WIRED

# Bank Agrees to Reimburse Hacking Victim $300K in Precedent-Setting Case

By Kim Zetter | November 30, 2012

In a case watched closely by banks and their commercial customers, a financial institution in Maine has agreed to reimburse a construction company $345,000 that was lost to hackers after a court ruled that the bank's security practices were "commercially unreasonable."

People's United Bank has agreed to pay Patco Construction Company all the money it lost to hackers in 2009, plus about $45,000 in interest, after intruders installed malware on Patco's computers and stole its banking credentials to siphon money from its account.

Patco had argued that the bank's authentication system was inadequate and that it failed to contact the customer after its automated system flagged the transactions as suspicious. But the bank maintained that it had done due diligence because it verified that the ID and password used for the transactions were authentic.

The case raised important questions about how much security banks and other financial institutions should be reasonably required to provide commercial customers.

Small and medium-sized businesses around the country have lost hundreds of millions of dollars in recent years to similar thefts, known as fraudulent ACH (Automated Clearing House) transfers, after their computers were infected with malware that swiped their bank account credentials. Some have been lucky to recover the money from banks that valued their business, but others, like Patco, were told by their banks that they were responsible for the loss.

Although the assets of customers with personal bank accounts are protected under federal law, commercial bank accounts are not. The only recourse such customers have when their bank refuses to assume responsibility for stolen funds is to try to pursue their money in state courts under the Uniform Commercial Code.

People's United Bank agreed to the settlement only after an appellate court indicated that the bank's security system and practices had been inadequate under the UCC.

"This case says to banks and to commercial customers … that there are circumstances in which the bank cannot shift the risk of loss back to the customer, and we're not going to assume that security procedures are commercially reasonable just because the bank has a system that they say is state of the art," says attorney Dan Mitchell, who represented Patco.

Last year, a U.S. District Court in Maine ruled that People's United Bank wasn't responsible for the lost money, and granted the bank's motions for a summary dismissal of Patco's complaint. A magistrate agreed with the ruling saying in part that although the bank's security procedures "were not optimal," it was comparable to that offered by other banks.

But judges with the First Circuit Court of Appeals ruled last July that the bank's security system wasn't "commercially reasonable," and advised the two parties to try to come to a settlement, which they did about a week ago. Patco will not be reimbursed attorney's fees in the settlement.

Patco, a family-owned business in Sanford Maine, sued Ocean Bank, which is owned by People's United Bank, after discovering in May 2009 that hackers were siphoning about $100,000 per day from its online bank account. The hackers had sent a malicious e-mail to employees that allowed them to surreptitiously install the Zeus password-stealing trojan on an employee computer.

After obtaining Patco's banking credentials and waiting for its account to fill up with money, the hackers used the credentials to initiate a series of electronic money transfers over seven days. Nearly $600,000 worth of transfers were made out of the account via six transactions before Patco realized it had been hacked.

Ocean Bank, after being notified of the fraud, was able to block about $240,000 in transfers. But Patco was unable to retrieve the rest.

Patco, which had been banking with Ocean Bank since for 24 years, sued the bank for failing to notice the fraudulent activity and stop it, saying that its security system was not "commercially reasonable" under Article 4A of the Uniform Commercial Code. Under Article 4A, a bank receiving a payment order generally bears the loss of any unauthorized requests for fund transfers. The code also maintains that "burden of making available a commercially reasonable security procedures" belongs to the bank because they "generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud."

Patco maintained that the bank's security system was both inadequate and that the bank did not comply with its own security procedures.

Although the bank's security system flagged the transactions as unusually "high-risk" because the timing, value and geographical location of the transactions were inconsistent with the pattern of other transactions Patco had made, the bank didn't notice the alerts and let the transfers go through without notifying Patco.

Patco generally only made transfers once a week on Fridays, to make payroll payments, and the company made them from computers housed in its offices in Maine, which all used the same IP address. The most it ever transferred was about $36,000. Most of the fraudulent transactions were made in amounts exceeding $90,000, and they were transferred to multiple people who had never received payments from Patco before. The fraudulent activity was caught only after some of the transactions were sent to bank accounts that didn't exist, causing the transfer to fail. When Patco was notified about the failed transactions, they determined the transactions had never been authorized.

Patco accused the bank of failing to implement "best" security practices by requiring customers to use multifactor authentication.

The bank used a system called NetTeller, made by Jack Henry & Associates, a firm that works with numerous banks. Jack Henry uses the same system for 1,300 of its 1,500 bank customers. The system offers a number of authentication options, but the bank rejected most of them, and also configured the system in a way that made it more risky for customers like Patco.

"They had a decent system, but they configured it improperly and they didn't use it properly," says Mitchell.

Although the system used challenge questions to ferret out fraudsters, the system only used three security questions, and asked one or more of them at every transaction Patco made. Because the hackers had installed keystroke logging software onto Patco's computers, they were able to record not only the user name and password for the account, but the responses to the three security questions that Patco employees set up for the account.

The appellate court ruled that the bank had substantially increased the risk of fraud by asking the security questions with every transaction and that this, in conjunction with a number of other failures, rendered the security system unreasonable.

Although the UCC places some burden on the customer to "exercise ordering care" the court found that it was unclear what obligations a customers had when the bank's security system was found to be commercially unreasonable.

Patco is not the first company to sue its bank over fraudulent money transfers. Experi-Metal sued its bank, Comerica, in 2009 after losing more than $550,000 in fraudulent wire transfers. Other cases are wending their way through courts around the country.

In 2010, the FBI disrupted a multinational cybertheft ring involving fraudulent ACH transfers. The thieves, using the Zeus malware, targeted small and medium-sized businesses, municipalities, churches and individuals. The scammers were able to steal more than $70 million from victims.

*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.*