

ALM Properties, Inc.

Page printed from: <http://www.nlj.com>

[Back to Article](#)

Select 'Print' in your browser menu to print this document.

Print Options: [With Ads](#) | [Without Ads](#)

Font Size:

# 1st Circuit wrestles with requisite level of bank security

How far does a bank have to go to warn commercial customers of potential fraud? That was the issue before the U.S. Court of Appeals for the 1st Circuit in oral arguments on April 5.

Sheri Qualters

April 05, 2012

How far does a bank have to go to warn commercial customers of potential fraud? That was the issue before the U.S. Court of Appeals for the 1st Circuit in oral arguments on April 5.

Patco Construction Co. Inc. is appealing an August 2011 ruling in favor of People's United Bank issued by Judge Brock Hornby of the District of Maine. Hornby granted a summary judgment motion to the bank, which does business as Ocean Bank, and denied Patco's summary judgment motion.

Patco, a real estate developer and contractor, claims that the district court erred by ruling as a matter of law that the bank's security procedures were commercially reasonable according to the terms of the Uniform Commercial Code. Article 4A of the code requires banks "to adopt commercially reasonable security procedures for authenticating payment orders," according to Patco's brief.

In May 2009, \$588,851.26 was fraudulently withdrawn from Patco's account, according to its brief. The company lost at \$345,444.43 because \$243,406.83 was ultimately blocked or recovered.

Although the bank determined that the transactions were "uncharacteristic, highly suspicious, and potentially fraudulent," Patco claims in its brief that the bank didn't review them or contact Patco to determine if they were legitimate.

Patco alleges that it was only able to stop the fraudulent transactions because of a routine bank notice sent by U.S. mail to a company principal about the earlier transactions.

Also according to Patco, the bank's use of so-called challenge questions, designed to determine whether the person requesting the transaction was authorized, opened the door to cybercriminals. That procedure, which went into effect as of June 2008 on every automated clearing house transaction over \$1, gave cyberthieves the opportunity to capture the password information with every transaction, according to Patco.

Patco claims the case, *Patco Construction Co. Inc. v. People's United Bank*, presents an issue of first impression in the circuit.

People's United argues in its brief that summary judgment was appropriate because it met all the terms of the Uniform Commercial Code's Section 202(b), which states that the consumer bears the risk of loss under certain conditions. Those conditions include the following: the customer and the bank have an agreement that a security procedure will verify authentication payment orders; the bank's security procedure is commercially reasonable; and the bank's acceptance of the payment complied with the security procedure.

The bank claims its authentication system at the time was a premium product from the vendor that "exceeded the standard for banks of its size at the relevant time."

Chief Judge Sandra Lynch sat on the panel with Judge Jeffrey Howard and Senior Judge Kermit Lipez.

At the oral arguments, Patco's lawyer, Dan Mitchell, a partner at Portland, Maine-based Bernstein Shur, argued that because the challenge questions were asked for every transaction of more than \$1 — and because of the bank's knowledge of the potential fraudulence of certain transactions — the questions "created an obligation on [the bank's] part to do something more." Mitchell also said that because the bank made the aberrant decision to use a \$1 transaction amount as the threshold for challenge questions, when it got these red flags, "it was incumbent upon them to do something more."

Lipez said that it doesn't sound as though Patco's obligation to do something more was straightforward as notifying your client. "You're suggesting that they should have introduced some other internal security measures."

"A communication [that a transaction was high-risk] would have been fine," Mitchell said. "In fact, the record shows that now they do something very similar."

Lynch asked Mitchell, if the bank's procedures were found to be commercially unreasonable, "does that end the case or is there some role for the fact that your client's negligence, let's just assume some negligence, plays a role and how much money gets recovered here? Are there negligence-type concepts in this area of law?"

"I don't believe so, your honor, " Mitchell answered.

"So this is an all or nothing regardless of your client's behavior?" Lynch asked.

"With respect to the question of whether the bank's security procedures were commercially unreasonable, I believe so your honor," Mitchell said.

At the beginning of People's United's oral argument time, Lynch asked the bank's lawyer, Brenda Sharton, a partner at Boston's Goodwin Procter, whether commercial unreasonableness was the only question in this case.

Sharton said, "It is, it's a matter of law," but asserted that Patco's conduct should also be assessed in terms of commercial reasonableness.

"I want to start by saying: Beware the insidious nature of hindsight. We have to bring ourselves back to 2009 and, frankly, even back to 2005 with the [Federal Financial Institutions Examination Council] guidance," Sharton said. "The bank went out and purchased the premium product from the industry leader in online banking programs. It utilized it within its parameters, then it even supplemented it with other controls."

Lynch said the \$1 threshold protects more customers, but "it also increases the risk in absolute dollar terms to your bigger customers because the asking of the questions occurs much more frequently on their accounts. If you know that malware, spyware is out there, it just gives them more occasions once they've installed it to get the answers to the questions."

"Our leading expert...says by increasing the challenge questions, you increase security," Sharton said.

Near the end of the oral arguments, Lynch said to Sharton that the fact that malware knows the answers to the questions means that the challenge questions are "no security at all. You know it's high risk [but] you don't tell the customer. All you do is ask them the questions they already have the answers to. Why is that a security device against that type of fraud?"

Sharton said that in May 2009, "banks were just starting to become aware of this and deal with that as a risk threat."

There's sparse case law on the issues, said Mitchell in an interview after the oral arguments. "On the consumer side, for a consumer transaction, there are different protections in place," he said. "If Patco were a consumer retail banking customer, it wouldn't be here."

Sheri Qualters can be contacted at [squalters@alm.com](mailto:squalters@alm.com).

Copyright 2012. ALM Media Properties, LLC. All rights reserved.