Taming the Beast: An Assessment of the Fraud Risk Implications of the Electronification of the U. S. Payments System

Robert W. Jones, CFE, Director of Fraud Risk Management and Loss Analytics,

FleetBoston Financial

Introduction

The U.S. payments system is glacially, but inexorably, metamorphasizing from a paper to an electronic state. We may be seeing, finally, the beginning of what was predicted in 1974, when the National Automated Clearing House Association[1] was born: that is, the demise of the paper check. It is clear, however, that the U.S. payments system remains tied to paper. In 2000, the last year for which reliable data are available, the Federal Reserve estimates that Americans wrote 50 billion checks with a value of $48 trillion,[2] 60% of all cashless transactions conducted in the United States. However, that represents a significant reduction from 1979, when checks totaled 85% of the volume of cashless payments.[3] During the same period, electronic options have trended up, at a steep rate. Debit card use has increased from 1.1 million transactions valued at $33.6 billion in 1994[4] to 8.3 million transactions valued at $348 billion in 2000.[5] ACH debits have grown from 886 million transactions in 1994[6] to 5.6 billion transactions valued at $5.7 trillion in 2000.[7]

The parties to the payments system, consumers, retailers, payments processors, and financial institutions have different, and often competing, interests in the system's evolution. Consumers want convenience and security. NACHA, the Federal Reserve system, regional ATM networks, Small Value Payments Company (SVPCo)[8], the Electronic Check Clearing House Organization (ECCHO)[9] and other groups, including the Banking Industry Technology Secretariat (BITS)[10], are seeking ways to streamline the payments system, cut costs and to reduce risk and float. Of course, each wants to accomplish these in ways that benefit its own interests. For example, NACHA hopes to drive more volume through the automated clearinghouses while SVPCo sees the ATM/POS networks as providing the best way to electronify payments at the point of sale. ECCHO sees Electronic Check Presentment (ECP) as a means of squeezing expense out of the payments system without adding to fraud risk. Traditional retailers want to reduce their check-related expenses and card-related interchange charges. At the same time, the burgeoning online retail market requires new approaches to payments.

Paper-based check fraud cost banks nearly $700 million dollars in 1999, the last period for which reliable data are available. During the same period, commercial banks were successful in averting fraud attempts totaling $1.5 billion [11] Check fraud losses are increasing 15% annually.[12] However, anecdotal data suggest that the losses are well in excess of $1 billion per year to banks, with another $10 billion lost by retailers and other companies. To mitigate the effect of these losses, virtually every large bank (assets >$50 billion) and most medium-sized banks (assets $20-50 billion) have installed software that identifies suspicious transactions for further analysis.

The purpose of this paper, then, is to examine the impact these new "electronified" check transactions, which have been designed to increase the efficiency of the payment system, will have on check fraud losses. In particular, the paper will focus on projects involving the conversion of paper checks to ACH, ECP (Electronic Check Presentment) or electronic debits. In some cases, risks will increase. In others, risks will decrease. In others, risks will remain the same. In some, liabilities will shift and, in others, liabilities will remain unchanged.

The electronification of payments is not a new concept. Recurring consumer credits processed through automated clearinghouses (ACH) are widespread, particularly for federal payments to Social Security beneficiaries and direct deposits of salary. For instance, during 1998, 2.7 billion ACH credits totaling $7.8 trillion were processed in the United States.[13] Similarly, recurring ACH consumer debits are a common, popular way to pay insurance premiums and make loan payments. Traditionally, these ACH payments have been between parties with well-founded relationships who use the ACH network because it is fast, reliable, inexpensive and, until now, virtually free of fraud. However, the industry initiatives to convert paper checks to electronic debits, and pay for goods and services over the Internet with funds from a checking account, will, I submit, increase the combined fraud losses of merchants and financial institutions and will redistribute fraud losses away from financial institutions to merchants. There are three reasons for this increase. First, the new environment creates new opportunities for criminals with no offsetting expectation of losses from other sources to decrease. Second, the parties to the transactions do not have an established relationship and the transaction may be the only encounter between the payer and the payee. Finally, the liability for forged maker's signatures will be transferred, for the most part, from the financial institutions to the merchants. Hence, a primary objective should be for the financial services and retail industries to take steps to manage these risks.

Three specific risk areas that will benefit from electronification are losses arising from insufficient funds, closed accounts and stop payments. This is not an insignificant benefit. In 1999, insufficient funds losses accounted for 26% of the $679 million estimated to have been lost by the commercial banking industry. Closed account losses were 10% of the total and stop payments were 2%.[14] By converting the transaction to electronics, the time it takes for a depositor to be notified that a check he or she accepted is no good is dramatically decreased. This time reduction limits the number of times someone can write worthless checks and directly translates into reduced losses both for financial institutions and merchants. Merchants will be the major beneficiaries from this reduction.

Chart 1 lists the major check fraud components and the outcome likely to be experienced by each party to electronified check transactions.

Chart 1

FRAUD TYPE	MERCHANT/ ORIGINATOR	CONSUMER	ODFI	RDFI
CLOSED ACCOUNT	BETTER	NO CHANGE	NO CHANGE	NO CHANGE
COUNTERFEIT/ALTERED	WORSE	NO CHANGE	WORSE	BETTER
FORGERY	WORSE	NO CHANGE	WORSE	BETTER
FRAUDULENT ORIGINATIONS	NO CHANGE	NO CHANGE	WORSE	NO CHANGE
IDENTITY THEFT	WORSE	NO CHANGE	WORSE	BETTER
INSUFFICIENT FUNDS	BETTER	NO CHANGE	NO CHANGE	NO CHANGE
STOP PAYMENT	BETTER	NO CHANGE	NO CHANGE	NO CHANGE

Automated Clearing House Initiatives

The Special Committee on Paperless Entries (SCOPE) was formed in 1968 by a group of California bankers to seek ways to automate the payments system. The first automated clearinghouse association was formed in 1972, with NACHA being organized in 1974 as an arm of the American Bankers Association. Its function was to promote ACH and to write rules to regulate the behavior of the parties to the transactions. Since separating from the ABA in 1985, NACHA has continued to be an aggressive, and successful, advocate for the ACH movement. In 1988, ACH volume exceeded one billion transactions. In 1992, two billion transactions were processed. In 1994, the volume reached 3 billion. In 1997, it exceeded 4 billion, and in 1999, surpassed 5.3 billion.[15]

Re-Presented Checks (RCK)

Checks returned unpaid because of insufficient or uncollected funds are now eligible to be converted into ACH debits and presented through the ACH network for collection. Retailers pushed for this product to increase their recovery of funds from checks they accept for payment that are returned by the paying bank.

Since banks typically post ACH transactions before paper transactions, the retailer can take advantage of the fact that there may more likely be money in the account to pay the ACH debit. The retailer has three chances to collect the money owed: the initial check presentation plus: one paper re-presentation and one ACH re-presentation (RCK), or two ACH re-presentations (RCK). NACHA Operating Rules and the Uniform Commercial Code govern RCK transactions. Specifically, which state's Uniform Commercial Code will govern the transaction would depend on: 1) contractual arrangements among parties; and 2) at what point in the check's processing cycle the legal question arises.

Converting Consumer Checks to ACH Transactions At The Point Of Purchase (POP)

Retailers and bankers view the conversion of paper checks presented at the point of sale to ACH transactions as a way to electronify transactions for consumers who want to continue to use paper checks or who do not have debit cards. NACHA Operating Rules support Point of Purchase (POP) entries. In this approach, the consumer presents a paper check to a merchant at the point of purchase. The merchant uses a terminal to scan the Magnetic Ink Character Recognition (MICR) information on the bottom of the check. The merchant obtains written authorization from the consumer to send the payment electronically, then voids the check and returns it to the consumer along with a copy of the authorization. The authorization may be included on the consumer's receipt. Later, the merchant or a company servicing the merchant creates an ACH debit in the amount of the check and transmits the transaction to its acquiring financial institution (the Originating Depository Financial Institution, or ODFI), which transmits the transaction to the ACH network for collection. NACHA Operating Rules and Regulation E govern this transaction. The ODFI makes all the usual ACH warranties.[16] It also warrants that the check was returned to the consumer and that the check has not been otherwise been used. Its contractual relationship with the merchant determines how these warranties are supported. The risk inherent in accepting checks, especially those with forged maker’s signatures, is largely shifted from the paying financial institution (RDFI), which principally bears the risk in the paper check world, to the ODFI, and, therefore, to the merchant or guarantor. According to NACHA, 515 retailers offered check conversion at the point of sale in January 1998. By January 2000, the number had risen to nearly 25,000. During the same period, the number of transactions rose from 41,800 to 1,500,000 per month.[17] During 2001, 64.2 million POP transactions were processed.[18]

Telephone Authorization Of Non-Recurring Consumer Debits (TEL)

NACHA Operating Rules have always required consumers to authorize ACH debits to their accounts in writing or electronically in a "similarly authenticated"[19] manner. On September 11, 2000, NACHA approved the establishment of a new Standard Entry Class (TEL) to identify these transactions.[20] Three scenarios are allowed:

1. Consumer calls company with which consumer has existing relationship.
2. Company calls consumer with whom company has existing relationship.
3. Consumer calls company with which consumer has no prior relationship.

Prior to executing an ACH transaction, the company is required to allow the customer the option of requesting an authorization in writing. If the customer does not want to be provided with the authorization in writing in advance and if the business does not tape-record the conversation, the company must provide the consumer five pieces of information about the transaction and a written notice prior to settlement of the transaction. Catalog merchants and collection agencies are the most common users of this transaction. NACHA Operating Rules govern ACH debits initiated under this method of authorization. During 2001, 6.3 million TEL transactions occurred.[21]

Spontaneous Internet-Generated ACH Transactions (WEB)

As previously mentioned, current NACHA Operating Rules require consumers to authorize ACH debits to their accounts in writing or to use digital signature technology to authorize transactions initiated over the Internet. Since use of digital signature technology has not grown so fast as NACHA had anticipated, NACHA is considering other methods to authorize ACH transactions over the Internet. The NACHA Operating Rules and Regulation E govern transactions initiated in this manner. Of the many Internet-based payment risk issues that need to be resolved, the issue of liability for unauthorized transactions when third parties issue or control the security procedures needs discussion. During 2001, 54 million WEB transactions occurred.[22]

Lockbox Accounts Receivable Check Truncation (ARC)

On March 15, 2002, NACHA adopted rules authorizing the truncation of consumer checks, sent through the mail, at the point of receipt (lockbox) and sending debits representing those checks through the ACH network for collection. Under the rules, lockbox operators have two choices in how they notify consumers of the service and whether the operators obtain explicit authorization. The so-called "opt in" provision (*Notification with Authorization)* requires consumers to positively respond that they want their checks truncated by providing written authorizations. The "opt-out" provision (*Notification to Consumer*) gives consumers the option to respond that they do not want their checks truncated. The ACH debit records contain the names of the payees so that the consumers' banks are able to provide descriptive entries for the debits. The NACHA Operating Rules and Regulation E govern these transactions.

Truncation of Non-Consumer Checks

Until now, all check electronification initiatives addressed only consumer checks. The prohibition against truncating such checks at the point-of-purchase has resulted in a number of intractable logistical issues. For example, checkout clerks are expected to be able to discriminate between a consumer’s check and a business check. Too, many small and mid-sized businesses prefer to use checks to pay for small purchases. The confusion and inconvenience spawned by the initial prohibition drove the Electronic Check Council, at its September 2000 meeting, to recommend that the NACHA Board initiate, on a very limited basis, a corporate check truncation pilot.

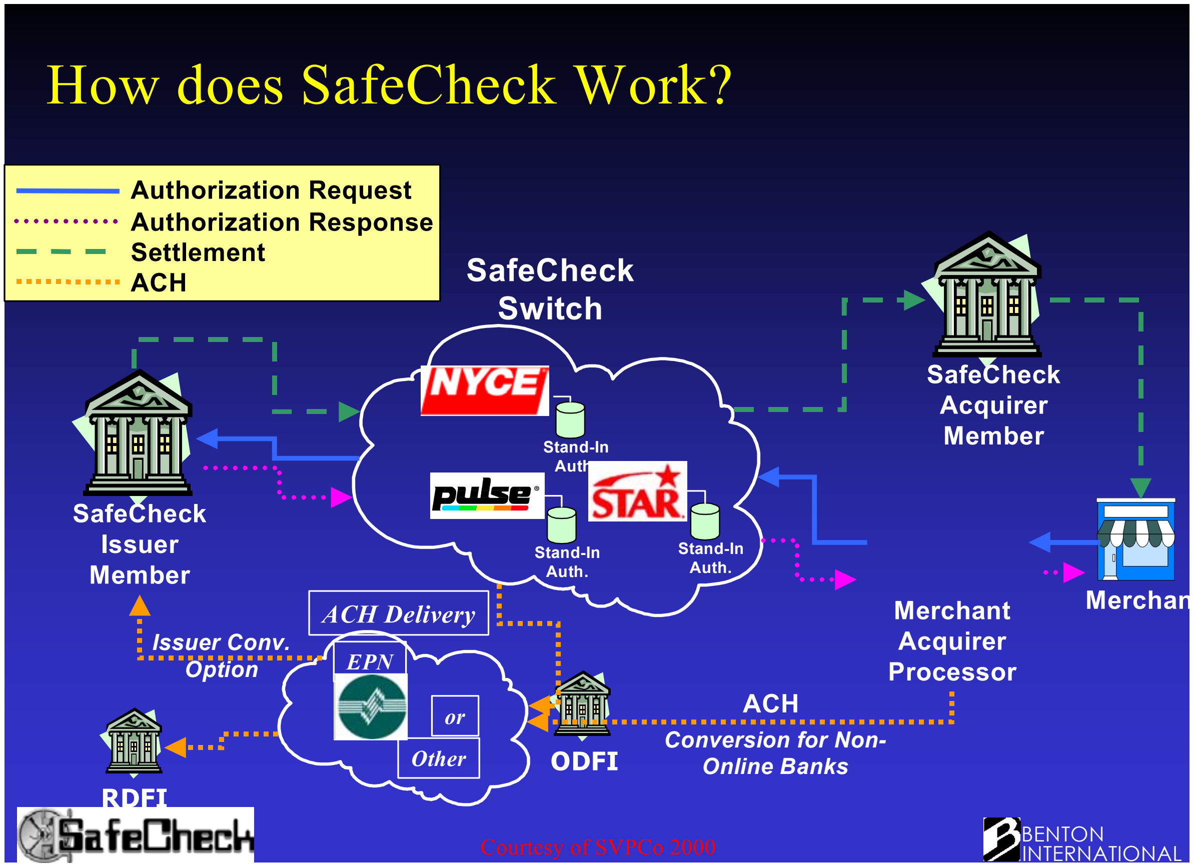
Electronic Funds Transfer Network Initiatives

A different approach to check electronification leverages the ATM/POS network infrastructure. The most prominent product is SVPCo’s SafeCheck. As with ACH-based check conversion, the MICR information on the consumer’s check is scanned. However, the MICR information is sent via the ATM/POS network to participating banks.

SafeCheck is a four-product suite. The first, most basic, product provides check verification, responding to the point-of-sale that the account exists and contains a balance sufficient to pay for the transaction. The next product converts the transaction to ACH. The third product both verifies and converts the check. The fourth product directly debits the consumer's account.

The ultimate success of this approach rests on the successful resolution of several issues, both technological and behavioral. First, because the transaction is on-line, the transmission and response must occur in less than five seconds. Next, the system must be tolerant of the habits of both the check-writing public and the check-accepting merchant. Most people understand the role of float and rely on a certain delay between the time they utter the check and their bank pays it. Thus, they occasionally write checks without sufficient funds at that time. Similarly, merchants do not care if funds exist at the time of transaction, so long as they exist when the check is presented for payment. Solving this is not particularly daunting. Most banks currently apply some logic to the return decisioning process, calculating the time the account has been open, average balances, previous overdraft experience, etc. Including such logic in the verification process would meet the common interests of all the parties. Consumers would be able to buy goods and services without having to wait for payday. Merchants would not have to deny sales to their good customers. Banks would continue to collect fees from their customers who rely too aggressively on float.

SafeCheck is a very young product with big dreams. In June 2000, SVPCo Chief Operating Officer Henry C. Farrar predicted that SafeCheck could eliminate "18 billion checks accepted annually by merchants at the point of sale."[23] Mr. Farrar pointed to the feasibility of the process by announcing that 100 transactions had been successfully completed.[24] A diagram provided by SVPCo that illustrates the transaction flow appears on the next page.



How does SafeCheck Work?

- Authorization Request
- Authorization Response
- Settlement
- ACH

SafeCheck Switch

NYCE

Stand-In Auth

pulse

STAR

Stand-In Auth.

Stand-In Auth.

SafeCheck Issuer Member

SafeCheck Acquirer Member

Merchan

Merchant Acquirer Processor

ACH Delivery

Issuer Conv. Option

EPN

or

Other

ODFI

ACH

Conversion for Non-Online Banks

RDFI

SafeCheck

Courtesy of SVPCo 2000

BENTON INTERNATIONAL

Figure 1

Electronic Check Presentment Initiatives

The private sector has taken the lead in promoting ECP. It has been a key initiative for BITS for the past three years, working with ECCHO and SVPCo to encourage more bank participation to make the payments system more efficient through the acceptance and use of ECP. The Federal Reserve Banks and other private exchanges also make ECP available to financial institutions. In the ECP process, depositary banks create files of the information contained in the MICR band of their processed checks. The banks then exchange these files with each other or through a clearinghouse such as SVPCo or the Fed. This process allows paying banks to debit their customers' accounts on the same day the depositary bank receives the check. The primary barrier to ECP growth is the requirement to enter into bilateral agreements, which results in a logistical quagmire. SVPCo, with its sponsorship of multilateral agreements, offers a more efficient approach. In any case, ECP is expected to mature in three stages:

1. ***ECP with paper checks to follow (the current stage)***.
   In this stage, banks continue to exchange paper checks as they do today. Presentment continues to occur when the paying bank receives the paper checks. The advantage in this stage to the paying bank is an increase in float resulting from debiting its customers' accounts one or two days in advance of presentment. Because debits are posted sooner, depositary banks get preliminary electronic notifications about closed and blocked accounts, insufficient funds, stop payments from one to six days sooner. The deadline for returning the paper checks is still based upon the day and time the paying bank received the paper checks.

2. ***ECP with image to follow***.
   In this stage, participating banks are assumed capable of creating and receiving images of checks. The bank of deposit will truncate the paper checks. The paying bank will receive the ECP file late in the evening (of the day the depositor negotiated the check with the depositary bank). It will receive a second file containing images of all of the checks in the ECP file a few hours later during the early morning hours of the following day. Presentment will be based upon the business day of receipt of the images (the business day following receipt of the ECP file). The deadline for returning the check images will be based upon the day and time the paying bank received the check image file.

3. ***ECP with images on demand***.
   In this stage, the participating banks will continue to exchange ECP files as they did in stages one and two. This stage differs from stage two in that paying banks will not receive images of all of the checks being presented. They will only receive images of the checks they want to review. "Images on demand" will mean different things to different banks. Where some may want to continue to receive all of the images, others may want to see only those images of checks over a certain dollar amount and others may want to see images of a few specific checks.

The date and time of the availability of the ECP file will determine presentment and the associated returned item deadline.

The rules promulgated by the Electronic Check Clearing House Organization (ECCHO), the local clearinghouses, Federal Reserve Bank Circulars, Regulation CC, correspondent bank agreements and the Uniform Commercial Code in force in the state in which the paper check is negotiated govern ECP transactions.

Fraud Risks Associated With The Conversion Of Paper Checks To Electronic Transactions

The risks associated with check electronification vary by type of transaction. However, some issues apply to all types of conversion transactions. The Uniform Commercial Code gives the paying bank until midnight of the day following presentation to review a paper check and to make a decision to pay or return a check. A paying bank that fails to detect a forged maker's signature or a counterfeit check within that time loses its right to return the check to the depository bank.[25]

In the various truncation scenarios previously discussed, the conversion of paper checks to electronics changes the rules for when banks can return unauthorized debits. This has significant implications for both merchants and banks. With a paper check, a bank must return the check with a forged maker's signature by its midnight deadline. For a merchant who accepted the check, this means that he or she will receive the returned check back within a few days after accepting it. For converted checks the merchant can receive returns (unauthorized transaction), for two months or more after the check was converted. Since Regulation E and NACHA Rules grant consumers approximately 60 days to refute ACH transactions, merchants can accept many checks with forgeries before they receive any notification of the situation. This situation is disadvantageous to the merchant. To put the impact of this liability transfer in perspective, forged makers' signature losses to the banking industry in 1999 totaled $177 million, and counterfeit losses totaled $75 million.[26]

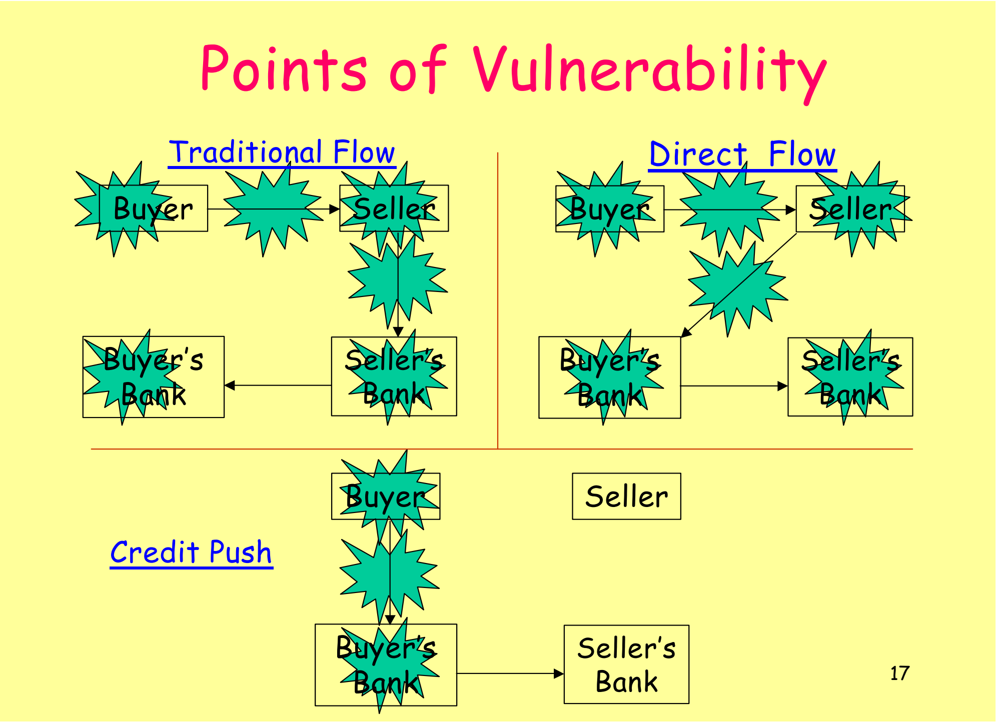
Check electronification at the point of sale introduces two new risks to the ACH. First, the relationship between consumer and originator is changing. Fraud was largely unknown in the traditional environment of recurring transactions within existing relationships. Now, however, the ACH debit may well be the first and only encounter between the consumer and the retailer. Second, the origination of ACH transactions is being transferred from secured corporate data centers to unsecured retail point-of-sale counters. This transfer can increase unauthorized transactions originated by dishonest customers, merchants and clerks and will result in higher bank losses. If not controlled, it may well cause the loss of consumer confidence in electronic banking. For example, a dishonest customer, knowing that the merchant has returned his check, has less compunction about alleging an unauthorized transaction. A dishonest clerk can scan a counterfeit check brought from home and take the corresponding amount of cash from the register, thus appearing to be in balance. Since the merchant participates in Point of Purchase, he does not expect the check to be in the cash register and, thus, does not know his clerk has stolen until the legitimate customer whose account number was used detects the spurious debit and complains to the RDFI.

As with other ACH transactions, the ODFI is ultimately responsible for any loss that might occur while the merchant is responsible to the ODFI for the loss. While the financial loss resulting from such criminal behavior lies with the ODFI, the RDFI bears the brunt of the customer dissatisfaction resulting from the consumer claims of unauthorized transactions.

The two elements that make the Internet attractive to commerce are the same that make the generation of spontaneous authorizations for non-recurring ACH transactions originating on the Internet the most problematic of all the initiatives: volume and velocity. Literally thousands of spurious transactions can be generated virtually instantaneously. There is a broad consensus in the fraud risk management community that the Internet is an extremely fertile environment for fraudsters. According to the GartnerGroup, "Credit card fraud is 12 times as high on the Internet as in physical stores, and more than 92% of chargebacks come from Internet transactions … ."[27]

Figure 2 graphically displays the points of vulnerability in Internet-generated check transactions.

Figure 2[28]



Points of Vulnerability

This raises several questions requiring affirmative answers:

- Does the buyer authorize the seller to originate the transaction?
- Does the seller authenticate the buyer?
- Is the transmission of the transaction protected from intercept?
- Is the seller's site secure?
- Do the banks have filters in place to detect fraudulent transactions?
- Do the banks conduct effective due diligence on new on-line merchants?

Maintaining the security and integrity of transactions flowing over a public access network is difficult. The difficulty arises because the transactions are in a form that can be modified without detection, repeatedly sent, altered and are exponentially increasing in volume. For e-commerce to work, we need to be able to employ methods that identify, authenticate, and assure privacy and non-repudiation that are appropriate for the transaction involved. Although experts continue to explore the use of alternate, more efficient technologies, most agree that Public Key Infrastructure (PKI) is an acceptable security method for use over the Internet when totally open communication between unknown parties is required. PKI allows messages to be "tamper-proofed" to assure their integrity while digital signatures assure authentication and non-repudiation. Unfortunately, PKI has not been widely accepted because of its high implementation and maintenance costs and its lack of interoperability between systems.

In the absence of a widely accepted PKI infrastructure for securing communications and commerce between parties over the Internet, most banks and merchants rely on a combination of Secure Socket Layer (SSL), user identification numbers, and passwords. SSL technology is built into all of the commonly used Internet browsers to provide security between the consumer's Internet browser and the merchant or bank Web site. To assure that only an authorized person is performing a transaction, most sites require a combination of user identification numbers and passwords. While not so secure as other technologies, SSL provides sufficient security for the limited types of transactions currently allowed in home banking applications.

In addition to the technical issues, the "know your customer" requirement becomes particularly difficult for the ODFI. In the physical world, retailers can be vetted by "drive-by's", giving the banker some solace in knowing that the retailer at least exists at the location and that the location seems to be able to sustain the level of activity claimed by the retailer. That capability disappears in the virtual world. That is why I am convinced that while consumer-generated fraud impacting retailers will be the greatest risk at the physical point-of-sale, merchant-generated fraud impacting ODFI's will be the greatest risk on the Internet.

ECP

ECP does not present additional fraud risk to the payments system. In fact, it has the potential to reduce losses. If the paying bank posts transactions from the ECP file, even if they reject, the depository bank will receive notice of the likely return of the item the next day, thus enabling it to protect itself and, potentially, its customer. If, on the other hand, the paying bank does not post such items, the depository bank will receive notification at the same time as it now does, resulting in neither advantage nor additional disadvantage.

Statutory/Regulatory Issues

The attempt to regulate check electronification is addressed from three, sometimes complementary, sometimes conflicting, perspectives: Regulation E, NACHA Rules, and the Uniform Commercial Code as adopted/adapted by State legislatures.

The Electronic Fund Transfer Act {15 USCS §§ 1693 et seq.}[29] was passed in 1978 to address the rights of consumers *vis-à-vis* the other participants in electronic funds transfer systems. Its provisions are codified in 12 CFR 205 (Regulation E). The Official Staff Commentary (12 CFR 205 (Supp. I)) is designed to help financial institutions understand and comply with the regulation.

In March, 2001, the Board issued its revisions to the Official Staff Commentary on a wide-reaching series of issues that reflected the Board's acknowledgement that Reg E's tenets had been overtaken by the marketplace's embrace of technological advances, particularly as demonstrated by check electronification initiatives. Another reason for the update was to attempt to rationalize the confusion caused as the differences among various payment instruments become increasingly blurred. For example, most debit cards contain a VISA or MasterCard logo and can be used like a credit card in point-of-sale locations where debit cards are not accepted. So, a consumer asked to provide his credit card number to authorize a telephone or Internet transaction might give his debit card number instead. This puts the merchant payee in a difficult position. Regulation Z (12 CFR 226) does not require a written, signed, or "similarly authenticated" authorization, but Regulation E does. How is the merchant to know he is charging a checking account and not a credit card account? The Fed's proposed comment purports to "clarify" the situation by reiterating the authorization requirement.[30]

NACHA Rules are given deference in the Official Staff Commentary to Regulation E. The Fed and NACHA view themselves as partners in simultaneously promoting and regulating the automated clearinghouse. There are, however, differences between NACHA Rules and Regulation E that promote confusion. The most glaring example is how the two deal with allegations of unauthorized debits. Regulation E, in § 205.6, *Liability of consumer for unauthorized transfers*, gives the consumer the option of advising his financial institution in person, telephonically, or in writing. NACHA Rules, on the other hand, require the RDFI to provide the ODFI an affidavit signed by the consumer alleging an unauthorized ACH debit.

. The situation is further clouded by the appearance of the Check Truncation Act that was drafted by the Federal Reserve in an attempt to facilitate check truncation. The Act has not yet been formally introduced, so I will not deal with it here. The most recent draft version (as of December 2001) can be found at: http://www.federalreserve.gov/paymentsystems/truncation/default.htm

Fraud Risk Mitigation Strategies

The management of fraud risk requires a union of technology and sound practices. In the current environment, however, a comprehensive technological solution is not available, so we must rely on rules, policies and procedures. The following outlines some thoughts for developing a proactive approach to mitigate the risks of check electronification. It includes leveraging existing methods and technologies and changes to association rules. Future risk management approaches should use new technologies and methods, as they become available.

The ACH Network

By allowing ACH transactions to be created at unsecured point-of-sale terminals, we have created an environment in which unauthorized fraudulent transactions can be created and placed into the ACH network. The Internet presents even a greater risk. In this environment, criminals can create unlimited numbers of unauthorized fraudulent transactions at high velocity. The ODFI plays a critical role in preventing unauthorized transactions from entering the ACH network, for once the fraudulent transactions are in the system, it becomes a Herculean task to track down the source and measure the impact. Hence, operating rules need to be changed to require ODFIs to be proactive in preventing the introduction of such fraudulent transactions into the system. If check electronification is to have the impact on the payments system its proponents hope, substantive safeguards need to be implemented.

Detecting Fraud Patterns in POP Origination

Because an ODFI warrants all transactions, it must have an operating process in place to monitor the volume and value of POP transactions originated by a merchant and returned to the merchants from RDFI's. The objective of the monitoring would be to detect patterns of fraudulent transactions originated at merchant locations. Successful application of that process would enable the ODFI to prevent additional fraudulent transactions from entering the ACH network and to report these anomalies to NACHA in a timely manner.

To the extent they can, all financial institutions should monitor and benchmark loss data associated with electronification in order to identify early trends and fraud patterns. The benefits of close monitoring and reporting are evidenced by a reduction in the average rate of growth in check fraud losses by members of the BITS Fraud Reduction Steering Committee, which in partnership with the ABA, monitors and benchmarks check fraud losses on a regular basis. The capture of such loss data is an important addition to the ABA's 2002 Deposit Account Fraud Survey.

Point of Purchase (POP) Refunds

At this time, the NACHA Rules do not permit this transaction, though many advocate its acceptance to help bring check electronification transactions into the mainstream. They argue that retailers traditionally make refunds in the same medium as the original transaction: credit card debits offset by credit card credits; cash purchases refunded in cash, etc. However, NACHA should make any changes to this prohibition very cautiously. ODFIs must understand that they warrant the legitimacy of all transactions. Therefore, they should be required to have an operating process in place to prevent the introduction of unauthorized transactions into the system. For example, an ODFI should be able to maintain a file of all of the POP entries its customers originate for a period of 90 days, enabling it to compare the total POP refunds requested to the amount of the original purchase on the file.

Manual Input of POP Transactions

Current NACHA Rules do not permit the manual entry of information. That prohibition exists because of the ease with which a dishonest sales clerk can steal money from his employer. All the clerk needs to do is to obtain checking account numbers, which he can easily get from customers who pay by check, enter their account numbers into the POS terminal and take an equal amount from the cash drawer. Of course, as mentioned earlier, a clerk can scan a spurious check and accomplish the same result. However, easing this restriction would make such thefts easier. Therefore, I think it is important for NACHA to maintain its current rule by requiring an ODFI to warrant that, with the exception of the amount of a transaction, POP transactions sent from the ODFI do not contain MICR band information entered manually.

RCK Limited Presentations

Similarly, an ODFI should have an operating process in place to prevent the introduction of the third or subsequent presentation of an RCK transaction into the system within one year of the presentation of the first RCK transaction. However, due to the ease with which an originator can alter the appearance of a new RCK from previous ones, the ODFI's process needs to be designed to identify only the obvious re-presentments of RCK transactions. NACHA should promulgate rules to sanction ODFIs that fail to exercise such care.

ECP

ECP and its electronic return notification capability have the potential to provide significant benefit to both banks and their customers. Banks should carefully consider implementing ECP systems.

Responsibility of RDFIs

RDFIs should integrate the fraud detection systems they use for paper checks with their ACH and online processes. However, to make such integration effective, RDFIs should assure that their ACH operating systems are capable of identifying the check serial number field.

Conclusion

The largest threat to the success of ACH-based check electronification on the Internet is the lack of a real-time, on-line ability to determine if an account number exists, if it contains a balance sufficient to pay for the services or goods, and if the person originating the transaction is authorized. Credit card fraud has been significantly reduced because of the successful application of neural-net technology that addresses these issues. Significant differences between plastic and checks make replication of credit cards' success particularly daunting. Unlike with credit cards, there is no industry-wide Demand Deposit Account numbering convention. A checking account number can have as few as six and as many as 13 digits. Additionally, the number on the MICR line of the check may not be the actual account number. This problem arises from the wholesale consolidation of the U.S. banking industry. Most acquiring banks do not force their new customers to use new checks, primarily to minimize customer discomfiture and to avoid the costs of printing new stock. In any case, customers tend to use their old check supply until it is exhausted. Thus, though virtually all banks uniformly programmatically translate the numbers on checks to the numbers in their systems, their approaches to the translation are not uniform.

Electronic Funds Transfer applications like SafeCheck have the potential to provide a partial solution to these issues. By communicating directly with the paying bank, both physical and virtual merchants can assure themselves that the account does, in fact, exist and contains an available balance to pay the debit. However, they still have to take the customer at his word that he is authorized to make the transaction. Additionally, EFT-based electronification products are not nearly so mature as the Automated Clearinghouse.

The management of electronified check fraud risk relies on a combination of practice and technology. As discussed earlier, virtually all of the large banks and most medium-sized banks are working to turn their fraud filters on to ACH transactions. However, those enhancements will protect only the RDFI side of the bank from a relatively low number of attempted frauds. To protect itself, the ODFI side must employ both sound credit risk modalities and systems that provide effective surveillance of transactions originated by the bank's customers. For example, most banks use some kind of quantitative process to determine the amount of risk they are willing to accept from business customers originating ACH consumer debits. The credit risk managers need to understand, however, that their potential exposure is actually 60 times the daily limit because of the time consumers have to allege unauthorized debits. This reality makes the need for truly effective "Know-Your-Customer" practices essential.

Financial institutions also need to review the section of their customer service organizations that perform investigations, to ensure fraud allegations are handled and internally routed correctly.

Last, as with any kind of risk management, we must gather data. Through its analysis we are able to establish reasonable metrics and benchmarks. Such metrics and benchmarking have yielded positive results in dealing with traditional, paper-based check fraud. The problem facing the fraud risk management practitioner attempting to manage electronification fraud risk is the paucity of real data. As of this writing, all we have to work with is anecdote. However, the financial services industry has taken the first steps to gather data, through the ABA's inclusion of electronic-based transaction fraud in its biennial survey and BITS' continuing commitment to check fraud reduction. As check electronification gains consumer and retailer acceptance, fraud data will be forthcoming and the chance of our managing electronification fraud will be enhanced.

[1] In 1999, the name was changed to "NACHA – The Electronic Payments Association".

[2] Federal Reserve Bank of Boston, Financial Services Policy Committee, Press Release, "Fed Announces Results of Study of the Payments System. First Authoritative Study in 20 Years". November 14, 2001. Boston, MA.

[3] Ibid.

[4] Bank for International Settlements, Statistics on Payment Systems in the Group of Ten Countries, Basel, 1998. Pp. 97-98.

[5] Federal Reserve Bank of Boston, p. 2.

[6] Bank for International Settlements, pp. 97-98

[7] Federal Reserve Bank of Boston, p.2.

[8] SVPCo, owned by 22 banks, was organized by the New York Clearinghouse to foster Electronic Check Presentment (ECP), the inter-bank check truncation process.

[9] The ECP rules-making organization, headquartered in Dallas, TX.

[10] The Banking Industry Technology Secretariat is the technology arm of the Financial Services Roundtable, an industry trade association, membership to which is open to the 125 largest financial service firms in the United States.

[11] The American Bankers Association Deposit Account Fraud Survey Report 2000, p.7.

[12] p. 7.

[13] See *6*.

[14] ABA Deposit Fraud Survey Report 2000, p. 7.

[15] NACHA historical and volume data cited here were taken from a document prepared for me in July 2000, by Jane Larimer, NACHA General Counsel. Note the difference between NACHA statistics and those compiled by the Basel Committee: 1998 NACHA volume includes both credit and debit transactions as well as ACH transactions where the sender and receiver are the same bank. Basel volume cited in note *6* just includes credits where the sender and receiver are different entities. This discrepancy is exacerbated as the consolidation of the financial services industry continues.

[16] NACHA Operating Rules require the ODFI to warrant to the RDFI that the consumer has authorized the debit. The ODFI, in turn, has contractual recourse against its customer, the originator, if the consumer claims the debit was, in fact, unauthorized.

[17] Roth, A. (2000, September 27). "7 Banks to Offer E-Conversion of Checks", American Banker OnLine, Vol. 165, page 1.

[18] NACHA, The Electronic Check Council. "2001 ACH Statistics: e-Check Applications ". Found at http://ecc.nacha.org/, June 13, 2002.

[19] Federal Reserve System (2000, June 22). Request for Comment. "The phrase 'similarly authenticated' was added to Regulation E in 1996 (61 FR 19678, May 2, 1996), and was intended to permit electronic authorizations. The supplemental information indicated that the authentication method should provide the same assurance as a signature in a paper-based system, and cited security codes and
digital signatures as examples of authentication devices that could meet the requirements of § 205.10(b); and comment 10(b)-5 was added to the staff commentary to provide guidance on electronic authorizations." P. 11.

[20] Grant, N. (2000, September 20). NACHA memorandum to Electronic Check Council members.

[21] NACHA, The Electronic Check Council, p. 1.

[22] Ibid, p. 1.

[23] Marjanovic, S. (2000, June 14). Banks Tap ATM Systems to Banish 18B Checks. American Banker ONLINE. Vol. 165, p. 1.

[24] Marjanovic, S. p.1.

[25] There are two clearinghouses, both in the Southwest, that have varied this rule and hold depositary banks liable for the transaction after the midnight deadline has passed.

[26] ABA Survey, p. 14.

[27] Ptacek, Megan J. (2000, July 24) eCharge Purchases a Charter for its Fraud Protections. American Banker ONLINE. Vol. 165, p. 1.

[28] Slater, Alan T. (2000) Slide from Bank Administration Institute presentation.

[29] P.L. 90-321, Title IX, § 902 (May 29, 1968), as added, P.L. 95-630, Title XX, § 2001, 92 Stat. 3728 (Nov. 10, 1978).

[30] Board of Governors of the Federal Reserve System , 12 CFR Part 205, [Regulation E; Docket No. R-1074] Electronic Fund Transfers, ACTION: Final rule; official staff interpretation. Section 205.12Š Relation to Other Laws, March 15, 2001. P. 13.
"12(a) Relation to Truth in Lending
Comment 12(a)-1 is revised as proposed to distinguish between two types of unauthorized transfers: those where a consumer's access device is used to withdraw funds from a checking account with an overdraft protection feature, and those where the consumer's access device is also a credit card separately used to obtain cash advances. Examples illustrate how these rules apply in various situations. The majority of commenters addressing this subject supported the proposed revision. "

About the Author

Robert W. Jones is the Director of Fraud Risk Management and Loss Analytics at FleetBoston Financial in Boston, Massachusetts. In that capacity, Mr. Jones is responsible for leading FleetBoston's fraud reduction and operating risk analytics programs. He joined FleetBoston in January, 2000, after a 21-year career with KeyCorp, where he was responsible for all fraud detection and prevention systems and programs.

Mr. Jones co-chairs the Fraud Reduction Steering Committee of the Banking Industry Technology Secretariat (BITS) and is a member of the BITS Advisory Group. He is also a member of the American Bankers Association Deposit Account Fraud Committee. In 1998 he chaired the Financial Institution Fraud Committee of the Association of Certified Fraud Examiners. He is co-author of BITS' electronification fraud White Paper, an abbreviated version of which appeared in the September 2000 issue of the *Risk Management Association Journal.*

Mr. Jones is a graduate of the Utica College Master of Science Degree program in Economic Crime Management and currently serves as an Adjunct Professor at Utica College of Syracuse University. He frequently lectures domestically and internationally on issues of fraud management pertaining to the banking industry.