Online Banking Security Procedures for Commercial Customers

Related Industries

Financial Institutions

AUTHORED ARTICLE | Winter 2013

The Bankers' Statement – Winter 2013

Published in the Winter 2013 issue of *The Bankers' Statement*

Article 4A of the Uniform Commercial Code (Article 4A) sets forth the rights, duties and liabilities of banks and their commercial customers with respect to funds transfers. Today, the vast majority of funds transfers occur electronically (i.e., by wire transfer) through the placement of payment orders by commercial customers via their online bank accounts. These online bank accounts are protected to varying degrees by one or more security procedures (e.g., user IDs and passwords, challenge questions, token codes, risk scoring and monitoring, customer notification, etc.). The number, type and extent to which these security procedures are employed will often depend on the capabilities of the bank and the needs and financial resources of a particular commercial customer.

In theory, these security procedures are intended to provide benefits to both the bank and its customers. For the bank, the security procedures offer greater assurance that the online payment orders issued in a customer's name are in-fact authorized by such customer and can be safely acted upon. For a customer, the security procedures serve as a safeguard against unauthorized access to and use of such customer's bank accounts and confidential information. Unfortunately, due to the drastic increase and sophistication of cybercriminals, a commercial customer's online bank accounts may still be susceptible to improper access and use despite the customer and bank's adherence to one or more agreed-upon security procedures. For example, cybercriminals are often able to use phishing emails and various types of malicious software (malware) to obtain confidential banking information (e.g., user IDs, passwords and answers to challenge questions) from the individual users of a commercial customer's online bank accounts. With this information, these criminals can then attempt to access the customer's online bank accounts and, if successful, initiate fraudulent payment orders for substantial sums of money. If the bank acts on any of these unauthorized payment orders, the question becomes who should bear the risk of loss for any funds of the customer that cannot be recovered – the customer or the bank?

Article 4A provides the answer to this risk of loss question. Under Article 4A, the risk of loss for any payment order fraudulently initiated by a cybercriminal and acted upon by a bank will generally fall on the customer in whose name such payment order was issued if all of the following elements are met:

1. the customer and the bank have agreed that the authenticity of payment orders issued to the bank in the name of the customer will be verified by the bank prior to acceptance pursuant to agreed-upon security procedures;
2. such security procedures are “commercially reasonable”; and
3. the bank acted on the payment order which turned out to be fraudulent in good faith and only after verifying its authenticity in compliance with such security procedures.

With respect to determining whether certain security procedures are “commercially reasonable,” Article 4A requires that the following factors be considered:

1. the wishes of the customer expressed to the bank;
2. the circumstances of the customer known to the bank, including the size, type and frequency of payment orders typically issued by the customer;
3. whether alternative security procedures were offered to, but not elected by, the customer; and
4. the types of security procedures generally in use by similarly situated banks and customers.

If each of the three elements identified above are met, then the risk of loss for any damages incurred by the commercial customer as a result of the bank acting on a fraudulent payment order from a cybercriminal will generally be borne by the customer, as Article 4A deems it ultimately the customer's “fault” for allowing a third-party (i.e., the cybercriminal) to improperly obtain access to the customer's online bank accounts despite adequate security measures being in place and followed by the bank. On the other hand, if it is found that any one or more of these elements have not been met, then the risk of loss will shift to the bank and it will be the bank that is required to refund to the customer all amounts that were transferred out of the customer's bank accounts as a result of the fraudulent electronic payment orders and not otherwise recovered. The only exception to this shifting of the risk of loss onto the bank would be if the bank could establish that the customer was nonetheless bound by the fraudulent payment orders under the law of agency. To do this, the bank would need to show that there was some type of pre-existing relationship between the customer and the cybercriminal that justifies holding the customer responsible for the cybercriminal's actions (e.g., if the cybercriminal was a customer insider). Establishing such an agency relationship would be unlikely.

As one could imagine, commercial customers incurring significant financial losses as a result of fraudulent electronic payment orders may decide to file lawsuits against their banks in an effort to recover funds lost due to the online fraud. Until recently, it appears that customers were largely unsuccessful in bringing such lawsuits. However, since June 2011, at least two federal courts have ruled that a bank's security procedures did not satisfy Article 4A's requirements and, therefore, the bank could be held liable for acting on fraudulent electronic payment orders. The opinions of those courts, and the implications that these decisions could have for online security procedures and bank liability going forward, are discussed in further detail below.

The Ocean Bank Decision

In a recent case, *Patco Construction Company, Inc. v. People's United Bank (d/b/a Ocean Bank)*, 2012 U.S. App. LEXIS 13617 (1st Cir. July 3, 2012), the U.S. Court of Appeals for the First Circuit found that the security procedures implemented by a New England community bank, Ocean Bank (later acquired by People's United Bank), with respect to the online bank accounts of Patco Construction Company (Patco), a small property development and contractor business, were not "commercially reasonable" within the parameters of Article 4A. As a result, the court held that Ocean Bank could be found liable for over $345,000 in losses from Patco's bank accounts caused by fraudulent payment orders placed over a period of seven days by a cybercriminal who used keylogger malware to steal confidential banking information (usernames, passwords and answers to challenge questions) from Patco employees.

In the case, the court discussed the bundle of security measures that Ocean Bank employed for Patco's online bank accounts. Those protections included log-in IDs and passwords, computer tracking cookies, risk profiling and scoring reports, and challenge questions triggered for high-risk transactions or transactions over certain dollar amounts. The court also stressed those security measures that were not implemented for Patco's online bank accounts, including, among other things, bank monitoring of the risk-score reports that were generated, and manual review and customer notification of high risk-scoring transactions.

Ultimately, the court ruled that the security procedures used by Ocean Bank were not "commercially reasonable" for the purpose of protecting Patco's accounts. In reaching this decision, the court found the following failures of Ocean Bank's security, when considered collectively, to be determinative:

1. *Dollar Threshold for Triggering "Challenge" Questions*. Prior to the fraudulent payment orders occurring, Ocean Bank made a "one-size-fits-all" decision to lower the "challenge" question dollar threshold for all of its commercial customers from $100,000 to $1. This decision was found by the court to be unreasonable when specifically applied to Patco in light of the frequency, dollar amount and regular characteristics (e.g., dates and recipients) of its prior payment orders. The court agreed with Patco's position that Ocean Bank's practice with respect to challenge questions greatly increased the risk of cyberthieves stealing the answers to such challenge questions because, given the de minimis $1 threshold, such information would need to be provided by a user each and every time he or she accessed Patco's online account to place a payment order.

In making this decision, the court also noted that the bank's reliance on challenge questions without implementing additional layers of security was cautioned against by bank regulators and by the third-party vendors that supplied such security software, not common amongst New England community banks in combating the ever-growing problem of internet fraud, and especially unreasonable given the fact that the bank had itself previously been the victim of fraud involving keylogging malware.

1. *Failure to Monitor High-Risk Reports and Review and Notify Patco of High Risk-Scoring Transactions*. The court found it particularly troublesome that no one at the bank actually monitored the high-risk transaction reports being generated for Patco. The court noted that the risk profiling procedures implemented for Patco rated online transactions on a scale from 0 to 1,000 (with anything more than 750 being considered high-risk), that the highest risk score that any Patco online transaction had received prior to the ones in question was 214, and that the risk scores of the fraudulent electronic

payment orders ranged from 563 to 790 as a result of each of them having irregular payment characteristics (e.g., orders placed from unrecognized computers and IP addresses, in extraordinarily large amounts and to recipients to whom Patco had never before issued payment orders). Given the high-risk reports resulting from these abnormal payment orders, the court found that the bank could and should have manually reviewed the transactions further to determine their legitimacy and/or notified Patco before allowing the transactions to be completed.

The Comerica Bank Decision

In the June 2011 case of *Experi-Metal, Inc. v. Comerica Bank*, 2011 U.S. App. LEXIS 62677 (E.D. Mich. June 13, 2011), the U.S. District Court for the Eastern Division of Michigan also considered whether the security procedures implemented by a bank with respect to a particular commercial customer's online bank accounts passed muster under Article 4A's risk of loss test. Experi-Metal, Inc. (EMI), a Michigan-based metal fabricating company, was the victim of an email phishing scheme wherein cybercriminals obtained the log-in information of EMI's controller and used such information to initiate 93 fraudulent online payment orders totaling more than $1.9 million. The bank, Comerica Bank (then the 31st largest bank in the U.S. by total assets), had implemented various security procedures to protect EMI's accounts, such as user IDs and passwords, challenge questions and token codes, and had also established an internal bank policy for responding to fraudulent payment orders initiated through phishing schemes. Nonetheless, the court held that the risk of loss test had not been satisfied because the bank had not set forth evidence that it had acted in good faith in processing the fraudulent payment orders.

With respect to the good faith requirement, the court noted that the burden of proof under Article 4A was on the bank to establish:

1. that its employees did in-fact act honestly when processing the fraudulent payment orders (i.e., that they had a “pure heart and empty head”), and
2. that the processing of such fraudulent payment orders comported with reasonable commercial standards of fair dealing (i.e., that the bank's response and processing of the payment orders was in-line with what other similarly situated banks would have done if one of their customers was victimized by a phishing scheme).

The court found that Comerica Bank had failed to set forth any evidence that this second element of good faith had been established. Instead, as noted by the court, the evidence suggested that it was unlikely that the banks response and actions did comport with reasonable commercial standards of fair dealing given, among other things:

1. the bank had prior notice that phishing emails had been sent out to its customers;
2. the time it took the bank to stop processing the fraudulent payment orders (over six hours after the first order was received by the bank);
3. EMI's limited history of placing online payment orders (only two had been previously placed);
4. the volume and frequency of the fraudulent orders that were placed; and
5. that the recipients of all of the payment orders were located in foreign countries notorious for higher instances of cybercrime.

As a result, the court found that the good faith requirement under the Article 4A risk of loss test had not been met and, therefore, Comerica Bank bore the risk of loss for $560,000 in EMI funds that could not be recovered.

Implications

It remains to be seen to what extent the *Ocean Bank and Comerica Bank* decisions will be used by other courts to question the sufficiency of a bank's online security procedures and/or hold a bank responsible for commercial customer losses resulting from fraudulent electronic transactions initiated by cybercriminals in circumvention of such security procedures. What is certain, however, is that the instances and complexity of cybercrime affecting the U.S. online banking system continues to rise at an alarming pace, and the amount of potential losses that banks could be subject to for implementing inadequate security procedures are considerable. As such, these recent decisions should serve as a reminder to all banks that they need to remain steadfast and proactive in their commitment to providing sufficient protection for their commercial customers' online bank accounts. Risk assessments should be conducted on a periodic basis to determine if the number, types and combinations of online security procedures employed by the bank (either internally or through third-party vendors) are sufficient in light of recent threats, current technology, customer awareness and regulatory guidance.[1] Applicable bank policies should be reviewed and, if necessary, revised to ensure that such online security procedures are being offered and implemented on a personalized, customer-by-customer basis after thorough analysis of whether such procedures are commercially reasonable for a particular customer. Bank employees should receive comprehensive training on the bank's security procedures and how to properly respond in the unfortunate circumstance when fraudulent online transactions are acted upon by the bank prior to the cybercriminals' activities being discovered. Finally, proper documentation should be generated by the bank at all stages of the security procedure assessment, selection and implementation process.