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