North Dakota Law Review

Volume 91 | Number 2 Article 3

1-1-2015

Increasing the Role of Agency Deference in Curbing Online Banking Fraud

Stephanie L. Tang

INCREASING THE ROLE OF AGENCY DEFERENCE IN CURBING ONLINE BANKING FRAUD

STEPHANIE L. TANG*

ABSTRACT

Over the past few decades, online banking has gone from a seldom-used, novel technology to one used by over seventy percent of all bank account holders. While online banking may present many benefits, it also opens up consumers to many unknown risks. Fraud is one of the biggest risks associated with online banking. Under Article 4A of the Uniform Commercial Code, a bank is typically not liable for losses due to fraudulent transfers if it has followed "commercially reasonable" security procedures to verify the transaction. Unfortunately, this issue has been sparsely litigated in American courts, and the small handful of cases available offers little guidance to protect either consumers or banks.

In Part II, this article summarizes the history of online banking and presents the challenges banks face in growing consumer confidence. Following in Part III, the article proceeds to analyze interagency guidance on curbing online banking fraud and prior cases assessing the "commercial reasonableness" of banking security procedures. In Part IV, the article then explores approaches taken by the European Union and Malaysia in combating online banking fraud and examines the crucial role of agency deference in other areas of U.S. banking law, including bank charter applications and the interpretation of the Glass-Steagall Act. Consequently, in Part V, this article recommends that banks and courts should give increased deference to existing interagency guidance and look to current, successful initiatives developed in other countries in an effort to increase consumer confidence in online banking and to protect banks from future liability.

* Associate Attorney at Hurst, Robin, & Kay, LLC; J.D., magna cum laude, University of Illinois, 2015; B.A., Northwestern University, 2012. I wish to thank Summer Kim for her mentorship and guidance, including but certainly not limited to the content of this article. I would also like to thank my parents for their endless encouragement and Mark Scott for his undying love and support throughout the writing process.

I. INTRODUCTION

With the influx of Internet users over the past decade, online banking has become ubiquitous and is now an integral element of the banking experience for many consumers. A 2013 study conducted by Pew Research Center found more than half the adults in the United States use online banking.[1] Although online banking is more popular among those ages

1. Susannah Fox, *51% of U.S. Adults Bank Online*, PEW RES. CTR. (Aug. 7, 2013), http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/.

eighteen to twenty-nine, the study found forty-seven percent of seniors (over age sixty-five) were online bankers as well.[2] Further, the number of people who bank online appears to be increasing. In 2014, Nielsen Holdings published new data reporting eighty-two percent of Americans polled stated "they banked online at least once in the past 30 days."[3] The number of online banking users is taken into a more staggering reality when expanded to the global scale. A 2015 study by the Federal Reserve Board found seventy-four percent of all consumers with bank accounts bank online.[4]

Why are so many consumers drawn to online banking? Among other benefits, online banking draws consumers in with promises of cost savings, reduced wait times, increased customization, and convenient access to services.[5] Additionally, online banking helps save consumers time by offering online bill pay and automatic payment alerts.[6] Bill Orr, editor of *CyberBanking*, summarized the core benefit of online banking as "[t]he triple anys—anytime, anywhere, anyway."[7] The focus of banks on online banking services reflects recent consumer preference studies indicating seventy-seven percent of Americans prefer paying bills online.[8] As a result of the increased convenience and feasibility of online banking, banks that fail to provide online services are finding it hard to attract or retain depositors.[9]

However, the ease and efficiency that draw so many consumers to online banking come with some inevitable risks. Economists argue some consumers may be reluctant to adopt online banking because it does not allow consumers to witness the real-time transactions in the same way visiting a physical bank location does.[10] This reluctance leads to a general lack of consumer confidence and trust in Internet banking.[11]

---

2. *Id.*

3. *The Evolution of Modern Banking*, NIELSEN (Mar. 19, 2014), http://www nielsen.com/content/corporate/us/en/insights/news/2014/the-evolution-of-modern-banking html.

4. FED. RESERVE BD., CONSUMERS AND MOBILE FINANCIAL SERVICES 2015 9 (Mar. 2015), http://www federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

5. Ali Reza Montazemi & Hamed Qahri Saremi, *Factors Affecting Adoption of Internet Banking*, EUROPEAN FIN. REV. (Dec. 29, 2013), http://www.europeanfinancialreview.com/?p=623.

6. *4 Advantages of Online Banking*, ACCOUNTNOW, INC. (2015), http://www.accountnow.com/content/online-banking/4-advantages-of-online-banking-2/.

7. Jon Newberry, *'Anytime, Anywhere, Anyway': Online Banking Offers Greater Convenience and Easier Financial Planning*, 82 A.B.A. J. 94 (1996).

8. *The Evolution of Modern Banking*, *supra* note3.

9. *See id.*

10. Montazemi & Saremi, *supra* note 5.

11. *Id.*

The lack of consumer trust in Internet banking is further exacerbated by constant reports of online banking fraud, a problem that has plagued online banking services from their inception.[12] Shirley Inscoe, a senior analyst with Aite Group, recently stated, "We're hearing that the fraud has evolved, there are new types of malware being deployed and . . . we're seeing that fraud spike again."[13] Inscoe observed that over the past several years, fraudsters have become "more sophisticated" and "work a lot harder to impersonate the customer."[14] Federal agencies such as the Federal Bureau of Investigation ("FBI") and Federal Deposit Insurance Corporation ("FDIC") have issued several alerts during this time period to warn banks of recent cyber criminal trends.[15] Nevertheless, the race to prevent online fraud is still considered a "cat and mouse game."[16]

The question then becomes: how do we protect consumers from online banking fraud across all banks? In the United States, "allocation of losses from fraudulent transfers is governed by Article 4A of the Uniform Commercial Code" ("UCC").[17] Generally, a bank is not liable for losses if it followed "commercially reasonable"[18] security procedures to verify the transaction.[19] However, what is "commercially reasonable" has been sparsely litigated, with only four cases issued in the United States thus far which provide little guidance to banks regarding their potential liability.[20] The high costs of judicial discretion point to the potential role for cost-benefit analysis ("CBA") by agencies within the area of online banking fraud. By engaging in CBA, banking agencies may help build consumer confidence and increase transparency regarding online banking fraud prevention.[21]

---

12. *See* Keith Button, *Wire and Online Banking Fraud Continues to Spike for Businesses*, AM. BANKER (Oct. 7, 2013), http://www.americanbanker.com/issues/178_194/wire-and-online-banking-fraud-continues-to-spike-for-businesses-1062666-1 html (discussing numerous online banking fraud reports).

13. *Id.*

14. *Id.*

15. *See id.*; FEDERAL DEPOSIT INSURANCE CORPORATION, FED. BANKING L. REP. P 95-500 (C.C.H.), 2008 WL 8634530 (Oct. 28, 2008).

16. Button, *supra* note 12 (quoting Avivah Litan, Vice President of Gartner, Inc.).

17. Melissa Waite, Comment, *In Search of the Right Balance*: Patco *Lays the Foundation for Analyzing the Commercial Reasonableness of Security Procedures Under UCC Article 4A*, 54 B.C. L. REV. 217, 218 (2013).

18. *See infra* Part III.B.

19. U.C.C. § 4A-202 (AM. LAW INST. & UNIF. LAW COMM'N 1989).

20. *See infra* Part III.B.

21. John C. Coates IV, *Cost-Benefit Analysis of Financial Regulation: Case Studies and Implications* 14 (ECGI Working Paper Series in Law, Working Paper No. 23, 2014) (noting that even in areas where quantification is difficult, "conceptual CBA" is helpful for establishing baselines and alternatives).

In order for banks to achieve a balance between protecting consumers against online banking fraud and the costs of additional safeguards, courts should follow uniform and objective "best practices" determined by agency experts when adjudicating liability. Part II of this article will outline the history of online banking and the challenges banks face in building consumer confidence in the face of online banking fraud. Part III will review interagency guidance on curbing online banking fraud and prior court's assessments of what constitute "commercially reasonable" banking security procedures. Part IV will present several comparative perspectives, first presenting strategies employed in Europe and Malaysia in dealing with online banking fraud, and second, presenting a short analysis of the role of agency deference in other areas of banking law. Finally, Part V will outline a recommendation advocating for increased deference by American banks to existing interagency guidance documents, given the success of the initiatives discussed in Part IV.

II. BACKGROUND

Before exploring ways to safeguard banks from liability, it is important to understand the development of online banking and the parallel growth of online banking fraud throughout the past decade. This Part outlines the timeline from the inception of online banking and discusses the problems banks now face in a perpetually evolving, technology-dependent society.

A. HISTORY OF ONLINE BANKING IN THE UNITED STATES

Online banking in the United States first sprouted in New York in 1981 when four of the city's main banks began offering home banking services through the videotex system.[22] Over the following decade, many banks started viewing online banking as a necessary strategy to, among other advantages, diminish transaction costs and bundle services with minimal overhead.[23] In 1995, Security First Network Bank became the nation's first Internet-based bank, marking a vast departure from the traditional brick-and-mortar money transactions.[24] That same year, Wells Fargo became the first U.S. bank to offer account services online.[25] In 1998, a large number

22. M. Edwards, *Computer Giants Giving a Major Boost to Increased Use of Corporate Videotex*, COMMC'N NEWS (Oct. 1, 1984), http://www.thefreelibrary.com/Computer+Giants+Giving+a+Major+Boost+to+Increased+Use+of+Corporate. . .-a0586601.

23. Sharil Sharma, *The Pragmatic Review on Internet Banking and Associated Services in India*, INT'L J. OF COMPUTING AND CORP. RES., July 2004, at 1, 3.

24. Newberry, *supra* note 7, at 94.

25. Sharma, *supra* note 23, at 5.

of mergers and acquisitions occurred throughout the financial industry.[26] These mergers and acquisitions significantly expanded banks' customer bases, resulting in a flood of banks turning to the Internet as a "flashy" way of maintaining customers and building loyalty.[27]

Although many banks began adopting online banking services at this time, many customers were initially reluctant to transition to electronic transactions.[28] However, the advent of new electronic commerce companies, such as America Online, eBay, and Amazon, ultimately sold consumers on the benefits of transacting online.[29] To keep up with the trend, eighty percent of U.S. banks offered online banking services in 2000.[30] The customer base for online banking jumped drastically after the Y2K scare ended, with consumers beginning to trust that both online banking and the Internet as a whole were safe.[31] The post-Y2K spike highlights the importance of assured banking security in growing a customer base for online banking services.

With growing feelings of security regarding online banking, the number of banks offering interactive web-based services grew from six in 1996 to over six thousand in 2004.[32] Over the past fifteen years, the percentage of Internet users that bank online has jumped from less than 0.4% in 1999 to 51% in recent years.[33] As of 2010, most bank customers (36%) prefer to conduct banking online compared to any other method.[34] This greatly outweighs any other method of banking, including visiting physical branches (25%) and using Automated Teller Machines ("ATMs") (15%).[35] It is clear from the recent trend towards online services that banks need to prioritize security measures to maximize and ensure consumer protection.

---

26. *Id.* at 3.

27. *Id.*

28. Saleh M. Nsouli & Andrea Schaechter, *Challenges of the "E-Banking Revolution"*, FIN. & DEV. (Sep. 2002), http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli htm (finding that although Singapore and Australia had the most banks offering e-banking services in 2000, they were not among the top ten countries where e-banking was the most popular per capita).

29. Sharma, *supra* note 23, at 3.

30. *Id.*

31. *Id.*

32. Nick Semanko, *A. Electronic Banking*, *in* 24 ANN. REV. BANKING & FIN. L. 97, 98 (2005).

33. *Compare* Sharma, *supra* note 23, at 5, *with* Fox, *supra* note 1.

34. *ABA Study: Consumers Prefer Online Banking*, THE FIN. BRAND (Oct. 12, 2010), http://thefinancialbrand.com/14005/aba-ipsos-banking-delivery-channel-survey/ (quoting findings of a study completed by the American Bankers Association).

35. *Id.*

B. OBSTACLES AND RISKS OF ONLINE BANKING

With the rapid increase of online banking services comes new obstacles and risks facing banks offering these services. Two paramount concerns for banks offering online banking services are building consumer confidence and preventing phishing and other fraudulent activities.

1. *Consumer Confidence*

While online banking purportedly offers many advantages compared to the traditional brick-and-mortar bank, research indicates consumers are still reluctant to hop on board. Scholars speculate consumers view online banking as a novelty that is not compatible with their past experience in banking.[36] Together, these factors lead to a high level of uncertainty, which causes consumer reluctance towards engaging in online banking relationships.[37]

In a 2004 study comparing Internet experts and average consumers, eighty-one percent of experts considered online banking a low-risk activity, but only forty-six percent of consumers agreed.[38] Further, seventy percent of experts thought online bill paying was low-risk, while only forty-one percent of consumers agreed.[39] "[A]mong [consumers] who had not banked online, six percent cited privacy concerns, twenty-six percent cited security, and an additional twenty-two percent said they were simply not comfortable with the idea of banking through a computer."[40]

One can argue that this same mistrust on the individual consumer level translates, if not multiplies, to the business customer level as well. In fact, research indicates fraudsters are increasingly targeting small to mid-sized business bank accounts because they typically lack sophisticated security measures in place and may have accounts with smaller community banks that have lower levels of security.[41] The story of Sign Designs, Inc. is one particularly telling example of a small business losing a large sum of money

36. Montazemi & Saremi, *supra* note 5.

37. *Id.*

38. Julie Dunn, *Survey Reveals High-Risk Net Use, Few See a Problem in Giving Personal Data to Financial Institutions Via E-mail, Which Could Open Them Up to Fraud*, DENVER POST (Aug. 17, 2004).

39. *Id.*

40. *Id.*

41. Riva Richmond, *Wanted: Defense Against Online Bank Fraud*, WALL ST. J., Feb. 8, 2010, http://online.wsj.com/articles/SB10001424052748703483604574630690362605018 ("Cybercriminals have found a rich new hunting ground: small businesses' bank accounts."); *Online Banking Fraud: Who is Liable and How Can it be Prevented?*, BNC BANK, https://www.bncbank.com/files/OnlineBankingFraud.pdf.

to online fraud.[42] Sign Designs, an electric sign maker, had an account with Bank of Stockton, a local community bank.[43] One day in 2010, Sign Designs logged onto its online bank account only to find almost $100,000 had been sent to seventeen mystery people the previous day.[44] In its defense, the Bank of Stockton noted that they should not be liable for the business' losses because Sign Designs failed to take advantage of security measures that potentially would have avoided the loss.[45] Sign Designs represents only one of thousands of small businesses whose bank accounts have been drained in a similar fashion.[46] It is therefore critical that banks take measures to safeguard their online banking procedures to build necessary consumer trust.

2. *Risks of Fraud*

A large risk banks face when moving to the online sector is opening themselves up to phishing. Phishing is defined as a scheme where an e-mail induces potential victims to log-in to websites that seem legitimate.[47] These emails often purport to be from, or related to, financial institutions involved in high-profile mergers, acquisitions, or failures.[48] This is a strategy to prompt consumer attention and create a sense of urgency and legitimacy for requesting personal information.[49] Once a victim inputs a username and password, his or her personal information is transmitted to scammers who in turn use the information to withdraw funds or apply for credit.[50]

The risk of phishing has gone up substantially over the years, with phishers becoming more sophisticated and finding new channels to retrieve information over the past decade. The 2008 U.S. Federal Deposit Insurance Corporation Technology Incident Report compiled suspicious activity reports filed quarterly by banks nationwide.[51] The Report found 536 cases of computer intrusion in 2007, with an average of $30,000 acquired per transaction. A 2012 report by JP Morgan estimated the total revenue loss from online fraud was $3.4 billion, a $700 million increase over 2010

42. Richmond, *supra* note 41.
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*
47. Semanko, *supra* note 32, at 98.
48. FED. RESERVE BD., FED. BANKING L. REP. P 95-500 (C.C.H.), 2008 WL 8634530 (Oct. 28, 2008).
49. *Id.*
50. Semanko, *supra* note 32, at 96.
51. Sharma, *supra* note 23.

results.[52] These reports highlight the necessity of addressing online banking fraud to prevent future loss in funds. Moreover, in addition to the quantifiable cost of fraud, banks may suffer significant reputational harm from a security breach.[53]

III. REGULATION OF ONLINE BANKING FRAUD IN THE UNITED STATES[54]

There are two primary resources American banks can turn to when trying to protect themselves from claims of inadequate security procedures. The first is the Authentication Guidance published by the interagency body, the Federal Financial Institutions Examination Council ("FFIEC"), which outlines minimum-security procedures all banks should follow. The second are the few cases American courts have adjudicated on the issue of what constitutes a "commercially reasonable" banking security procedure under Article 4A of the UCC. These two areas provide a basis of comparison for banks seeking to protect themselves against future liability.

A. THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL GUIDANCE

The FFIEC is a formal interagency body of the United States government composed of five banking regulators: the Federal Reserve Board of Governors ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), the National Credit Union Administration, the Office of the Comptroller of the Currency ("OCC"), and the Consumer Financial Protection Bureau.[55] The primary role of the FFIEC is to "prescribe uniform principles, standards, and report forms . . . to promote uniformity in the supervision of financial institutions."[56] In May 2014, Thomas J. Curry, Comptroller of the Currency and FFIEC Chair, stated that "helping to make banks less vulnerable and more resilient to cyber-attacks" has been one of

52. 2012 Online Fraud Report, JP MORGAN, CYBERSOURCE CORP. (2012), https://www.jpmorgan.com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey=id&blobwhere=1320571432216&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs.

53. Nikil Chande, *A Survey and Risk Analysis of Selected Non-Bank Retail Payments Systems,* Discussion Paper 2008-17, Bank of Canada 8 (2008), http://ideas repec.org/p/bca/bocadp/08-17 html#author.

54. For the purposes of this paper, the author is going to primarily confine the scope of analysis to online banking fraud with regards to the liability of banks to business customers under the UCC. However, the author recognizes the role of Credit Rating Agencies, individual consumers, and Automated Clearing House ("ACH") payments in this field as well.

55. *About the FFIEC*, FED. FIN. INSTS. EXAMINATION COUNCIL, http://www ffiec.gov/about htm (last visited Mar. 27, 2014).

56. *Id.*

the FFIEC's top priorities.[57] This focus is reflected in two major initiatives launched by the FFIEC: (1) the launch of the FFIEC's new website on cyber security,[58] and (2) an updated Authentication Guidance to serve as a standard for all banks to follow.[59] These resources are intended to help institutions manage cyber security and protect consumers from risk of cyber crimes.

The FFIEC's 2011 Authentication Guidance updates and reinforces the expectations set forth in the previously published 2005 FFIEC Guidance.[60] The 2011 Guidance was designed to establish minimum-security procedures all banks should follow in protecting themselves against risk of fraud.[61] These procedures include adopting authentication techniques, such as device identification and asking challenge questions as barriers to protect customers from fraud.[62] The Guidance further stresses the effectiveness of certain procedures over others in preventing bank fraud.[63] This helps banks and courts understand what the "best practices" are for protecting bank customers.[64]

Approaching promulgation of Guidance documents this way allows the FFIEC to conduct a form of informal CBA whereby the public is able to understand why these agencies chose these methods as the "best."[65] This in turn allows consumers to compare their current bank's practices to those recommended by the FFIEC to determine whether investing with the bank online is a sound financial decision. By including a CBA within the Guidance publication and weighing the pros and cons of major fraud prevention processes, the five FFIEC agencies effectively split the cost and

57. Thomas J. Curry, Comptroller, Office of the Comptroller of the Currency, Remarks by Thomas J. Curry Comptroller of the Currency Before RMA's Governance, Compliance, and Operational Risk Conference 7, (May 8, 2014), http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-69a.pdf.

58. *See Cybersecurity Awareness*, FED. FIN. INSTS. EXAMINATION COUNCIL (Sept. 29, 2014, 9:54 AM), http://www ffiec.gov/cybersecurity htm.

59. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, SUPPLEMENT TO AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (June 28, 2011), http://www ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf.

60. *Id.* at 1.

61. *Id.*

62. *Id.* at 6-7.

63. *See, e.g.*, *id.* at 6. The Guidance finds that "simple device identification" is less effective than using "one-time" cookies. *Id.* The Guidance reasons banks have found fraudsters can easily copy cookies to their computers from banks only using simple device identification, thereby giving them relatively easy access to users' accounts. *Id.* In contrast, using "one-time" cookies creates a more unique "fingerprint" for a customer, looking at additional factors including "PC configuration, Internet protocol address, geolocation, and other factors. *Id.*

64. *Id.* at 1.

65. *See* Coates, *supra* note 21, at 898 (arguing a potential benefit of CBA as a whole may be to "enhance public understanding of why regulations are adopted").

time of reviewing fraud prevention procedures while increasing transparency to the public.

Other agencies have followed suit and produced written reports supplementing the FFIEC Guidance, thereby providing further direction to banks in risk-management strategies to pursue in preventing online banking fraud. For example, the OCC published a bulletin building off FFIEC reports that provided their "key components" of a payment risk-management system.[66] Within this report, the OCC noted several "adequate procedures" for banks to follow, including clearly defined responsibilities over internal controls for each transaction, board approval for risk management procedures, and procedures directly proportional to the scope and complexity of a given bank's procedures.[67] In this way, the OCC again weighed potential costs and benefits of certain fraud prevention procedures and gave its recommendations for banks and consumers to consider.

Critics argue courts may rely too heavily on recommendations from FFIEC Guidance and other agency analysis because Article 4A of the Uniform Commercial Code simply requires courts to consider whether a particular banking procedure is reasonable *for the particular bank*, not "whether the security procedure is the best available."[68] Comment 4 to UCC Article 4A-203 notes, "The concept of what is commercially reasonable in a given case is flexible," indicating there are likely differences in what is a "commercially reasonable" security procedure in a small rural bank versus a more sophisticated urban bank.[69] To respond to this concern, courts should take measures such as, using this example, holding urban banks with a larger consumer base and more complex financial transactions to a higher standard of security than their smaller rural counterparts.

B. CASES ASSESSING THE "COMMERCIAL REASONABLENESS" OF ONLINE BANKING PROCEDURES TO PREVENT BANKING FRAUD

In the United States, the allocation of losses from fraudulent bank transfers or business customers is governed by Article 4A of the UCC.[70]

66. *Description: Risk Management Guidance, OCC Bulletin 2006-39*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Sept. 1, 2006), http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39 html (last updated Oct. 23, 2013).

67. *Id.*

68. U.C.C. § 4A-203 cmt. 4 (AM. LAW INST. & UNIF. LAW COMM'N 1989).

69. *Id.*

70. *See id* § 4A. The Electronic Funds Transfer Act and Regulation E provide that individual consumers receive heightened protection against unauthorized transfers from their bank account. However, this Act does not apply to business customers. *See* Federal Reserve Act, 12 U.S.C. § 226 (2012); 15 U.S.C. § 1601-03 (2012); Electronic Fund Transfer Act, 15 U.S.C. § 1693 (2012); Richmond, *supra* note 41.

Generally, under the UCC, a bank is not liable for losses if it followed "commercially reasonable" security procedures to verify the transactions, and the bank followed those procedures in good faith.[71] While this standard is codified, it is so sparsely litigated that banks have a difficult time knowing what security procedures they need to have in place in order to protect themselves. As of 2015, only four cases have analyzed what constitutes "commercially reasonable" online banking security procedures. To decide what is "commercially reasonable," the UCC directs courts to consider "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 . . . and security procedures in general use by customers and receiving banks similarly situated."[72] While this is a good starting place, it becomes evident when looking at the case law that courts are still confused as to what the threshold requirements are for a given bank's security procedures.

The first case where a court reviewed a bank's security procedure was in *Regatos v. North Fork Bank*.[73] The bank's procedure entailed sending a signed order to the bank by fax, a confirmatory phone call between the customer and a sole bank officer, and a signature comparison between the faxed order and a signature card.[74] The *Regatos* court found the procedure was commercially reasonable because the bank employee could recognize the customer's voice as he had dealt with him repeatedly over several years.[75]

Next, in *Filho v. Interaudi Bank*, the United States District Court for the Southern District of New York evaluated another multi-layered security procedure.[76] This procedure paralleled the one in *Regatos* in that it consisted of a logged and recorded telephone confirmation with the customer, who was required to correctly answer security questions before the bank would release the funds.[77] The *Filho* court found the bank's security procedure was commercially reasonable because the additional verification provided by the security questions compensated for the lack of voice recognition.[78] Like the court in *Regatos*, the *Filho* court focused on the importance for banks to implement multifactor authentication in their

71. U.C.C. § 4A-203 cmts. 3-4 (AM. LAW INST. & UNIF. LAW COMM'N 1989).
72. U.C.C. § 4A-202 (AM. LAW INST. & UNIF. LAW COMM'N 1989).
73. 257 F. Supp. 2d 632 (S.D.N.Y. 2003).
74. *Id.* at 646
75. *Id.*
76. No. 03 Civ. 4795(SAS), 2008 WL 1752693, at *4 (S.D.N.Y. Apr. 16, 2008).
77. *Id.* at 5.
78. *Id.*

security procedures.[79] In *Regatos*, the court's determination of commercial reasonableness hinged on the bank's use of an outside voice recognition confirmation method.[80] Similarly, in *Filho*, the court's holding that the bank's procedure was commercially reasonable was based on the dual components of an out-of-bank authentication procedure and a knowledge-based requirement (the security question).[81] Consequently, these cases suggest it is crucial for banks to adopt security measures with multiple verification processes in order to protect themselves against liability for fraudulent transfers. However, one important limitation of the applicability of these cases today is that *Regatos* and *Filho* both addressed wire transfers by fax, a practice that has recently lost popularity amongst banks.

The Texas Court of Appeals in *All American Siding & Windows, Inc. v. Bank of America*, *N.A.* affirmed the emphasis on layered security measures in the context of online ACH payments.[82] In this case, Bank of America's procedure consisted of a personalized ID, passcode, and digital certificate verification technology.[83] The court found the security procedure was commercially reasonable for ACH payments submitted via online banking because, among other reasons, the bank adhered to the 2005 FFIEC Guidance.[84] Further, the court noted Bank of America acted in good faith because there was no evidence in the record that the bank had received the required paperwork to confirm a fraudulent transaction had occurred.[85] While the bank did reference the 2005 FFIEC Guidance, it was only a cursory reference, and it was left unclear to what extent the court considered the contents of the Guidance in reaching its decision.[86]

Most recently, the United States Court of Appeals for the First Circuit evaluated the commercial reasonableness of online banking security procedures in *Patco Construction Co. v. People's United Bank*.[87] Unlike *Regatos, Filho*, and *All American Siding & Windows, Inc.*, the court for the first time found the bank's security procedures were not commercially reasonable as a matter of law.[88] The bank's security procedure proceeded as follows. First, each client was assigned a unique ID and password, and then each client provided personalized answers for the challenge

79. *Id.*
80. Regatos v. N. Fork Bank, 257 F. Supp. 2d 632, 646 (S.D.N.Y. 2003).
81. *Filho*, 2008 WL 1752693, at *5
82. 367 S.W.3d 490, 501 (Tex. App. 2012).
83. *Id.* at 500.
84. *Id.* at 501.
85. *Id.*
86. *Id.*
87. 684 F.3d 197, 200 (1st Cir. 2012).
88. *Id.* at 211.

questions.[89] The system would ask challenge questions to confirm a client's identity and installed a digital certificate on the device for future authentication.[90] Further, the online system would require clients to answer one of their preset challenge questions any time a transaction amount exceeded one dollar.[91] In analyzing this dollar threshold, the court reasoned that it substantially increased the risk of fraud for any clients who initiated frequent, routine transfers.[92] "[T]he increase in risk," the court argued, "was sufficiently serious to require a corollary increase in security measures . . . ."[93] The lack of additional security measures to account for the increased risk was a red flag indicating the procedures were not commercially reasonable.

In addition to faulting the bank for not implementing additional security measures proportional to the higher levels of risk, the *Patco* court also reprimanded the bank for its failure to implement widely available security procedures that other banks had implemented.[94] As in *All American Siding & Windows, Inc.*, the court analyzed security devices advocated for in the 2005 FFIEC Guidance for online banking procedures and found the bank's process did not adequately follow the Guidance's recommendations.[95] For example, the court noted that bank employers never monitored the risk scores that their online system generated, whereas many other banks had employees monitoring risk scores and verifying high-scoring transactions.[96]

The court's ruling in this case summarizes the two takeaways banks may pull from the limited case law on commercial reasonableness. First, any additional exposure to risk may warrant consideration of additional security procedures in a given bank. Second, courts so far have taken a comparative approach in determining whether a given bank's security procedures are commercially reasonable by looking at agency guidance and similarly situated banks. With this in mind, it is important to remember that these cases are few and far between, so there is still considerable leeway for further clarification by the court.

One potential method of how this wide discretion could be narrowed is by taking the approach of the courts in *All American Siding & Windows,*

89. *Id.* at 202.
90. *Id.* at 202-203.
91. *Id.* at 203.
92. *Id.* at 210.
93. *Id.* at 212.
94. *Id.* at 213.
95. *Id.*
96. *Id.*

Inc. and *Patco* in noting banks' compliance with the guidelines set forth by the FFIEC. Even in these cases, the bank simply noted the existence of the Guidance without going into an in-depth discussion of the weight the Guidance had on their decision. These cases serve to highlight the costs of only having judicial discretion without any substantial agency or expert deference. Without clear standards for liability, banks are arguably hesitant to invest in procedures in which there is no clearly defined benefit. In turn, consumers are hesitant to invest in online banking for fear their assets will not be properly protected.

Further, it is important to quickly note here the distinction between federal and state banks within the U.S. banking system. The United States has a unique "dual banking" system, with parallel and co-existing state and federal banking systems.[97] On the most elementary level, the federal banking system is based on a federal bank charter and defined under federal law, whereas state banks are characterized by state chartering with powers characterized under state law.[98] As discussed above, judicial determination of bank liability for online banking fraud under the federal system is already inconsistent and arbitrary. Given the inconsistencies that exist at the federal level, the inconsistencies will likely only multiply on the state bank level, making it even more difficult for banks to avoid liability if sued for losses from security breaches by business customers.

C. STALL OF ANTI-PHISHING LEGISLATION

Besides the FFIEC Guidance, Congress has taken several steps to impose penalties on creators of computer spyware that facilitates phishing. First, the United States House of Representatives passed the Internet Spyware (I-SPY) Prevention Act of 2007 in May 2007.[99] The Act has yet to pass in the Senate.[100] The Act, if passed, "would make it illegal to access a PC without authorization or to exceed authorized access by copying software to code to further another criminal act, impair security procedures, or steal the personal or financial information of another end-user."[101] It

97. Comptroller of the Currency Administrator of National Banks, *National Banks and The Dual Banking System*, OFFICE OF THE COMPTROLLER OF CURRENCY 1 (2003), http://www.occ.gov/publications/publications-by-type/other-publications-reports/national-banks-and-the-dual-banking-system.pdf.

98. *Id.*

99. William Jackson, *House Passes Bill To Criminalize Spyware Fraud*, NEWSBYTES NEWS NETWORK, Oct. 8, 2004, http://gcn.com/articles/2004/10/08/house-passes-bill-to-criminalize-spyware-fraud.aspx.

100. See Internet Spyware (I-SPY) Prevention Act of 2004, H.R. 4661, 110th Cong. (2007).

101. Frank Washkuch, Jr., *I-SPY Act Passes House, but Anti-Spyware Legislation Faces Tough Hurdle in Senate*, SC MAG. (May 23, 2007), http://www.scmagazine.com/i-spy-act-passes-house-but-anti-spyware-legislation-faces-tough-hurdle-in-senate/article/35033/.

appears the Act may have reached a standstill in the Senate, with commentators speculating this may stem from the Act's failure to focus on the enforcement of anti-spyware measures.[102]

Second, the House passed the Security Protect Yourself Against Cyber Trespass Act, or SPY Act, on June 6, 2007.[103] This bill differed from the I-SPY Act because the SPY Act "prohibits any deceptive or unauthorized use of spyware."[104] However, the Senate, again, did not pass the bill.[105] With Congress stalling action on these and similar acts, it appears banks will likely be unable to turn to anti-phishing legislation for guidance in the near future. With judicial discretion proving too arbitrary and Congressional action proving fruitless, increased deference to the FFIEC appears to be the most promising course of action in helping protect both banks and consumers.

IV. COMPARATIVE ANALYSIS

In determining the feasibility and effectiveness of increased FFIEC deference in protecting banks from being held liable for fraudulent transactions, it is helpful to look both at other countries' approaches to the problem as well as the prevalence of agency deference in other areas of banking law. This Part will first discuss the salient features of the initiatives set forth in Europe and Malaysia for fraud protection and the role key expert organizations have played in promulgating and promoting each of these initiatives.[106] It will then turn to agency deference in other areas of banking law to demonstrate viability of agency deference in online banking fraud prevention. Together, these comparative points boost the argument for increased deference to the FFIEC in determining reasonable online banking security procedures.

---

102. *Id.*

103. Securely Protect Yourself Against Cyber Trespass Act or Spy Act, H.R. 964, 110th Cong. (2007).

104. Jackson, *supra* note 99.

105. *See* Securely Protect Yourself Against Cyber Trespass Act or Spy Act, H.R. 964, 110th Cong. (2007).

106. These two examples are not meant to serve as a comprehensive representation of fraud prevention strategies. The author chose to analyze the Single Euro Payments Area because it addresses fraud prevention through unification of systems of credit and debit transfers across multiple countries in developed economies, much like the unification the author is proposing for banking systems across state borders in the United States. The author chose to analyze the example of the Inter-Bank GIRO roadshows in Malaysia because these are catered on a community level to smaller rural communities that do not have access to online banking. The United States has similar rural areas where such unification between rural and urban systems would prove beneficial, which is discussed in Part IV, *infra*.

A. PAYMENT INTEGRATION UNDER THE SINGLE EURO PAYMENTS AREA

The Single Euro Payments Area ("SEPA") is a European Union ("EU") regulation that streamlines all electronic payments in the Euro area, advertising "fast and secure transfers" between any bank accounts.[107] SEPA spans twenty-eight EU countries and the additional European Economic Area countries,[108] and came into full effect in February 2014, when all prior national payment schemes were closed down and replaced with SEPA schemes.[109] This means all credit transfers and direct debits in the Euro area are made under the SEPA Credit Transfers and SEPA Direct Debits system, respectively.[110] As of August 1, 2014, most European banks now comply with SEPA guidelines.[111] The main proponents of the SEPA initiative—EU governments, the European Parliament, the European Commission, and the European Central Bank ("ECB")—sought to incentivize use of electronic payment instruments, in conjunction with reducing the overall cost of wholesale cash distribution.[112] Within SEPA, each consumer has an International Bank Account Number ("IBAN") and a Business Identifier Code ("BIC"), which are required to make or receive any Euro electronic payments.[113] Having an IBAN and BIC allows you to make and receive payments, collect a direct debit on any Euro account, and make a credit transfer to any euro account within SEPA.[114]

The European Commission addressed how SEPA relates to fraud in their October 2004 Action Plan.[115] The Commission noted that before SEPA was implemented there were ten million fraudulent transactions in

107. *Questions and Answers on SEPA*, EUROPEAN COMM'N, http://ec.europa.eu/internal_market/payments/sepa/faq/index_en htm (last visited Feb. 11, 2016).

108. *EPC List of SEPA Scheme Countries*, EUROPEAN PAYMENTS COUNCIL, http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-list-of-sepa-scheme-countries/epc409-09-epc-list-of-sepa-scheme-countries-v23/.

109. *Banking and Finance*, EUROPEAN COMM'N, http://ec.europa.eu/finance/payments/sepa/index_en.htm.

110. *Questions and Answers on SEPA*, *supra* note 107.

111. Craig Ramsey, *SEPA – Is the Burden Turning into a Benefit*?, ACI UNIVERSAL PAYMENTS (Sept. 5, 2014), http://www.aciworldwide.com/what-we-know/expert-view/2014/9/5/sepa-is-the-burden-turning-into-a-benefit.aspx.

112. *SEPA – Vision and Goals*, EUROPEAN PAYMENTS COUNCIL, http://www.europeanpaymentscouncil.eu/index.cfm/about-sepa/sepa-vision-and-goals/ (last visited October 15, 2014).

113. *IBAN and BIC*, EUROPEAN PAYMENTS COUNCIL, http://www.europeanpaymentscouncil.eu/index.cfm/sepa-credit-transfer/iban-and-bic/ (last visited March 31, 2016).

114. *Id.*

115. *Fraud and Counterfeiting: Non-Cash Means of Payment*, EUROPEAN COMM'N, http://ec.europa.eu/internal_market/payments/fraud/index_en htm#maincontentSec2 (last updated Nov. 2, 2016).

the SEPA area per year, amounting to approximately €1 billion in losses.[116] The Commission recognized that without intervention, the high rate of fraud might negatively impact consumer confidence in electronic payments, especially given rapid technological developments and criminals' adaptation to the developments as they arise.[117] In light of this concern, the Commission notably commended the SEPA Cards Framework, developed by the European Payments Council ("EPC").[118] The Framework requires any card scheme to support fraud prevention activities connected to EPC resolutions on card fraud.[119] Implementing this framework successfully in the card fraud area highlights the potential benefits for other areas of online banking fraud.

Conversely, there may be a downside to SEPA's simplification of monetary transactions. With all of the SEPA banks adopting the same procedures, if a fraudster finds a way to crack one bank's system, it could lead to a rapid influx of hacks over a short period of time. McAfee, an online security firm, found it was this simplification that made SEPA a major target for fraud.[120] McAfee Blogger Ryan Sherstobitoff postulated, "Typically in these organized fraud campaigns we see a lot of mule activity in countries other than the nation hosting the victim's bank."[121] Another critic, Monique Goyens, director general of the Bureau Européen des Unions de Consommateurs, asserted, "The complete lack of security regarding key aspects of SEPA . . . is practically a call for tender to fraudsters. Nothing requires banks to check the reliability of the issuer of the direct debit payment."[122]

Specifically, in the fraudulent transactions McAfee identified, fraudsters initiated SEPA credit transfers through an automated transfer

116. Comm'n of the European Communities, *Commission Staff Working Document: Report on Fraud Regarding Non Cash Means of Payments in the EU: the Implementation of the 2004-2007 EU Action Plan, EUROPEAN COMM'N* 6 (2008) [hereinafter *EU Action Plan*] http://ec.europa.eu/internal_market/ payments/docs/fraud/implementation_report_en.pdf.

117. *Id.*

118. *Id.* at 9; *see SEPA Cards Framework Version 2.1*, EUROPEAN PAYMENTS COUNCIL, (Dec. 18, 2009), http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/other-documents/sepa-cards-framework-v-21/cards-scf-006-09-v-2-1pdf/.

119. *EU Action Plan*, *supra* note 116, at 9-10.

120. *AFP Fraudwatch: SEPA Provides Juicy Fraud Target in Europe*, ASS'N FOR FIN. PROF'LS (Nov. 28, 2012), http://partners niceactimize.com/index.aspx?page=news608 [hereinafter *AFP Fraudwatch*].

121. *Id.* A "money mule" is an individual who transfers illegally acquired money either in person, or electronically, to fraudsters. Brook Satti, *Emerging Trends in Money Mule Schemes*, SECURITY INTELLIGENCE (Sept. 11, 2014), https://securityintelligence.com/emerging-trends-in-money-mules-schemes/.

122. Tim Wright, *The Single Euro Payments Area and the Risk of Fraud*, E-FIN. & PAYMENTS L. & POL'Y 13 (Jan. 2013), https://www.pillsburylaw.com/siteFiles/News/EFPLP January2013Wright.pdf.

system, which sent a withdrawal request to the victim's account and created a mule account.[123] In response, Ben Knieff, Director of Financial Crime Marketing at NICE Actimize, recommends that European banks should take additional measures to account for the increased risk of SEPA-based payments compared to alternative payment methods.[124] ACI Worldwide also cautioned that while SEPA will allow for greater transparency for banks across borders, this also means they will face increased risks as a result of SEPA.[125] Despite the added risk of fraud, Knieff stresses, "There are many advantages to SEPA, and the fraud risks do not outweigh these advantages."[126] ACI Worldwide follows Knieff's logic by arguing the potential impact of security failure on revenue and a bank's customer experience creates a business incentive for making investments in additional security procedures.[127] This way, SEPA banks can work towards multi-channel monitoring for every consumer transaction.[128] SEPA serves as an example where another developed economy performed a CBA on unifying credit and debit transfers and found the benefits of consolidation with the help of expert guidance outweighed the costs.

B. A GRASSROOTS INITIATIVE FOR CONSUMER CONFIDENCE: INTER-BANK GIRO

Even if courts and banks look to the factors set forth in documents such as the FFIEC Guidance, this may not be sufficient for bank customers to feel secure in using banking products. Malaysia highlights another way expert banking authorities can help build consumer confidence and unify banks' authentication systems.[129] Compared to the SEPA countries and the United States, online banking systems are largely unused and unfamiliar in Malaysia.[130] Although seventy-four percent of all Malaysian bank account holders have online bank accounts, only forty-three percent of this subset actively engages in online banking transactions.[131] Consequently, their

123. *Id.*
124. *Id.*
125. Ramsey, *supra* note 111.
126. *AFP Fraudwatch*, *supra* note 120.
127. Ramsey, *supra* note 111.
128. *Id.*
129. Encik Abu Hassan Alshari Yahaya, *The Benefits of Online Banking Services and Inter-Bank GIRO (IBG) in Malaysia*, BANK FOR INT'L SETTLEMENTS 2 (Dec. 2, 2013), http://www.bis.org/review/r131211g.pdf.
130. *Id.*
131. *Id.*

online bank fraud rate accounts for a mere 0.0002% of total transactions made annually nationwide.[132]

Malaysian banks have adopted the Inter-Bank GIRO ("IBG"), a paperless system through which a customer of a participating bank can transfer funds through direct credits and debits to any other customer of another participating bank.[133] To promote adoption of the IBG system, the Association of Banks in Malaysia ("ABM"), Bank Negara Malaysia, the Association of Islamic Banking Institutions Malaysia ("AIBIM") and other banking institutions organized "Experience IBG" roadshows to travel around Malaysia.[134] These roadshows provided information to consumers and small businesses to learn the benefits of online banking and the security checks in place by other Malaysian banks.[135] Each roadshow consisted of exhibition booths by major banks to showcase their electronic banking systems, promotional offers for attendees who sign up for online banking, and informational videos.[136] In conjunction with the roadshows, several major Malaysian banks held weeklong "Open Day" events, which were intended to reach out to consumers in smaller towns.[137] By gathering in one condensed area, all participating banks were incentivized to present the most innovative security procedures to attract attendees.

Results of this initiative indicate such methods both increase consumer confidence in online banking, particularly in rural areas, and decrease the rate of fraud nationwide. During the first four roadshows, sixty-six percent of all participants signed up for online banking services.[138] This suggests that roadshow attendees learned about the benefits of online banking and felt confident enough to sign up for online banking services as a result.[139] Moreover, while many other countries are suffering from increased rates of online banking fraud, Malaysia actually enjoyed a decline of fraudulent transactions.[140]

---

132. *Id.*

133. *Interbank GIRO (IBG) Procedures*, ASS'N OF BANKS IN SING., http://abs.org.sg/docs/library/ibg_procedures.pdf; *Frequently Asked Questions on Interbank GIRO (IBG) Transfers*, HSBC, https://www hsbc.com my/1/PA_ES_Content_Mgmt/content/website/pdf/personal/pib/IBG- FAQ.pdf.

134. Yahaya, *supra* note 129, at 1.

135. *Id.*

136. *Id.* at 2.

137. *Id.* at 2.

138. *Id.* at 1.

139. *Id.*

140. *Id.* at 2 (indicating losses from internet banking fraud went down from 0.0002% to 0.0001% in the first nine months of 2014).

C. AGENCY DEFERENCE IN OTHER AREAS OF U.S. BANKING LAW

The idea of deferring to agency expertise when litigating cases is long established in banking law as a whole. One particularly salient example of the level of deference given to banking agencies is seen in the separation of commercial and investment banking as defined by the Glass-Steagall Act.[141] In an article examining judicial review of legal interpretations of the Act by the federal banking agencies (the OCC, FRB, and FDIC), the author found that with the exception of the FRB, "courts have consistently deferred to the banking agency's interpretations of the Glass-Steagall Act . . . ."[142] Another area where banking agencies receive a substantial level of deference is in bank charter applications. In the representative case of *Camp v. Pitts*, the Supreme Court reviewed the OCC's denial of respondent's charter application under the National Bank Act.[143] The Court upheld the OCC's decision on the grounds that the agency stated a determinative reason for denying the new bank's application as an uneconomic venture.[144]

Specifically, courts afford banking agencies in these areas *Chevron* deference in reviewing the agency's construction of the governing statutes. This means if a reviewing court finds Congress has explicitly left a gap for the agency to fill with a regulation, the court will defer to an agency's interpretation of the Act if it is based on a "permissible construction of the statute."[145] These regulations are given controlling weight unless they are "arbitrary, capricious, or manifestly contrary to the statute."[146] The great weight given to agency interpretation in this and other areas of banking law lies in the expertise of a given agency. Further, courts have stressed that they must afford deference to banking agencies so the agencies can continue updating banking laws to fit the changing financial needs of both

---

141. *See* Glass-Steagall Act, 12 U.S.C. §§ 24, 78, 335, 377, 378 (2012) (defining "investment banking" as "the business of issuing, underwriting, selling, or distributing, at wholesale or retail, or through syndicate participation, stocks, bonds, debentures, notes, or other securities").

142. Linda B. Matarese, *Has the Chevron Deference Made a Difference When Courts Review Federal Banking Agency Interpretations of the Glass-Steagall Act?*, 33 HOW. L.J. 195, 201 (1990) (noting a single instance where the Supreme Court rejected the FRB's ruling); *see* Sec. Indus. Ass'n v. Bd. of Governors of the Fed. Reserve Sys., 468 U.S. 137, 142-43 (1984).

143. 411 U.S. 138, 138 (1973).

144. *Id.* at 143.

145. Chevron U.S.A. Inc., v. Nat. Res. Def. Council, Inc., 467 U.S. 827, 843 (1984).

146. *Id.* Another area where banking agencies are afforded great deference is in cases adjudicated on bank failures. *See generally* Franklin Savings Ass'n v. Director, Office of Thrift Supervision, 934 F.2d 1127 (10th Cir. 1991) (ruling in favor of the agency, finding "absent extraordinary circumstances, the decision of the director as to what information he must review should be left to his discretion").

consumers and banks.[147] The preexisting high level of deference given to banking agencies in other areas of banking law suggests it is feasible to grant a similar level of deference to the FFIEC's expertise in protecting banks from being held liable for online banking fraud.

V. RECOMMENDATION

The costs of letting judges decide liability of banks based on arbitrary factors may prove disastrous in the future, both for banks and their customers. On the one hand, businesses may be reluctant to use online banking services because they are worried they will lose their money if fraudsters penetrate the bank's system. On the other hand, a bank may be held liable in one jurisdiction, while a bank with an identical security procedure may be exempt from liability. Instead, when determining liability of banks under the UCC, courts should follow the examples of SEPA, the IBG roadshows, and other areas of banking law and defer to the FFIEC's analysis of the costs and benefits of different online fraud prevention procedures.

With the support of the European governments and banking authorities, the banks within the SEPA area streamlined their credit and debit transfer procedures for the benefit of consumer transaction efficiency. Skeptics argue uniform procedures could potentially lead to a flood of fraud attacks if fraudsters penetrate the procedure. Nevertheless, even SEPA skeptics find the benefits of unified fund transfers outweigh the potential risks of fraud. If U.S. courts give greater weight to compliance with FFIEC Guidance in determining liability, banks will be incentivized to follow more streamlined fraud prevention procedures similar to the unified procedures seen in the SEPA system.

To maximize the ability to work together, transparency is of utmost importance in adopting uniform security procedures. Banks in the United States should follow the example set by the "Experience IBG" roadshows in Malaysia and other similar programs in achieving this goal. As in Malaysia, these presentations should be organized through U.S. banking institutions and organizations and catered to building consumer confidence. Moreover, similar presentations should be scheduled for board members of banks to help protect banks as well. The content for these presentations should be drawn from interagency reports such as those drafted by the FFIEC and from pending legislation. Using these sources will provide an overview of preexisting technologies adopted by banks across the United States. By fostering awareness through both consumers and the banks

147. Matarese, *supra* note 142, at 260.

themselves in conjunction with FFIEC documents, banks will want to adopt additional security procedures to attract new clients and protect themselves from liability under the UCC's "commercial reasonableness" standard.

Moreover, the banking agencies afforded deference in other areas of banking law are the same ones that comprise the membership of the FFIEC. It would not be a stretch, therefore, to grant the combined efforts of these agencies a similar level of deference as they receive in these other areas in adjudication of online banking fraud. While the FFIEC has only issued Guidance documents in helping banks adopt security procedures, the courts should look at the bank's compliance with the Guidance suggestions as a large factor in determining reasonableness under the UCC.

One major downside to relying on FFIEC Guidance is the significant amount of time it still requires to produce the documents. A six-year period elapsed between the first and second Guidance issuance. Given the rapid rates of development of new technology and fraudster strategies, there may be new technological advances that arise during the publication period that are not accounted for within the Guidance. However, the Guidance documents can still provide an overview of the categories of areas courts should look for in determining the reasonableness of a bank procedure.[148] This benefit alone will help promote unification between bank procedures and build certainty for banks to protect themselves from liability.

VI. CONCLUSION

While many consumers are attracted to the convenience and speed of online banking, it is important to remember its potential risk of fraud. In the United States, banks are not liable for losses if they followed "commercially reasonable" security procedures to verify the transaction.[149] However, courts have only litigated the "commercial reasonableness" of online banking security procedures a few times to date, and the costs of relying solely on judicial discretion are too high. With an objective reasonableness standard, such as that imposed by the UCC, it is to the advantage of U.S. banks to maintain uniform online banking security procedures. In working towards this uniformity, U.S. banks should follow the examples set by SEPA in Europe and the "Experience IBG" roadshows in Malaysia.

148. *See About the FFIEC*, *supra* note 55 (categorizing ideal security procedures into several groups for banks to consider: layered security programs, device identification, challenge questions, and malware).

149. U.C.C. § 4A-203 (1989).

Specifically, both banks and courts should increasingly rely on the Guidance promulgated by the FFIEC to determine reasonableness under the UCC. This not only parallels the deference given to the SEPA governments and the IBG roadshow organizers, but also reflects the prominent trend of deference to banking agencies in other areas of American banking law. These three comparative points serve as examples where the benefits of regulation outweigh the costs of wide discretion in prevention techniques. The FFIEC has the expertise to weigh the costs and benefits of implementing certain fraud procedures in banks and publicize their findings to banks and the public at large. By following these publications' baselines and alternatives analysis, banks can not only increase consumer confidence in online banking but also protect themselves from liability in the future.