Banking and Financial Services Litigation Alert

Litigation risks and developments in banking and financial services law

A publication of Nixon Peabody LLP

AUGUST 1, 2012

First Circuit faults bank for "one-size-fits-all" approach to cyber security measures

By W. Scott O'Connell and Daniel Deane

Following a landmark decision in July by the First Circuit U.S. Court of Appeals in Boston, commercial banks are advised to review their cyber security measures. The First Circuit's ruling, that the cyber security measures employed by a local community bank in Maine were not "commercially reasonable," resuscitates a business customer's attempt to hold its bank liable for six unauthorized transfers totaling nearly $350,000. The decision, *Patco Construction Co. v. People's United Bank*,[1] authored by Chief Judge Sandra Lynch, hinges on interpretation of Article 4A of the Uniform Commercial Code ("UCC"),[2] which allocates the risk of loss between parties involved in "funds transfers."[3] As the First Circuit is the first federal appellate court to interpret the meaning of "commercially reasonable" in the context of an Article 4A claim, the ruling is likely to have a broad impact in the industry.

The plaintiff, Patco, is a small property developer and contractor located in southern Maine that began banking with Ocean Bank[4], a local community bank, in 1985. Patco enrolled in Ocean Bank's "eBanking" program in 2003, primarily for making weekly payroll payments. Ocean Bank took steps to ensure the safety and security of its online banking platform, including purchasing the Jack Henry & Associate's "Premium" security package, which employed six key features: (1) user IDs and passwords; (2) invisible device authentication (*i.e.*, placing a "cookie" onto customers' computers so that they could be identified in the future); (3) an adaptive risk profiling and monitoring system; (4) the use of "challenge questions" for specified situations; (5) a dollar amount rule that would result in

---

[1] CA No. 11-2031, 2012 U.S. App. LEXIS 13617 (1st Cir. July 3, 2012).

[2] All 50 states have adopted Article 4A of the UCC. The Maine statute at issue in *Patco* is identical to Article 4A in all relevant parts.

[3] As noted by the court, Article 4A was designed to address wholesale wire transfers and commercial ACH (Automated Clearing House) transfers, generally between businesses and their financial institutions. Electronic *consumer* payments, on the other hand, are governed by federal statute, the Electronic Fund Transfer Act (EFTA), 15 U.S.C. § 1693, *et seq*.

[4] Ocean Bank was later acquired by People's United Bank in early 2009, but continued to operate under the Ocean Bank name until July 2010.

an alert or other procedure for every transfer made above a threshold amount; and (6) a subscription to the eFraud Network, which maintains a database on known frauds.

Despite these safeguards, in May 2009, hackers somehow acquired Patco's user IDs, passwords, and "challenge question" answers, and transferred $588,851 from Patco's account into unauthorized third-party accounts. Ocean Bank quickly blocked or recovered some of the money, but Patco was left with a residual loss of $345,444. The parties disagree as to how Patco's authentication credentials were stolen. Patco claims that hackers employed a "keylogger," a form of computer malware that imbeds itself within the victim's computer system and records the user's keystrokes when the user logs onto a financial website. That keystroke information is then transmitted to the hacker. Ocean Bank, however, theorizes that Patco's credentials may have been compromised by the negligence of its employees.

In September of 2009, Patco sued Ocean Bank, then a division of People's United, in a six-count complaint asserting liability under Article 4A of the UCC, and several common law theories of liability including negligence, breach of contract, breach of fiduciary duty, and unjust enrichment. Less than a year into the case, the federal district court in Maine granted summary judgment in favor of the defendant bank, ruling that it was not liable under Article 4A because it had employed "commercially reasonable" security measures, and that the remaining counts were either preempted by the UCC provision or could not succeed for the same reasons. Construing the meaning of "commercially reasonable" for Article 4A purposes, and writing on a blank slate, the First Circuit reversed the grant of summary judgment and remanded the case back to the district court for further proceedings.

The First Circuit began its analysis by noting the risk-shifting scheme created by Article 4A. Under that scheme, the bank receiving the payment order initially bears the risk of loss for any unauthorized transfer. That risk of loss can be shifted to the customer if the bank can establish an agency relationship between the sender of the order and the customer. Commentary to Article 4A recognizes, however, that establishing an agency relationship is difficult in the electronic age, where payment and transfers are ordered by a message on a computer screen. Accordingly, the drafters of Article 4A provided a second method for shifting the risk of loss.

Where the bank and its customer have agreed to electronic transfers verified by a security procedure, an electronic transfer is effective, even if unauthorized, if: (a) the security procedure "is a commercially reasonable method of providing security against unauthorized payment orders," and (b) the "bank proves that it accepted the payment order in good faith and in compliance with the security procedure and of any written agreement or instruction of the customer." *Patco*, 2012 U.S. App. LEXIS 13617, at *29-30 (quoting Me. Rev. Stat. Ann., tit. 11, § 4-1202(2)). Critically, the commercial reasonableness of a security procedure depends on the needs and circumstances of each particular customer. Article 4A provides that banks should consider "the wishes of the customer" as well as "the circumstances of the customer," including the "size, type and frequency of payment orders normally issued by the customer to the bank"; alternative available security procedures; and security procedures "in general use by other customers and receiving banks similarly situated." *Id.* at *30-31 (quoting Me. Rev. Stat. Ann., tit. 11, § 4-1202(3)).

The First Circuit found that Ocean Bank's security procedures failed the Article 4A test because they were employed in a "one-size-fits-all" manner, rather than being tailored to the particular needs and

circumstances of Patco. *Id.* at *41. In particular, although Ocean Bank had purchased Jack Henry's "Premium" security package, there were two critical flaws in how Ocean Bank used the system. First, Ocean Bank did not tailor its dollar amount indicator to Patco's circumstances. Initially, Ocean Bank set the dollar amount indicator at $100,000. For any transfer of $100,000 or more, the user was required to answer the "challenge questions" that had been created by the customer. In June 2008, Ocean Bank lowered the dollar amount threshold to $1. But all of Patco's payroll withdrawals were in the tens of thousands and never exceeded $37,000. Accordingly, before June 2008, none of Patco's transfers would have triggered the dollar amount threshold, and after June 2008, every Patco transfer triggered it. Because Patco was effectively required to answer the challenge questions for every weekly payroll transfer after June 2008, the risk of a keylogger attack was greatly increased. If Patco's computer systems were attacked by a keylogger, it was more likely that the keylogger software would record the challenge question answers (along with the user ID and password) before the customer could detect and remove the malware. Thus, Ocean Bank's overuse of challenge questions actually increased the risk of cyberattack.

Second, Ocean Bank did not take full advantage of Jack Henry's adaptive risk profiling and monitoring system. The Jack Henry system monitored Patco's transactions and generated risk-scoring reports based on criteria designed to detect suspicious activity. The May 2009 unauthorized transfers were scored as "high risk" because they did not match the predictable profile of an authorized Patco transfer. Patco payments were generally processed weekly on Fridays, never exceeded $37,000, were ordinarily directed to the same accounts, and always originated from a single static IP address located at Patco's offices in Sanford, Maine. The monitoring system did not work, however, because Ocean Bank personnel did not review these risk-scoring reports. The only consequence of a high risk score was that the user attempting to process the transaction would be prompted to answer the challenge questions, which the customer would be required to do for all transactions after June 2008 in any event. Thus, by lowering the dollar amount threshold to $1 and by failing to monitor the risk-scoring reports, Ocean Bank failed to reasonably account for Patco's particular circumstances. According to the First Circuit, Ocean Bank's procedures effectively "deprived the complex Jack Henry risk-scoring system of its core functionality." *Id.* at *37.

The First Circuit also criticized Ocean Bank for failing to take advantage of any additional emerging security technologies. *See id.* at *41-42. For example, Patco's expert testified that by May 2009, many other commercial banks employed hardware-based tokens, which generate one-time passwords that are constantly refreshed within seconds. Banks that do not use tokens use some other form of additional security, such as manual review of transactions or customer verification with regard to suspicious activity. In light of the flaws in Ocean Bank's security procedure, and its failure to implement additional and more reliable methods, the First Circuit concluded that Ocean Bank's security procedure was not commercially reasonable. The First Circuit also disagreed with the district court that the breach of contract and breach of fiduciary duty claims were preempted by Article 4A, and it therefore revived those claims, too.

Perhaps the silver lining for banks is the First Circuit's recognition that Article 4A is not "a one-way street," as it imposes obligations and responsibilities on customers as well as banks. *Id.* at *47. Acknowledging that legal and factual issues remained with regard to Patco's claims, the First Circuit affirmed the district court's denial of Patco's cross-motion for summary judgment. The First Circuit remanded the case to the district court for consideration as to whether, and if so, to what extent, the

customer still bears any obligations or responsibilities even where the bank's security system is commercially unreasonable. The court also noted that several material disputes of fact remained to be resolved. For example, Ocean Bank disputes Patco's claim that the unauthorized transfers were caused by malware and keylogging. Ocean Bank argues that Patco cannot prove that its security credentials were misappropriated in a keylogger attack because Patco had scrubbed its computers before a forensic specialist could analyze the computers and locate any potentially responsible malware. To the extent the case proceeds to trial, it is likely Ocean Bank will argue that Patco is responsible for its losses because it lost its credentials through its own negligence or the negligence of its employees. The First Circuit observed, however, that given the relatively modest amount at stake, and the substantial issues to be resolved, the parties would be wise to devote their resources to achieving a settlement.

The legal analysis in Patco, involving a small customer and modest losses, is equally applicable to much larger and more sophisticated customers with the potential for much larger losses. Given that the First Circuit is the first federal appellate court to speak authoritatively on the subject, the First Circuit's interpretation of the "commercially reasonable" test is likely to reverberate far beyond the borders of the First Circuit. For that reason, all commercial banks should take heed and review their security procedures. Security systems that merely rely on asking customers for IDs, passwords, and challenge questions are clearly insufficient. Additional layers, such as password tokens and customer verification, should be considered. Above all, banks need to design platforms that seek input about each customer's particular circumstances, and the available security procedures should effectively utilize that customer information. By requiring more input from their customers, banks may also be able to shift some responsibility back to the customer.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- W. Scott O'Connell at soconnell@nixonpeabody.com or (603) 628-4087/(617) 345-1150
- Daniel Deane at ddeane@nixonpeabody.com or (603) 628-4047