

Increased Bank Liability for Online Fraud: The Effect of *Patco Construction Co. v. People's United Bank*

I. INTRODUCTION

In an age where online transactions are quickly replacing face-to-face interactions, there is a growing opportunity for criminals to capitalize on the lack of traditional safeguards that would normally protect an individual's identity.¹ Unfortunately, consumers and their banks have not been immune to these cyber-threats or third-party fraud.² In fact, many consumers are reluctant to use online banking fearing that their personal information may be stolen through fraudulent phishing³ attempts.⁴ A consumer's social security number, date of birth, and credit card information may all be stolen by criminals who use this information to access bank accounts and steal money.⁵ To counteract this growing threat, financial institutions have begun to develop advanced security measures to enhance authentication procedures related to protecting user identity in online banking.⁶ The Federal Financial Institutions Examination Council (FFIEC)⁷ is an organization devoted in part to the authentication of identity in online banking transactions and has issued a guidance document entitled Authentication

1. See David Navetta, *The Duty to Authenticate Identity: The Online Banking Breach Lawsuits*, 8 A.B.A. SCITECH L. 22, 22 (2011).

2. See *id.*

3. David Koenigsberg, *XII. Security with Online Banking*, 25 ANN. REV. BANKING & FIN. L. 118, 119 (2006) ("Phishing, an example of access theft, 'uses spoofed e-mails, purporting to be from reputable companies, requesting unsuspecting consumers to provide personal financial information.'").

4. *Id.* at 118 ("[H]alf of U.S. consumers are reluctant to bank online for fear of losing their personal information.").

5. *Id.* at 119 ("The average loss per individual from phishing is \$2,320.").

6. See Navetta, *supra* note 1, at 22.

7. FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, <http://www.ffiec.gov/> (last visited Oct. 13, 2012) ("The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions . . .").

in an Internet Banking Environment (“2005 Guidance”)⁸ and a 2011 FFIEC Supplement⁹ focused on outlining additional security recommendations for banks.¹⁰

However, despite a number of recent court decisions addressing the topic, the exact law surrounding bank liability for third-party fraud has been hard to define.¹¹ The First Circuit Court of Appeals’ holding in *Patco Construction Co. v. People’s United Bank*,¹² will undoubtedly have a significant influence on establishing the legal standard for bank security systems.¹³ However, the First Circuit’s holding that the security measures at issue were not “commercially reasonable”¹⁴ was improper for two main reasons. First, its policy of avoiding a one-size-fits-all approach to fraud prevention ignored previous precedent related to online banking.¹⁵ Second, its holding will have the negative effect of increasing fraud liability for banks that offer online banking services and creating a large burden for smaller banks that will need to implement additional advanced security measures in order to meet this heightened “commercially reasonable” standard.¹⁶

This Note examines the First Circuit’s decision in *Patco*, concluding that the First Circuit’s holding was misguided based on precedent and important policy considerations. Part II provides a brief introduction of the existing law surrounding bank liability for online fraud and the role of the FFIEC.¹⁷ Part III introduces the *Patco* case,

8. *Authentication in an Internet Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL (Oct. 12, 2005), available at http://www.ffiec.gov/pdf/authentication_guidance.pdf.

9. *Supplement to Authentication in an Internet Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL (June 28, 2011), available at [http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20\(FFIEC%20Formatted\).pdf](http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formatted).pdf).

10. See Navetta, *supra* note 1, at 23.

11. See *id.* at 22.

12. *Patco Const. Co. v. People’s United Bank*, 684 F.3d 197 (1st Cir. 2012).

13. See Tracy Kitten, *3 Lessons from PATCO Fraud Ruling*, BANKINFO SECURITY (July 20, 2012) [hereinafter *3 Lessons*], available at <http://www.bankinfosecurity.com/3-lessons-from-patco-fraud-ruling-a-4970>.

14. U.C.C. § 4A-202 (2011) (“A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.”).

15. See *infra* Part IV.B.

16. See *infra* Part IV.B. 1,2.

17. See *infra* Part II.

discussing the facts behind the fraud attacks, Ocean Bank's security system, the district court's decision, and the First Circuit's reversal.¹⁸ Part IV discusses whether or not the First Circuit's holding was correct by examining previous decisions related to online banking and highlighting important policy considerations.¹⁹ Part V of this Note provides recommendations for attorneys representing both banks and consumers in light of the *Patco* decision.²⁰

II. BANK LIABILITY

Before there was guidance from the FFIEC, the majority of states used Uniform Commercial Code § 4A-202²¹ to establish the burden for any loss that occurred during the transfer of funds through online banking.²² Under this section, if banks met certain security requirements related to authenticating identity, then consumers would bear the risk of any loss.²³ In order to have the benefit of this standard, a bank's security procedures must have been found to be "commercially reasonable."²⁴ However, Article 4A does not establish the specific parameters of a security procedure that will be accepted by the courts, leaving this to be developed on an ad hoc basis.²⁵

Due to the vague standard established by the U.C.C., the FFIEC

18. See *infra* Part III.

19. See *infra* Part IV.

20. See *infra* Part V.

21. See U.C.C. § 4A-202 (2011); see also Edwin E. Smith et al., *First Circuit Sheds Light on the Scope of "Commercially Reasonable" Security Measures for Funds Transfers*, BINGHAM MCCUTCHEN LLP (July 24, 2012), <http://www.bingham.com/Alerts/2012/07/First-Circuit-Sheds-Light-on-the-Scope> (summarizing U.C.C. §4A-202).

22. See Navetta, *supra* note 1, at 23; see also Stuart R. Hene, *Funds Transfers Under UCC Article 4A: What Is A Commercially Reasonable Security System?*, 64 CONSUMER FIN. L. Q. REP. 331, 331 (2010) ("Article 4A funds transfers may be originated in numerous ways; e.g., a telephone call, a facsimile (FAX) message, or an internet transfer. Many of these transfers are now originated over the internet, and at the core of this information infrastructure is cyberspace.").

23. See Smith et al., *supra* note 21 (stating that a bank could shift responsibility by implementing a "commercially reasonable" system); see also Navetta, *supra* note 1, at 23 ("Pursuant to this section, if a bank satisfies certain security requirements, including those directly related to authenticating identification, its customers will be liable for fraudulently transferred funds, even if the transfer was initiated by a criminal hacker. Conversely, if the bank fails to meet such requirements, the bank will bear the risk of such losses.").

24. See Hene, *supra* note 22 (summarizing the factors that a court is to consider under Article 4A).

25. See *id.*

has long been concerned with the authentication of identity in online banking transactions.²⁶ By issuing the 2005 Guidance, the FFIEC hoped to aid banks and their consumers by providing security recommendations for online banking transactions.²⁷ After the 2005 Guidance was issued, however, online banking threats began to change dramatically.²⁸ In fact, advancements in technology created new avenues²⁹ through which cyberthreats might arise.³⁰ As a result, a significant gap between the FFIEC recommendations and the type of security measures that would be effective arose, leading to a spike in fraud rates and the number of at-risk customers.³¹ The increased number of fraud cases led to an increase in litigation as courts struggled to find the correct balance between consumer and bank liability.³² The *Patco* case followed this long line of litigation³³ that supported strictly following U.C.C. § 4A-202 and deferring to FFIEC recommendations to determine what is a “commercially reasonable” system.³⁴ However, the First Circuit’s decision will likely make a large dent in this legal landscape.

26. See Navetta, *supra* note 1, at 22.

27. See *id.*

28. FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, *2011 FFIEC Authentication Guidance: A New Standard for Online Banking Security* (2011) [hereinafter *2011 FFIEC Authentication Guidance*], http://ffiec.bankinfosecurity.com/whitepapers.php?wp_id=492.

29. *Cyber Security: Responding to the Threat of Cybercrime and Terrorism: Hearing Before Subcomm. on Crime and Terrorism of the S. Judiciary Comm.*, 112th Cong. 1 (2011) (statement of Gordon M. Snow, Assistant Director, Cyber Division, FBI) (outlining how “smart home” products, industrial control systems, and malicious software are capable of becoming significant threats).

30. *2011 FFIEC Authentication Guidance*, *supra* note 28.

31. *Id.*

32. See *Experi-Metal, Inc. v. Comerica Bank*, No. 09-14890, 2011 U.S. Dist. LEXIS 62677 (E.D. Mich. June 13, 2011); *Braga Filho v. Interaudi Bank*, 334 F. App’x 381 (2nd Cir. 2009); *Covina 2000 Ventures Corp. v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, No. 06 Civ. 15497, 2008 U.S. Dist. LEXIS 32799 (S.D.N.Y. Apr. 21, 2008); *Regatos v. N. Fork Bank*, 257 F. Supp. 2d 632 (S.D.N.Y. 2003); *Centre-Point Merchant Bank Ltd. v. American Express Bank Ltd.*, No. 95 Civ. 5000, 2000 U.S. Dist. LEXIS 17296 (S.D.N.Y. Nov. 27, 2000).

33. See *id.*

34. See Kevin Funnell, *Patco and Experi-Metals: How Much Hope Do They Really Give Small Businesses?*, BANK LAWYER’S BLOG (July 31, 2012), http://www.banklawyersblog.com/3_bank_lawyers/2012/07/patco-and-experi-metals-how-much-hope-do-they-really-give-small-businesses.html.

2013]

THE EFFECT OF PATCO

385

III. PATCO

A. *Fraud Attacks on Patco Construction Co.*

In 2009 Patco Construction Co. (PATCO) revealed that over \$580,000 of its funds were stolen from the firm's commercial bank account by an unknown third-party through a series of fraudulent online transactions.³⁵ PATCO's accounts were held at Ocean Bank, a division of People's United Bank located in southern Maine.³⁶ These fraudulent withdrawals were made on PATCO's accounts over the course of several days beginning on May 7, 2009.³⁷ The third-party initially withdrew over \$50,000 from PATCO's account by supplying the proper credentials of one of PATCO's employees.³⁸ The credentials used to access the account included the employee ID, password, and answers to challenge questions.³⁹ The initial withdrawal was directed to the accounts of several unknown individuals.⁴⁰ As a result of the nature of the withdrawal, Ocean Bank's security system produced a risk score of 790 out of 1000 for this transaction.⁴¹ Typically, risk scores over 750 were considered to be high risk.⁴² Factors such as a high risk amount and IP anomaly⁴³ contributed to the high risk score.⁴⁴ Although the risk score of this transaction might have been alarming, no one at Ocean Bank was monitoring these types of transactions, and PATCO was not notified of the suspicious withdrawals.⁴⁵

The third parties then initiated more fraudulent transactions on

35. *See* Patco Const. Co. v. People's United Bank, 684 F.3d 197, 199 (1st Cir. 2012); *see also* Tracy Kitten, *Inside the PATCO Fraud Ruling*, BANKINFO SECURITY (July 9, 2012) [hereinafter *Inside the PATCO Fraud Ruling*], <http://www.bankinfosecurity.com/inside-patco-fraud-ruling-a-4927>.

36. *Patco*, 684 F.3d at 199.

37. *Id.* at 204.

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

42. *See Inside the PATCO Fraud Ruling*, *supra* note 35 (stating that the range of risk scores is from 0-1000 with risk scores over 750 being considered high risk).

43. "IP Anomaly" is the appearance of a new, previously unrecognized IP address that the Bank had never seen in a transaction. *See id.*

44. *Patco*, 684 F.3d at 204.

45. *Id.*

May 8, 11, 12, and 13.⁴⁶ All of these additional transactions produced high risk scores, and the proceeds were sent to individuals to whom PATCO had never sent funds.⁴⁷ On May 14, it was finally determined that the fraudulent transactions were a string of thefts when PATCO informed Ocean Bank that it had not authorized the transactions.⁴⁸ In total, the amount of money withdrawn from PATCO's account was \$588,851.26, of which only \$243,406.83 was recovered.⁴⁹ Following the fraudulent withdrawals, Ocean Bank claimed that it gave PATCO several recommendations about how to protect its system and mitigate the damage from the attacks.⁵⁰ However, PATCO claims that it only received a single instruction to hire a forensic professional to check its system for a security breach.⁵¹

B. Ocean Bank's Security System

Beginning in 2004, Ocean Bank began using NetTeller, an online banking platform provided by Jack Henry & Associates⁵² (Jack Henry).⁵³ However in 2007, in response to the authentication guidelines outlined by the FFIEC in 2005,⁵⁴ Ocean Bank began working with Jack Henry to conduct a risk assessment and implement a new security system that integrated a multifactor authentication system.⁵⁵ A new

46. *Id.* at 205.

47. *Id.*

48. *Id.*

49. *Id.*

50. *Patco Const. Co. v. People's United Bank*, 684 F.3d 197, 204 (1st Cir. 2012) (“[Ocean Bank] instructed Patco to disconnect the computers it used for electronic banking from its network; to stop using these computers for work purposes; to leave the computers turned on; and to bring in a third-party forensic professional or law enforcement to create a forensic image of the computers to determine whether a security breach had occurred.”).

51. *Id.* at 206.

52. Jack Henry & Associates, Inc. is a provider of core information processing solutions for banks. See JACK HENRY, <http://www.jackhenry.com/Default.aspx?P=4fc1d089-10b0-4cd1-8e4c-9c6efcd85686> (last visited Feb. 9, 2013).

53. *Patco*, 684 F.3d at 201 (stating that Jack Henry provided NetTeller to between 1,300 and 1,500 bank customers).

54. *Id.* (“Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents.”).

55. *Id.* at 202 (“The bank determined that its eBanking product was a “high risk” system that required enhanced security, and in particular, multifactor authentication.”).

system, provided by Cyota Inc.,⁵⁶ was incorporated into Ocean Bank's existing online banking security system that had been provided by Jack Henry to comply with FFIEC guidance.⁵⁷ The Cyota system included six distinct features.⁵⁸ First, user IDs and passwords were implemented in order for PATCO employees or online banking customers to access relevant accounts.⁵⁹ Second, invisible device authentication was installed through the use of "cookies."⁶⁰ Third, the system included "risk profiling" which produced risk scores for every transaction based on a multitude of data.⁶¹ Fourth, users were asked to answer challenge questions depending on the type of transaction and risk score.⁶² Fifth, a dollar amount rule was implemented which automatically triggered challenge questions for transactions over a certain dollar figure.⁶³ Finally, a subscription to the "eFraud network" was offered so that the bank and other financial institutions could report IP addresses that had been associated with fraud.⁶⁴ However, the bank's new security system

56. Cyota, Inc. focuses on online security and anti-fraud solutions for financial institutions and was acquired by RSA Security in December 2005. *See RSA Security to Acquire Cyota; Creates Leading Provider of Layered Authentication Solutions*, RSA: THE SECURITY OF EMC (Dec. 5, 2005), http://www.rsa.com/press_release.aspx?id=6316.

57. *Patco*, 684 F.3d at 202 ("Through collaboration with RSA/Cyota, Jack Henry made two multifactor authentication products available to its customers to meet the FFIEC Guidance: the "Basic" package and the "Premium" package. Ocean Bank selected the Jack Henry "Premium" package, which it implemented by January 2007.").

58. *Id.* at 202-03.

59. *Inside the PATCO Fraud Ruling*, *supra* note 35 ("PATCO employees were required to enter a company ID/password, as well as a user-specific ID and password to access online banking.").

60. *Id.* ("The system used "cookies" to create a log of known devices customers used to access accounts. If the cookie changed or was new, it could impact the risk score, potentially triggering challenge questions.").

61. *See* Smith et al., *supra* note 21, at 2 ("Cookies" were placed onto computers that correctly logged into an account to flag certain computers as low risks when logged in."); *see also* *Inside the PATCO Fraud Ruling*, *supra* note 35 ("Jack Henry's adaptive monitoring provided a risk score for every log-in attempt and transaction based on a multitude of data, including IP address, device cookie identification, geo location and transaction history.").

62. *Inside the PATCO Fraud Ruling*, *supra* note 35 ("[U]sers were required to establish three challenge questions and responses, which could come into play for various reasons, as detailed above. If the user failed to answer the questions in three attempts, then that user would be blocked from online banking.").

63. *See* Smith et al., *supra* note 21 ("When a certain dollar figure transaction was entered, challenge questions were asked. However, Ocean Bank lowered the trigger amount from \$100,000 to \$1.00 before the fraudulent withdrawals"); *see also* *Inside the PATCO Fraud Ruling*, *supra* note 35 ("The Jack Henry system allowed the bank to set transaction thresholds, above which challenge questions would be triggered - even if user ID, password and device cookies all were valid.").

64. *See* *Inside the PATCO Fraud Ruling*, *supra* note 35 (stating that banks could use

did not include every possible security feature.⁶⁵ For instance, the package did not include: (1) out-of-band authentication that would allow for authentication via telephone, e-mail or text message;⁶⁶ (2) user-selected pictures to assist with account recognition;⁶⁷ (3) tokens, such as a USB device, that would automatically generate passwords;⁶⁸ or (4) the monitoring of risk-scoring reports by bank personnel.⁶⁹ Ultimately, each of these factors proved to be very important when the court made its decisions regarding whether or not Ocean Bank's security system was "commercially reasonable" and whether the bank was liable for third-party fraud.⁷⁰

C. District Court's Decision

At the district court level, the court referred to the FFIEC guidelines and held that Ocean Bank had sufficiently followed and implemented a multifactor authentication system as recommended by the 2005 Guidance.⁷¹ In this decision, the court separated its approach into three factors for determining the reasonableness of the bank's security measures and the existence of layered security measures.⁷² First, the court looked to the "something you know" factor, referring to bank's implementation of challenge questions and passwords.⁷³ Next,

the network to report IP addresses that had been previously connected with fraud).

65. *Patco*, 684 F.3d at 203 ("There were several additional security measures that were available to Ocean Bank but that the bank chose not to implement . . .").

66. *Inside the PATCO Fraud Ruling*, *supra* note 35 ("[O]ut-of-band generally refers to transactions authenticated via telephone, e-mail or SMS/text message to a customer.").

67. *Id.* ("The use of user-selected pictures for authentication was available, but Ocean Bank declined the option.").

68. *Id.* ("Physical devices such as USB, smartcard or password-generating tokens were not available from Jack Henry, but were offered by other vendors. Ocean Bank did not offer tokens until after the PATCO fraud incidents.").

69. *Id.* ("At the time of the fraudulent transactions, bank personnel did not monitor the risk-scoring reports they received, the court says, nor did the bank conduct any ongoing review of transactions that generated high-risk scores. The bank had the ability to manually monitor high-risk transactions through its transaction-profiling and risk-scoring system, but chose not to do so.").

70. *Patco*, 684 F.3d at 203.

71. *Patco Const. Co. v. Peoples United Bank*, CIV. 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011), *aff.g* *Patco Const. Co. v. People's United Bank*, No. 2:09-CV-503-DBH, 2011 WL 2174507 (D. Me. May 27, 2011); *see also* Navetta, *supra* note 1, at 24-25.

72. *Id.*

73. *See* Bert Knabe, *Is Protecting Businesses Deposits the Banks Responsibility?*, LUBBOCK AVALANCHE-J. (June 8, 2011), <http://lubbockonline.com/interact/blog-post/bert->

the court looked at the “something you have” factor by examining the use of device cookies to identify particular computers used to access online banking accounts.⁷⁴ Under this system, if the cookie changed or was installed on a different computer, the transaction was assigned a higher risk score, which could then result in the user being asked a challenge question.⁷⁵ Finally, under the “something you are” factor, the court focused on the bank’s examination of the online identity, such as the IP address, of individuals accessing an online banking account.⁷⁶ The court also focused on the bank’s use of layered security.⁷⁷ In this case, the implementation of layered security included controls to analyze customer behavior, such as risk profiling.⁷⁸ Using the information obtained through risk profiling, the bank’s system would assign a risk score to a particular banking session that could trigger challenge questions.⁷⁹

In its decision, the district court specifically stated that Ocean Bank’s security was not optimal.⁸⁰ However, the court held that a “commercially reasonable” system does not have to be the best security system available.⁸¹ As a result, the court found that the bank had technically implemented multifactor authentication per the FFIEC 2005 Guidance and was not liable for the loss suffered by PATCO.⁸²

knabe/2011-06-08/protecting-businesses-deposits-banks-responsibility.

74. *See id.*; Patco Const. Co. v. Peoples United Bank, CIV. 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011), *aff.g* Patco Const. Co. v. People’s United Bank, No. 2:09-CV-503-DBH, 2011 WL 2174507 (D. Me. May 27, 2011); *see also* Navetta, *supra* note 1, at 24-25.

75. Patco Const. Co. v. Peoples United Bank, CIV. 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011), *aff.g* Patco Const. Co. v. People’s United Bank, No. 2:09-CV-503-DBH, 2011 WL 2174507 (D. Me. May 27, 2011); *see also* Navetta, *supra* note 1, at 24-25 (2011).

76. *See* Knabe, *supra* note 73.

77. Patco Const. Co. v. Peoples United Bank, CIV. 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011), *aff.g* Patco Const. Co. v. People’s United Bank, No. 2:09-CV-503-DBH, 2011 WL 2174507 (D. Me. May 27, 2011); *see also* Navetta, *supra* note 1, at 24-25 (2011).

78. *See* Navetta, *supra* note 1, at 24-25 (2011). (“[T]he location of the user logging in; when and how often the online banking system was previously used by the customer; the activities the user typically engaged in; the Internet Protocol (IP) address typically used by the customer to log-in; and the size, type, and frequency of payment orders normally issued by the customer.”).

79. *See id.*

80. *See id.*

81. *See id.*

82. *See id.* (stating that although the challenge questions were held to be irrelevant, because they were triggered for every transaction, the system was still technically a multifactor authentication system).

D. First Circuit Reverses

In July 2012, the First Circuit found that Ocean Bank's security was not "commercially reasonable" for several reasons.⁸³ First, the Bank's practice of requiring every transaction of \$1 or more to be approved via challenge questions increased the risk of fraud.⁸⁴ Here, despite the fact that Ocean Bank thought it was using the safest setting, no specific transaction would be afforded additional security because every transaction was flagged on this factor.⁸⁵ Furthermore, asking challenge questions for every transaction allowed fraudsters the opportunity to capture the answers through malware.⁸⁶ By lowering the dollar amount requirement to \$1 for every transaction, Ocean Bank deprived the complex system "of its core functionality."⁸⁷ Second, the First Circuit held that Ocean Bank's failure to properly monitor transactions and notify customers of high risk transactions were unreasonable practices.⁸⁸ In this case, Ocean Bank had failed to notify PATCO of the suspicious transactions despite a risk score of 790, which was much higher than PATCO's typical risk scores.⁸⁹ As a result, the First Circuit found that Ocean Bank had implemented a "one-size-fits-all" approach to providing online banking security, which exposed PATCO to additional risk.⁹⁰ Finally, the First Circuit held that PATCO failed to implement additional, available security procedures to offset the negative effects of the \$1 dollar rule and its failure to notify PATCO about at-risk customers.⁹¹ Ultimately, "these collective failures, taken

83. See *Patco Const. Co. v. People's United Bank*, 684 F.3d 197, 199 (1st Cir. 2012); see also *Inside the PATCO Fraud Ruling*, *supra* note 35.

84. See *id.*

85. See Greg Pulles & Brent Ylvisaker, *First Circuit's Ruling Finds Bank's Actions "Commercially Unreasonable" Under UCC Article 4A* (July 9, 2012), DORSEY & WHITNEY LLP, http://www.dorsey.com/eU_finreg_patco_070912/ ("The bank thought it was making the system safer by setting the threshold at \$1, effectively asking the challenge questions for every transaction.").

86. *Id.* ("The court's conclusion that asking challenge questions for every transaction enabled fraudsters using malware or keylogging to capture the answers.").

87. See *Patco*, 684 F.3d at 199 ("The \$1 dollar amount rule guaranteed that challenge questions would be triggered on every transaction, unless caught by a separate eFraud Network.").

88. See *id.* at 211.

89. *Id.* at 204 (PATCO's usual risk scores ranged between 10 and 214).

90. See *id.* at 212.

91. *Id.* ("Ocean Bank introduced no additional security measures in tandem with its decision to lower the dollar amount rule, despite the fact that several such security measures

as a whole, rendered Ocean Bank's security procedures commercially unreasonable."⁹²

E. Questions Left Open

Although the First Circuit's reversal was significant, a number of important questions were still left unanswered.⁹³ The primary question left undecided was whether PATCO had satisfied its obligations and responsibilities under U.C.C. § 4A-202.⁹⁴ The First Circuit remanded this question to the district court in order to resolve the genuine and disputed issues of fact that were material to this question.⁹⁵ The parties also disagreed on what particularly triggered the fraud attacks.⁹⁶ Another point of contention surrounded whether or not PATCO had been offered the opportunity to receive e-mail alerts.⁹⁷ On one hand, Ocean Bank claimed that it began offering e-mail alerts in 2007.⁹⁸ However, PATCO claimed that it was never made aware of this option and its requests for e-mail alerts were ignored.⁹⁹ As a result, the First Circuit could not make a decision regarding whether these alerts were made available or whether they would have had a significant impact.¹⁰⁰

were not uncommon in the industry and were relatively easy to implement.”).

92. *Id.* at 213.

93. *Patco Const. Co. v. People's United Bank*, 684 F.3d 197, 214 (1st Cir. 2012) (“There remain several genuine and disputed issues of fact which may be material to the question of whether Patco has satisfied its obligations and responsibilities under Article 4A, or at least to the question of damages.”).

94. *Id.*

95. *Id.*

96. *Id.* (“The parties disagree over whether key-logging malware enabled the fraudulent transactions.”).

97. *Id.* (“As to the genuine and disputed issues of fact, the parties dispute the facts surrounding Patco's lack of e-mail alerts.”).

98. *Id.* at 203 (“Ocean Bank asserts that on December 1, 2006, as it began to implement the Jack Henry system, it also began to offer the option of e-mail alerts to its eBanking customers.”).

99. *Patco Const. Co. v. People's United Bank*, 684 F.3d 197, 214 (1st Cir. 2012) (“Patco alleges that it requested e-mail alerts from the bank, but that the bank ignored these requests and never notified Patco when e-mail alerts became available to bank customers.”).

100. *Id.* (“[N]either party has submitted into the record an example of such an e-mail alert or specified when such an e-mail alert would have been sent, such that it is unclear what Patco would have learned from such an e-mail alert and whether and when such an e-mail would have placed Patco on notice of the fraudulent transfer.”).

IV. WAS THE FIRST CIRCUIT'S HOLDING CORRECT?

A. *Precedent*

The First Circuit's decision that Ocean Bank's security system was commercially unreasonable ignored precedent that focused on conformance to FFIEC guidelines, and thus overlooked a number of policy considerations related to online banking. In several prior decisions,¹⁰¹ courts have focused on conformance to FFIEC guidelines as one of the key factors in determining whether a bank can be held liable for third-party fraud.¹⁰² Pursuant to FFIEC recommendations, Ocean Bank offered a security system equipped with User ID, Password, Device ID, Risk Profiling, and Challenge Questions.¹⁰³ However, these factors were found to be insufficient as the First Circuit decided to enforce a higher standard than merely conforming to FFIEC recommendations.¹⁰⁴ This decision was a significant detour from previous holdings that determined a system was "commercially reasonable" strictly in light of FFIEC conformance.¹⁰⁵

For example, in an earlier case, *Experi-Metal, Inc. v. Comerica Bank*,¹⁰⁶ the court concluded that, while the bank had not adopted the best security system possible, the system could still be considered "commercially reasonable" based on following the then-existing standards suggested by the FFIEC.¹⁰⁷ In *Experi-Metal*, the court focused primarily on whether the banks initiated layered security through behavioral analytics to further authenticate a customer's

101. See *Experi-Metal, Inc. v. Comerica Bank*, No. 09-14890, 2011 U.S. Dist. LEXIS 62677 (E.D. Mich. June 13, 2011); *Braga Filho v. Interaudi Bank*, 334 F. App'x 381 (2nd Cir. 2009); *Covina 2000 Ventures Corp. v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, No. 06 Civ. 15497, 2008 U.S. Dist. LEXIS 32799 (S.D.N.Y. Apr. 21, 2008); *Regatos v. N. Fork Bank*, 257 F. Supp. 2d 632 (S.D.N.Y. 2003); *Centre-Point Merchant Bank Ltd. v. American Express Bank Ltd.*, No. 95 Civ. 5000, 2000 U.S. Dist. LEXIS 17296 (S.D.N.Y. Nov. 27, 2000).

102. See *Navetta*, *supra* note 1, at 24; see also *Hene*, *supra* note 22 (discussing five past cases and their definitions of the commercially reasonable standard).

103. *Patco Const. Co. v. People's United Bank*, 684 F.3d 197, 202-203 (1st Cir. 2012).

104. *Id.* at 210-213.

105. *Experi-Metal, Inc. v. Comerica Bank*, No. 09-14890, 2011 U.S. Dist. LEXIS 62677 (E.D. Mich. June 13, 2011); see also John Kraher, *Wire Transfers, Good Faith, and "Phishing"*, 65 CONSUMER FIN. L. Q. REP. 420, 420 (2011).

106. *Experi-Metal*, 2011 U.S. Dist. LEXIS 62677.

107. Kraher, *supra* note 105.

identity as recommended by the FFIEC.¹⁰⁸ The *Experi-Metal* court concluded that although the bank had implemented layered security, it did not implement behavioral analytics to further authenticate the identity of users.¹⁰⁹ As a result, the court treated the FFIEC recommendations like de facto regulation and found that the bank failed to act in good faith, because it did not strictly conform to these guidelines.¹¹⁰

The district court followed this precedent in *Patco* by holding that existing layered security measures incorporating some behavioral analytics were sufficient to determine reasonableness.¹¹¹ The court looked to the 2005 Guidance and noted that the guidance did not recommend any specific security measures or procedures.¹¹² Instead, the court analyzed the agreement between PATCO and Ocean Bank and whether Ocean Bank had implemented multi-factor authentication requirements.¹¹³ The court felt that it was enough that Ocean Bank had technically met the requirements of the 2005 Guidance and ruled that the system was “commercially reasonable.”¹¹⁴ The First Circuit, however, decided to require more than a technical implementation of FFIEC recommendations largely based on a policy decision to require more than one-size-fits-all approach.¹¹⁵

108. *Experi-Metal*, 2011 U.S. Dist. LEXIS 62677; see also Navetta, *supra* note 1, at 22,24 (quoting the FFIEC’s key point) (“The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of singlefactor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.”).

109. *Id.*

110. See Navetta, *supra* note 1, at 25.

111. See *id.*

112. *Patco Const. Co. v. Peoples United Bank*, CIV. 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011), *aff.g* *Patco Const. Co. v. People’s United Bank*, No. 2:09-CV-503-DBH, 2011 WL 2174507, at *7 (D. Me. May 27, 2011) (“The Guidance does not endorse any particular technology for compliance with the Guidance.”).

113. See *Patco Const. Co. v. Peoples United Bank*, CIV. 09-503-P-H, 2011 WL 3420588 (D. Me. Aug. 4, 2011), *aff.g* *Patco Const. Co. v. People’s United Bank*, No. 2:09-CV-503-DBH, 2011 WL 2174507, at *32 (D. Me. May 27, 2011).

114. See *id.*

115. See *Inside the PATCO Fraud Ruling*, *supra* note 35.

One of the main implications of this decision will be determining which party was better equipped to bear the responsibility of making sure certain security measures are effective.¹¹⁶ Attorneys for small businesses argue that these companies are often not equipped to bear the risk and lack a proper understanding of cyberthreats when they accept a bank's security procedures.¹¹⁷ Consequently, small business owners believe that banks should bear a higher responsibility for making sure that their own security procedures are effective based on the current make-up of cyberthreats.¹¹⁸ While banks may be better equipped to bear the responsibility for their security systems than small business owners, it is a more difficult argument to assert that they should be responsible for implementing security measures beyond what the FFIEC recommends.¹¹⁹ In an area of law where neither courts nor the FFIEC have specified a definite standard for determining the commercial reasonableness of a security system, there could be several negative consequences stemming from the decision to require banks to do more.

B. Negative Consequences of the Holding

1. Increased Liability for Banks Whose Customers Are the Victims of Third-Party Fraud

The *Patco* decision could increase bank liability far beyond the scope of the protective language contained in their online banking agreements.¹²⁰ While requiring banks to do more than rely on their contracts in order to comply with the "commercially reasonable" standard for their systems does have some merit, it may be burdensome to force them to meet an undefined standard. After *Patco*, it is no longer sufficient to have a generally accepted security procedure in place and conformance to FFIEC guidelines will not provide a safe harbor for

116. Joe Palazzolo, *Cyberthieves Hit Owners*, WALL ST. J., July 19, 2012, at B7, available at: http://online.wsj.com/article/SB10001424052702303612804577533503876570164.html?mod=djemSB_h#.

117. *Id.*

118. *Id.*

119. See Navetta, *supra* note 1, at 23.

120. See Funnell, *supra* note 34.

2013]

THE EFFECT OF PATCO

395

banks attempting to avoid liability.¹²¹ Instead, a bank's security system will now be subject to an additional prong of analysis regarding whether or not it is being implemented in a way that makes sense to the court.¹²² In fact, if a bank's procedures do not pass a specific judge's examination or a court finds that they were not implemented perfectly, the bank may be exposed to additional liability.¹²³ Furthermore, banks may be assigned an even greater responsibility for educating their customers in online security.¹²⁴ While fraud prevention education may result in a decreased chance of cybertheft,¹²⁵ it will impose a large burden for banks to not only protect their customers, but to also educate them. Client education is now strongly recommended by FFIEC guidelines, but it is unclear whether education will either provide an additional defense for banks whose customers don't take their advice or provide another means for fraud victims to allege bank liability.¹²⁶

One effect of the increased liability for banks is that they will likely shift the additional costs and burden to their customers.¹²⁷ The increased liability will force banks to pay more in settlements, implement more expensive security protocols, and take the time to examine what the cost of doing business with certain customers might be.¹²⁸ Hence, banks will likely charge more for their services to account for the increased cost.¹²⁹ In fact, the First Circuit's decision may persuade banks to not even consider certain small businesses as customers if they could be considered at-risk and require extra security, education, and liability.¹³⁰

A counterargument exists that the *Patco* decision may not be as

121. See 3 *Lessons*, *supra* note 13 (interview with information security attorney Joe Burton) ("It's not enough just to have a generally accepted security procedure in place if that procedure is not implemented in a way that makes sense.").

122. See *id.*

123. See Funnell, *supra* note 34.

124. See *id.*

125. *Id.*

126. *Id.*

127. Palazzolo, *supra* note 116.

128. *Id.*

129. *Id.*

130. See *id.* ("William T. Repasky, a Louisville, Ky., lawyer who represents financial institutions, says the First Circuit ruling could prompt some banks to view small businesses as higher risk customers. As a result, banks might then begin to pass on to small business customers their own increased costs for added security and customer education, he predicts.").

favorable for bank customers as predicted.¹³¹ One major question left undecided by the First Circuit was: What is the responsibility of the customer even if a bank's security procedures are found to be commercially unreasonable?¹³² Since the First Circuit remanded this decision to the lower court, this unanswered question may actually end up favoring banks regardless of the reasonableness of their procedures.¹³³

2. Cost Burden on Smaller Banks

A clear consideration in the First Circuit's decision in *Patco* was which specific security measures had been implemented and which had not been put in place.¹³⁴ According to the First Circuit, Ocean Bank chose not to implement out-of-band authentication¹³⁵ and tokens, which were both security measures recommended by the FFIEC and offered to the bank by their security provider.¹³⁶ In addition to these recommended measures, the First Circuit also addressed two other measures¹³⁷ that the bank chose not to implement which might have protected its customers from third-party fraud.¹³⁸ By pointing out these security omissions and the fact that Ocean Bank was able to upgrade its procedures after the fraud attacks, the First Circuit implied that it will view the offering of additional security procedures as a positive factor for banks trying to avoid liability for third-party fraud.¹³⁹ As a result,

131. See *3 Lessons*, *supra* note 13.

132. See *Patco Const. Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012); see also *3 Lessons*, *supra* note 13.

133. See *3 Lessons*, *supra* note 13 (interview with information security attorney Joe Burton) ("It opens the possibility that you have a circumstance where you had a commercially unreasonable procedure that was utilized by the bank, but the liability might not be on the bank because there may be responsibility [on] the customer.").

134. See *Patco*, 684 F.3d at 203-04.

135. *Id.* at 203 ("Out-of-band authentication generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction. Examples of out-of-band authentication include notification to the customer, callback (voice) verification, e-mail approval from the customer, and cell phone based challenge/response processes.") (footnote omitted) (citations omitted) (internal quotation marks omitted).

136. *Id.* at 204 ("Tokens are physical devices (something the person has), such as a USB token device, a smart card, or a password-generating token.").

137. *Id.* at 203-04 (mentioning user-selected picture and monitoring of risk-scoring reports).

138. *Id.* at 204.

139. *Id.* at 204 ("Since then, the bank has instituted a policy of calling the customer in the case of uncharacteristic transactions . . .").

the First Circuit established that merely implementing the few security measures that are both recommended by the FFIEC and offered to the bank will not be sufficient.¹⁴⁰ If banks want to avoid the possibility of any potential liability, they will be additionally burdened to implement *all* available security measures and upgrade their systems anytime they are offered a new feature.

The negative effect of this movement is evident for smaller banks and financial institutions that do not have extensive resources and capabilities.¹⁴¹ First, smaller banks, which may have a number of small business customers, will be burdened by lawsuits and the need to purchase additional fraud insurance.¹⁴² Also, smaller banks may not have the ability to pay the high costs to implement and maintain more expensive and advanced security systems offered and recommended to them.¹⁴³ In fact, the First Circuit's policy of deterring a one-size-fits-all approach to security is in stark contrast to the practice of many small banks which simply launch a standardized approach to fraud detection.¹⁴⁴ Finally, smaller banks will be even more inclined to reconsider taking small businesses or other at-risk companies on as customers.¹⁴⁵ When dealing with small banks that do not have the resources to monitor a significant percentage of their daily log-ins and transactions, businesses should be more inclined to implement their own security procedures.¹⁴⁶

Proponents for additional responsibility for banks will be quick to point out that the *Patco* ruling will not necessarily bring burdensome implications for banks across the country because of the number of questions left undecided or remanded.¹⁴⁷ However, this particular ruling should be considered a significant one despite any questions that

140. See *Patco Const. Co. v. People's United Bank*, 684 F.3d 197, 204 (1st Cir. 2012).

141. See *3 Lessons*, *supra* note 13.

142. See Client Alert, Richard J. Bortnick & Gary M. Klinger, Cozen O'Connor LLP, *First Circuit Court of Appeals Holds Bank's Online Security Measures "Commercially Unreasonable" in Landmark Decision*, (July 20, 2012), http://www.cozen.com/admin/files/publications/GIG%20ALert_7_20.pdf (stating that consumers need to purchase tailored insurance to protect themselves).

143. *Id.*

144. See *3 Lessons*, *supra* note 13 (stating that Gartner's Litan says Ocean Bank's practices were not atypical for small banks that typically launch a standardized approach to fraud detection and that consumers should bear the risk).

145. See Funnell, *supra* note 34.

146. *3 Lessons*, *supra* note 13.

147. See Funnell, *supra* note 34.

may be left open.¹⁴⁸ This decision is the first appellate case of its type, and it will have precedential value because it looks to balance the responsibilities of customers and banks in online transactions, which has proven to be a very difficult thing to do.¹⁴⁹ Also, the decision has significance because of its potential ability to “open the floodgates” for fraud victims to sue their banks.¹⁵⁰

V. ADVICE FOR LEGAL COUNSEL

While the negative consequences of the *Patco* decision may be evident, it is unclear which security protocols will be sufficient to protect banks and customers. For legal counsel representing banks and customers, advising their clients may prove to be a very difficult task under the new totality of the circumstances standard.¹⁵¹ There are a few recommendations that may guide attorneys who are trying to assist their clients.¹⁵² For counsel representing banks and financial institutions, it is important to emphasize the need to continue to take the same precautions that were important before the *Patco* decision.¹⁵³ These measures include: (1) requiring that customers maintain their own security and confidentiality for authentication credentials; (2) limiting the type of data that a customer may provide to the bank; and (3) requiring customers to notify them of any data breaches or unauthorized access to its accounts.¹⁵⁴

After *Patco*, more focus will be placed on a bank’s ability to tailor its security to an individual customer.¹⁵⁵ Banks should attempt to

148. 3 *Lessons*, *supra* note 13 (interview with information security attorney Joe Burton) (“The ruling is a ‘fairly significant’ one, Burton points out, since it’s the first appellate case of this type. ‘It’s going to have precedential value because it’s an appellate court case, and as you know there really are a small number of cases that have considered the question of apportioning responsibility between a customer and the bank.’”).

149. *See id.*; *see also* Pulles & Ylvisaker, *supra* note 85 (stating that the case has significance as it is one of first impression).

150. *See* Bortnick & Klinger, *supra* note 142 (mentioning that the PATCO decision could have significant implications for financial institutions and their insurers by opening the floodgates for potential lawsuits).

151. *See* *Patco Const. Co. v. People’s United Bank*, 684 F.3d 197 (1st Cir. 2012) (noting that the court considered all relevant factors in making its decision).

152. *See* Ronald Weikers et al., *A Practical Approach to Mitigating Data Breach Risk in an Interconnected World*, 2011 EMERGING ISSUES 5832.

153. *See id.*

154. *See id.* (outlining recommendations for attorneys who are representing banks).

155. *See* Pulles & Ylvisaker, *supra* note 85 (stating that the 1st Circuit focused on

create individualized customer profiles and select appropriate security measures based on the customer's specific circumstances.¹⁵⁶ The First Circuit suggested two proactive measures for banks to avoid a one-size-fits-all approach: (1) manual reviews of suspect transactions by actual personnel to determine the legitimacy of a transactions; and (2) customer verification or notification to authenticate uncharacteristic or suspicious transfers.¹⁵⁷ Attorneys should recommend that banks adopt the most of state of the art technology that their size will allow for and should look to similarly sized banks to examine the type of security measures that they have in place.¹⁵⁸ In line with these recommendations, the FFIEC's 2011 Supplement went into effect in January 2012 and recommended that banks adapt their security measures to anomalous customer behavior.¹⁵⁹ As a result, whether courts choose to follow the *Patco* reasoning or rely on conformance to FFIEC recommendations, it will be important for banks to implement an individualized security procedure in a way that adapts to changing circumstances.

On the other side of the spectrum, attorneys representing consumers should stress the importance of taking every precaution in their power to mitigate security risks. As they should have done pre-*Patco*, counsel should advise their clients to: (1) conduct effective pre-contract due diligence; (2) require banks to comply with a customer's own internal security policies; (3) require immediate notification in the event of a security breach; and (4) require the vendor to obtain cyber-liability insurance.¹⁶⁰ The main obligations for customers following the *Patco* decision are still undetermined, because the exact responsibilities

Ocean Bank's failure to tailor its security system).

156. *Id.* (“[B]anks need to create an individual customer risk profile that is then used to select appropriate security procedures for the customer based on those individual circumstances.”).

157. *See* Bortnick & Klinger, *supra* note 142 (listing three ways that the court identified to enhance security procedures).

158. Pulles & Ylvisaker, *supra* note 85 (“A bank then needs to adopt state of the art technology, appropriate for its size and comparable to what other banks in its position are using, and must review that security protocol periodically.”).

159. *Id.* (“[T]he FFIEC in 2012 issued new guidance on authentication (not discussed by the parties or the court in *Patco*), the most significant aspect of which is a mandate that banks must put in place a security procedure that identifies, addresses and reacts to anomalous customer behavior.”).

160. *See* Weikers et al., *supra* note 152 (outlining recommendations for attorneys who are representing consumers).

of the customer were left open on remand.¹⁶¹ Nevertheless, legal counsel should still advise their clients to request e-mail alerts from their banks, check their balances daily,¹⁶² and purchase insurance that is tailored to their specific needs.¹⁶³

VI. CONCLUSION

The First Circuit's decision to find that Ocean Bank's multifactor authentication security measures were not "commercially reasonable" created several negative consequences for banks and consumers that will change the landscape of online banking. With banks now facing serious and potentially costly liability implications for cyber-fraud, it is now time for banks to revisit their contracts, procedures, disclosures and account applications in order to meet any additional obligations that will arise.¹⁶⁴ Both the FFIEC and the courts have struggled to keep up with the rapidly changing landscape of cyberthreats. With major advancements in technology happening every day, a growing number of new threats to banks are also born. For attorneys trying to stay ahead of the curve, it will be important to advise their clients to take any and all steps to protect themselves, because if the First Circuit's decision has shown anything, it is that this landscape is far from stable.

ROBERT K. BURROW

161. Patco Const. Co. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012).

162. See Pulles & Ylvisaker, *supra* note 85 (listing ways which the consumer may still be held liable despite the reasonableness of a security system).

163. See Bortnick & Klinger, *supra* note 142 (stating that parties should not rely on others to protect them).

164. See Pulles & Ylvisaker, *supra* note 85 (noting that as a case of first impressions there could be "serious and potentially costly implications" and stating that banks should revisit their "procedures, disclosures, the account application, and account agreement").