, whether personal

[92] *Id.* at *2.

[93] *Id.* at *4.

[94] MICH. COMP. LAWS § 440.4702(3) (2010).

[95] *See* Experi-Metal, Inc. v. Comerica Bank, No. 2:09-cv-14890, 2010 WL 2720914, at *6-7 (E.D. Mich. July 8, 2010).

[96] Experi-Metal, Inc. v. Comerica Bank, No 2:09-cv-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011).

[97] *Id.* at *1 (citing MICH. COMP. LAWS § 440.4702).

[98] *Id.*

[99] *Id.* (emphasis added).

[100] Id. at *14 ("This trier of fact is inclined to find that a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier. Comerica fails to present evidence from which this Court could find otherwise.").

or business, access to perform electronic funds transfers. Generally, when a criminal compromises an online authentication system, the bank may be held financially liable for the resulting fraud. Traditional tort negligence analysis, when applied to online authentication environments, will likely result in banks' civil liability for loss when the banks fail to implement recommended authentication procedures.

A. Shames-Yeakel v. Citizens Financial Bank

The issue with the plaintiffs' negligence claim is their argument that Citizens breached its duty to sufficiently secure its online banking system.[101] A number of courts have recognized that fiduciary institutions have a common law duty to protect their customers' confidential information against identity theft.[102] The discussion of the FFIEC Guidance bolstered the plaintiffs' claim.[103]

The *Jones* rationale is inapplicable here,[104] however; Citizens did not reimburse the plaintiffs' financial loss, so causation of economic loss remains an issue for the fact finder.[105] The court stated, "Assuming that Citizens employed inadequate security measures, a reasonable finder of fact could conclude that the insufficient security caused Plaintiffs' economic loss."[106]

The judge held that enough evidence existed to allow the case to proceed to trial and denied Citizens' motion for summary judgment.[107] At trial, the plaintiffs could have presented additional information on the theories advanced in the complaint. The survival of the motion for summary judgment marks an important milestone in this sort of litigation. By establishing legal precedent, other trial attorneys will point to the decision in *Shames-Yeakel* to support new negligence claims.[108] Despite the parties choosing to settle, this case serves as an important example of what authentication controls the courts consider insufficient. Based on the Supplemental Guidance, a single factor is no longer sufficient for high risk transactions.

[101] Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994, 997 (N.D. Ill. 2009).

[102] *See, e.g.*, Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994, 1008 (N.D. Ill. 2009) (citing Jones v. Commerce Bancorp, Inc., No. 06 Civ. 835(HB), 2006 WL 1409492, at *2 (S.D.N.Y. May 23, 2006)).

[103] *Id.* at 1009.

[104] *Id.* (citing *Jones*, 2007 WL 672091 (holding that a plaintiff had failed to establish causation of damages, where the defendant bank had reimbursed the plaintiff's monetary loss)).

[105] *Id.* at 1009.

[106] *Id.*

[107] *Id.*

[108] At the time of press, over seventy court documents cited to *Shames-Yeakel*. *See, e.g.*, Brief of Defendant-Appellees at *14 n.11, Karadimas, v. JPMorgan Chase Bank, No. 10-4337-cv, 2011 WL 2678143 (2d Cir. June 29, 2011).

B. Patco Construction Company v. People's United Bank

Similar to *Shames-Yeakel*, a commercial account was the centerpiece of this case, which meant that the existing Regulation E protections for consumer accounts did not apply. Thus, the plaintiffs had a more difficult burden of proof because they could not pursue a strict liability claim. Unlike *Shames-Yeakel*, the state did not have an analogous regulation to that of Michigan that would afford the plaintiffs a strict liability cause of action. The bank used stronger authentication questions, but appeared to lack the use of other anti-fraud controls as discussed in the FFIEC Guidance. For example, the bank did not deploy anomaly detection where the suspicious transactions might have been flagged for further review.[109] In an anomaly detection system, the system develops a baseline of "normal" activity and flags deviations from this pattern. For example, if Patco transferred funds monthly to cover payroll, then the bank might have required that any funds transferred that exceeded this usual threshold volume required voice verification.

The surviving negligence claim parallels that of *Shames-Yeakel*. The core issue rests on the duty of care that the bank should have employed. Unlike the Michigan statutory definition of "commercially reasonable" discussed in *EMI*,[110] here the courts will have to decide exactly what this means in context. The plaintiff's claim lies somewhere between the probably legally insufficient single password of *Yeakel* and the "commercially reasonable" controls of *EMI*.

C. Experi-Metal, Inc. v. Comerica Bank

The EMI case establishes that the parties may define "commercially reasonable" security controls in a contract, but does not provide common law guidance on what the courts may consider reasonable security.[111] The parties' agreement on commercially reasonable security controls resembles the speed limit on a highway.[112] A speed limit of sixty-five miles per hour represents a reasonable speed during ordinary weather conditions, but cars should travel at slower speeds during a thunderstorm.[113] The standard established in EMI represents a

[109] *See also* Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, 16 C.F.R. § 681 app. A, supp. A(21), 72 Fed. Reg. 63,771 (as amended by 74 Fed. Reg. 22,646) (2011) (indicating that when "[a] covered account is used in a manner that is not consistent with established patterns of activity" the bank must notify the customer).

[110] *See supra* 92–95.

[111] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2011 WL 2433383, at *1 (E.D. Mich. June 13, 2011).

[112] *See* AM. BAR ASSOC., *supra* note 23, at n.44.

[113] *Id.*

contractually agreed upon threshold for reasonable security by holding the parties may define the term "commercially reasonable" via contract. Banks, like drivers on the road, may choose to take additional actions if external conditions warrant additional caution.

While the court resolved the question of what is commercially reasonable in reliance on the contract, the ruling still serves as an example of what the courts will consider reasonable security controls in other contexts without a pre-established contractual basis.[114] The court, by evaluating the language of the contract, found that the underlying security measures discussed represented a reasonable standard.[115]

EMI attorney Richard B. Tomlinson commented at the conclusion of the trial, "If Comerica had some simple technology in place to score" anomalies and take action, "those transactions would have triggered an alert."[116] He correctly indicated that the court would rule on reasonable fair dealing and not commercially reasonable security. While the case established that token-based authentication might provide a "commercially reasonable" solution to the authentication problem, the plaintiff continued to allege that the security measure the bank employed did not provide a reasonable level of security for online banking in terms of fraud monitoring. In light of several recent developments in computer crime (discussed in the next Part), the plaintiff may have a point.

D. *Potential Bank Defense Claims and Federal Response*

Banks will continue to attempt to minimize their liability in two ways: through the use of contractual language and by applying exceptions that exist in federal law. Banks might attempt to avoid liability through the gist of the action doctrine, contract provisions, and contributory negligence affirmative defenses.

Banks as defendants can not rely on the "gist of the action" doctrine. This doctrine "is designed to maintain the conceptual distinction between breach of contract claims and tort claims" and precludes "plaintiffs from recasting ordinary breach of contract claims into tort claims."[117] The doctrine only applies when the relationship between

[114] *Experi-Metal, Inc*, 2011 WL 2433383 at *1.

[115] *Id.*

[116] Tracy Kitten, *EMI, Comerica Await Verdict*, BANK INFO SECURITY (Jan. 28, 2011), http://www.bankinfosecurity.com/articles.php?art_id=3304&pg=1 (quoting Richard B. Tomlinson, EMI attorney).

[117] Pediatrix Screening, Inc. v. TeleChem Int'l, Inc., 602 F.3d 541, 550 (3d Cir. 2010) (quoting eToll, Inc. v. Elias/Savion Adver., Inc., 811 A.2d 10, 14 (Pa. Super. Ct. 2002)).

the parties exists solely by contract; the gist of the action doctrine does not bar a tort claim where there exists a duty in addition to the contract.[118] The duty of a bank to protect customer's funds extends from customer expectations and federal regulations.[119] Thus, any attempt by a bank to apply the gist of the action doctrine based purely on the existence of a contract between the parties will fail. Banks face state and federal statutory requirements, along with contractual obligations to protect customer's accounts. Therefore, customers have multiple grounds upon which to rest a complaint that includes tort and contract claims.

Uniform Commercial Code section 4A-202 sets out the relevant standard for security procedures related to payment orders in contracts.[120] In this section of the UCC, the code allows the parties to contract for automated payments provided that the bank employs a "commercially reasonable method of providing security against unauthorized payment orders" and that the bank accepts the payment order in good faith and in compliance with the contracted process.[121] The code has an ambiguous definition of a security procedure.[122] Still, the Federal Trade Commission has successfully brought actions against companies for security breaches based in part on similar definitions of commercially reasonable security measures.[123] For a bank to avoid liability for fraudulent transfers, the parties must follow an agreed upon security procedure.[124] The existence of lawsuits in this area indicates that the industry, consumers, and judges can reasonably disagree about what constitutes "commercially reasonable." Banks will likely attempt to follow the model established by *EMI* where the contract with the customer indemnifies the bank for loss to avoid the current ambiguity.

Banks also attempt to minimize their obligations by requiring the consumer to use reasonable information security practices and procedures by way of contract. Buried within the terms of service for online banking services, customers must often implement several

[118] Niagara Mohawk Power Co. v. Stone & Webster Eng'g Corp., 725 F. Supp. 656, 668 (N.D.N.Y. 1989).

[119] *See supra* Part II.

[120] U.C.C. § 4A-202(b) (2005).

[121] *Id.*

[122] U.C.C. § 4A-201 (2005) ("'Security procedure' means a procedure established by agreement . . . 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 . . . of the payment order or communication.").

[123] FTC v. Neovi, Inc., 598 F. Supp. 2d 1104 (S.D. Cal. 2008).

[124] *See, e.g.*, Hedged Inv. Partners, L.P. v. Norwest Bank Minn., 578 N.W.2d 765, 773 (Minn. Ct. App. 1998).

additional programs to protect their systems.[125] Banks often require a personal firewall, antivirus software, and secure Internet access.[126] The implementation of these controls requires additional hardware and software configuration, resulting in only the most sophisticated consumers having the required protections in place. By placing a high level of responsibility for security software on the consumer, the banks might arrive at a situation where few consumers can achieve the base level of security. The terms of service often require these sophisticated steps before the bank assumes liability.[127]

Banks also avoid negligence claims by requiring consumers to agree to terms that recognize that the information security measures the banks already employ are "commercially reasonable." Comerica did not have an unusual Term & Conditions agreement, and now that a court has ruled on the terms of the agreement in one jurisdiction, other banks will likely impose similar terms. This may have the effect of minimizing the implementation of stronger controls. Regulations such as GLBA merely require the implementation of "commercially reasonable" information security controls.[128] Should banks satisfy this requirement in contractual agreements versus enhanced security controls, innovation and overall security will suffer. Since this flaw leaves the banks with power to decide what measures to implement, federal regulators may wake up to this threat. Guidance and regulation for banking will have to become more prescriptive.

While private citizens may continue to pursue FDIC reimbursement from the banks under Regulation E, commercial parties such as Patco and EMI will not be able to recover under this existing Federal regulation.[129]

Federal regulators may follow the established model created and drafted into law for health care providers in the Health Insurance Portability and Accountability Act (HIPAA).[130] HIPAA established privacy and security guidance for Covered Entities when accessing, storing, handling, processing, or disposing of Protected Healthcare In-

[125] *Bank of America - Bank of America Online Banking Security Check*, FRAUDWATCH INT'L, http://www.fraudwatchinternational.com/phishing/individual_alert.php?fa_no=238989&modealert (last visited Feb. 25, 2012). *See also CitiBusiness Online: Security and Accountability Solutions*, CITI BANK, http://www.citibank.com/us/citibusinessonline/securitytoken.htm [hereinafter *CitiBank Online Safety Guide*] (last visited Feb. 25, 2012).

[126] *Citibank Online Safety Guide*, *supra* note 125.

[127] *Id.*

[128] Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, § 508, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

[129] Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205.1 (2010).

[130] H.I.P.A.A. Enforcement Rule, 68 Fed. Reg. 18,895 (Apr. 17, 2003) (to be codified at 45 C.F.R. pt. 160).

formation (PHI).[131] After the initial adoption of the act, Congress clarified the security provisions and commented on "reasonable information security controls" with accompanying commentary in the Federal Register.[132] In response to the challenges in the banking industry, Congress may follow this same approach.

Should these other methods fail to avoid litigation, banks may raise a contributory negligence tort claim. As testified to in *Patco*[133] and alleged in *EMI*, the criminals must have obtained the customer username and password (credentials) in some fashion. Criminals may have obtained access to the online systems through brute force guessing (i.e. trying every possible variant of a password via a specialized script), but more often criminals obtain valid credentials from another avenue. Social engineering or phishing rely on the victims' gullibility and trick them into divulging their credentials. Criminals may also install malware on the computer to capture credentials that victims type in to authenticate their identity on a website. Regardless of the method, a criminal obtains the victims' credentials through some action or inaction on the part of the victims. Banks could use this action or inaction to establish that the customers negligently contributed to the loss of funds.

The provisions in existing contracts regarding browser software, personal firewalls, and antivirus software establish the baseline expectations of a bank. Should a customer lack one or more of these controls, the bank could raise an affirmative defense. Case law does not appear to exist on this point, since most customers have settled their claims against banks. However, some case law does exist regarding contributory negligence and traditional check fraud.[134] If more cases proceed to trial, then courts might expand the scope of the contributory negligence doctrine. However, the recently released supplement to the FFIEC Authentication Guidance may change this balance.

E. *New FFIEC Authentication Guidance Released*

The FFIEC circulated a draft document entitled "Interagency supplement to Authentication in an Internet Banking Environment" for

[131] *Id.*

[132] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. 40,868, 40,916 (July 14, 2010) (to be codified at 46 C.F.R. pt. 164).

[133] Patco Const. Co., Inc. v. Peoples United Bank, No 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011).

[134] *See* Commercial Credit Equip. Corp. v. First Ala. Bank of Montgomery, 636 F.2d 1051, 1056–57 (5th Cir. Unit B Feb. 1981) (holding that a bank could raise a contributory negligence defense against a payor).

comment by member agencies[135] and later released the final Supplemental Guidance.[136] The FFIEC Supplement focuses on four areas:

- Better risk assessments to help institutions understand and respond to emerging threats, including man-in-the-middle or man-in-the-browser attacks, as well as key loggers;
- Layered security that provides both widespread use of multifactor authentication, especially for so-called "high-risk" transactions and fraud detection;
- More effective monitoring and reporting including audit features, multiple control features to authorize fund transfers, and independent review of security and fraud prevention programs;
- Heightened customer education initiatives, particularly for commercial accounts.[137]

These updates should not come as a surprise based on the *EMI* case or developments in online fraud tools such as Zeus.[138]

Zeus serves as one example of the new breed of man-in-the-middle attacks that may upset the balance between shared responsibilities for fraud losses.[139] The user accidentally installs the Zeus Trojan Horse by clicking on a web page link or downloading pirated software.[140] Once installed, Zeus waits for the user to log onto a bank website and steals the authentication credentials.[141] Additionally, Zeus tricks the user into supplying additional information by substituting HTML code for page elements from the bank.[142] By doing so, Zeus may steal user PIN or one-time-use token-generated passwords.[143] Zeus then sends these credentials to criminals who use them to perpetuate additional fraud.[144] Even more worrisome, approximately 3.6 million U.S. machines carry this infection and antivirus software does not detect most variants.[145] Current protection technologies do a poor job of protecting users against attacks such as Zeus.[146] The draft FFIEC gui-

[135] Tracy Kitten, *First Look: New FFIEC Guidelines*, BANK INFO SECURITY (Feb. 22, 2011), http://www.bankinfosecurity.com/articles.php?art_id=3374.

[136] *See generally* FFIEC SUPPLEMENT, *supra* note 52. Scott Fryzel, *The FFIEC's Supplement to Authentication in an Internet Banking Environment*, 128 BANKING L.J. 827 (2011) (providing general background on the FFIEC Supplement and prior cases).

[137] *Id.*

[138] Dan Goodin, *Word's Nastiest Trojan Fools AV Software*, THE REGISTER (Sept. 18, 2009, 12:37 AM), http://www.theregister.co.uk/2009/09/18/zeus_evades_detection/.

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] Trusteer, *Measuring the in-the-wild Effectiveness of Antivirus Against Zeus*, (Sept. 14, 2009), http://www.trusteer.com/files/Zeus_and_Antivirus.pdf.

[143] *Id.*

[144] Goodin, *supra* note 138.

[145] *Id.*

[146] *Id.*

dance provides additional measures that, if adopted by banks, would mitigate some of the risk.[147] The FFIEC Supplement calls on banks to address man-in-the-middle attacks by relying on multifactor authentication and back-end anomaly detection systems.[148]

As the legal and criminal spheres have advanced, the federal guidelines provided to banks must also evolve. The FFIEC Supplement highlights the need for banks, being the party with access to information about "normal" account activity, to put in place systems designed to "detect anomalies and effectively respond to suspicious or anomalous activity."[149] Another aspect of the guidance suggests the use of layered controls, analogous to the castle perimeter defense model discussed in Part II.[150] Banks may implement "out-of-band verification for transactions"[151] or "policies and practices for addressing customer devices identified as potentially compromised" by a Trojan or other malware.[152] Complex device identification systems could move beyond simple Internet Protocol Address (IP) to interrogate the end-user computer for details such as processor type, memory, installed browser, and in the mobile space, unique mobile handset identifiers combined with geo-location.[153] The combination of these techniques might better secure online accounts against attackers.

More importantly, the new FFIEC Guidance shifts the balance for protecting consumers back towards banks. By recognizing that personal consumer protections, such as antivirus software, provide limited protection against threats, the FFIEC has tacitly recognized that banks must do more to protect consumers. The courts will likely follow the advice of the FFIEC and alter the courts' analysis of the duty of care for banks. "'Security is a shared responsibility,' Johnson, Risk Management Vice President, says. 'Responsibility for secure transactions resides at both the business and consumer [sic], as well as at the financial institution.'"[154] Expanding Regulation E to commercial ac-

[147] Kitten, *supra* note 135.

[148] *Id.*

[149] FFIEC SUPPLEMENT, *supra* note 50, at 5; *see also id.* at 4 ("[F]raud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response.").

[150] *Id.*

[151] *Id.* at 4.

[152] *Id.* at 5.

[153] *See* FFIEC SUPPLEMENT, *supra* note 50, at 6.

[154] Linda McGlasson, *Should Banks Be Liable for Business Losses to Fraud?*, BANK INFO SECURITY (Apr. 7, 2010), http://www.bankinfosecurity.com/articles.php?art_id=2390 (quoting Doug Johnson, Risk Management Policy Vice President, American Bankers Association). *See also* Larry Lawrence & Bryan D. Hull, *Risk of Loss for Unauthorized Funds Transfers*, 2 PAYMENT SYS., § 14:30 (2011).

counts would expand the coverage provided by statute and further push the balance towards banks to protect both types of checking accounts.[155] The current regulations attempt to balance responsibility for protecting funds between the bank and the consumer.[156]

V. CONCLUSION: BANKS' LIABILITY FOR ONLINE THEFT DUE TO INSUFFICIENT AUTHENTICATION

Following the FFIEC release of the supplemental guidance, courts will still find in favor of banks that employ statutory minimum authentication protections present in current federal and state laws. Plaintiffs will attempt to recover under strict liability and traditional negligence claims. Plaintiffs will point to evolutionary authentication schemes similar to those made available by Google for e-mail and online tools to sway the balance against what the banks might consider a commercially reasonable authentication. If Google can afford this level of protection for e-mail, banks will struggle to explain why they did not make a similar investment to safeguard financial information.

The problems of assigning liability in tort negligence cases are not new. Courts have long struggled with the proper balance between a bank's negligence and a customer's contributory negligence. These customer actions include selecting poor passwords, installing malware such as keyloggers that record typing, and a failure to implement freely available security software.[157] The FFIEC Supplement seems to point towards regulators assigning greater responsibility on the banks. The courts will follow this direction and increasingly hold banks liable. Banks must implement the current Guidance and Supplement. Even if the courts did not hold the banks liable for negligence in the three cases above, future courts will hold other banks liable for insufficient information security controls. These three cases are the mine canaries that indicate the direction that future lawsuits will pursue. The state of the definition of "commercially reasonable" protections will continue to evolve, with the FFIEC Supplement serving as the new baseline.

[155] *See* McGlasson, *supra* note 154.

[156] *See supra* Part II.

[157] Keylogger software surreptitiously records the users key strokes and forwards along user names and passwords to an attacker.