BDN MAINE

After Sanford company's money stolen, court rules banks are responsible if hacked

By Seth Koenig | November 30, 2012

SANFORD, Maine — A recent court ruling involving a Sanford construction company and its bank could have nationwide implications as attorneys and policy makers debate who's at fault when anonymous computer hackers steal money electronically.

People's United Bank agreed last week to reimburse Patco for $345,000 in funds stolen by hackers after the First Circuit Court of Appeals in Boston decided the bank was liable in the case, Patco attorney Dan Mitchell confirmed Thursday.

The latest development creates a precedent in what is still considered largely uncharted legal ground surrounding emerging cyber security threats and who is most responsible for keeping commercial bank accounts safe: banks or their corporate customers?

"There had been no cases that had been decided that construed this law before," Mitchell said. "From now on, when cases come up like this, there will be at least one legal guidepost for them to rely on."

Chris Pinkham, president of the Maine Bankers Association, called the Patco case "uncharted legal territory."

"I think one of the questions that came out in this case early on is where is the line between the responsibility of the bank to provide a security system and the responsibility of the consumer to react to security needs and protect their passwords and computers," Pinkham said Friday. "Patco is the only case that comes to mind in terms of legal challenges on this front."

The prolonged Patco case is rooted in a May 2009 incident in which malware was unintentionally downloaded onto construction company computers, and the program recorded employee keystrokes when the computers were used to access bank accounts online.

The keystrokes were transmitted to off-site hackers who used the information to replicate passwords and the answers to security questions used to verify the identity of account holders, and the culprits drained the Patco accounts of approximately $345,000.

Patco sued the bank — which was Ocean National Bank when the breach occurred, and became People's National Bank after a subsequent merger — for reimbursement of the lost funds.

Central to the ensuing case was Article 4A of the Uniform Commercial Code, which dictates that banks must prove they have "commercially reasonable" security systems in place to protect fund transfers for commercial clients. If so, the banks are considered to have met legal requirements for security, and if breaches occur beyond those measures, they are not liable.

The trouble, said Mitchell, is that Article 4A of the Uniform Commercial Code was adopted in Maine in 1989 — long before the widespread use of Internet banking — and "commercially reasonable" as it applies to modern cyber security had yet to be defined legally.

"This case, which went to the First Circuit Court of Appeals, was certainly the highest level court that has ever weighed in on what 'commercially reasonable' security systems are," Mitchell said.

The First Circuit Court of Appeals overturned a lower court ruling in favor of the bank, deciding that the bank did not have "commercially reasonable" security in place to protect Patco's accounts, even though the hackers obtained the information needed to break into the accounts using the company's computers, not the bank's.

Mitchell said the debate over Article 4A's application to modern threats only affects commercial customers, as federal laws protect members of the public and their personal accounts.

"[Federal laws] hold consumers harmless," he said. "Whether we were running antivirus or whatever, it wouldn't matter, we'd be protected. Commercial customers are treated differently, because they're deemed to be more sophisticated and better able to protect themselves. But in this day and age of cyber security, your typical small business isn't any better able to protect themselves than your average consumer."

In the Patco case, the bank used a security system developed by a third-party vendor, which applied "risk" scores to each transaction based on factors such as whether the account was accessed by one of the user's regular computers, and whether the amount transferred fit within the company's regular pattern of transactions.

"If your transaction looked too anomalous or too 'risky,' it would trigger your challenge question," Mitchell said.

But in what was supposed to be an extra layer of security for commercial customers, Mitchell said, Patco administrators were asked their challenge question — "What's your mother's maiden name?" is a common such question — each time they accessed their accounts.

The unintended consequence of that added step, however, was that the frequency with which the Patco users were asked their challenge question increased the odds that a keylogger program, like the one which ultimately infected the company's computers, would have a chance to record the answers to those security questions.

Another factor in the case, Mitchell said, was that even when the bank's security system flagged transactions as suspicious, the bank did not have an effective procedure in place to follow up on that alarm.

"The typical Patco transaction averaged a risk score of something like 20 on a scale of 0-to-1,000," Mitchell said. "The highest ever was around 240. The first fraudulent transaction generated a risk score of 800. So the program was actually pretty good; the bank just didn't have any process in place to look at that information and do anything with it."

That has changed since the case, Mitchell said.

In addition to counting the security measures in place on the Patco account as not "commercially reasonable," and therefore providing future lawyers and policy makers an example of what type of system might fall short, the First Circuit Court of Appeals provided some interpretation of what the previously vague threshold of "commercially reasonable" should be, Mitchell said.

"The court also made some more general statements, for example, that a commercially reasonable security system must take into consideration the individual circumstances of a customer. One-size-fits-all systems aren't going to work," he said.

The ripple effect through the banking industry, Mitchell acknowledged, is that a legal precedent now places a high standard for banks for security on commercial accounts. That means banks which were not previously fine-tuning their security systems for each individual commercial customer must do so, a potentially cumbersome and expensive task.

"Yes it is a burden, but the technology that's available is amazing. Our computers know an awful lot about us and they can process that information in amazing ways," Mitchell said. "If you have thousands of customers, and you think about having to understand the use patterns and tendencies of each of those customers, for you and I, that's really burdensome. It's not nearly as burdensome for computers.

"Between commercial customers and banks, who's better positioned to deal with that? Banks are in a better position," he continued. "Someone's got to bear that risk. It makes more sense to place it on the banks. To the extent that there is some added burden upon banks to reach out to customers and learn more about customers. … that is a cost of doing business."

Pinkham said the banking industry has learned from the Patco case.

"This is a court case that was decided and appealed and reversed based on a fact pattern," Pinkham said. "But the fact of the matter is the best practices in securing your accounts today are different than they were four or five years ago, and we have to be vigilant."

Part of that vigilance, he said, should come in the form of outreach and education of all customers — commercial and consumer — about best safety practices, better antivirus protections and safer password choices.

"We're learning that the education can't stop at a certain level, because bad guys are really bad and they're not going to stop," he said.

Pinkham added that the Maine Bankers Association likely will explore with state lawmakers the possibility of updating the Uniform Commercial Code to be more specific and considerate of modern security threats, to avoid future guesswork on what's "commercially reasonable" in the 21st century.

"If this was good enough 25 years ago, then clearly it's not good enough today," he said. "I think it would be timely to review all that, and I would also add that what we have for a UCC in Maine is different than what they have in New Hampshire and Massachusetts. It's a states' rights issue. But the days of doing business only in one state are gone."

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