Commercial Financial Services Brief: Internet Banking - Is Your Bank Protected Against Liability for Unauthorized ACH Transfers?

July 12, 2012

In its recent decision in *Patco Construction Company v. People's United Bank*, the U.S. Court of Appeals for the First Circuit raised the stakes for those banks offering internet-based ACH fund transfer services. Patco, a small property development business, maintained an account with People's United Bank which was accessible by means of internet banking services. Patco used the internet banking system primarily for purposes of making weekly payroll payments. These payments shared certain characteristics, including that they were all made on the same day of the week and originated from a single IP address.

Over a period of a week a series of fraudulent withdrawals occurred from Patco's account by means of the bank's internet banking system. The perpetrators used the proper credentials of one of Patco's employees to access the internet banking system, including the employee's ID, password and answers to challenge questions. The login occurred from an unrecognized device and from an IP address never used by Patco. The bank's security system flagged the first transfer as a "high risk" transaction.

Over the course of the week, seven fraudulent transfers were made in a total amount of over $588,000.00. Patco was not notified of the warnings about these transfers and it appears that no one at the bank was monitoring these high risk transactions. The scheme unraveled because portions of the transfers were returned to the bank because some of the account numbers to which the money was sent were invalid. As a result, the bank sent a notice by U.S. Mail to one of Patco's principals regarding the return of a portion of the transfers. The first written notice was received one week after the first fraudulent transfer was made.

The internet banking agreement between Patco and the bank provided, among other things, that the use of Patco's password constituted authentication for all transactions and that the bank did not assume any responsibility related to Patco's use of the internet banking system. Patco sued the bank to recover its losses and the bank asserted a number of defenses to the claims, including defenses under Article 4A of the UCC. Under Article 4A, a bank receiving a payment order bears the risk of loss for any unauthorized funds transfer unless the risk of loss is shifted to the account holder by either (1) the bank showing that the payment order was actually initiated by a duly authorized person, or (2) the bank and its customer (a) have agreed that the payment order will be verified pursuant to a security procedure, (b) the security procedure is

a commercially reasonable method of providing security against unauthorized payment orders and (c) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure, the written agreement or an instruction of the customer restricting acceptance of payment orders consistent with the written agreement.

The issue of commercial reasonableness is determined by the courts. Whether a system is commercially reasonable is not based on whether the system is the best available but rather on whether it is reasonable for a particular customer based on factors that include the wishes of the customer expressed to the bank, the types of transfers (size, type, frequency, etc.) normally issued by the customer and security procedures in general use by customers and banks that are similarly situated. A security procedure may also be deemed commercially reasonable if the procedure was chosen by the bank's customer (and the bank's customer refused a procedure that was commercially reasonable) and the customer agreed in writing to be bound by payment orders issued in compliance with the procedure chosen by the customer.

The Court found that the bank's security procedure was not commercially reasonable for a number of reasons, including:

- The bank required the customer to answer challenge questions for every transaction over $1.00, thereby increasing the number of times the customer had to type that information (and make it potentially available to malware), particularly when the customer engaged in regular, high dollar amount transfers. The Court went on to note that security experts warned against the regular and frequent use of challenge questions because of the risks posed by malware of having the answers intercepted.
- The bank failed to monitor the warnings issued by its security system.
- The bank failed to notify its customer regarding the security warnings.
- The bank's security procedure failed to take into account the specific circumstances of the customer.

The Court viewed these failures as a whole (in other words, any one of them was not determinative) in reaching its conclusion that the bank's security procedure was not commercially reasonable. The Court's decision did not reach the issue of whether the customer might still have some liability for the unauthorized transfers. The Court noted that Article 4A is not a one way street imposing liability on the bank. For example, the customer still has obligations to exercise reasonable care to discover and report unauthorized transactions within a reasonable time. It is also important to note that Article 4A does not apply to consumer electronic transfers, which are subject to Regulation E and the Electronic Funds Transfer Act.

What lessons should a bank take from this decision?

1. Make sure the security procedures fit the customer. Understand the customer's business, the typical amounts of transfers, where they are originated, and how often they will be made. One size does not fit all.

2. Have someone assigned to monitor warnings from your security system on a daily basis.
3. Notify your customer when a warning is generated by the security system. This should be done by the most expeditious method feasible. U.S. Mail will typically not be sufficient for these purposes. Email, fax or telephone are the preferred methods. Your agreement with your customer should specify what notice is acceptable in these circumstances.
4. Stay up to date. Pay ongoing attention to developments in the industry and the risks associated with specific policies. What may be a best practice today may not be tomorrow.
5. Make sure your internet banking agreement and procedures comply with the requirements of Article 4A in order to shift liability to the customer.
6. Training, training, training! Make sure your staff are properly trained on appropriate security procedures.