Proskauer

Door to Increased Liability for Banks Opened by U.S. Court of Appeals for the First Circuit

July 18, 2012

The United States Court of Appeals for the First Circuit has opened the door to increased liability for banks when hackers make fraudulent withdrawals. In *Patco Construction Co., Inc. v. People's United Bank*, ___ F.3d ___, 2012 WL 2543057, the Court held that Ocean Bank, a division of People's United Bank, failed to establish "commercially reasonable" measures to prevent six fraudulent withdrawals from an account held by a local business. Following *Patco*, online security protocols characterized by "one-size-fits-all" approaches will be suspect, and might lead to bank liability for fraudulent transfers.

Patco is the first federal appellate court opinion to reject a bank's reliance on the commercial reasonableness of its security procedures. The bank failed to prevent almost $600,000 in fraudulent withdrawals from the account of Patco Construction Company in May 2009. Although the bank's security system flagged each transaction as "high risk" because they were inconsistent with the timing, value, and geographic location of Patco's typical orders, the Court was critical of the fact that no bank employee reviewed the transactions or notified Patco of the activity, and the transactions were allowed to be processed. Patco sued the bank, alleging that it should bear the loss because its security system was not commercially reasonable under Article 4A of the Uniform Commercial Code. The district court granted summary judgment to the bank, holding that its security systems were commercially reasonable.

Article 4A of the Uniform Commercial Code governs the rights, duties and responsibilities of banks and their commercial customers with respect to electronic funds transfers. According to the Court, banks typically bear the risk of loss of any unauthorized funds transfer, although banks may shift the risk of loss to the customer in one of two ways. First, the Court noted that banks may shift the risk of loss to the customer by showing that the payment order was appropriately authorized, which presents challenges in the context of online banking. Second, the Court added that banks may shift the risk of loss to the customer if they verify transfers pursuant to "commercially reasonable" security procedures. Although the UCC offers some guidelines, it states that the "[c]ommercial reasonableness of a security procedure is a question of law" to be determined by the courts, and that "[t]he standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank . . . ."[1]

In reversing the district court's holding, the three-judge panel paid particular attention to the bank's decision to lower the amount threshold that triggered its customers to answer challenge questions before its online system would accept a funds transfer. Reducing this threshold to $1, and thus requiring challenge questions for almost all transactions, came back to haunt the bank when this particular precaution proved to be the only security procedure it employed. The Court specifically took note of the widespread prevalence of computer malware known as "keyloggers" that are able to secretly infect computers, monitor and record the keystrokes of users, and then transmit challenge question answers to cyber thieves. The Court found that the bank "substantially increase[d] the risk of fraud by asking for security answers for every $1 transaction, particularly for customers . . . which had frequent, regular, and high dollar transfers."[2]

The Court also focused on various other security tools the bank did not incorporate into its systems, including customer notifications and employee monitoring of risk-scoring reports, as well as a user-selected picture function and tokens. Viewing all of these facts together, the Court concluded that "it was these collective failures as a whole, rather than any single failure, which rendered [the bank's] security system commercially unreasonable."[3]

The Court remanded the case to the district court for the parties to brief the obligations that Article 4A imposes on commercial customers when a bank's security protocols are commercially unreasonable. The Court, though, did note that customers have "obligations and responsibilities as well," with other provisions in Article 4A making clear that the statute is not a "one-way street."[4]

In light of *Patco*, banks may consider incorporating the following as they review their online security procedures.

- Contemplate adding security measures beyond challenge questions.
- Consider heightened security steps for high-dollar transactions.
- Utilize systems that can recognize atypical transactions for a given customer. These systems can be configured to prompt a reaction (and potentially a rejection) once they recognize a departure; red flag alerts are then transmitted to the customer in a timely fashion.
- Bear in mind how threats and security are evolving in the industry, and keep pace with that evolution.

[1] Me. Rev. Stat. Ann. tit. 11, § 4-1203 cmt. 4.

[2] *Patco Constr. Co., Inc. v. People's United Bank*, No. 11-2031, 2012 WL 2543057, at *12 (1st Cir. July 3, 2012).

[3] *Id.*

[4] *Id.* at *16.

Related Professionals

- **Margaret A. Dale**
  Partner