CARLTON FIELDS

What Makes a Bank's Information Security Procedures "Commercially Unreasonable?"

February 20, 2014

In *Patco Construction Co., Inc. v. People's United Bank,* a federal court ruled that failing to review and respond to security alerts may render a bank's information security procedures commercially unreasonable. In "non-legalese," that means that if a security incident occurs due to a bank's failure to review and respond to security alerts, the bank may be liable for losses and damages. The following reviews the *Patco* case and discusses what may cause the information security program of a bank or financial institution to be found commercially unreasonable (at least according to one court's interpretation). Today, most banks have well-written and thorough information security plans and procedures. Those policies and procedures typically require an enterprise IT infrastructure that facilitates and implements rules via software and technology. Banks invest heavily in software and hardware tools, which they buy and design to implement security protocols; and they conduct behavioral and perimeter security analysis, generate alerts, flag suspicious behavior, and spot malicious activity. However, the *Patco* court found that these efforts, without more, are not enough. In addition to written rules and investment in technological defenses, the *Patco* court ruled that bank personnel must review and respond to threat alerts immediately and effectively. If they don't, their security program may be deemed commercially unreasonable. Over seven days in May 2009, Patco's bank authorized six fraudulent withdrawals, totaling $588,851.26. The bank's security system flagged each of these transactions as unusually "high-risk" because they were for greater-than-usual amounts, and because they were inconsistent with the timing, value, and geographic location of Patco's regular payment orders. However, the bank did not notify Patco of this information and allowed the payments to go through. Patco then sued the bank in federal court in Maine alleging that it "should bear the loss because its security system was not commercially reasonable" under Article 4A of the Uniform Commercial Code ("UCC"), which was codified under Maine law. The district court dismissed Patco's suit and Patco appealed. Patco signed up for eBanking in 2003. In doing so, Patco entered into several agreements with its bank including the eBanking for Business Agreement. The eBanking agreement relieved the bank of most liability, and

included language stating that use of the bank's "eBanking for business password constitutes authentication of all transactions performed by you or on your behalf," that the bank "did not assume any responsibilities," and that "electronic transmission of confidential business and sensitive information" was at Patco's risk. The eBanking agreement also limited the bank's total liabilities to those resulting from its gross negligence, and limited any payouts to six months of fees. Patco used eBanking to make regular weekly payroll payments. These were made on Fridays, and always initiated from a computer at Patco's offices. Transactions always originated from a single static IP address, and were quickly followed by weekly withdrawals for tax withholding and 401(k) contributions. Patco's bank used an adaptive monitoring system that provided a risk score to the bank for every log-in attempt and transaction based on a multitude of data, including IP address, device cookie ID, Geo location, and transaction activity. Whenever a user's activity differed from its normal profile, the bank's software reported an elevated risk score. In addition, the bank implemented a "dollar amount rule," meaning it set a dollar threshold amount above which a transaction automatically triggered challenge questions even if the user ID, password, and device cookie were all valid. The bank set the dollar amount rule at $1, which meant that almost every transaction would initiate a challenge question prompt. In court, Patco argued that the bank's security system was not commercially reasonable because the $1 threshold the bank set meant that Patco had to answer challenge questions on every transaction it made, thereby increasing the risk that the answers to its challenge questions would be compromised (the more frequently a security question and answer are used, the greater the chance they will be exposed to hackers). Patco also argued that the bank did not incorporate its security measures adequately by failing to monitor high risk score transactions, and did not provide email alerts or other immediate notices of suspicious activity. The bank argued that its security program was reasonable, and should be binding because Patco agreed to it. The appeals court agreed with Patco and reversed the lower court's order. In its decision, the court said, "the bank substantially increased the risk of fraud by asking for security answers for every $1 transaction, particularly from Patco, which had frequent, regular, and high dollar transfers." Additionally, the court found that bank personnel failed to monitor the risk-scoring reports and therefore failed to notify Patco of suspicious activity that resulted in a high risk that fraudulent activity would go undetected. The court said "it was foreseeable that the use of the same challenge questions for high-risk transactions as were used for ordinary transactions was ineffective as a stand-alone backstop to password/ID entry," and ruled in favor of Patco. So, what does *Patco* tell us about the scrutiny on bank and financial institution information security plans and procedures? First, it makes clear that courts are willing to apply "old law" or rules written for conventional transactions to online and technology-assisted transactions. Second, it should signal to lawyers advising banks on eBanking agreements that shifting risk and liability requires more than wordplay. And third, the case demonstrates that even when banks make investments and have excellent rules in place, if the rules and procedures are poorly implemented, they could still be held liable for damages arising from fraudulent transactions. All this leads to an obvious question: How can banks minimize risk and ensure that their eBanking agreements will be enforceable in court? One answer is to design and implement an information security program that not only has adequate security

protocols and mechanisms, but one that has also been thoroughly reviewed for effectiveness. The security consequences of every step in the design and construction of the information security program should be identified and evaluated. If something increases risk, it should be eliminated. If something reduces risk, it should be incorporated and continuously evaluated to ensure it remains effective given the current threat environment. Banks should also consider deploying a "red team" to independently test and verify security options and settings to ensure that the overall effectiveness of the security program is not being undermined by results that may not be initially obvious. Red teams should include IT, legal, and other subject-matter-experts such as privacy professionals and compliance specialists. Finally, banks should employ independent third parties to conduct periodic risk assessments and penetration testing of their entire security platforms to look for gaps and areas of improvement.*Patco* suggests that courts (and regulators) will be closely scrutinizing the effectiveness of bank security programs. The focus will not likely be on whether banks have implemented the latest safeguards and technology, but rather on whether they are using these tools appropriately and effectively to minimize risk. According to *Patco*, anything less does not meet the "commercially reasonable" threshold of an acceptable information security program.

Related Practices

Technology
Cybersecurity and Privacy
Consumer Finance
Consumer Finance

Related Industries

Technology