ACH Risk: Here and Now

Trends Underscore Improved ACH Risk Monitoring Need

Participation in the Automated Clearing House (ACH) network provides financial institutions with many significant opportunities. Compared to paper check processing, ACH offers numerous advantages including enhanced efficiency, reduced processing costs, clearly defined settlement times, control over payment timing, new revenue streams and increased customer retention.

With these opportunities, however, come risks.

Originating depository financial institutions (ODFIs) are responsible for settling payments originated into the system using their routing number(s) (RTN).

Although ACH transactions can help avoid some of the risks associated with other payment types, such as forgery or unintended destruction, ODFIs can gain from better understanding of their ACH risk exposure and strategies for mitigating that exposure. With effective monitoring, ODFIs can more securely participate in the ACH network.

Says Rich Oliver, Federal Reserve Bank of Atlanta executive vice president and Federal Reserve Retail Payments Office manager, "Risk mitigation in the ACH network is important to all participants and is consistent with the Federal Reserve Banks' mission and our role as the nation's largest ACH operator."

This paper supports the mission of Federal Reserve Banks to provide the nation with a safe, flexible and stable monetary and financial system by providing information on the topics outlined below.

- An overview of trends and factors driving the need to monitor, including the following:
  - Double-digit growth in ACH transaction and dollar volumes in recent years.
  - Outsourcing of ACH origination.
  - Emergence of new ACH payment types.
  - Reliance on manual, outdated systems for monitoring ACH risk at many institutions.
  - Relative inexperience and lax practices of some depository financial institutions (DFIs) within the ACH network.
- A discussion of the major categories of risk and the steps DFIs and others can take to help mitigate these risks. These categories include three primary risks:
  - Operational. The risk that a human error or computer mishap may delay or alter an ACH transaction.
  - Credit. The risk that an ACH originator may not have the necessary funds on the settlement date.
  - Fraud. The risk that dishonest or criminal attempts may be made to misappropriate funds.

Trends and Drivers

Fourth Quarter 2005 Results Signal Continued Rapid Growth

The ACH network was conceived in the early 1970s as a way to head off capacity constraints and inefficiencies associated with paper check processing. Transaction volume has grown at double-digit rates for the past 13 years[1] and – if 4Q 2005 results are an indication – show no sign of letting up any time soon.

According to the National Automated Clearing House Association (NACHA), the ACH network grew by 15 percent in 4Q 2005 compared to 4Q 2004. A total of 2.8 billion transactions, including 1.59 billion debits and 1.22 billion credits, were transmitted during 4Q 2005, representing more than $6.3 trillion.[2]

Expansion Contributes to System Risk and Complexity

The rise in ACH volume has been fueled in large part by a significant increase in the number and variety of institutions using the network, totaling more than 25,000 today.[3] With this expansion has come a more complex electronic payments industry that poses challenges to monitoring risk. For example, ODFIs may enter into agreements that grant service providers access to the ACH network through the

ODFI's RTN. That service provider may itself be originating payments for a number of other organizations. This is an acceptable practice, as long as it is done in accordance with *NACHA Operating Rules*, the proper controls are in place and the ODFI understands that it bears ultimate responsibility for the payments.

With new players and new business models increasingly being introduced into the system, the principle of "Know Your Customer" has never been more important. This is the case whether a DFI is processing payments directly for a customer or using a third-party processor to do so, or is providing access to the ACH network to a third-party originator through the DFI's RTN. Originating ACH payments that are not prefunded or collateralized can be viewed similarly to providing short-term, unsecured credit. Knowing the creditworthiness of the customer (and their customers, as applicable) helps ODFIs make better business decisions.

Emergence of New Payment Types Pose Unique Challenges

Payments originated over the Internet (WEB) represent the second-fastest-growing class of ACH transactions, trailing only Accounts Receivable Conversion (the process of converting checks into ACH debits). The WEB classification has been in use for just a few years and already represents nearly 10 percent of all ACH transaction volume,[4] encompassing all types of transactions: business-to-business (B2B), consumer-to-business (C2B), business-to-consumer (B2C), and peer-to-peer (P2P), the last which involves consumers exchanging funds among themselves.

This trend shows no sign of slowing down. Accounts at online payments processor, PayPal®, grew to more than 86 million in 2005, up from 40 million in 2003.[5] While PayPal helped to pioneer the P2P transaction category by enabling consumers to exchange funds electronically, the company has recently added services to make it more attractive to businesses both small and large.[6]

Although millions of Internet-initiated payments are successfully settled each day, the anonymity and global reach of the Internet should sensitize ODFIs to the unique risks of WEB payments. The WEB designation was created in order to address these risks, and WEB entries require additional security procedures and obligations. Despite these precautions, vulnerabilities exist and will be further explored in a subsequent section on fraud risk.

Another relatively new, fast-growing classification is telephone-initiated payments (TEL). TEL is designed to allow consumers to authorize one-time electronic debits to their accounts over the telephone to pay for goods or services, an example of a C2B transaction. Overall, TEL transactions increased 27 percent in 4Q 2005, over 4Q 2004, according to NACHA. With this payment type comes a unique set of risks to the ODFI, again discussed in a later section.

Generally speaking, WEB and TEL transactions may be more susceptible to returns than other payment classifications. According to Primary Payment Systems, Inc. – a private-sector provider of services to help mitigate losses associated with various types of financial risk – the banking industry may process more than $10 billion in WEB and TEL returns annually during the next several years.[8]

Financial Institutions in Various States of Preparedness for Addressing ACH Risk

While no comprehensive industry study has been conducted to identify the types of systems financial institutions have in place for monitoring ACH risk, smaller institutions may be most exposed. This notion is supported by a series of interviews regarding ACH risk that the Federal Reserve Banks conducted with financial institutions in 2004.

"Our discussions revealed that smaller institutions tend to monitor their risk using manual processes," notes Rich Oliver. "Even with the best of intentions, these methods may be subject to inconsistency and human error, exposing these institutions to operational risks and making them more susceptible to credit and fraud risk."

The situation may be attributable, in part, to the fact that the tools needed to help efficiently and cost-effectively monitor risk have been unavailable until recently.

Addressing the Different Types of ACH Risk

Offering ACH services can make good business sense. Mitigating risk exposure is essentially a balancing act between risk tolerance and desire to provide uninterrupted banking services. Financial institutions typically do not price ACH products to compensate for potential losses or the cost of elaborate or labor-intensive risk management systems.[9] This is another reason why it is critical to monitor risk in an automated and cost-efficient manner.

The first step toward more effectively monitoring risk exposure is understanding the different types of ACH risk and how they can affect institutions. In addition to the discussion below, NACHA's *ACH Risk Management Handbook* provides valuable risk management guidance.

Operational Risk

A variety of risks lie within the walls of every DFI. Operational risk can occur with a slip of a finger on the keyboard or the failure of a piece of hardware or software. It can come from ill-defined communications protocols and/or narrow decision windows. As a result, ACH processing may be interrupted or the timing altered.

To decrease operational risk and increase decision window times, it is important to be able to quickly identify and act upon anomalies at the customer level. Customer-level control enables ODFIs to monitor a specific batch within an ACH file without delaying the processing of the rest of the file.

Related to the ability to act quickly is the need for clearly defined communications protocols and an efficient notification system in the event of credit or debit cap breaches, or other issues that may impact the decision whether to release or reject an ACH batch. Because this is often both an operational and a business decision, ODFIs may want to include both payments/credit staff and customer-relations staff in the notification process.

Another method for improving an ODFI's decision making is having the ability to self-monitor ACH transactions. With access to information on demand throughout the day, ODFIs can address potential trouble spots as they arise.

Finally, in the event of a hardware, software or power failure, it is important to maintain access to ACH activity. Service support that uses Web-based technology affords access to authorized/credentialed personnel from virtually any computer terminal with an Internet connection.

In spring 2006, the Federal Reserve Banks will introduce the FedACH Risk℠ Origination Monitoring Service as the latest addition to FedACH® Services. This first-of-its-kind service in the ACH industry will provide ODFIs with enhanced control and flexibility to help monitor ACH risk in a highly efficient, consistent and cost-effective manner.

The Service will be accessed via the FedLine Web® or FedLine Advantage℠ access solution through FedACH Information Services (where DFIs see their settlement and file information). ODFIs can subscribe to both a FedLine® access solution and to FedACH Information Services to use the FedACH Risk Origination Monitoring Service.

This new service provides ODFIs with the ability to monitor ACH risk without purchasing additional ACH software and hardware. ODFIs subscribing to the service can enlist various criteria to monitor ACH risk:

- Set and control debit and credit caps in three ways:
  - ODFI RTN. Choose to compare a sum of all batches associated with a specific RTN to predefined caps.
  - Inclusive. Define and set caps for an inclusive list of company IDs associated with an RTN. This customization helps to prevent initiation of payments from originators not defined in advance. Batches with undefined company IDs can be pended rather than processed.
  - Select. Determine individual company IDs; set and monitor caps for each. Batches from undefined company IDs will be processed without review by the service. This feature affords the most refined control over monitoring criteria.
- Monitor accumulated credit and debit totals over a single processing day or across multiple exposure days. Monitoring across multiple exposure days allows specified debit and credit cap dollar limits to be compared to cumulative totals.
- Set end-of-day defaults to release or reject pended batches in extraordinary situations where batches remain pended at end of day.
- Restrict ACH origination to designated originators.
- Reject transactions at the batch level without holding up entire ACH files.
- Receive e-mail notification for up to three separate contacts when caps are exceeded.
- Specify one additional e-mail contact per company ID.
- Access for authorized/credentialed personnel to ACH monitoring information from virtually any Internet connection.
- Generate a current and next day summary report of monitoring criteria.
- Create a report listing "Management Criteria Event History," which details changes made to the monitoring criteria.
- Provide a reporting listing "Origination Monitoring Event History Information," which details batch monitoring information by the selection criteria of date, monitored batch status, SEC code, debit amount, credit amount and/or batch number.
- Monitor ACH risk as part of an integrated ACH and account management system.

Credit Risk

Credit risk-related losses typically arise from failure or bankruptcy of a company, or other circumstances where the originator may not have the necessary funds to honor a credit or debit transaction at the time of settlement.

When initiating ACH credit transactions, the ODFI is exposed to credit risk between the time it releases the originator's ACH batch until the funds are drawn from the originator's account, generally one or two business days after origination. Because *NACHA ACH Rules* do not allow reversal of ACH credits due to failure of the originator to have the necessary funds available at settlement time, the ODFI is financially responsible for payment of those credits for up to two days. For example, if a business originates an ACH payroll transaction (B2C) then – prior to the settlement date – closes its account or has its assets frozen, the ODFI must fund that payment, potentially resulting in a loss of the total amount.

When processing ACH debit transactions, common in B2C transactions for subscription services and mortgage payments, items settle one business day after the day of origination. As a result, ODFIs may make funds available to the originator for the total value of the file on the settlement date. Because payments may be subject to return, the ODFI experiences credit risk from the time it grants the originator credit for the total value of the batches, until the time frame for returns has expired. Like checks, ACH items can be returned for several reasons such as "insufficient funds," "account closed," "unauthorized transaction" and "payment stopped." The most common return reason is "insufficient funds."

In general, returns are due back to the ODFI by the opening of business on the day following the original settlement date. Consumer ACH debit items returned as "unauthorized" or "revoked authorization" must be returned within 60 days, which is the time frame established by the *NACHA ACH Rules*. When an ODFI receives a returned ACH debit, it will charge the item back to the originator's account. If the account is closed, has a negative balance or is frozen due to bankruptcy, the ODFI may suffer a loss for the amount of the returned payment.

The key to controlling credit risk is for the ODFI to know its customer. As a means of controlling credit risk, *NACHA ACH Rules* now require each ODFI to establish exposure limits for each of its corporate originators prior to the release of ACH credit and debit entries for that originator. The *NACHA ACH Rules* also require ODFIs to annually audit these limits.

The ability to place credit and debit caps on originators, systematically monitor their ACH activity and receive alerts when caps are exceeded are all effective methods for mitigating credit risk. Because ACH payments take one to two days to settle means that an ODFI may also want to monitor cumulative ACH totals across multiple exposure days for any given originator, in addition to the origination process day.

Fraud Risk

Fraud risk may result from DFI employees or DFI customers' employees attempting to embezzle money, from external sources gaining unauthorized access to the system, from identity theft or from businesses engaging in unscrupulous sales and marketing practices.

While any ACH transaction may be subject to fraud risk, much of the publicity has focused on WEB and TEL transactions.

The Internet enables criminals to test compromised information rapidly, cheaply and anonymously, enabling them to be more efficient in culling through stolen account numbers. A study by the Gartner Group, a provider of research and analysis on the global information technology industry, indicated that of 5,000 online adults, approximately 40 percent "think or are sure" they have been involved in a "phishing" attack (the practice of luring people to fraudulent Web sites designed to look like those of legitimate businesses for the purpose of stealing information).[10] Payments containing stolen account numbers may be originated into the ACH network via an unsuspecting ODFI, which could be responsible for the amounts returned should the fraudulent acts be identified.

In recent years, the telemarketing industry has come under scrutiny due, in part, to some unscrupulous companies and individuals using this medium for fraudulent gain. Some have abused TEL transactions to further their illegal causes.

Legitimate TEL transactions require that the originator have a written agreement with the consumer or that the consumer has purchased from the originator within the past two years. Where no prior relationship exists, outbound sales soliciting ACH payments are not allowed. The consumer must be the one to have initiated the call.[11]

There are several ways to reduce the risk of fraudulent activities perpetrated by a customer's employees. One method is to place specific limits on the dollar amount an originator is authorized to originate and systematically monitor those limits. Another method is to confirm control

totals with someone at the originator other than the person(s) who created and sent the batch(es).

DFIs can reduce the chance of fraudulent activities by ensuring that no single employee is responsible for the receipt, handling and transmission of batches. Separation of duties between the employee who originates the ACH payments and the employee who establishes host communications to transmit the payments to the ACH operator is key. Responsibilities should always be rotated among employees and all changes made to payments must be authorized by the customer and documented by employees. The implementation of sound personnel practices; maintenance of good physical security over computers, communications, and operations areas; and the implementation of stringent data security procedures are also ways to help control fraud risk.

While protecting against fraudulent ACH transactions may be difficult, a system that provides the flexibility to monitor all originators by company ID numbers and to pend batches associated with companies not authorized by the ODFI to originate can be a powerful tool against fraud.

The Federal Reserve Banks' Efforts to Help Mitigate ACH Risk

The Federal Reserve Banks have developed a suite of FedACH Risk Management Services to provide DFIs with tools to help mitigate ACH risk. The FedACH Risk Returns Reporting Service has been available to FedLine Web access solution Subscribers since October 2003. In spring 2006, the Federal Reserve Banks will introduce the FedACH Risk Origination Monitoring Service. Following this service, plans are to offer ACH risk management services for receiving DFIs.

The intent of the FedACH Risk Origination Monitoring Service is to provide ODFIs with enhanced control and flexibility in monitoring ACH risk in an efficient, consistent and cost-effective manner. The aforementioned Federal Reserve Bank interviews with financial institutions regardng ACH risk found that the proposed features of the service were meaningful and beneficial to ODFIs.

More than 80 percent of interviewees felt that the FedACH Risk Origination Monitoring Service would add value to ACH operations. In particular, they valued the ability to set and monitor credit and debit caps at the company ID level, with more than 87 percent indicating they would use this feature. Another desirable feature was the ability to monitor caps over multiple exposure days, rather than just on the origination process day. When asked to choose one option over the other, 70 percent opted for multiple days monitoring. A majority of participants also named e-mail as the preferred notification method for cap breaches, another feature of the FedACH Risk Origination Monitoring Service.

Conclusion

There are many rewards to be had by using the ACH network, including reduced costs, increased efficiencies and new business opportunities. To get the most from these benefits, it is critical to understand the trends driving the need for better, more automated risk monitoring systems. Because ACH risk is something that can impact an entire organization, it is advisable to involve many operations aspects, including areas such as audit, credit and risk, cash/treasury management, sales and operations. Finally, by looking to NACHA, Regional Payments Associations, the Federal Reserve Banks and other organizations for educational opportunities, ACH network participants can keep current with rules, best practices and new payment opportunities. A little knowledge goes a long way in helping to limit ACH risk exposure.

NOTES:

1 www.nacha.org/news/Stats/ACH_Statistics_Fact_Sheet_2002.pdf (1991-2002 data), www.nacha.org/news/Stats/stats2004/ACH%20Statistics%20Fact%20Sheet%202004.pdf (1994-2004 data) and www.nacha.org/News/Stats/stats2005/4th%20Quarter%202005.pdf (2005 data)

2 www.nacha.org/News/Stats/stats2005/4th%20Quarter%202005.pdf

3 www.ny.frb.org/aboutthefed/fedpoint/fed31.html

4 www.nacha.org/News/Stats/stats2005/4th%20Quarter%202005.pdf

5 *The New York Times*, December 18, 2005, *When PayPal Becomes the Back Office, Too* (Bick) and eBayPayPalWorksWithLEToFightInternetCrime.ppt (eBay/PayPal combined company PowerPoint presentation)

6 *American Banker*, June 17, 2005, *PayPal's Next Move In Business Payment* (Wolfe)

7 www.nacha.org/News/Stats/stats2005/4th%20Quarter%202005.pdf

8 *BAI Banking Strategies*, July/August 2004, *Fraud Looms: Crooks sniff opportunity and strike first via identity theft, phishing and ACH fraud. What trouble does Check 21 invite?* (Swift/Hoffman)

9 *The Journal of Lending & Credit Risk Management*, May 1999, *Understanding and managing ACH credit risk* (Weber) v81 i9 p66(6)

10 *BAI Banking Strategies*, July/August 2004, *Fraud Looms: Crooks sniff opportunity and strike first via identity theft, phishing and ACH fraud. What trouble does Check 21 invite?* (Swift/Hoffman)

11 www.nacha.org/ACH_Rules/ach_rules.htm Telephone-Initiated Entries (TEL) NACHA RULE.