Mainebiz
Maine's Business News Source

Federal Lawsuit Outlines Online Banking Procedures

Dan Mitchell | November, 26 2012

Last July, the federal First Circuit Court of Appeals issued a first-of-its-kind decision regarding the obligations of banks and their commercial customers in response to online cyber-thefts. The decision, Patco Construction Co. v. People's United Bank, involved a company in Sanford that lost $345,000 in an online cyber- heist of its business checking account in May 2009.

The prevalence of this type of fraud, known as corporate account takeover, is impossible to ignore. At a recent cybercrime symposium in New Hampshire, a room full of security officers from regional businesses listened to one speaker after another discuss the rising number of cybercrime cases, the increasing sophistication of cybercriminals and the international scope of the problem. Despite the efforts of law enforcement and a vastly increased sense of awareness on the part of the most businesses, cybercrime continues to be a low-risk, high reward activity.

In Patco, the court held that the bank's security procedures for authenticating the identities of online banking customers were not commercially reasonable. Following the decision, the bank eventually repaid the customer's entire account loss, and the case now is closed. For banks and customers looking to understand the significance of Patco, several things stand out from the case.

The law that governs here is not federal law, as one might expect, but comes from Article 4A of the Uniform Commercial Code as enacted in each of the states. All states have enacted a version of Article 4A, most in the late '80s and early '90s (Maine enacted its version in 1989), and for the most part these statutes have not been updated since the time of their enactment.

In Maine, as in most other states, determining which party to a commercial banking relationship bears the risk of loss under Article 4A for a fraudulent online transaction depends on the answers to three basic questions:

- Did the bank and its customer have an agreement that the bank would use a certain set of security procedures to verify the authenticity of the transaction?
- Were those security procedures commercially reasonable?
- And did the bank follow the security procedures?

The burden of answering these questions rests with the bank, but if the answer to each question is yes, Article 4A shifts the risk of loss from the bank to the customer.

Each case is unique on its facts. In Patco, the bank had purchased a relatively sophisticated security system from a national vendor, but internally it made configuration decisions that downgraded the system's effectiveness. It also didn't have procedures in place to review, much less act upon, abnormally high risk scores that were generated by the system for high-risk transactions, such as the fraudulent ACH transfers that wiped out Patco's checking account.

Both banks and commercial customers should review their account agreements to see what, if anything, they say about the types of security procedures the bank will use to authenticate transactions. Some accounts still are governed by outdated form agreements that say little or nothing about security procedures. Ultimately, this serves neither party's interests.

Obviously, every detail of how a bank's security procedures function cannot, and should not, be divulged to a customer, lest they become more vulnerable to penetration by cybercriminals. Customers must, however, have at least a general understanding of what the bank's security procedures are, how they function and what role the customer will be expected to play. Patco also teaches that banks should avoid one-size-fits-all approaches to security, which highlights the need for banks to communicate with customers to understand how they use their accounts.

Commercial customers should understand they share responsibility with their banks to guard against unauthorized transactions. Although banks are in a better position to understand and monitor the prevalent threats to secure online banking, this does not absolve customers from their legal obligation to observe reasonable practices. Maine is fortunate to have excellent security consultants available locally. Businesses should consult them to assess their own internal procedures, evaluate foreseeable risks and implement preventative action plans. Businesses also should consider purchasing insurance to cover cyber losses, which are not covered by most standard casualty policies.

Our ability to conduct banking online has revolutionized business as we know it, but it brings new risks. Banks and customers must recognize that the best way to manage these risks is to work together in an environment of communication and collaboration. This was true before the Patco decision, and it remains true after it.

Dan Mitchell is a shareholder and member of Bernstein Shur's Litigation Practice and Data Security Team. He can be reached at 207-228-7202 or dmitchell@bernsteinshur.com.