Portland Press Herald

# Court rules for business in banking cyber theft

The Maine case could set a precedent in determining a bank's level of responsibility to its online customers.

*July, 16 2012*
*From staff reporters*

While Patco Construction Co. owners Mark and Greg Patterson were focused on the success of their small business in Sanford, cyber thieves were helping themselves to a cut of the profits.

The hits were quick and the withdrawals significant: from $57,000 to $116,000 each over eight days.

It took Ocean Bank six days to notify Mark Patterson of the first irregular withdrawal from the company's e-banking account, but by that time, a little more than $476,888 had been siphoned -- an amount that would ultimately grow to nearly $589,000.

When the bank refused to take responsibility for more than half of the loss, Patco went to court. The company lost the first round, when a U.S. District Court judge ruled in favor of the bank.

But last week, the U.S. Court of Appeals for the First Circuit reversed that ruling, saying the bank lacked a reasonable security measure to safeguard online banking for its business customers.

The ruling is the first to address the issue and could set a precedent nationwide for a bank's level of responsibility to protect businesses' accounts online, said Dan Mitchell, an attorney with the Portland law firm of Bernstein Shur.

"Any small business in any state that finds itself in a lawsuit with its bank over whether reasonable security procedures were used in online banking fraud will turn to this case," said Mitchell, who represents Patco. "That's not to say this ruling comes down heavily on one side or another, but it is clearly an important guidepost for this type of situation."

Ocean Bank's attorney Brenda Sharton, of Boston's Goodwin Procter law firm, declined to comment on the appeals court ruling because the case remains pending.

The appeals court also remanded other disputed issues in the case back to the trial court to resolve.

In the Patco incident, which occurred in early May 2009, the bank was able to block or recover $243,406, but left Patco responsible for recovering the remaining $345,444, court documents state.

The bank convinced the trial court in 2011 that it had reasonable security procedures that were followed when the theft occurred, and that therefore the risk of a loss shifted to Patco, as stipulated in the bank's agreement with the company.

The bank had a multifactor-authentication system, which used a password and challenge questions to access the account. The bank also provided account activity email alerts to its e-banking customers, the court documents state.

"The bank is saying we should have caught the activity," said Patco's co-owner, Mark Patterson. "They asked me if I reconciled my online bank account every day and I told them, 'No. I do it every month like I've always done it.' "

Patterson said the bank claims I should have had an information technology expert on site, "but small businesses may not have that. I certainly don't."

He said he tried to settle with the bank for a little more than $250,000, but the bank refused.

Mitchell, Patco's attorney, said it is clear the bank failed to adequately protect its customer.

It not only lacked "reasonable" security measures for the site, but failed to properly monitor its system, which generated "red flags" on these transactions, he said.

Mitchell said that because the withdrawals drastically veered from the characteristics of Patco's online banking activity, company officials should have been notified immediately.

The bank's system asked the questions every time the account was accessed.

Mitchell said there is no federal law that protects business bank customers from cyber fraud, as there is for individual customers.

But, businesses operate under a state law that basically sets up a contract to address electronic funds and how risk of loss is allocated in situations like this, he said. The law is generally the same in states across the nation because businesses do banking across state lines.

Mitchell said that under the law the bank bears the risk of loss in the first instance. After that, the bank can shift the burden of loss if it has an agreement with the customer that it is going to use a set of security measures, that the measures and procedures are reasonable, and that the procedures are followed.

"The reality in this, given the way technology is advancing and given the techniques used by cyber thieves, is that to think that the average small business is in a better position than an individual consumer to police this stuff probably doesn't hold true," Mitchell said.

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