First Circuit Ruling Finds Bank's Actions "Commercially Unreasonable" Under UCC Article 4A

Authors

Greg Pulles
Brent Ylvisaker

Related Services

Financial Services Regulatory

July 9, 2012
Attorney Articles

In a case of first impression with serious and potentially costly implications for commercial banks, the First Circuit has held that a bank's authentication procedures for electronic payments were commercially unreasonable under Uniform Commercial Code ("UCC") Article 4A. The case involved UCC 4A Section 202(b), which provides that a customer is liable for a payment order received by a bank if the bank and customer have agreed that payment orders will be verified by a specified security procedure and "the security procedure is a commercially reasonable method of providing security against unauthorized payment orders." The trial court held in favor of the bank; the First Circuit reversed. *Patco Construction Company, Inc. v. People's United Bank*, United States Court of Appeals for the First Circuit, Docket No. 11-2031, July 3, 2012.

The bank authorized six fraudulent withdrawals, totaling just under $600,000, from an account held by Patco Construction Company ("Patco"), after the perpetrators correctly supplied Patco's customized answers to security questions. The fraudsters probably obtained the answers by insertion of Zeus/Zbot malware on one of Patco's computers. The bank's security system flagged each of these transactions as unusually "high-risk" because they were inconsistent with the timing, value, and geographic location of Patco's regular payment orders. The bank, however, allowed the payments to go through. Patco's complaint alleged that the bank should bear the loss because its security system was not commercially reasonable under Article 4A.

The bank's security procedures had these central features that we believe were key to the case:

(1) The bank asked "challenge questions" when a transaction exceeded a dollar threshold. The bank thought it was making the system safer by setting the threshold at $1, effectively asking the challenge questions for every transaction.

(2) The bank knew the "identity" of its customer's terminals and if a transaction entered from a different terminal, the transaction was identified as high risk.

(3) The bank did not have in place any additional "reactive measures" when its system identified a transaction as anomalous or high risk – i.e. no customer contact was initiated.

Although the court found that the totality of the circumstances, including the bank's asserted failure to tailor security to the individual customer, led to its conclusion that the procedures were commercially unreasonable under Article 4A, we believe the result was driven by:

(1) The court's conclusion that asking challenge questions for every transaction enabled fraudsters using malware or keylogging to capture the answers.

(2) The court's belief that the bank should have notified the customer when a transaction risk score was rated "high risk" due to originating from a "not before used" terminal and where the transaction was anomalous (e.g. too large etc. based on history of prior customer transactions).

The First Circuit offered a ray of hope to the bank, affirming the trial court's decision not to award summary judgment to Patco on its Article 4A claim, because more needed to be known and argued about the customer's conduct, and whether that conduct would absolve the bank. For example, the customer had not signed up for e-alerts and did not check its balance daily.

The decision, however, mandates that commercial bankers examine their contracts and, more importantly, their procedures. Specifically, the FFIEC in 2012 issued new guidance on authentication (not discussed by the parties or the court in Patco), the most significant aspect of which is a mandate that banks must put in place a security procedure that identifies, addresses and reacts to anomalous customer behavior. To address Patco, banks need to create an individual customer risk profile that is then used to select appropriate security procedures for the customer based on those individual circumstances. One size does not fit all, to use the First Circuit's phrase.

A bank then needs to adopt state of the art technology, appropriate for its size and comparable to what other banks in its position are using, and must review that security protocol periodically. Customers may be given a menu with prices, so long as the choices and risks are clear. One only has to review the record in Patco to see the many points at which the bank and the customer were out of sync. Did the customer get email alert sign up opportunities or not? Was the bank's internet navigation tool off the mark? Did the customer really understand the need to check its balance daily?

It's time to revisit procedures, disclosures, the account application, and account agreement to address the additional obligations this decision creates in the area of authentication of electronic payment orders.