FEATURE

Theft in Plain Sight

Lessons from the *Patco v. United* case

BY SCOTT VAN VOORHIS

Scott Van Voorhis
is a freelance writer.

The case of the Maine bank forced to shell out hundreds of thousands of dollars after a business customer's account was hacked has served up a sharp wakeup call for financial institutions.

Banks and credit unions across New England have scrambled over the past few years to beef up their online defenses in the wake of the notorious *Patco vs. Peoples United* case, in which online fraudsters lifted nearly $600,000 from a construction contractor's account at Ocean Bank, which was later acquired by People's United Bank, a large regional bank headquartered in Connecticut.

DANIEL MITCHELL

The Sanford, ME-based contractor, Patco, sued Ocean Bank, and Patco won a hefty settlement after a federal court found the bank's security system was not "commercially reasonable." However, the court ruling found fault not with the relatively modern online security system the bank had installed, but rather the way it had set it up and monitored it. Most notably, the hackers initially gained entry not directly through the bank's system, but by installing Zeus malware on the computer at Patco Construction which was used to make electronic funds transfers.

"Credit unions and banks need to constantly reassess their systems," said Sari Stern Greene, president of Sage Data Security, an independent information security firm headquartered in Portland, Maine.

Cyber thieves strike

The *Patco* case makes for a chilling read, whether you are a small bank or credit union looking to protect yourself from online bank robbers or a small business with an account to protect.

Using the Zeus malware surreptitiously installed on Patco's computers, the cyber thieves were able to record keystrokes and figure out the company's login info for the commercial account it maintained at Ocean Bank. The cyber robbers then lifted more than $588,000 from the account, used by the contractor to make payroll, in several separate transactions over a number of days in May 2009, ranging from $56,000 to more than $115,000.

Once alerted, Ocean Bank scrambled to cancel the transfers – out to Florida and California where Patco does not do business – leaving the construction contractor with a roughly $350,000 loss. When Ocean Bank refused to make him whole or settle, Mark Patterson, the company' chief executive, filed suit in federal court. After losing the first round, a second federal court reversed part of the earlier ruling, finding Ocean Bank's security arrangements had not been adequate after all.

Patco and the bank, now People's United, then came to an out of court settlement in November.

"A lot of banks and credit unions are very interested in the decision," said Daniel Mitchell, Patco's lawyer in the case and an attorney with Portland-based Berstein Shur. "The last three or four years, the learning curve has really been tremendous for financial institutions in learning about data security and developing better protocols."

> Ocean Bank lowered the threshold for challenge questions from $100,000 all the way down to $1, giving cyber thieves tracking the keystrokes on Patco's computers multiple opportunities to figure the answers to the challenge questions.

Warning signs missed

Ordinarily, Patco would have been simply been out of luck. After all, the bank had spent good money on an online security system, which should have covered it from any claims, and the virus had originated on Patco's computers. But Patco's

lawyers were able to make a case that Ocean Bank failed to properly utilize the protections it had put into place.

"They had a really good system," noted Mitchell, Patco's lawyer. "They didn't implement it the right way."

For starters, there were all sorts of warning signs the bank failed to heed.

The money transfers out of Patco's payroll account were for significantly larger amounts than usual, at odd times, to individuals with whom Patco had never done business before, using IP addresses that were not recognized as valid IP addresses of the construction company.

Moreover, the bank's own security system flagged the transactions as high risk, giving scores in the high 700s on a scale zero to 1,000, Mitchell said. Previous Patco transactions were never rated higher than 214.

Still, possibly the most damning piece of evidence related to how Ocean Bank adjusted the settings on its online security system.

A year before the cyber heist, in 2008, Ocean Bank decided to lower the threshold at which challenge questions are asked of customers, and of course; potential thieves seeking to access a commercial account (see related article, page 6). While the previous threshold had been set at $100,000, Ocean Bank lowered it all the way down to $1. Instead of making its customers safer, this decision had the exact opposite effect, meaning that account holders were forced to submit their challenge questions, such as their mother's maiden name and the like, on a regular basis.

And this in turn meant that the cyber thieves who were tracking the keystrokes on Patco's computers had multiple opportunities to figure the answers to the challenge questions, said Sage Data's Greene.

Lessons learned

The Patco case, while unfortunate for the contractor and bank, has had at least one beneficial side effect: It has provided a badly-needed wakeup call to small banks and credit unions over the threats of cyber thievery.

Playing out in the public domain over a couple years in a court case widely watched in financial industry, smaller banks and credit unions have moved to close loopholes and strengthen their online security, said Greene, who appeared as an expert witness on behalf of Patco. The *Patco* ruling itself offered up some common sense suggestions for how Ocean Bank could have more effectively used the system it had in place.

To avoid an Ocean Bank-like cyber debacle, financial institutions should have personnel reviewing suspect transactions identified by their online security systems, actively seek to notify customers of transactions that appear suspect. Moreover, they should also avoid blanket security measures and try and tailor them to fit the profile of individual account holders.

In addition, Greene said many institutions are now using multi-factor identification, meaning that someone trying to transfer money needs to match up in two other ways and can't just gain entry by regurgitating a challenge question.

In fact, Greene contends that customers also need to up their game in order to thwart increasingly sophisticated cyber thievery.

One simple and effective way of doing this is to have a computer reserved just for banking business and not for anything else. This can effectively seal it off form the threats that can come from visiting various websites and unwittingly becoming a target for hackers.

"Do your online banking on a restricted computer and don't do anything else on it," she said. BNE

PREVENTATIVE MEASURES

- Have financial-institution personnel reviewing suspect transactions identified by their online security systems actively seek to notify customers of transactions that appear suspect.
- Avoid blanket security measures. Instead, tailor security measures to fit the profiles of individual account holders.
- Consider adopting multi-factor identification, which requires more than an answer to a challenge question.
- Advise customers – particularly business customers – to do online banking on a restricted computer that is not used for anything else.