Not Your Father's ACH

By George F. Thomas

The Automated Clearing House (ACH) offers a fast, inexpensive and reliable means of moving payments. It has also been a very safe payments mechanism for the past 30 years. As a result, recently introduced types of ACH payments have increased in volume by leaps and bounds, but have also significantly increased the risk to the entire 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 most recently implemented application—back-office conversion.

The Landscape

The greatest potential for risk is with Web, telephone and pre-authorized payment and deposit transactions, and remotely created demand drafts (cross-channel risk) that are being originated through third-party merchant processors. Based on return pattern tracking for these transaction types, it has become apparent that most of the questionable behavior has originated primarily with third-party merchant processors.

When dealing with non-traditional ACH origination through a third-party merchant processor, what might appear on the surface as a very lucrative business opportunity could put your institution at financial risk or in many cases, reputation risk, which can be more damaging. And that is exactly what will result from dealing either directly or indirectly with organizations that have deceptive marketing practices or that engage in illegal activities (for example, Internet gambling and tobacco sales) or other questionable business practices.

If your community bank is engaged in, or contemplating the notion of, entering the non-traditional ACH origination business through a third-party merchant processor, then it is an absolute necessity that you have the right risk controls in place.

Most financial institutions employ their "Know Your Customer" procedures for direct customers including third-party merchant processors, but there is little or no discipline around such procedures for the customers of the third-party merchant processor which can include other third-party merchant processors, independent sales organizations and merchants.

Many of the merchants that use third-party processors do so because they could not pass the standard know-your-customer procedure if they approached your

financial institution directly. Like cockroaches, these merchants cannot withstand the light of scrutiny.

Dealing with Third Party Processors

A number of financial institutions have a policy that they will not do business with third-party merchant processors because of the risks. For financial institutions that choose to process ACH debit and demand draft transactions for third-party merchant processors it's imperative to follow sound 'Know Your Customer's Customers Procedures & Policies' (see related sidebar below). Banks need to be able to:

- Identify all merchants that the third-party merchant processor will originate transactions for using a set of predetermined information.
- Identify any other third-party merchant processors or independent sales organizations that may be originating transactions through them.
- Screen all merchant information supplied and perform basic due diligence on the merchant.

Once you've completed the above due diligence you can move to establishing standard policies and procedures for which failure to comply will result in termination of the business relationship. And don't do business with companies that have unsatisfactory records with the Better Business Bureau. This puts the burden on the merchant to clean up their record. Community banks should also:

- Require a unique merchant identifier based on the correct company name in the ACH transactions—no acronyms, abbreviations or telephone numbers.
- Identify any other third-parties or independent sales organizations doing business through the primary merchant processor with unique company identification numbers to provide better tracking.
- Request that the third-party merchant processor cease origination services for any merchants that violate or do not pass the due diligence procedures of the institution.
- Terminate third-party merchant processors who fail to:
  a. Provide accurate merchant information.
  b. Notify the bank of new merchants, independent sales organizations or other third-party processors.
  c. Terminate bad originators.
  d. Switch ACH activity to

more ...

Due Diligence Procedures

Many of the third-party merchant processors that have brought questionable and fraudulent originators to the ACH network are now moving from the larger institutions, and more and more of this activity is beginning to show up at community banks. The due diligence procedure must be an ongoing process and should include the following considerations:

1. **Identify all merchants that the third-party merchant processor will originate transactions for and include the following information:** company name, address, phone number, principals, type of business and any other "doing business as" names.
2. **Identify any other third-party merchant processors or independent sales organizations that may be originating transactions through them.**
   a. Identify all merchants or customers that those entities represent supplying all of the information listed above.
3. **Screen all merchant information supplied and perform basic due diligence on the merchant:**
   a. Screen companies for business types that the financial institution knows are illegal or would not be comfortable originating for (gambling, tobacco sales, telemarketing, pornography, etc.)
   b. Perform a Better Business Bureau (www.bbb.org) check for each origination customer. The process takes only seconds and will provide the bank the ability to double check information the business supplied.
   c. Direct merchants, with an unsatisfactory rating, to the risk or compliance function at your financial institution. All problem merchants identified by the network operators have had an unsatisfactory record. In most cases, that merchant would not have passed a bank's "know your customer" procedures if they applied directly.
      i. Risk managers can visit www.badbusinessbureau.com, http://www.consumeraffairs.com/search_page.htm, www.complaints.com for additional information and specific complaints about the company.
      ii. Check with ACH operators or NACHA for any prior history.

—George F. Thomas

demand drafts once notified of a problem.

e. Offer demand drafts to avoid ACH return scrutiny.

Monitoring return activity is critical for the financial institution: The return rates can supply an early notification that there are problems with the business practices of an originator that may have slipped through the initial screening process.

The Story's Moral

The originating depository financial institution (ODFI) is the gate keeper of the ACH Network. (Third-party merchant processors should never have direct access to the ACH.) The ODFI warrants that all debit activity is authorized and is financially liable for all activity that it brings to the system. These responsibilities include prohibiting illegal activity, making the participants financially whole for fraudulent activity, and ensuring that the poor and elderly are not taken advantage of by unscrupulous telemarketers.

While the financial rewards of doing this type of business may seem appealing on the surface, the risks are huge. Remember, you community bank is not protected by the 60-day return window for unauthorized transactions. It is at risk for at least two years or longer based on the breach of warranty timeframes for each state. If you cannot produce a valid authorization and the activity is fraudulent, your institution is on the hook for all the financial consequences and reputation risk that such activity will surely bring.

Remember the vast majority of originators are legitimate, but it is your job to ensure that the bad ones never initiate a transaction into the ACH network. ib

George F. Thomas is president and CEO of Radix Consulting Corp., a consulting firm in Oakdale, N.Y., specializing in electronic payments.