Connecticut Law Tribune

September 24, 2012

An ALM Publication

BUSINESS LITIGATION

Cyber Attacks On Commercial Banks

Recent rulings seem to put bigger burden on financial institutions

By SETH N. STRATTON

A July 2012 First Circuit decision is the second recent federal court decision appearing to impose what may be a heavier burden on banks to protect their customers from cyber thieves.

Seth N. Stratton

In *Patco Construction Co. v. Peoples United Bank*, 684 F.3d 197 (1st Cir. 2012), the court addressed whether a bank's security measures to protect customers from online threats were "commercially reasonable." In finding that they were not, the First Circuit is creating a trend on the heels of a 2011 decision by the Eastern District of Michigan in *Experi-Metal Inc. v. Comerica Bank*, No. 09-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011), which held that a bank's conduct in a similar circumstances failed to meet the "good faith" standard.

The "commercially reasonable" and "good faith" standards derive from Article 4A of the Uniform Commercial Code. Article 4A was created to address fund transfers between businesses and their financial institutions. A bank receiving a payment order from one of its customers for a funds transfer bears the risk of loss if that the payment order was not authorized by the customer. The bank, however, may shift the risk of loss to the customer for a payment order not authorized by the customer by (1) using a commercially reasonable security procedure to verify that the payment order was authorized and, (2) upon proof that it accepted a payment order in compliance with such security procedure and in good faith. See UCC § 4A-202. Many banks, understandably, seek to shift that risk.

Patco Construction Case

Patco involved a cyber attack on Patco Construction Company's accounts at Ocean Bank (a community bank in Maine which was then a division of People's United Bank). Patco's computers were allegedly infected with a virus that kept track of responses to online banking security challenge questions. Hackers used this information to access Patco's accounts online and make six wire transfers in seven days totaling $588,851. Though the bank's security program detected all of the withdrawals as "high risk" due to the timing, amounts and geographic locations of the transferees, the bank did not take immediate action nor notify the customer. The bank was ultimately able to block or recover about $243,407, but $345,444,43 was lost.

The agreement Patco entered into with Ocean Bank provided that use of the ebanking password "constitutes authentication of all transactions performed by you or on your behalf." Ocean Bank did not assume any responsibilities under the agreement and use was at Patco's risk. Ocean Bank was liable only for its gross negligence, limited to six months of fees. To protect its customers, the bank utilized a "Premium" security package offered by its service provider, which included six key features: (1) user identification and a password to login; (2) "cookies" to flag low-risk computers; (3) score-based risk profiling; (4) three user-selected challenge questions to verify users; (5) automatic asking of challenge questions when a transaction met a certain dollar threshold; and (6) comparison of transaction characteristics, such as IP address, to those of known fraud to restrict access from suspect computers.

The withdrawals at issue triggered many flags, including the use of a non-authenticated device, high-risk dollar amount, an IP address anomaly and a "risk score distributor per cookie age." The bank's security program thus deemed the transactions as "very high-risk." Unfortunately, however, the bank did not monitor the transactions or the risk ratings and Patco was not notified of the high-risk transfers until six days later.

The court addressed whether, under these circumstances, Ocean Bank's conduct was "commercially reasonable" under UCC Article 4A. (The parties disputed whether Maine or Connecticut law applies. The court noted, however, that both states have adopted Article 4A and, thus, the result would be the same under either state's law.) The court found that the bank's security procedures were not commercially reasonable. This was not due to the failure of one specific security measure, but rather, "collective failures" by the bank.

The court highlighted as a crucial failure the bank's lowering of the dollar amount threshold triggering the challenge questions from $100,000 to $1, thereby triggering such questions on every transfer and dramatically increasing the chances that answers to challenge questions could be

Attorney Seth Stratton is a member of Fitzgerald Attorneys At Law P.C., where his litigation practice focuses on corporate, commercial and personal disputes, including bank litigation, zoning and land use litigation,insurance coverage disputes, commercial collection actions, and state and federal appeals. Fitzgerald Attorneys at Law maintains offices in Hartford and East Longmeadow, Mass.

detected by keylogging malware prior to being discovered. The court also appeared troubled by the bank's lack of monitoring when other risk factors were triggered. Even though the bank's security system flagged each transaction as a very high risk, nothing was done with this information. Finally, the court criticized the bank's use of a "one-size-fits-all" approach to security procedures, explaining that the bank should have tailored its procedures more specifically to its individual customers — for instance, by monitoring the account when unusually high risk transfers were made — as required by Article 4A.

Experi-Metal Inc. Case

Experi-Metal involved a phishing attack that resulted in unauthorized wire transfers through Experi-Metal's online banking accounts, of which $560,000 could not be recovered. Experi-Metal brought suit in federal court in the Eastern District of Michigan against its bank, Comerica Bank, to recover its losses under Article 4A. Here, the court, unlike in *Patco,* found it undisputed that Comerica's security measures were commercially reasonable, but found the acceptance of payment orders was not in good faith.

The cyber thieves' approach in this case was different than in *Patco.* Comerica employed a "secure token technology" for its online accounts. An Experi-Metal employee opened a phishing e-mail containing a link to a Web page purporting to be a "Comerica Business Connect Customer Form." Following the e-mail's link, the employee provided his security token identification, WebID and login information to a phony site. Cyber thieves then used this information to gain access to Experi-Metal's accounts.

In roughly six hours, 93 fraudulent transfers were made totaling $1,901,269. The majority of the transfers were directed to bank accounts in Russia, Estonia and China. A vigilant JP Morgan Chase employee noticed the suspicious wires to Moscow and alerted Comerica. Comerica succeeded in recovering only a portion of the transfers.

Among other issues, the court considered whether Comerica acted in "good faith" in accepting the orders on Experi-Metal's account. Experi-Metal argued, supported by expert testimony, that Comerica should have engaged in fraud scoring and screening to immediately stop transactions triggering certain risk factors. The court, however, stopped short of holding that Comerica was required to engage in active fraud monitoring for its security procedures to be deemed commercially reasonable.

Nonetheless, the court held that, even if the security procedures themselves were commercially reasonable, the bank must still bear the burden of proving that it accepted wire transfer payment orders in good faith under Article 4A. The court explained that the good faith requirement was an objective rather than subjective inquiry could not be met by the "pure heart and empty head" standard.

The court highlighted several factual considerations: (1) the high volume and frequency of the payment orders and related book transfers to fund such orders; (2) a $5 million overdraft created by those book transfers in what was otherwise a zero balance account; (3) Experi-Metal's limited prior wire activity; (4) the destinations and beneficiaries of the funds; and (5) the fact that Comerica was aware of and had even issued client alerts on prior and current phishing activities.

Banks blindly relying on customer agreements to put the risk on the customer will likely be rejected under the 'pure heart and empty head' standard.

The court concluded that it was "inclined to find that a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier" and that Comerica failed to satisfy its burden to present evidence to the contrary.

Lessons For Banks

- *Experi-metal* supports the position that risk scoring, active monitoring and notification are not per se required. But *Patco* cautions banks that do have risk scoring capability not to sit on the information, but rather act upon it, if customers are at risk.
- Active monitoring and immediate customer notification of uncharacteristic transactions make it more likely that a court will deem a bank's security procedures to be reasonable and its responsive conduct to be in good faith.
- Security procedures and responses to fraud should be tailored to each customer, rather than a "one-size-fits-all" solution.
- Blindly relying on customer agreements to put the risk on the customer will likely be rejected under the "pure heart and empty head" standard.

Lessons For Businesses

- The First Circuit left open for review on remand the responsibility of *Patco* to mitigate potential losses, noting that Article 4A is not a "one-way street." Thus, a bank's commercial customers may have some mitigation responsibility, even when a bank's security system is found to be commercially unreasonable.
- In *Patco,* shortly after the fraudulent transfers, Patco hired an IT consultant who ran anti-malware scans, quarantined and then deleted suspect malware. Ocean Bank argued that this made it impossible to determine if the type of keylogging malware that would have intercepted authentication credentials was present. The court noted that, on remand, this dispute "may be material." Thus, businesses that are subject to cyber attacks should be careful to preserve evidence that may be needed to prove a subsequent claim under Article 4A.

Lessons for Litigators

- Courts following the *Patco* and *Experi-Metal* precedents will likely require a similar factual inquiries and banks will be hard-pressed to resolve suits through dispositive motion practice. This, in turn, gives commercial customers leverage when bringing such suits.
- The courts in both *Patco* and *Experi-Metal* focused on the fact that each bank was aware of the risk based on past incidents. Lawyers representing either party should be cognizant of and prepared to address this important factual consideration.
- In *Experi-Metal,* the court rejected as unqualified Comerica's expert's opinion on reasonable commercial standards of fair dealing in responding to phishing attacks due to his "lack of experience as a banker with Internet banking systems, specifically online wire transfer activity and 'phishing' issues." Effective litigation experts must, therefore, keep pace with ever-changing online banking technology and security, as well as the evolving cyber threats seeking to infiltrate customer accounts. ■