July 13, 2012

Court Rules Bank's Security Procedures Were Not Commercially Reasonable

In an important decision last week, the U.S. Court of Appeals for the First Circuit held, as a matter of law, that a Maine-based bank's online banking security procedures were not commercially reasonable, even though its selected authentication technology fully complied with the Federal Financial Institutions Examination Council (FFIEC) guidelines for Authentication in an Internet Banking Environment.[1] A detailed review of this cautionary case offers some useful lessons for all financial institutions that offer online services to retail or corporate customers. In *Patco Construction Company v. People's United Bank,*[2] Patco Construction Co. (Patco) brought suit alleging that People's United Bank should bear the loss resulting from fraudulent withdrawals totaling almost $350,000[3] from Patco's electronic banking account at Ocean Bank, a southern Maine community bank that was acquired by People's United Bank. After the district court granted summary judgment in favor of the bank on the basis that the bank's security procedures were commercially reasonable, the First Circuit reversed the district court's decision and allowed the lawsuit to continue, finding that the Maine bank's security procedures were, as a matter of law, not commercially reasonable. The principal underlying message of the court's holding in *Patco* is that in order for a bank to avoid, or at least minimize, its liability arising from fraudulent transactions initiated through online banking systems, the bank should do the following:

- Establish security procedures which comport with applicable regulatory guidelines, currently the FFIEC guidelines for Authentication in an Internet Banking Environment.
- Ensure the security procedures offer choices to its customers.
- Ensure its customers are fully aware of the choices of security procedures.
- Enter into Electronic Banking Agreements with customers that require customers to agree to be bound by any payment order that is issued in the customer's name, whether or not authorized by the customer, if the payment order is accepted by the bank in compliance with the customer's chosen security procedure.
- Follow all established security procedures in good faith, including carefully reviewing and responding to all alerts generated by installed security monitoring systems regarding suspicious activity.

FFIEC Guidelines The current FFIEC guidelines recommend the use of multifactor authentication with business customers. These are some possible authentication factors:

- Something a user knows-- password or personal identification number.
- Something a user has-- physical device such as a password-generating security token, USB security token or smartcard.
- Something a user is - biometric characteristic such as a fingerprint, voice pattern, iris configuration or facial structure.[4]

FFIEC guidelines also recommend layered security programs that use different controls at different points in a transaction process so that a weakness in one control may be compensated for by the strength of a different control. Effective controls in a layered security program may include the following (FFIEC strongly encourages banks to use the first two controls):

- Detect and respond to suspicious activity-- Processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to (i) the initial login and authentication of customers and (ii) the initiation of electronic transactions involving transfers of funds to third parties.
- Control of administrative functions-- Security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations or limitations. Enhanced controls could include an additional authentication routine or transaction verification routine prior to implementation of the access or application changes, such as out-of-band authentication, verification or altering.
- Dual customer authorization through different access devices.
- Out-of-band verification for transactions (e.g., telephone or email verifications for Internet-based transactions).
- Enhanced controls over account activities such as transaction value thresholds, payment receipts and number of daily/weekly transactions.
- Internet protocol (IP) reputation-based tools that block connections from IP addresses known or suspected to be associated with fraudulent activities.[5]

The FFIEC guidelines also indicate that it is the expectation that "financial institutions should perform periodic risk assessments considering new and evolving threats to online accounts and adjust their customer authentication, layered security and other controls as appropriate in response to identified attacks."[6] These periodic risk assessments should be performed "as new information becomes available, prior to implementing new electronic financial services, or at least every twelve months."[7] **UCC Article 4A** Under Uniform Commercial Code Article 4A, if a bank and customer have agreed to use a security procedure, a payment order received by a bank is effective as an order of the customer, whether or not authorized by the customer, if (i) the security procedure is commercially reasonable and (ii) the bank accepted the payment order in good faith and in compliance with the security procedure.[8] Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank; the circumstances of the customer known to the bank, including the size, type and frequency of payment orders normally issued by the customer to the bank; alternative security procedures offered to the customer; and security procedures in general use by customers and banks that are similarly situated. A security procedure is deemed to be commercially reasonable if: (i)The security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer; and (ii) The customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.[9] **Lessons from *Patco*** In order to avoid or minimize bank liability resulting from fraudulent electronic transactions from customer accounts, banks should:

- **Establish security procedures** - Establish customer security procedures that include multifactor authentication and a layered security program that, at a minimum, includes the ability for the bank to detect and respond to suspicious activity and establishes enhanced controls for customer administrators.

- **Offer customers choices** - Offer to its customers, and make sure the customers are fully aware of, choices of security procedures such as dual customer authorizations through different access devices, out-of-band verifications of transactions and customer specific account limitations.
- **Execute customer agreements** - Enter into Electronic Banking Agreements with customers that require customers to agree to be bound by any payment order that is issued in the customer's name, whether or not authorized by the customer, if the payment order is accepted by the bank in compliance with the customer's chosen security procedure.
- **Follow security procedures** - Follow the customer's accepted security procedures in good faith when processing electronic payment orders.
- **Implement transaction monitoring systems** - Implement tools that can detect anomalies and establish policies and procedures to ensure effective monitoring and responses to each alert. As noted in the *Patco* case, it is not sufficient simply to install monitoring systems. Financial institutions must assign sufficient staff resources to review and respond to each alert and effectuate out-of-band verification of suspicious transactions, as appropriate, via telephone or e-mail or otherwise.

As your institution prepares to conduct its next periodic risk assessments of online banking systems, we encourage you to review the lessons of the *Patco* case and, at a minimum, ensure that your processes, procedures and systems comply with the above recommendations. Our lawyers have significant experience advising clients regarding the design and implementation of security policies, procedures and systems that conform to regulatory guidelines and reduce the likelihood of finding of civil liability in favor of your customers. If you have any questions concerning the *Patco* case or would like assistance in preparing for your next periodic risk assessment, please contact any of the lawyers listed in this alert.

---

[1] *Patco Construction. Company. v. People's United Bank*, 2012 U.S. App. Lexis 13617 (1st Cir. Me. July 3, 2012). [2] Id. [3] In May 2009, there were fraudulent withdrawals totaling $588,851.26 from Patco's account, of which $243,406.83 was recovered or blocked, leaving a loss of $345,444.43. [4] Federal Financial Institutions Examination Council, Authentication in an Internet Banking Environment, pg. 3. [5] Federal Financial Institutions Examination Council, Supplement to Authentication in an Internet Banking Environment, pg. 4-5. [6] Id. at 1. [7] Id. at 3, citing FFIEC IT Examination Handbook, Information Security Booklet, July 2006, Key Risk Assessment Practice section. [8] U.C.C. 4-202(b). [9] U.C.C. 4-202(c).