Payment Protocols

Managing your community bank's ACH and demand draft risk

By George F. Thomas

Would anyone in their right mind attempt to drive a car blindfolded? Well, the answer would be an emphatic "No" because of the dire consequences. So, why do so many banks operate their ACH and check systems completely in the dark? Surely the potential consequences of such actions could be just as dire.

Bank regulators have introduced ACH risk management reviews as key components of their examination procedures because the newer types of ACH payments have increased risk to banks and the entire ACH network. The newest forms of ACH transactions include Internet authorized payments, debits authorized over the telephone, check-to-ACH conversions at the point-of-sale or the lockbox, and the latest product back-office conversion. Besides the ACH, the payment instrument of choice for fraudulent and illegal activity is now the remotely created check or demand draft.

While the newer ACH transaction types and the use of demand drafts created the opportunity for increased risk, the risk was actually introduced by the poor due diligence practices of banks for Know Your Customer and in the case of merchant payment processors, the absence of any procedures required by the bank for Know Your Customers' Customers.

The Office of the Comptroller of the Currency was the first to focus on ACH risk with the issuance of its OCC Bulletin 2006-39 that provided guidance for ACH Risk Management. Last year, the OCC followed up with another bulletin OCC 2008-12 that provided risk management guidance for banks that deal with payment processors. The main focus of this bulletin was due diligence, underwriting and monitoring of entities that process payments for telemarketers and other merchant clients.

The FDIC issued its Financial Institution Letter titled "Guidance on Payment Processor Relationships" on Nov. 10, 2008. The letter points out the risks that banks face when dealing with payment processors and outlines steps to mitigate that risk. The following excerpt highlights the need for effective due diligence:

> "Due diligence and effective underwriting are critical for an effective risk management program. Financial institutions should implement policies and procedures to reduce the likelihood of establishing or maintaining an inappropriate relationship with a payment processor through which unscrupulous merchants can access customers' deposit accounts."

Community banks should expect to see increased regulatory scrutiny on their activities in the origination of ACH debit transactions and the origination of demand drafts (remotely

created checks) whether they are initiated as paper deposits or deposited as images with remote deposit capture.

The Proactive Tool

Many community banks have adequate due diligence procedures for all of their direct customers, some might not. The majority of originating banks working with third-party payment processors have no idea of the business nature of the transactions that are being submitted by those third-party payment processors. These banks view the third-party payment processor as their customer and not the merchants that are the customers of the third-party payment processor. It gets worse and more complex when there is a nesting of third-party payment processors.

The primary third-party payment processor that has the relationship with the originating bank in many cases has no idea of the nature of the transactions being submitted by the nested third-party payment processors. To make matters worse, some financial institutions allow the third-party payment processors to originate transactions directly into the ACH or check clearing systems; the originating financial institution does not even see the transactions and has no idea of what is taking place.

Since the check clearing and ACH payment systems can't stop unlawful debit transactions once they are entered into the system, it is imperative that they be stopped before they are entered into the system. The vast majority of the illegal and fraudulent transactions are initiated using debit transactions through the ACH or demand drafts through the check collection system. The only way to prevent illegal or fraudulent transactions is to shore up the due diligence procedures.

Community banks know their customers and their customers' customers. However, as part of knowing their customers' customers, banks should require that more stringent due diligence procedures be employed by third-party payment processors and have procedures in place themselves to verify this before transactions are entered into the payment systems.

Clearly, due diligence is the first and only proactive defense available to prevent the illegal or fraudulent use of ACH debits or demand drafts. The following recommended procedures should be put into practice to ensure an adequate Know Your Customers program for dealing with direct customers and Know Your Customers' Customers when dealing with the third-party payment processors:

Know Your Customer

1. Obtain the merchant's:
    - name (including all "doing business as" names),
    - Address, phone number,
    - Type of business or principal business activity,

- taxpayer ID number, principals' names, principals' addresses, principals' phone numbers, principals' taxpayer ID numbers, geographic location, Web site address, and sales history;
- Visit the business location

2. Conduct a background check of the merchant and its principals by, at a minimum, doing the following:
   - Reviewing the merchant's Web site, advertising, products and services;
   - Cross-checking the merchant's provided information;
   - Verifying the information provided by the merchant with external agencies having the ability and expertise to provide such verification (such as the Better Business Bureau or Dunn & Bradstreet.); and,
   - Validating the taxpayer ID numbers through income tax filings, incorporation documents, business papers or bank account information.

3. Review the merchant's sales history;
4. List permissible payment types including standard entry class codes**,** if applicable; and standard industrial codes
5. Use a unique company identifier for each merchant or third party payment processor and including the name of each merchant or third-party processor (for example, no acronyms, abbreviations or telephone numbers) for all transactions submitted for processing;
6. Outline merchant termination procedures

Know Your Customers' Customers

1. Require each third-party payment processor with which it does business *by agreement* to:
   - Identify each of the merchants for which the third-party payment processor would be originating transactions and provide the name of the company, address, type of business, telephone numbers and principals to the bank at least semi-annually;
   - Perform due diligence procedures described above for each direct merchant that the third-party payment processor processes for;
   - Identify all nested third-party payment processors that each third-party payment processor does business with;
   - For the nested third-party processors, require by agreement that each identify all merchants for which they process for and provide the same due diligence as listed for a direct merchant.

2. Require that all parties using the ACH processing system be bound by the National Automated Clearing House Association rules and that all transactions will be in compliance with all state and federal laws.

3. Require that each third-party payment processor cease origination services for any merchants or third-party payment processors that violate or do not meet the due diligence procedures of the third-party payment processor;
    - Terminate merchants and nested third-party payment processors that fail to:
        - Provide accurate merchant information;
        - Notify the third-party payment processor/bank of new merchants, independent sales organizations or other nested third-party payment processors;
        - Terminate merchants that engage in activity that violates state or federal laws;
        - Terminate merchants tha**t** switch ACH activity to demand drafts once notified of the problem; or
        - Terminate merchants that offer demand drafts to avoid ACH return scrutiny
4. Perform the following verification procedures at least semi-annually:
    - Review merchant listings provided by third party payment processors;
    - Review company names and type of business for consistency; and
    - Perform background checks on a random sample of merchants supplied by each third-party processor**.**

The consequences for a bank of failing to do proper due diligence or ensuring that payment processors that the bank has taken on as a customer fail to perform proper due diligence can be quite severe and may include some or all of the following:

- Subpoenas by law enforcement;
- Meeting the requirements of Assurances of Discontinuance;
- Adverse publicity;
- Fines by regulators;
- Fines by law enforcement;
- Regulatory scrutiny;
- Loss of reputation; or
- Financial loss.

The Reactive Tool

While due diligence is an absolute necessity, community banks should consider using automated risk management monitoring systems to ensure that their customers and the customers of third-party payment processors continue to meet their obligations. If your community bank originates ACH transactions or accepts demand draft deposits, it should not operate its check and ACH operations blindfolded. If it is relying solely on its ACH origination software or has not automated its check processing system to analyze patterns of unacceptable returns, then your institution could be at risk of transaction fraud.

The onus is not only on banks that originate transactions. Receiving banks should have automated systems in place to detect unusual patterns of transactions to minimize the risks of fraudulent transactions against their customers' deposit accounts.

The cost for low- to medium-range service offerings such as a Software as a Service model can be acquired for a one-time set-up fee of approximately $10,000 with an annual usage charge starting at $6,000 annually. The size of the fee depends on transaction volume. Enterprise based software models can range from $40,000 to $100,000 with an annual maintenance fee of 10 percent to 20 percent of the initial licensing fee cost.

Products are in the market that can analyze all of a community bank's incoming and outgoing ACH transactions and provide proactive alerts that will do the following:

- Form an essential component of a comprehensive risk management program that will meet the requirements of internal and external audit as well as banking regulators;
- Establish limits for originators for the gross value of debit and credit transactions, gross limits by standard entry class and limits on returns;
- Analyze debit transactions to determine the amount your financial institution should keep in reserve;
- Detect violations of NACHA rules such as an originator not responding to notifications of change, using acronyms or telephone numbers in the company name field or excessive resubmissions of items that were previously returned.;
- Provide case management support to resolve problems and report NACHA rules violations;
- Focus appropriate attention on unauthorized and invalid account returns which can be used to detect fraudulent activity and rogue originators;
- Use threshold analysis to detect unusual return activity based on percentages or gross limits on the number of acceptable returns over a period of time (for a day, week or month)
- Track returns to forward items to quantify risk exposure by originator for a given period of time;
- Detect suspicious pattern alerts for excessive transactions against a consumer or corporate account that could potentially be fraudulent;
- Provide special emphasis on corporate unauthorized returns that were originated using consumer standard entry class codes;
- Analyze returns based on standard entry class codes.

While there are a limited number of companies that offer automated ACH transaction monitoring solutions, to my knowledge, there are no solutions on the market to automate the process of tracking demand drafts.

Risk management is essential to protect the integrity of the ACH and check clearing networks; it is a bank's responsibility to do everything in its power to ensure that illegal and fraudulent transactions do not enter the payments systems. Proactive steps must be

taken to monitor your community bank's payment activity to detect and eliminate fraudulent and illegal behavior as quickly as possible. Payment system risk management is of great interest to the regulatory agencies, and rest assured that this will be an area of focus on your community bank's next regulatory examination.

George F. Thomas is president and CEO of Radix Consulting Corp., an electronic payment consulting firm in Oakdale, N.Y. The company specializes in risk management, business-to-business payments, check conversion and account to account payments. Reach him at gfthomas@radixconsulting.com or (917) 923-9319.