THE NATIONAL LAW JOURNAL

Revived suit over bank security measures potentially opens door to more cases

By Sheri Qualters
The National Law Journal | July 5, 2012

In a rare reported case about the commercial reasonableness of a bank's security measures under the Uniform Commercial Code, the U.S. Court of Appeals for the First Circuit has reversed a district court's rejection of a suit against a bank where fraudulent withdrawals occurred.

Lawyers say that the ruling could open the door to more UCC actions against banks following fraudulent transactions, but they emphasize that the fact pattern is unlikely to be replicated in many other cases.

On July 3, a unanimous panel reversed a summary judgment ruling in favor of People's United Bank, which does business as Ocean Bank, in a suit brought by Patco Construction Co. Inc. The appeals court also affirmed a denial of Patco's summary judgment motion on its UCC liability claim and remanded the case.

Patco, a real estate developer and contractor, sued Ocean Bank in September 2009 in Maine Superior Court. Patco claimed it lost $345,444.43 out of $588,851.26 worth of fraudulent withdrawals. Another $243,406.83 of the total was ultimately blocked or recovered. In October 2009, the bank removed the case to federal court.

Patco claimed it became aware of the fraudulent transactions days after they began because a company principal received only routine bank notices by U.S. mail. Patco claimed Ocean Bank failed to review or alert it about transactions that were "uncharacteristic, highly suspicious, and potentially fraudulent."

One of its six claims was that the bank's security procedures did not comply with the UCC's Article 4A, which requires banks "to adopt commercially reasonable security procedures for authenticating payment orders." That claim was the focus of April 5 oral arguments at the First Circuit.

Patco also sued for negligence, breach of contract, breach of fiduciary duty, unjust enrichment and conversion. Patco further claimed that Ocean Bank's use of so-called challenge questions, which determine whether an authorized person was requesting the transaction, made Ocean Bank's customers vulnerable to keyloggers or malware that captures that information. Starting in June 2008, Ocean Bank began using the challenge questions on every automated clearinghouse transaction of more than $1.

In in August 2011, Judge Brock Hornby of the District of Maine granted the bank's summary judgment motion and denied Patco's. Hornby's ruling fully adopted a magistrate judge's recommended decision that Patco bore the loss of the fraudulent transfers. The magistrate judge ruled that the bank's security procedures were commercially reasonable and that Patco had agreed to them. The magistrate judge also ruled that UCC's Article 4A displaced Patco's negligence, breach of contract and breach of fiduciary duty claims. The ruling further held that the unjust enrichment, conversion and UCC liability counts failed on the ground that the bank could not have been unjustly enriched or wrongly converted Patco's funds, if it employed commercially reasonable security procedures.

Chief Judge Sandra Lynch wrote the opinion in *Patco Construction Co. Inc. v. People's United Bank*, joined by Judge Jeffrey Howard and Senior Judge Kermit Lipez.

Lynch wrote that Ocean Bank's use of challenge questions for every electronic transaction of more than $1 substantially increased the risk of fraud, particularly for customers with frequent, regular and high-dollar transactions: "[W]hen it had warning that such fraud was likely occurring in a given transaction, Ocean Bank neither monitored that transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable. We emphasize that it was these collective failures taken as a whole, rather than any single failure, which rendered Ocean Bank's security system commercially unreasonable."

Ocean Bank's challenge questions for transactions of more than $1 "also ignored Article 4A's mandate that security procedures take into account 'the circumstances of the customer' known to the bank," Lynch wrote.

Lynch also rejected Ocean Bank's arguments about a risk profile it developed for Patco: "This argument misses the mark because, in fact, the risk profile information played no role. It triggered no additional authentication requirements, and the bank did nothing with the information generated by comparing the fraudulent transactions against Patco's profile." .

Lynch went on to state that "[t]he bank's generic "one-size-fits-all" approach to customers violates Article 4A's instruction to take the customer's circumstances into account."

Lynch criticized Ocean Bank for not adding extra security measures in conjunction with its decision to lower the dollar-amount rule from $100,000 to $1 "despite the fact that several such security measures were not uncommon in the industry and were relatively easy to implement." This was particularly unreasonable in light of the bank's knowledge of an upswing in fraud through keylogging and malware and two fraudulent incidents on the bank's system by May 2009.

The First Circuit reversed the lower court's UCC ruling on the ground that "the collective failures, taken as a whole, rendered Ocean Bank's security procedures commercially unreasonable." The court's conclusion on the commercial reasonableness issue also prompted it to vacate the district court's summary judgment on the unjust enrichment and conversion claims. Lynch wrote that the common law claims of breach of contract and breach of

fiduciary duty survive because they're "not inherently inconsistent" with the UCC Article 4A claim.

But the First Circuit affirmed the dismissal of the negligence claims on the grounds that they are "inconsistent with the duties and liability limits set forth in Article 4A."

Lynch noted that it's unclear whether commercial customers have any obligations when a bank's security system is found to be commercially unreasonable: "In short, we leave open for the parties to brief on remand the question of what, if any, obligations or responsibilities are imposed on a commercial customer under Article 4A even where a bank's security system is commercially unreasonable. The record requires further development on these issues, precluding summary judgment at this stage."

Dan Mitchell, a partner at Portland, Maine-based Bernstein Shur who represented Patco, said that, although these types of cases are dependent upon their facts, the court's critique of the bank's "one-size-fits-all" security system will be closely parsed by the banking and bank security community. "There are some statements in the opinion that could be read to have more general application. The court made some pronouncements with regard to commercial reasonableness under Article 4A that I suspect banks are going to want to analyze closely and evaluate," Mitchell said.

Mitchell said he's "not aware of any other reported cases where a court has evaluated a bank's security procedures for authenticating electronic transactions and found they were not reasonable." Other reported district court cases "didn't get decided based on an analysis of the commercial reasonableness" issue, he said.

The bank doesn't comment on pending litigation, said its lawyer, Brenda Sharton, a partner at Boston's Goodwin Procter.

Christopher Wolf, a partner at Hogan Lovells' who isn't involved in the case, said the decision can be seen as potentially opening the door to more UCC, contact and negligence claims against banks when there's been a loss through fraudulent online transfers.

However, 'it also can be limited to its unusual facts," said Wolf, who head the firm's privacy and information management practice group: "The absence of security tools to detect such unusual activity and hold up transactions seemed central to the court's holding. It is hard to imagine cases with such a combination of alleged security deficiencies coming along with any regularity."

Scott Vernick, a partner at Philadelphia's Fox Rothschild who isn't involved in the case, said the opinion is important because it interprets Article 4A of the UCC about what is commercially reasonable, but it's unlikely to open the floodgates to similar cases.

"The court addresses a very unique set of facts which are not necessarily going to be replicated in other cases," said Vernick, whose practice focuses on electronic data security issues.

Sheri Qualters can be contacted at squalters@alm.com.

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.