FEDERAL RESERVE BANK OF DALLAS

2200 N. PEARL ST.

DALLAS, TX 75201-2272

HELEN E. HOLCOMB
FIRST VICE PRESIDENT AND
CHIEF OPERATING OFFICER

July 21, 2003

Notice 03-36

TO: The Chief Operating Officer of each financial institution and others concerned in the Eleventh Federal Reserve District

SUBJECT

Managing the Risk of ACH Debit Entries

DETAILS

This notice is to inform you of ACH business practices that can impact your financial institution and ways you can manage the risk associated with ACH debit entries.

As you know, the Automated Clearing House offers a fast, inexpensive, and reliable means of making payments. It has also been a very safe payment mechanism for the past 30 years. As a result of these characteristics, the volume of ACH payments has grown substantially in past years, and new types of ACH payments have been introduced recently that promise further increases in ACH volume. The newest forms of ACH transactions include Internet authorized payments, debits authorized over the telephone, and check-to-ACH conversions at the point-of-purchase or the lockbox.

While the new business opportunities created by the expansion of the ACH are good for the industry, the ACH operators are detecting increased risks associated with some of these new ACH debit transactions. In some instances, dishonest persons are using the ACH to originate unauthorized debits. This rise in unauthorized debit entries creates customer service issues for receiving financial institutions whose customers' accounts are hit by unauthorized debits and creates risk for the ACH system as a whole. However, the greatest risk associated with unauthorized debit entries is the financial risk to an originating depository financial institution that introduces the unauthorized entries into the ACH system. Over the past year, there have been million-dollar court cases filed to recover losses from fraudulent transactions, with the ultimate financial burden falling on the originating financial institution because the originating company is no longer in business.

For additional copies, bankers and others are encouraged to use one of the following toll-free numbers in contacting the Federal Reserve Bank of Dallas: Dallas Office (800) 333-4460; El Paso Branch *Intrastate* (800) 592-1631, *Interstate* (800) 351-1012; Houston Branch *Intrastate* (800) 392-4162, *Interstate* (800) 221-0363; San Antonio Branch *Intrastate* (800) 292-5810.

Risk Management Tools

It is important to note that not all TEL and WEB entries are fraudulent; nor are all companies or third parties that originate such entries involved in fraudulent activity. There are many important and efficient uses of these new services. The risk to an originating depository financial institution can be effectively managed using methods familiar to all bankers.

1. Before you permit your bank's customer to originate ACH debit entries, you should take adequate steps to know your customer and its business. If your customer is using WEB entries, make sure that the customer is obtaining the necessary authorizations. If the customer is originating TEL entries, be familiar with the NACHA Operating Rules regarding the circumstances in which TEL entries may and may not be used. In accordance with the rules, determine the creditworthiness of the customer. Familiarity with your customer's business practices is an important protection against the losses that your bank might incur if your customers violate the applicable rules.

2. Make sure your contracts with your customers that originate ACH debit items require your customer to follow all the NACHA rules. Know the NACHA rules, especially your responsibilities and liabilities for payments settling against your account.

3. Monitor ACH returns. Pay special attention if your bank receives significant numbers of ACH return items that relate to debits originated by one customer. Your institution's daily settlement advices from the Federal Reserve will itemize the dollar volume of ACH returns being charged to your account and provide insights as to the need for further investigation of individual originators.

4. If your bank's customer is a third-party service provider, know your customer's customers. Make sure that the party that actually obtains the funds from ACH debit entries originated through your bank has followed all the rules. You may need to require your customer to disclose the terms and conditions under which your customer does business with its customers. Once again, creditworthiness checks are effective tools. Most companies will be happy to assist and be scrutinized.

5. Be cautious in allowing any of your customers to use your bank's electronic send and receive capabilities to an ACH operator. Your bank is responsible for settling all ACH transactions that are originated using your routing and transit number. The "know your customer" principle takes on huge importance when you hand your customer the keys to your bank's Fed settlement account. In addition to performing due diligence prior to permitting customers to use your bank's electronic access to an operator, it is important to monitor the account activity of customers who access the ACH using access capability.

6. Consider establishing a “return reserve” requirement for customers originating certain types of ACH debits through your bank. Fraudulent firms are likely to respond to such a requirement by taking their dishonest enterprises elsewhere.

Prudent risk management practices such as these should allow your institution to take advantage of the opportunities afforded by today’s ACH network while protecting your financial interests.

ATTACHMENT

To help illustrate the risks associated with these new ACH debit transactions, the Federal Reserve System has developed a business case that, while fictional, demonstrates the financial liability that an originating financial institution can bear with respect to these new transactions. The business case is attached at the end of this notice.

MORE INFORMATION

For additional information on managing the risks associated with ACH debits, please reference OCC Advisory Letter 2001-3, *Internet-Initiated ACH Debits/ACH Risks*, and NACHA’s Operations Bulletin, *Telephone-Initiated (TEL) Entries*, dated September 19, 2001. In addition, financial institutions can take advantage of educational and training materials available from NACHA and local ACH payments associations.

If you have any questions concerning the issues addressed in this notice, please contact one of the following account executives:

Rick Flansburg	(210) 978-1661
Michele Hitchings	(713) 652- 9141
Jim McCammon	(214) 922-5491
Susan Vice	(214) 922 -5430
Kathy Waggoner	(713) 652-9146

Paper copies of this notice or previous Federal Reserve Bank notices can be printed from our web site at **http://www.dallasfed.org/banking/notices/index.html**.

Sincerely,

Helen E. Holcomb

A Worst Case Fiction: The Bank of Anytown Failure

As of December 31, 2001, the Bank of Anytown was a small institution with $5 million in Tier 1 capital and $38 million in total assets. Early in 2002, a third party processor, AutoCo, approached the Bank with the idea of originating ACH debit transactions for Scamco, a telemarketing firm and customer of AutoCo. Though intrigued, the Bank indicated that they did not have the technical capability to originate large numbers of ACH entries. AutoCo offered to do so on behalf of the Bank and offered to pay the Bank a share of the Scamco fee income. The Bank allowed AutoCo to use their electronic access capabilities to originate the transactions to the ACH operator and settle the items through the Bank's Federal Reserve settlement account. In essence, the Bank was pleased to have the AutoCo/Scamco business, become an ACH originator, and derive new fee income.

AutoCo then began to originate through Bank of Anytown large numbers of Scamco's one-time consumer payments as ACH debits. In February, AutoCo originated $10 million in debit entries on behalf of Scamco. In March, the totals reached $15 million. Also during March, the Bank of Anytown began to receive a significant number of returns based on claims made by receivers that the original debit entries from Scamco were unauthorized. At first, Bank of Anytown was able to debit AutoCo's large account balance to cover these return items. By the beginning of March, everything unraveled. AutoCo made large withdrawals from its accounts at the bank. Shortly afterward, federal law enforcement agents arrived at the Bank with a court order freezing AutoCo's accounts and inquiring about Scamco. The newspapers reported that AutoCo's operations were shut down. Some of AutoCo's senior managers were arrested. Others were said to have left the country. But even after AutoCo dissolved, a deluge of ACH return items continued to pour into the Bank of Anytown. Each day, the Bank of Anytown's Fed account was debited for hundreds of thousands of dollars for the ACH return items.

When the Bank of Anytown contacted its ACH operator for help, the operator explained that under NACHA Rules and Regulation E, the receiving banks had the right to return ACH debit entries if the receivers said the items were unauthorized, and the Bank of Anytown was financially liable for settling the return items. Quickly, the Bank of Anytown's capital evaporated, and the bank was declared insolvent and placed in receivership on April 1, 2002.

Although the Bank of Anytown story is fictional, it points to an important lesson. A bank that permits a fraudulent party to introduce unauthorized debit entries into the ACH in effect gives that party the ability to loot the bank's Federal Reserve account. If an originator introduces $1 million in fraudulent debit entries through an originating depository financial institution that gives the originator immediate credit, the originator may easily disappear with the proceeds from the ACH entries long before the originating bank becomes aware of the fraud. Returns of unauthorized ACH entries may not start to come back to the originating bank until after the receivers of the unauthorized debits receive and review their bank statements, identify the unauthorized entries, and initiate the return process through the receiving depository institutions. Regulation E gives a consumer at least 60 days after the transmittal of a bank statement to report an unauthorized electronic fund transfer. Moreover, in some states, laws provide for the return of such items well beyond the existing ACH return timeframes, sometimes as much as two years.

Most of the $1 million in fraudulent debit entries that the fraudulent party originated through the originating bank will come back as debits to the originating bank's Federal Reserve account during the three months or so after the fraudulent entries were introduced into the ACH system.

While this case involves a third party processor originating entries for a fraudulent telemarketer, similar schemes are being employed by companies like Scamco originating entries directly through financial institutions that are active ACH originators, but that do not have sound "know your customer" business practices.