Rethink cyber security

Patco decision finds banks must do more

The cost of operating a technologically secure bank may have just gone up. The First Circuit's ruling in *Patco Construction Co. v. People's United Bank* means banks can be liable for the money cyber thieves steal from a customer's commercial account.

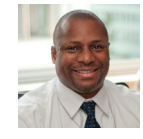
Patco joined Ocean Bank's "ebanking" program in 2003, primarily for weekly payroll; the payments exceed $37,000. In 2008, People's United Bank acquired Ocean Bank. In May 2009, hackers infiltrated Patco's account and initiated six fraudulent transfers totaling $588,851.26. The thieves apparently used computer malware to steal Patco's customized answers to security questions and passwords. The bank recovered just $243,406.83.

Patco sued, claiming the bank's "commercially unreasonable" security procedures allowed hackers to steal security data. Article 4A of the Uniform Commercial Code generally holds banks responsible for the loss of any unauthorized funds transfer, but banks may shift the risk of loss to a commercial customer *if* transfers follow commercially reasonable security procedures.

The bank argued that its ebanking agreement detailed the procedures and limited the bank's liability. The district court held that the bank's security systems were commercially reasonable. The First Circuit reversed the decision: The bank's "collective failures" made security procedures inadequate.

Initially, Patco users answered "challenge questions" for all transfers over $100,000, but in June 2008, the bank lowered the threshold to all transfers over one dollar. Before June 2008, none of Patco's transfers required challenge questions, but every transfer after June 2008 triggered them. Consequently, both thresholds were rendered ineffective. Given the prevalence of keystroke-copying malware, the court concluded the bank increased fraud risk by requiring questions for every transaction. It also criticized the bank for neither monitoring transactions for fraud nor notifying Patco before suspicious transactions were processed. It noted the fraudulent wires that were flagged as "highly suspicious" simply triggered the same challenge questions. This led the court to question the bank's decision not to strengthen its security with other readily available technology, such as security tokens.

Although the bank's security system was found commercially unreasonable, Patco may not be blameless. The court of appeals did not determine the party ultimately responsible for the loss. On remand, the First Circuit ordered the district court to determine the duties Patco had to allay the loss caused by the bank's inadequate procedures. Regardless of how the district court rules, the *Patco* decision suggests bank security programs that rely only on customer user names, passwords, and challenge questions will increase a bank's liability if a commercial account is compromised. Based on the court's analysis, at a minimum, banks should consider fortifying and tailoring their systems to meet the needs of each commercial customer. ■



Thomas Pinder is associate general council at ABA. Contact him at tpinder@aba.com

PHOTO: CARLOS A. OLIVERAS/SHUTTERSTOCK.COM