THE WALL STREET JOURNAL.

Cyberthieves Hit Owners

Courts Extend Legal Protection to Small Firms Whose Accounts Were Hacked

By Joe Palazzolo | July 19, 2012

Small-business owners whose bank accounts have been plundered by cyberthieves until recently had no one to blame but themselves.

But two recent court rulings are giving those business owners new hope that banks which don't cater to their specific security needs may be held liable for funds stolen by hackers who increasingly have focused on attacking small businesses.

Banks typically are responsible for losses when personal accounts are hacked. But state laws uniformly place the burden on commercial clients to show that banks didn't do enough to protect their money.

The laws generally have treated individuals and companies differently, reasoning that companies should be more sophisticated than individuals and have their own online security measures in place.

The two recent rulings may alter that equation, recognizing small-business owners often lack an understanding of cyberthreats when they accept bank security procedures, said lawyers who represent owners in such disputes.

The Boston-based First Circuit Court of Appeals ruled earlier this month that Ocean Bank in Maine lacked reasonable safeguards against hackers who siphoned nearly $600,000 from an account held by Patco Construction Company Inc., a Maine contractor and builder.

Patco co-owner Mark Patterson says he believes hackers gained access to Patco's accounts in May 2009 through a program that recorded employees' keystrokes, allowing the thieves to answer security questions posed by Ocean's system.

"Could we have done things better? Yeah," says Mr. Patterson. "But we're a small business we don't have an IT professional on staff. We're not banking specialists, and we don't know all the threats out there," he adds.

Separately, a federal district judge in Detroit last year ruled that a bank owned by Dallas-based Comerica Inc. CMA -1.83% was on the hook for $561,399 in funds stolen from accounts held by Experi-Metal Inc., a custom metals shop in Sterling Heights, Mich. Experi-Metal was the victim of a phishing scheme that lured an employee into providing account access information, according to court documents.

Richard B. Tomlinson, a lawyer who represented Experi-Metal, said he believes the courts are simply recognizing that small businesses need some of the protections extended to individual customers. "In the past, they often would just tell the customer, 'too bad,'" he said.

A spokesman for Comerica Bank declined to comment.

In the first half of 2012, the total number of targeted attacks on organizations rose to an average of 151 a day during May and June, according to data from security technology firm Symantec Corp. SYMC -2.43% released earlier this month.

The proportion of those attacks that were explicitly focused on small business rose to more than 30%, compared with 18% at the end of December 2011, according to its findings. In the report, Symantec defined small businesses as those with 250 employees or fewer.

Few small companies have sued their banks to recover funds stolen by hackers. Some would prefer to settle with their banks for pennies on the dollar or write down the loss than call attention to a security breach, legal experts say.

What's more, litigation is costly, particularly for small firms, because they generally don't have the clout to demand discounts from the outside lawyers they hire.

Until the two recent rulings, many lawyers might have advised small-business owners against trying to go after a bank for losses due to cyberhacking. Banks that take "commercially reasonable" steps to guard against cyberattacks and process transactions in good faith can't be held liable for funds stolen by hackers, cybersecurity experts say. Those steps are usually laid out in contracts between banks and their clients, adding another layer of protection for the banks.

After the two rulings, however, banks can't feel comfortable relying on their contracts to protect them from liability, according to Stewart A. Baker, a partner at Steptoe & Johnson LLP and a former Homeland Security official.

"Small businesses can't keep hackers out reliably, so they need help from the banks, which have greater visibility into fraud patterns," Mr. Baker wrote in a recent analysis of the First Circuit ruling at the Volokh Conspiracy blog.

"The truth is there are millions of small businesses that have no clue of the sophistication of the threat that is out to get them," says Brian Krebs, author of Krebs on Security, a blog that covers cybercrime and Internet security. "You've got one lady who's in charge of payroll, and she works nine to five and…God bless her, she's up against the Russian mob."

Chief Judge Sandra Lynch, who wrote the First Circuit ruling, said Ocean adopted a generic "one-size-fits all" approach to customer security that failed Patco.

Ocean Bank, which now goes by the name People's United Bank, approved the payments over the course of five days in May 2009. Once the fraud was discovered, the bank was able to claw back about $240,000. Patco sued Ocean to recover the rest. An estimated 1,300 to 1,500 other banks had security software similar to Ocean's at the time, according to court filings. A lawyer for Ocean Bank declined to comment. Many smaller or regional banks are eager to build up their small business customer base in order to better compete with big banks, which have gained market share over the past decade.

Ocean argued in court papers that its security at the time was above-average and that the hackers would have made off with far less had Patco checked its account daily.

But William T. Repasky, a Louisville, Ky., lawyer who represents financial institutions, says the First Circuit ruling could prompt some banks to view small businesses as higher risk customers.

As a result, banks might then begin to pass on to small business customers their own increased costs for added security and customer education, he predicts.