Boston College Law Review

Volume 54
Issue 6 *Electronic Supplement*

Article 17

4-23-2013

In Search of the Right Balance: *Patco* Lays the Foundation for Analyzing the Commercial Reasonableness of Security Procedures under UCC Article 4A

Melissa Waite
Boston College Law School, melissa.waite@bc.edu

IN SEARCH OF THE RIGHT BALANCE: *PATCO* LAYS THE FOUNDATION FOR ANALYZING THE COMMERCIAL REASONABLENESS OF SECURITY PROCEDURES UNDER UCC ARTICLE 4A

Abstract: On July 3, 2012, in *Patco Construction Co. v. People's United Bank*, the First Circuit held that security procedures used to verify electronic funds transfers initiated through online banking were commercially unreasonable. In reaching its decision, the court laid a strong foundation for analyzing commercial reasonableness in future cases. This Comment argues that future courts should build on this analysis by considering recent merger activity when determining the standard against which commercial reasonableness should be measured.

Introduction

Online banking systems have enjoyed growing and widespread popularity in recent years.[1] This is partly because of the ease with which Automated Clearinghouse ("ACH") payments can be made online.[2] ACH is an electronic method of funds transfer by which customers submit payment information to their bank through a secure online portal, funds from all submitted payments are collected and sorted according to their destination bank, and then the originating bank sends the funds to the destination banks in batches along with the payment

[1] *See* Jim Bruene, *Online Banking and Marketing Statistics from Net.Finance*, NetBanker (Apr. 20, 2007, 4:24 PM), http://www.netbanker.com/2007/04/online_banking_marketing_statistics_from_net_finance_conference.html (noting that one regional bank had "150,000 very active small-business online banking users," and that business customers there were "making $45 million in payments per month with the bank's DirectPay service" (internal quotations omitted)); Susannah Fox & Jean Beier, *Online Banking 2006: Surfing to the Bank*, Pew Internet & Am. Life Project 1–2 (June 14, 2006), http://www.pewinternet.org/~/media//Files/Reports/2006/PIP_Online_Banking_2006.pdf.pdf (describing online banking as a "mainstream internet activity" and noting that, as of 2005, "43% of internet users, or about 63 million American adults, bank online," up from 13% in 1998).

[2] *See Intro to the ACH Network*, NACHA, https://www.nacha.org/Intro2ACH (last visited Mar. 24, 2013). ACH provides greater efficiency in funds transfers than alternative wire transfer services. *See* Peter J. Mucklestone, *The Journey of a Check*, 2006 Prof. Law. 39, 43–45; *Intro to the ACH Network*, *supra*. ACH transactions have become enormously popular in the last three decades, with the number of ACH payments made in 2010 exceeding nineteen billion. *See History*, NACHA, https://www.nacha.org/aboutus_History (last visited Apr. 20, 2013); *Intro to the ACH Network*, *supra*.

information.[3] The receiving banks then use the payment information to distribute the funds to their customers.[4] In 2011, more than $20.2 billion in payments were made via ACH, and volume increased in each quarter of 2012.[5]

But electronic bank fraud has risen in stride with the number of ACH payments initiated online.[6] Indeed, the Federal Deposit Insurance Company (FDIC) and the Federal Bureau of Investigation (FBI) have both issued special alerts warning banks and small business owners about the rise in these types of Internet crimes.[7] In the third quarter of 2009 alone, fraud involving electronic funds transfers from business accounts resulted in more than $120 million in losses.[8]

The allocation of losses from fraudulent transfers is governed by Article 4A of the Uniform Commercial Code (UCC).[9] Generally, a bank is not liable for losses if it followed commercially reasonable security procedures to verify the transaction.[10] But only four cases have considered what constitutes commercially reasonable online banking security

---

[3] *See Intro to the ACH Network*, *supra* note 2; *see also* Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 200 (1st Cir. 2012) (discussing the parties' agreement relating to ACH payments submitted online).

[4] *Intro to the ACH Network*, *supra* note 2. This is a more cost-effective method of payment than wire transfers because ACH sends multiple transactions from multiple customers each time a batch is run, whereas a wire transfer represents only one customer's transaction and is sent one at a time as each request is received. *See id.* Because of the lag time between entry and batch release, ACH is most commonly used for recurring payments like payroll, whereas wire transfer services are more frequently used for transactions such as investments or capital distributions, where a quick turnaround time is at more of a premium. *See id.*

[5] *ACH Network Statistics*, NACHA, https://www.nacha.org/ACHntwkstats (last visited Apr. 14, 2013).

[6] *See* Robert W. Ludwig, Jr., et al., *Malware and Fraudulent Electronic Funds Transfers: Who Bears the Loss?*, 16 Fidelity L.J. 101, 101 (2010).

[7] *See id.* at 102–03.

[8] *Id.* at 101–02.

[9] U.C.C. § 4A-102 (1989).

[10] *See id.* § 4A-202. The bank also must have accepted the payment order in good faith and complied with the security procedures to escape from liability. *Id.* A security procedure is

> a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication.

Id. § 4A-201. Commercially reasonable security procedures are important because they take the place of traditional verification methods and provide the bank with a reasonable basis on which to accept the payment order. *See* Regatos v. N. Fork Bank, 257 F. Supp. 2d 632, 641 (S.D.N.Y. 2003).

procedures.[11] In 2012, in *Patco Construction Co. v. People's United Bank*, the U.S. Court of Appeals for the First Circuit addressed this question, holding that the online banking security procedures in place at a Maine community bank recently acquired by a larger, regional bank were not commercially reasonable as a matter of law.[12] Given the increasing popularity of ACH and other online payments and the associated increases in Internet-based fraud, the standard for commercial reasonableness will only become more important in the future.[13]

Part I of this Comment describes the commercial reasonableness standard for security procedures set forth by the UCC and examines the security procedure at issue in *Patco*.[14] Then, Part II discusses the precedent available to the First Circuit when considering *Patco* and explains the *Patco* holding.[15] Finally, Part III argues that future courts should build upon the First Circuit's strong foundation by carefully analyzing the particular circumstances of the customer and the bank, especially in light of the banking industry's recent history of frequent mergers.[16] It also offers recommendations that may help banks avoid litigating this issue in the future.[17]

I. An Introduction to Loss Allocation Under UCC Article 4A and *Patco Construction Co. v. People's United Bank*

Section A of this Part describes the role of commercial reasonableness of security procedures in Article 4A's loss allocation scheme for fraudulent transfers.[18] Section B then provides the factual underpinnings of the *Patco* decision, which are necessary to understand the First Circuit's commercial reasonableness analysis.[19]

---

[11] *See Patco*, 684 F.3d at 211; Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 WL 1752693, at *4–5 (S.D.N.Y. Apr. 16, 2008); *Regatos*, 257 F. Supp. 2d at 646; All Am. Siding & Windows, Inc. v. Bank of Am., N.A., 367 S.W.3d 490, 500–01 (Tex. App. 2012). Courts should expect more cases in this area in the coming years, because ACH's popularity has been increasing exponentially in recent years. *See History*, *supra* note 2 ("ACH payment volume continues to double every five years."). The minimal case law in this area is surprising, particularly because Article 4A's drafters predicted that the commercial reasonableness of security procedures was the issue most likely to be litigated under section 202(b). *See* U.C.C. § 4A-203 cmt. 4.

[12] *Patco*, 684 F.3d at 211.

[13] *See* Ludwig et al., *supra* note 6, at 102–03; *History*, *supra* note 2.

[14] *See infra* notes 18–48 and accompanying text.

[15] *See infra* notes 49–81 and accompanying text.

[16] *See infra* notes 82–101 and accompanying text.

[17] *See infra* notes 102–103 and accompanying text.

[18] *See infra* notes 20–28 and accompanying text.

[19] *See infra* notes 29–48 and accompanying text.

A. *Introduction to Loss Allocation Under UCC Article 4A*

Although Article 4A places the risk of loss for fraudulent electronic funds transfers on banks, it also offers two ways for banks to redistribute all or some of the loss to customers.[20] First, the bank could shift the loss to its customer by showing that the payment order at issue was submitted to the bank by the customer's agent.[21] Second, the bank could show that: (1) the bank and its customer have agreed on a security procedure for verifying transactions; (2) the security procedure is commercially reasonable; and (3) the bank accepted the payment order in good faith and verified it according to the security procedure.[22] If the bank meets this burden, then the liability for the loss passes to the customer.[23] The customer can only shift the liability back to the bank if the customer can prove that the fraudulent order did not result from a breach of its own security system.[24] Thus, commercial reasonableness is the touchstone for the allocation of losses from fraudulent electronic funds transactions.[25]

Article 4A then delineates the commercial reasonableness of a security procedure as a question of law.[26] To decide what is commercially

---

[20] U.C.C. § 4A-202 (1989); *id.* § 4A-203 cmt. 2. This cannot be varied by agreement, except where the bank agrees to accept additional liability, such as if the bank agrees to be liable for all losses due to malware-related fraud. *See id.* § 4A-202(f); *see also id.* § 1-302 (2001) ("Except as otherwise provided . . . , the effect of provisions of [the UCC] may be varied by agreement." (second alteration in original)).

[21] *See* Grabowski v. Bank of Bos., 997 F. Supp. 111, 123 (D. Mass. 1997) (discussing agency law's intersection with Article 4A); U.C.C. § 4A-202(a).

[22] *See* U.C.C. § 4A-202(b).

[23] *See id.*

[24] *Id.* § 4A-203(a)(2)(ii). This is true regardless of how the third party obtained the information or whether the customer was at fault for the security breach. *See id.*

[25] *See id.* § 4A-202(b); *id.* § 4A-102 cmt; *see also* Me. Rev. Stat. Ann. tit. 11, § 4-1102 cmt. (1991) (adopting U.C.C. § 4A-102).

[26] *See* U.C.C. § 4A-201. Commercial reasonableness as a matter of law is an aberration from the Code's general emphasis on questions of fact. *See, e.g.*, *id.* § 1-205 (2001); *id.* § 2-205 cmt. (2003). One Article 4A drafter, Frederick H. Miller, explained that because the commercial reasonableness of a security procedure was likely to be among the most commonly litigated questions under Article 4A, the drafters wanted to establish a firm string of case law to guide attorneys and banking professionals. E-mail from Frederick H. Miller, Professor Emeritus, Univ. of Okla. Coll. of Law, to author (Sept. 4, 2012) (on file with author); *see* U.C.C. § 4A-203 cmt. 4; *see also id.* § 2-302(1) (noting that unconscionability is a matter of law); *id.* § 2-302 cmt. 1 (stating that "[t]his section is intended to allow the court to pass directly on the unconscionability of the contract or particular clause therein and to make a conclusion of law as to its unconscionability"). Indeed, since its enactment, hundreds of cases have addressed UCC unconscionability. *See, e.g.*, Texaco, Inc. v. Golart, 538 A.2d 1017, 1020–21 (Conn. 1998); Emlee Equip. Leasing Corp. v. Waterbury Transmissions, Inc., 626 A.2d 307, 312 (Conn. App. Ct. 1993); Edart Truck Rental Corp. v. B. Swirsky & Co., 579 A.2d 133, 137–38 (Conn. App. Ct. 1990).

reasonable, Article 4A instructs 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."[27] The question for the court is not whether the security procedure was the best available, but rather whether it was reasonable for the particular customer and the particular bank.[28]

B. *The Security Procedures and Fraudulent Transfers Underlying* Patco

Pursuant to Article 4A, the First Circuit in *Patco* had to determine whether the security procedures in place at Ocean Bank when the underlying fraud took place were commercially reasonable.[29] In that case, the plaintiff, Patco Construction Co., brought suit in 2009 against People's United Bank in Maine Superior Court over fraudulent transfers initiated via Patco's online banking account that totaled $588,851.26.[30] Patco claimed that People's United Bank, the owner of Ocean Bank, was liable under Maine's enactment of UCC Article 4A and numerous common law claims.[31] Subsequent investigation of Patco's computer

---

[27] U.C.C. § 4A-202(c).

[28] *See id.* § 4A-203 cmt. 4. If a customer is offered a commercially reasonable security procedure, but opts for a lesser security procedure out of cost or convenience considerations, then the security procedure elected by the customer is presumptively reasonable. *See id.*; *see also Grabowski*, 997 F. Supp. at 120 (determining that a customer did not agree to security procedures where the written agreement was "a modification of the baseline loss allocation scheme of Article 4A and not an agreement on a security procedure"); Experi-Metal, Inc. v. Comercia Bank, No. 09-14890, 2010 WL 2720914, at *5–6 (E.D. Mich. July 8, 2010) (deciding that there was a material question of fact whether the customer agreed to security procedures in writing, which would leave losses from fraudulent transfers on the customer because the third-party fraudster obtained login credentials from the customer's online banking user through malware); U.C.C. § 4A-202(c) (noting the conditions under which a court should deem a security procedure commercially reasonable).

[29] *See Patco*, 684 F.3d at 211.

[30] *Id.* at 199–206. Of this amount, $243,406.83 was recovered, leaving a residual loss of $345,444.43. *See id.* at 205.

[31] *Id.* at 206; *see* ME. REV. STAT. ANN. tit. 11, § 4-1102 cmt. (1991); U.C.C. § 4A-102; *see also* Bob Sanders, *Ocean Bank to Take People's Name*, N.H. BUS. REV. (July 1, 2010), http://www.nhbr.com/businessnews/statenews/784102-257/ocean-bank-to-take-peoples-name.html (stating that Ocean Bank was acquired by the Chittenden family of banks before being sold to People's United Bank in early 2009). Patco brought common law claims of negligence, breach of contract, breach of fiduciary duty, unjust enrichment, and conversion. *Patco*, 684 F.3d at 206. For a discussion of the intersection between the UCC and the common law, see Regions Bank v. Provident Bank, Inc., 345 F.3d 1267, 1273–76 (11th Cir. 2003); Centre-Point Merch. Bank Ltd. v. Am. Express Bank, Ltd., 913 F. Supp. 202, 206–09 (S.D.N.Y. 1996);

network revealed a malware program, which was quarantined and deleted by a Patco consultant.[32]Ocean Bank removed the case to the U.S. District Court for the District of Maine.[33] There, the court granted summary judgment in favor of Ocean Bank, and Patco appealed to the First Circuit.[34]

Patco's appeal allowed the First Circuit to consider for the first time whether a bank's security procedures were commercially reasonable.[35] To answer this question, the First Circuit examined the security procedures employed by Ocean Bank.[36] Ocean Bank's online banking platform, NetTeller, used several complex security procedures designed to protect customers' accounts.[37] First, each corporate online banking client was assigned a unique company ID.[38] Next, employees designated by the corporate client were assigned a personal user ID and password.[39] Further, each user provided personalized answers for three challenge questions.[40] The first time that a user logged onto NetTeller from a new device, the system asked a challenge question to confirm the user's identity and installed a digital certificate on the device for future authentication purposes.[41]

Additionally, NetTeller built a risk profile for each user by tracking the user's online activity.[42] Then, it used the profile data to calculate a score for each transaction based on any deviation from previous transactions so that more unusual transactions were marked with higher

---

Hyung J. Ahn, Note, *Article 4A of the Uniform Commercial Code: Dangers of Departing from a Rule of Exclusivity*, 85 Va. L. Rev. 183, 196–212 (1999).

[32] *Patco*, 684 F.3d at 206. In November 2009, the FBI identified small- and medium-sized businesses holding accounts at local community banks and credit unions as among the most common targets of Internet-based fraud using malware, such as the Zbot found on Patco's computer system. *See id.*; Ludwig et al., *supra* note 6, at 103.

[33] *Patco*, 684 F.3d at 206; *see* Patco Constr. Co. v. People's United Bank, No. 2:09-cv-503-DBH, 2011 WL 2174507, at *1 (D. Mass. May 27, 2011), *aff'd in part, rev'd in part*, 684 F.3d 197 (1st Cir. 2012).

[34] *Patco*, 684 F.3d at 206; *see Patco*, 2011 WL 2174507, at *35.

[35] *See Patco*, 684 F.3d at 207–10.

[36] *See id.* at 201–02.

[37] *Id.*

[38] *Id.* at 202.

[39] *Id.*

[40] *Id.* at 202–03. Challenge questions help to verify a user's identity by requiring the user to provide specific personal information, such as his or her mother's maiden name. *See id.*

[41] *Patco*, 684 F.3d at 202.

[42] *Id.* This profile considered the location from which the user logged in, what the user did while logged in, and the size, type, and frequency of payment orders that the user input. *Id.*

scores.[43] NetTeller required the user to answer a challenge question before allowing high scoring transactions to be processed.[44] But although the risk-profiling system was in place in 2009 when the fraud underlying *Patco* occurred, Ocean Bank employees were not monitoring those risk scores.[45] Finally, NetTeller also required users to answer a challenge question any time a transaction amount exceeded a preset threshold.[46] In 2008, Ocean Bank set this amount at one dollar, requiring users to answer a challenge question for any transaction initiated online.[47] After considering both Ocean Bank's security procedures and the available security features in use at other banks, the First Circuit concluded that Ocean Bank's security procedure was not commercially reasonable.[48]

II. Uncharted Waters: The *Patco* Court's Commercial Reasonableness Analysis

In *Patco*, the First Circuit provided a much more detailed commercial reasonableness analysis than the three lower courts that had previously considered the same question.[49] The U.S. District Court for the

---

[43] *Id.* Lower scores corresponded to a low-risk transaction, whereas higher scores corresponded to a high-risk transaction. *Id.* at 213.

[44] *Id.* at 202. Challenge questions were prompted whenever a risk score exceeded 750. *Id.*

[45] *Id.* at 204. Patco's typical risk score was between 10 and 214. *Id.* Risk scores for the fraudulent transfers ranged from 563 to 790. *Id.* at 204–05. Had Ocean Bank been actively monitoring the risk scores, its agents would have been able to contact clients with high risk scores to confirm the ACH file before sending it. *See id.*

[46] *Id.* at 203.

[47] *Patco*, 684 F.3d at 203 Ocean Bank set this low threshold in an attempt to combat low-dollar fraud. *Id.* at 212. It changed the threshold from $100,000 to $1 after confirming with its service provider that the change would have no implications for NetTeller's security functionality. *See* Brief for Defendant-Appellee at 48, *Patco*, 684 F.3d 197 (2012) (No. 11-2031), 2012 WL 605503, at *48. Ocean Bank's purchase of NetTeller included a subscription to the eFraud Network, a database of IP addresses and other information about known fraudulent transactions at all member banks. *Patco*, 684 F.3d at 203. There were also a number of available security features that Ocean Bank declined to implement, including: (1) out-of-band authentication, which would have required a voice, text, or e-mail confirmation of each transaction entered; (2) user-selected pictures, meant to combat phishing; and (3) the use of tokens, which are physical devices that display a one-time-use code or password information that must be input by a user when he or she performs an online transaction. *Id.* at 203–04.

[48] *Patco*, 684 F.3d at 211.

[49] *See* Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 WL 1752693, at *4 (S.D.N.Y. Apr. 16, 2008) (holding that a security procedure consisting of a fax order and a logged telephone confirmation requiring customers to answer security questions on a recorded line was commercially reasonable for wire transfer fraud committed by plaintiff's business associate); Regatos v. N. Fork Bank, 257 F. Supp. 2d 632, 646 (S.D.N.Y. 2003) (holding that a security procedure consisting of a fax order and the customer's unlogged callback con-

Southern District of New York has confronted commercial reasonableness twice, and a Texas Court of Appeals considered it shortly before *Patco*.[50] Section A of this Part explores the facts and reasoning of these cases.[51] Section B then discusses the First Circuit's approach to analyzing commercial reasonableness.[52]

A. *Little Precedent Existed to Guide the* Patco *Court's Analysis*

The U.S. District Court for the Southern District of New York decided two of the three previous cases.[53] First, in 2003, in *Regatos v. North Fork Bank*, the court evaluated a security procedure consisting of a signed order sent 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 specimen signature.[54] The court held that it was commercially reasonable because the bank employee could recognize the customer's voice, having dealt with him repeatedly over the course of several years.[55] Then, in 2008, in *Filho v. Interaudi Bank*, the same court considered a security procedure consisting 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.[56] The court held that the security procedure was commercially reasonable because the additional verification provided by the security questions made up for the lack of voice recognition.[57]

These two cases highlighted the importance of multifactor authentication.[58] In *Regatos*, commercial reasonableness turned on the bank's use of an out-of-band voice recognition confirmation method.[59] In *Fil-*

---

firmation to the same bank representative on an unrecorded line was commercially reasonable for wire transfer fraud committed by an unknown party); All Am. Siding & Windows, Inc. v. Bank of Am., N.A., 367 S.W.3d 490, 501 (Tex. App. 2012) (holding that a security procedure consisting of a company ID, user ID, password, and digital certificate was commercially reasonable for ACH transactions initiated via an online banking portal).

[50] *See Filho*, 2008 WL 1752693, at *4; *Regatos*, 257 F. Supp. 2d at 646; *All Am. Siding*, 367 S.W.3d at 501.

[51] *See infra* notes 53–66 and accompanying text.

[52] *See infra* notes 67–81 and accompanying text.

[53] *See Filho*, 2008 WL 1752693, at *4; *Regatos*, 257 F. Supp. 2d at 646.

[54] *Regatos*, 257 F. Supp. 2d at 646.

[55] *See id.*

[56] *Id.*

[57] *See id.*

[58] *See Filho*, 2008 WL 1752693, at *5; *Regatos*, 257 F. Supp. 2d at 646.

[59] *See Regatos*, 257 F. Supp. 2d at 646; Fed. Fin. Insts. Examination Council, Authentication in an Internet Banking Environment 3 (2005) [hereinafter FFIEC Guidance], *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf. ("Out-of-band generally refers to additional steps or actions taken beyond the technology boundaries of a typical

ho, commercial reasonableness turned on the combination of an out-of-band authentication procedure (the telephone confirmation) and a knowledge-based requirement, the security question.[60] But these cases were of limited applicability to the situation underlying *Patco* because they addressed wire transfers initiated by fax, rather than ACH transactions initiated via online banking.[61]

In 2012, however, just before the *Patco* case was decided, the Texas Court of Appeals, Texarkana did address commercial reasonableness of security procedures used to verify online ACH payments in *All American Siding & Windows v. Bank of America*.[62] There, the security procedure consisted of an ID, passcode, and digital certificate verification technology.[63] The court held that the security procedure was commercially reasonable for ACH transactions submitted via online banking because the bank adhered to the Federal Financial Institutions Examination Council's ("FFIEC") 2005 guidance, a report that outlined online banking security procedure best practices.[64] But the court's focus on the 2005 guidance seemed to reflect only the importance of considering adherence to industry standards when conducting the commercial reasonableness analysis.[65] The court did not explicitly discuss Article 4A's mandate to consider the circumstances of the particular customer and the particular bank.[66]

---

transaction. Callback (voice) verification, e-mail approval or notification, and cell-phone based challenge/response processes are some examples.").

[60] *See Filho*, 2008 WL 1752693, at *5.

[61] *See supra* note 4 and accompanying text (discussing the distinction between wire transfer and ACH payments). *Compare* Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 204–05 (1st Cir. 2012) (discussing ACH fraud initiated online), *with Filho*, 2008 WL 1752693, at *5 (discussing wire transfer fraud initiated by fax), *and Regatos*, 257 F. Supp. 2d at 646 (discussing wire transfer fraud initiated by fax).

[62] *All Am. Siding*, 367 S.W.3d at 500–01.

[63] *Id.*

[64] *Id.* at 500–01. The FFIEC is an interagency body tasked in part with advising federally supervised financial institutions on best practices for online banking security. *About the FFIEC*, Fed. Fin. Institutions Examination Council, http://www.ffiec.gov/about.htm (last visited Mar. 24, 2013). The FFIEC recommends a multifactor authentication for high-risk transactions like electronic funds transfers. FFIEC Guidance, *supra* note 59, at 6. According to the FFIEC, multifactor authentication should incorporate something the online banking user knows (such as a password), something the user has (such as an ATM card or secure token), and something the user is (such as a finger print scanner or voice recognition software). *See id.*

[65] *See All Am. Siding*, 367 S.W.3d at 500–01.

[66] *Compare* U.C.C. § 4A-203 cmt. 4 (1989) (stating that "[t]he standard is . . . whether the procedure is reasonable for the particular customer and the particular bank"), *with All Am. Siding*, 367 S.W.3d at 500–01 (reasoning that "the Bank followed the guidelines of the

B. *The Commercial Reasonableness Analysis in* Patco

In *Patco*, the First Circuit took a much more thorough approach to analyzing commercial reasonableness than its predecessors.[67] The court considered the security procedure in totality, focusing on what was affirmatively included in the security procedure, what protections were available but not included, and what Ocean Bank knew about the risks of Internet-based fraud.[68]

First, the court found several problems in considering how effective Ocean Bank's security procedure would be at preventing fraud.[69] The court noted that by reducing the dollar-amount rule threshold to one dollar, Ocean Bank had substantially increased the risk of fraud for customers who, like Patco, initiated frequent, routine transfers.[70] At this threshold, the user would likely be prompted to answer many or all of his or her challenge questions before a keylogger installed on the user's computer was detected and removed.[71] Additionally, this rendered the risk score system irrelevant because a high risk score prompting a challenge question would not stop a fraudulent transaction if the fraudster could answer the challenge questions.[72] In the court's view, "the increase in risk . . . was sufficiently serious to require a corollary increase in security measures," but Ocean Bank did not make any additions to its security procedure.[73]

[FFIEC] and requires multifactor authentication . . . thereby demonstrating the commercial reasonableness of the security procedure" (internal quotations omitted)).

[67] *See Patco*, 684 F.3d at 211.

[68] *See id.* ("We emphasize that it was these collective failures taken as a whole, rather than any single failure, which rendered Ocean Bank's security system commercially unreasonable.").

[69] *See id.* at 210. The court focused on the security procedure as applied to Patco's typical transactions. *Id.* The vast majority of Patco's online banking transactions consisted of highly routine payroll transactions or associated tax payments. *Id.* at 200. These transactions were always made on Fridays, from the same IP address and physical location at Patco's Sanford offices, and they were always accompanied by weekly withdrawals for federal and state taxes. *Id.* The largest payroll ever run by Patco was $36,634.74. *Id.* By contrast, the smallest fraudulent transaction totaled $56,594. *Id.* at 204.

[70] *See id.*

[71] *See id.*

[72] *Id.* at 211. At the former threshold of $100,000, Patco would never have been prompted to input answers to its challenge questions due to the transfer amount, because the highest payment Patco made was $36,634.74. *Id.* at 211–12. Thus, the fraudsters would not have had the opportunity to obtain the challenge question answers with their keylogger and the fraud would have been prevented. *See id.* According to the First Circuit, the risk scoring system was otherwise irrelevant because Ocean Bank employees were not monitoring high-scoring transactions, and thus the system-generated risk scores contributed nothing to security beyond that provided by the challenge questions. *Id.*

[73] *Patco*, 684 F.3d at 212.

Next, the First Circuit considered other security features available and in use throughout the banking industry that were not provided to customers at Ocean Bank.[74] Here, the Court stressed that bank personnel were not monitoring the risk scores that NetTeller generated, whereas many other banks did have employees monitoring risk scores and verifying high-scoring transactions.[75] Furthermore, the court faulted the bank's failure to employ additional, widely available physical security devices as recommended by the 2005 FFIEC guidance for online banking security procedures.[76]

Finally, the First Circuit considered Ocean Bank's security procedure choices in light of its substantial knowledge of ongoing fraud.[77] The FFEIC and RSA/Cyota, a security device company that worked for Ocean Bank's online banking supplier, issued warnings to the banking industry about increased Internet fraud in 2005, four years before the fraud perpetrated in this case.[78] The FBI issued another industry-wide warning in 2009, highlighting the increased use of keyloggers in online fraud.[79] Moreover, Ocean Bank had experienced at least two incidents of fraud in which keyloggers may have played a role prior to the fraud underlying *Patco*.[80]

After weighing Ocean Bank's security procedure against additional procedures available and in use industry-wide, and considering Ocean Bank's knowledge of the threat posed by online fraud, the First Circuit held that, as a whole, the security procedures in place at Ocean Bank were not commercially reasonable.[81]

III. Building on *Patco*, Courts Should Consider the Impact of Mergers When Analyzing Commercial Reasonableness

The First Circuit's totality analysis laid a strong foundation for analyzing commercial reasonableness in *Patco*, but—where applicable—

---

[74] *See id.*

[75] *Id.*

[76] *See id.* at 211–14. The court's focus on the FFIEC guidance is consistent with the UCC's view that "security procedures are likely to be standardized in the banking industry." *See id.* at 213; U.C.C. § 4A-203 cmt. 4 (1989). *See generally* FFIEC Guidance, *supra* note 59 (discussing various security procedures available for use in online environments).

[77] *Patco*, 684 F.3d at 213.

[78] *Id.* at 211; *see* FFIEC Guidance, *supra* note 59, at 2, 7. Ocean Bank's online banking vendor hired RSA/Cyota to bring NetTeller into compliance with the FFIEC guidance. *See Patco*, 684 F.3d at 202.

[79] *See Patco*, 684 F.3d at 206; Ludwig et al., *supra* note 6, at 103.

[80] *See Patco*, 684 F.3d at 202.

[81] *Id.*

future courts should consider more carefully the impact of mergers on the industry standard to which a particular bank should be held.[82] The court's totality test reflected Article 4A's emphasis on balancing the particulars of each case with the baseline assumption that security procedures are likely to be standardized in the banking industry.[83] It carefully considered Patco's typical payment history and measured the bank's security procedures against a well-respected industry regulator's recommendations.[84] Additionally, the court emphasized that it was the collective failure of all the affirmative security measures and omissions, rather than one factor in isolation, which rendered the security procedures commercially unreasonable.[85]

But Article 4A also requires courts to consider "whether the procedure is reasonable for the . . . *particular bank*, which is a lower standard" than "whether the security procedure is the best available."[86] Under Article 4A, courts must compare the bank's security procedure to security procedures at other banks of similar size and situation, in part because larger banks in more urban environments are likely to be more sophisticated and have more resources available than smaller, rural, community banks.[87] Significantly, Article 4A advocates this approach because the purpose of the commercial reasonableness requirement is to encourage banks to use efficient procedures to combat fraud, not to render them "insurers against fraud."[88]

Accordingly, the First Circuit in *Patco* should have considered the impact of Ocean Bank's recent merger because Ocean Bank was still functionally a rural community bank when the fraud occurred.[89] Serious merger discussions often stop companies from making changes to their security systems, unless those changes are immediately necessary,

---

[82] *See* Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 211 (1st Cir. 2012).

[83] *See id.* at 211–13; U.C.C. § 4A-203 cmt. 4 (1989) (noting that although security procedures are likely to be standardized within the banking industry, courts must evaluate their commercial reasonableness in light of the particular customer and particular bank involved in a transaction).

[84] *See Patco*, 684 F.3d at 211–13; U.C.C. § 4A-203 cmts. 1–7.

[85] *Patco*, 684 F.3d at 211.

[86] U.C.C. § 4A-203 cmt. 4 (emphasis added).

[87] *See id.*

[88] *See id.* § 4A-203 cmts. 3–4.

[89] *See Patco*, 684 F.3d at 213; U.C.C. § 4A-203 cmt. 4. Instead, the opinion as a whole suggests that the First Circuit considered Ocean Bank's security procedures under the rubric of one of the premier regional banks in the Northeast. *See Patco*, 684 F.3d at 213; *About People's United*, People's United Bank, https://www.peoples.com/peoples/Footer/About-People%27s-United (last visited Apr. 20, 2013). Prior to the merger with People's United, Ocean Bank could best be descried as a rural community bank. *See* Sanders, *supra* note 31.

for a significant period of time before and after a deal has officially closed.[90] Thus, it does not necessarily follow that Ocean Bank had the same resources or operations platforms that were available at other People's United locations after being a part of People's United for just five months.[91] Nonetheless, the First Circuit held Ocean Bank's security procedure to the industry standard for its new and more robust regional parent, People's United.[92]

A better approach would have been to compare Ocean Bank with other Maine community banks since Ocean Bank was more closely analogous to that type of institution.[93] As Article 4A notes, there may be substantial differences in what constitutes a commercially reasonable security procedure between a small rural bank and a larger, more sophisticated urban bank.[94] Although the First Circuit did note that "many New England community banks" used secure tokens and manual review of risk scores as part of their online security procedures at the time of the *Patco* fraud, even this sample is too broad.[95] A cross-section of New England community banks includes both those located in rural areas like southern Maine and others in suburban Boston and Connecticut, whose proximity to major financial centers would likely render them more sophisticated than their more rural counterparts.[96]

The First Circuit's approach likely reflects a policy choice to incentivize bank compliance with industry-wide best practices for security, regardless of size or location.[97] The comments to Article 4A suggest that banks are in the best position to evaluate the performance of security procedures because they are closest to technological advancements in online banking security devices and the fraud necessitating their use.[98] But banks are also concerned with the additional expense and

---

[90] *See generally* Steven J. Pilloff, Bd. of Governors of the Fed. Reserve Sys., Staff Study 176: Bank Merger Activity in the United States, 1994–2003 (2004), *available at* http://www.federalreserve.gov/pubs/staffstudies/2000-present/ss176.pdf (documenting bank merger activity and its impact on the banking industry from 1994 to 2003); Stanley Foster Reed et al., The Art of M&A: A Merger/Acquisition/Buyout Guide (4th ed. 2007) (providing a step-by-step analysis of all aspects of a successful merger). Indeed, mergers have been a prevalent force in the banking industry in recent years. *See* Pilloff, *supra*, at 2.

[91] *See Patco*, 684 F.3d at 213; U.C.C. § 4A-203 cmt. 4; Reed, *supra* note 90, at 643–83; Sanders, *supra* note 31.

[92] *See Patco*, 684 F.3d at 211–14.

[93] *Id.* at 213; U.C.C. § 4A-203 cmt. 4.

[94] U.C.C. § 4A-203 cmt. 4.

[95] *See Patco*, 684 F.3d at 213.

[96] *See* U.C.C. § 4A-203 cmt. 4.

[97] *See Patco*, 684 F.3d at 211; U.C.C. § 4A-102 cmt.; *id.* § 4A-203 cmt. 3.

[98] U.C.C. § 4A-203 cmt. 3.

operational challenges presented by implementing new technology to combat fraud.[99] In contrast, regulatory agencies like the FFIEC are also close to these developments, but because these agencies focus on fraud prevention instead of profit, they are better equipped to view security innovations objectively and make balanced recommendations about their use.[100] Thus, resolving these types of factual considerations in favor of the customers incentivizes banks to either proactively comply with industry-wide best practices despite their initial costs or to insure themselves against losses resulting from fraudulent transactions.[101]

In the future, to avoid liability for fraud, banks of any size should implement security procedures that are in line with the 2005 FFIEC guidance whenever possible.[102] At a minimum, banks should ensure that their security procedures include some form of multifactor authentication because multifactor authentication has been strongly predictive of commercial reasonableness.[103]

---

[99] *See id.*

[100] *See* U.C.C. § 4A-203 cmt. 3; FFIEC Guidance, *supra* note 59, at 1.

[101] FFIEC Guidance, *supra* note 59, at 2–6 (discussing recommendations for financial institutions to safeguard their accounts against Internet-based fraud); *see* U.C.C. § 4A-102 cmt. (noting that the ability to plan for and insure against risk are fundamental motivations behind Article 4A generally). *But see* U.C.C. § 4A-203 cmt. 4 (cautioning against rendering banks "insurers against fraud").

[102] *See Patco*, 684 F.3d at 201–04. The First Circuit's emphasis on comparing Ocean Bank's security procedures to those in the FFIEC guidance pursuant to Article 4A's mandate to consider "security procedures in general use by customers and receiving banks similarly situated" implicitly endorses the FFIEC guidelines as a shorthand benchmark for general industry standards. U.C.C. § 4A-202(c); *see Patco*, 684 F.3d at 201; *see also* All Am. Siding & Windows, Inc. v. Bank of Am., N.A., 367 S.W.3d 490, 501 (Tex. App. 2012) (holding that security procedures that complied with the 2005 FFIEC guidance were commercially reasonable). The FFIEC guidance notes that security procedures for funds transfer systems should incorporate three levels of multifactor authentication. *See* FFIEC Guidance, *supra* note 59, at 3–4. Even *Regatos v. N. Fork Bank*, the 2003 case from the U.S. District Court for the Southern District of New York, which was decided before the FFIEC guidelines were promulgated, implicitly endorsed multifactor authentication procedures. *See* Regatos v. N. Fork Bank, 257 F. Supp. 2d 632, 646 (S.D.N.Y. 2003).

[103] *See Patco*, 684 F.3d 201–04 (noting that there was no multifactor authentication where lack of monitoring rendered the digital certificate ineffective against fraud); Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 WL 1752693, at *5 (S.D.N.Y. 2008) (noting that voice recognition and signature confirmation constituted multifactor authentication); *Regatos*, 257 F. Supp. 2d at 646 (holding that out-of-band confirmation consisting of logged telephone confirmation from client on recorded line constituted multifactor authentication); *All Am. Siding*, 367 S.W.3d at 501 (holding that a bank demonstrated the commercial reasonableness of its security procedures by following the FFIEC guidance and "requir[ing] multifactor authentication for its online banking customers" (internal quotations omitted)); *see also supra* note 66 (discussing the multifactor authentication promoted by the FFIEC guidance).

Conclusion

Only recently have courts begun to examine the commercial reasonableness of security procedures under Article 4A. Indeed, *Patco* was only the fourth case, and the first at the circuit level, to consider this issue. As Internet-based fraud becomes increasingly common, courts will have ample opportunity to define and shape the contours of commercial reasonableness under Article 4A. To that end, the First Circuit has provided a strong foundation on which future courts can develop a more precise and balanced rubric for commercial reasonableness of security procedures. Building on *Patco*, future courts should closely consider each bank's circumstances when choosing an industry standard against which to gauge the bank's security procedures, especially when the bank recently has been involved in a merger.

Melissa Waite

Preferred Citation: 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. E. Supp. 217 (2013), http://lawdigitalcommons.bc.edu/bclr/vol54/iss6/17/.