Customer Initiated ACH Transactions

By: Mike Hogan, EVP
U.S. Risk Financial Services

Bank regulatory authorities over the past twenty years have reinforced their concerns related to Customer Initiated ACH Transactions. As a result of regulatory pressure and adverse experience, bank management has become keenly aware of the potential credit risk exposure involved with these transactions.

Payroll fraud, kiting - these are among the latest threats to Automated Clearing House (ACH) payments, which are gaining extra attention from fraudsters.

- There will be 25 billion ACH transactions occurring annually by 2010, estimates NACHA, the electronics payment association. Many of these transactions will be check conversions at merchants, including Wal-Mart, Target and large supermarket chains.
- With these numbers growing every year, ACH fraud is also growing.

How ACH Fraud Happens

- Before ACH did check conversion, there was very little fraud, because most transactions were driven by relationship. Historically, a corporation had to get an individual's permission to credit, much less debit their account. Typically, banks knew the corporation involved, and knew they could depend on the corporation to stand behind its transactions if a debit or credit came into question.
- On the business side, the companies that were using ACH would set up accounts that would only accept ACH credits or issue them.
- As ACH has expanded past the payroll, social security payment or repetitive bill-pay solutions, transactions now include almost any kind of payment and check replacement truncation – and, in the process, the risk of fraud has grown.
- Today, these transactions may include point of sale or on the web or over the phone. In the process banks have lost the control that used to exist. For example: banks used to have control of the size of transaction a business can make and how much coverage it has to have over the two-day period it took for that transaction to settle.
- By the time the customers receive information on these transactions and protest the withdrawal, the bank is stuck with all the returns, because the perpetrator of the fraud has withdrawn all the money and left.

ACH Risk #1: Payroll Fraud

- A more recent type of ACH fraud is a combination of ACH fraud and what they refer to as "hacking or social engineering".
- Traditionally in the ACH process, a bank would set up a business to do its payroll through ACH, say, on the 13th and 28th of the month. The commercial customer would bring their tape to the bank that would run the tape on its machine, check that the nature and that amount of the check was proper.

The bank would call back and verify the amounts with the company before it released the payroll. The procedures were agreed upon, and the parties knew what was going to happen on a specific date and the specific amount involved.

- Financial institutions are doing all of this over the Internet in spite of the fact that banks do not have the same levels of control over these processes that they previously had.

- Scam artists are coming in through a firewall, with a stolen account numbers and passwords and are pretending to be that customer. They come in through an ACH account and clean it out. So instead of paying out the payroll, the payroll goes to the conman.

- Many banks are simply going back to the old way. Even though these transactions are coming through the Internet, it is prudent for the bankers to pick up the phone and call the customer to the verify authenticity of the transaction.

- ACH kiting is similar to check kiting and is an unusual kind of fraud. Experience show that when an ACH kiting happens, the losses can be substantial.

- The recommended resolution is, to focus on the procedures and monitor debit returns over a period of time. More sophisticated institutions will set up exposure limits for new customers, and set limits on single-day transactions. This way the bank limits its exposure to ACH kiting, and monitoring the new customer until the institution builds a credible history with the customer.

- The bank should monitor new accounts for at least three months, many banks monitor for six months. This is a credit product, and as such, banks should do their due diligence up front through their loan officer. The less sophisticated institutions see this as a deposit product and are more likely to get hit with fraud.

Who's at Risk?

- Larger institutions are getting hit with ACH fraud because they have more complex internet ACH transaction mechanisms in place and have done away with "call-backs" and manual controls. They also typically have much higher volumes.

- The ACH fraud is hitting regional and super regional banks. Many of them are restoring those manual controls (call-backs) rather than putting an automatic callback on every ACH transaction over a specified amount. The bank should look at whether the ACH transaction was scheduled. Most of them are, such as payroll payouts or regular outgoing debits go on schedules and most are for similar amounts and won't vary widely.

More Security, Monitoring Needed

- We agree with fraud experts that see the need for further tightening in security for online banking, including strong multi-factor authentication. Many ACH providers have built improvements into their systems, including methods for positive payer and payee capabilities, including check processing for corporations. In that manner, if a check gets converted to an ACH transaction, the corporation has not lost the opportunity for positive pay and payee. If something doesn't match when the bank is processing, the bank should stop the transaction and bring it to the attention of management of the commercial account.

- Unless an institution has miniscule volumes of ACH transactions, it needs to have some form of automated monitoring of transactions in order to evaluate what is originating out of the institution. The due diligence involved should include a set of criteria of the characteristics of who they'll do business with.

- Another area for financial institutions to improve their fraud detection and monitoring is the centralization of fraud prevention across all payment systems. This will result in less fraud, no matter what the payment mechanism is. Consistency of these checks and balances across all these systems would result in a higher level of detection and fraud prevention.

- If an institution has filters and ways to detect and monitor behaviors that may be suspicious, and share that information across ACH, wire transfers, checks and credit cards, as well as ATM activity, they will have a much better overall understanding of the potential for fraud, and know which individuals to pinpoint and worry about. Banks using this type of information across all activities will greatly improve their ability to fight fraud and improve regulatory compliance.

Financial institutions can help control credit risk by establishing or using existing credit ratings for all of their customers. Credit ratings provide a concise, comprehensive review of the credit risk aspects of the relationship and are used extensively in credit approval and monitoring systems. Credit ratings assist the institution in assigning credit (exposure) limits for its ACH originating customers. A dollar limit is assigned to each transaction or total file, which the bank monitors and that represents the total exposure that the financial institution wishes to accept for a particular customer.