Customer Authentication: The Evolution of Signature Verification in Financial Institutions

Edward J. Potter, President, PSI Fraud Solutions

Historical Perspective

Background

Negotiation is one of the most significant commercial concepts of the Western world because it replaced the dependence of trade on equal exchange of goods ("barter") or payment in precious metals. Reliance on financial instruments such as notes, drafts, demand items and bills of exchange allowed commerce to extend beyond local venues into the broader, worldwide arena. The discovery of the "New World" as well as the opening of trade routes into the previously isolated Orient necessitated the movement to a broadened sphere for trade. To facilitate this flourishing global commerce, banks became the focal point for exchanging and paying those financial instruments. When financial instruments were presented to banks for payment, banks authenticated the instruments by verifying their customers' signatures before effecting the payments.

The case of Price v. Neal[1], which imposed limitations on the paying banks' ability to recover looses on instruments with forged makers' signatures, proved to be a landmark decision and it is the foundation of modern check law in the United States. The doctrine established by this case significantly facilitated the negotiability of all financial instruments because it established the liability on the paying bank for paying only those checks and drafts authorized by its customers. The decision addressed what is one of the most problematic and important areas of negotiable instrument law, the allocation of losses that result from a forgery. Most importantly, however, the Price doctrine provided a sound legal footing for the financial instruments that would be necessary to support the emerging global commercial market.

From the early nineteenth century, Courts in the United States adopted the basic Price doctrine with certain restrictions. For example, the courts did not follow the Price doctrine in those instances of forged endorsement or material alteration of the check but allowed banks to seek restitution in those cases. The reason for this practice is that the courts also provided another way for paying banks to recover their payments – breach of warranty. When a warranty of good title was made a forgery of endorsement or a material alteration was considered to breach that warranty. Also, protection from a claim for restitution by a paying bank was available to a holder in due course who had paid value for a check and who had accepted the check in good faith.

[1] Price v. Neal, 3 Burr. 354 (Eng. 1762), 97 Eng. Reprint 871, 1 W. Bl. 390, 96 Eng.

The restrictions to the Price doctrine were important to the banks and were instrumental in the evolution of the payments system though the 19th Century. Banks were considered to be a vital contributor to the growth of the American economy as the United States realized its "manifest destiny" and the nation's trade and commerce reached into the newly populated frontier and as far as the Pacific Ocean.

The Evolution of Banking Practices as a Response to Check Volume Growth

The post-World War II economic boom gave rise to a payments system whose volume is being driven by consumer demands. "Today, as a nation, we write something on the order of 65 billion to 70 billion checks each year and many electronic bill presentment and payment services continue to receive paper invoices and send paper checks. Looking back, banks and policymakers in the 1960's were grappling with significant problems created by the growth of economic activity relative to our ability to process paper payments and other financial instruments."[2] This consumer-driven growth has fueled a paper-based payments system with an annual value in excess of $78 trillion as measured by the Federal Reserve Bank. The most recent estimates by the Federal Reserve Bank peg the volume of paper-based transactions closer to 50 billion items a year.

As recently as thirty years ago, most banks compared signatures on nearly all checks presented for payment. Checks were presented to the branch of account where the signature was compared to the signature on file for the holder of that account. This process, which came to be known as signature verification, was the sole methodology used to verify that the account holder had authorized the payment. Once verified, checks were stored in the back rooms of those branches until they were sent back to the account holders at the end of each month with a statement of the account activity for that month. This process worked well for virtually all banks as checks were primarily used in business-to-business transactions. During the late 1970's, consumers discovered the convenience of using checks to meet their financial obligations, and check volume grew through the 1980's and into the 1990's. The banks responded to this growth in the number of accounts as well as the volume of checks presented for payment by centralizing the signature verification, storage and statement rendition functions in one processing center. Once centralized, banks began to enhance the new processes by implementing new computer applications to improve the operating efficiency of the processing center's staff. Banks derived economies of scale from centralizing common functions, improving processes through new technologies, and developing the proficiencies of staff experts in specialized functions. This is particularly true for the signature verification function where expertise came only through experience.

As the average volume of checks increased and the average value of the check decreased, banks discovered that it was cost prohibitive to compare signatures on every check presented for payment. As a consequence, banks looked to new processes that

[2] Ferguson, Roger W. (October 2000). Presentation to a workshop on promoting the use of electronic payments, held at the Federal Reserve Bank of Chicago. Available: http://www.bis.org/review/r001016c.pdf

would help them to minimize expenses while focusing on the checks that posed the greatest risk. Banks centralized the signature verification function into the back office and developed new processes that enabled them to leverage the specialized skills of their back office staff while minimizing their risk of losses from paying unauthorized checks.

Current Customer Authentication Practices as Documented by ABA Surveys

Today, fraud, particularly that type of fraud associated with identity subversion, is a problem for banks regardless of size or location. In the early 1990's, that same type of fraud was mainly a problem of the large money center banks because they were accessible through their many branches, had a broader customer base with whom they were less familiar, and were frequently distracted due to mergers and branch consolidations. However, large money center banks had the resources to support their efforts to reduce the risk of losses to fraud. At first their efforts were focused on developing internal software applications. As vendors developed software that responded to the banks needs, the banks turned more to the vendor applications than their own internal software for support of the signature verification process.

In the early 1990's, banks looked primarily to their internal staff to develop applications in support of their signature verification functions. The reason is that there were no vendor applications available at that time. During the mid 1990's several vendors developed software that banks could use to help focus their back office staff on those checks that were the most likely to be fraudulent.

The American Bankers Association ("ABA") does a survey of all its member banks to document how banks respond to attempts to commit fraud. The survey includes banks of all sizes and the ABA publishes the responses by groups according to asset size. The most recent survey was done in 2000[3]. In that survey, the large banks' responses (large banks defined as banks with assets greater than $5 billion) showed that 57.6% of the banks with assets between $5 billion and $50 billion and 100% of the banks with assets over $50 billion used vendor application software to support their signature verification process. Interestingly, those same banks reported using internal software in addition to the vendor applications. Over 36% of banks whose asset sizes range from $5 billion to $50 billion and over 72% of the largest banks continued to supplement their use of vendor applications with applications developed internally.

Clearly, the largest banks have refined their back office signature verification process to include computer-based application software. This refinement provides those banks with the ability to safeguard customers through signature verification practices that are best practices and reasonable standards for the financial industry.

[3] American Bankers Association (2000). ABA Deposit Account Fraud Survey Report. Washington, D.C.: American Bankers Association.

Legal Perspective

Defining Reasonable Commercial Standards

Reasonable commercial standards within the financial industry have evolved as banks and other financial institutions have adopted new practices and implemented new technology infrastructures to accommodate the increasing demands of their commercial and individual customers. Such demands include the need for faster methods of payment, more "user friendly" payment products and wider acceptance of non-cash items as payments for commercial and consumer transactions.

The first attempts at regulating commercial and financial activity resulted in the Negotiable Instruments Law ("NIL") that was adopted as law in 14 states by 1898 and the remaining states by 1924. Although the NIL promoted uniformity it was too vague to achieve it. Courts in various states began to interpret the NIL in rulings that were diverse and far from uniform. In an effort to bring more standardization to financial transactions, this 19th century code was gradually replaced by the Uniform Commercial Code ("UCC"). The UCC movement started in the 1940's and was eventually adopted by all the states in the 1960's. However, the UCC was not able to keep up with all the changes in financial and commercial activity during the latter half of the 20th century so again the financial industry turned to the courts for support.

Uniform Commercial Code

The most current version of the UCC, the 1990 version, has been adopted by 48 of the 50 states. The earlier version is the 1962 version and it continues to be operative in New York and South Carolina.

Both versions of the UCC assert that, once a payor or drawee bank has paid a forged check, it may not recover the proceeds back from another bank or person who received the payment in good faith. This principle reflects back to the case of Price v. Neal, the holding of which continues to be accepted by American courts. However, the current version of the code recognizes that customers, as a matter of convenience, have turned to automation to authenticate their checks. The 1990 version of the UCC recognizes this, "In fact, Section 3-401(b) states that "a signature may be made

(i) manually or by means of a device or machine, and
(ii) by the use of any name, including a trademark or assumed name, or by a word, mark, or symbol executed or adopted by a person with present intention to authenticate a writing".

This section is very flexible and looks to the intention of the party and not the form of the signature".[4]

[4] Carrubba, Paul A. (1993). The Banker's Guide to Checks, Drafts, and Other Negotiable Instruments (p.55). Burr Ridge, Illinois: Irwin Professional Publishing.

The 1990 version of the UCC § 3-406 recognizes that banks no longer process checks with the same exactitude as in the past and mandates that a customer exercise ordinary care in the issuing and protection of financial instruments. In this same version, UCC § 3-406 (a) raises the issue of comparative negligence. Under this subsection a person whose failure to exercise ordinary care substantially contributes to the alteration of a check or the creation of a forged signature cannot assert the alteration or forgery against a bank that pays the item in good faith. This subsection of the UCC is basically unchanged from the 1962 version. By itself, this subsection protected not only persons acting in good faith but also those banks that observed reasonable commercial standards. This subsection did not protect a bank if it did not observe ordinary banking standards. "Subsection (b) is a substantial change from the earlier version of this section. Under the old version, if the person asserting the preclusion failed to exercise ordinary care, the right to assert the preclusion was lost. The drafters of the new version, however, recognized the inequities of such a provision and rightfully introduced the concept of comparative negligence."[5] Also under this concept, a bank can assert defenses even if it failed to follow its own procedures. Consider the case of a customer who left a signature replication stamp unsecured. The stamp is stolen and used to create checks. The paying bank does not verify the customer's signature. In this case, a court could find the customer to be fully liable because the customer's failure to exercise ordinary care and not the bank's failure substantially contributed to the creation of the forged checks.

Evolution into the New Payment Systems Environment

Defining the New Environment

The Payments System is currently defined as the combined paper-based processes, procedures, rules and regulations employed by the nation's banks and Federal Reserve System for the express purpose of moving funds between banks and individuals in support of commerce. The new Payment Systems environment will be defined by the major driving influences that are evolving from the current environment. Those influences include the proposed Check Truncation Act ("CTA"), the growth of point of purchase conversion and other electronified transactions' volumes and the emergence of new technologies, particularly those that utilize the Internet.

The new Payments Systems environment will be less paper-based and more electronified. The electronification of checks refers to the process of converting paper checks into some form of an electronic transaction such as a check image, an ACH debit or an electronic funds transfer (EFT) debit. The new environment will require banks and other participants (e.g. merchants, service providers) to assume more responsibility to ensure the validity of the transaction that they are about to originate.

[5] Ibid. (pp. 64-65).

The Check Truncation Act

The purpose of the CTA is to facilitate check truncation by eliminating some of the legal impediments to the use of electronics in check processing. This will allow all financial institutions to participate in an environment in which the truncation of checks can occur at any point in the payment process. Check truncation is the replacement of the original paper check with an accepted replacement that accurately represents the original transaction within the Payments System. The following principles have guided the drafting of the Check Truncation Act:

- The law should result in improvements to the overall efficiency of the nation's payments system;
- The law should foster innovation without mandating the receipt of checks in electronic form, significant operational changes, or specific technical solutions or operational processes;
- A financial institution and its customer should be in the equivalent legal and practical position whether receiving a substitute check or the original check;
- The burden associated with the rule should not outweigh the associated benefits for either financial institutions in the aggregate or their customers in the aggregate. It is recognized, however, that there are inherent difficulties in quantifying these burdens and benefits; and
- The financial institutions that choose to convert a check to, or receive a check in, electronic form receive most of the associated benefits, and thus should internalize the costs and risks related to the creation of a substitute check, to the extent practicable.[6]

One significant risk that check truncation poses to the paying bank is that it does not allow for the bank to review the original check. The original check has physical attributes such as color, styling and placement of corporate logos, that are helpful to bank staff in determining whether a document is counterfeit. In addition, safety features such as infrared or ultraviolet inks, two dimension bar codes, and watermarks that may be helpful to determine the validity of a check may not be transposed to the substitute check.

Point of Purchase Conversions

The point-of-purchase ("POP") conversion is a process whereby checks are converted into electronic debits and processed using the Automated Clearing House ("ACH") network. In this process, the consumer submits an original check and signs an authorization document, a copy of which is returned to him or her when the transaction is completed. The merchant scans the written check through a special reader that captures the account, check and routing number as well as the purchase amount. The check data is sent to an agent for authorization of the amount. Once authorized, the amount is converted to an electronic transaction and sent through the ACH network for payment.

[6] The Federal Reserve Board, Draft Check Truncation Act. See www.federalreserve.gov/PaymentSystems/truncation/actprin.htm

The consumer signs the separate authorization document and receives the original check back, which has been stamped "void" by the merchant.

New Emerging Payment Technologies and Products

Internet Banking

The emergence of the Internet as a premier growth medium for the new e-business environment has provided financial institutions with a new operating paradigm. As with all new paradigms, there are many opportunities and more than a few challenges. Financial institutions must learn to face these environmental uncertainties while continuing to meet their responsibilities to the marketplace. The opportunities offered by Internet banking include the ability for a financial institution to offer services to customers who are outside of their normal footprint without the legal hurdles presented by interstate banking strictures as well as to extend brand reach by forming e-business alliances with stock and mutual funds brokers, insurance companies to offer a more diversified portfolio of financial services.

Some of the new challenges of Internet banking are increased competition financial service providers (e.g., Fidelity, Vanguard and Equitable), "virtual" banks that exist solely on the Internet (e.g., X.com and Wingspan) and disintermediation of banks' traditional customer base by non-financial companies offering Web-based financial services through small financial institutions that would not otherwise have the market scope to reach these customers. While facing this competition, financial institutions are still mandated to operate under federal and state banking regulations that do not contemplate the existence of the non-financial institution Internet competitors.

Electronic Check Presentment

Electronic Check Presentment ("ECP") refers to the process of capturing and transmitting MICR line information between banks in lieu of physical documents. Depositing banks begin the funds collection process by transmitting MICR line information while continuing the presentment of physical checks via ground and air transportation. More recently, banks have been developing an image capture and exchange process that will eventually replace the need to exchange any paper at all.

Check Imaging

The term "check imaging" refers to the process whereby check images are captured via image cameras and stored in a digitized format. This process is usually accomplished on medium- to high-speed check processing equipment (such as that manufactured by IBM, NCR, Unisys and Banc Tec), which is used primarily in financial institution back offices for the capture, sorting and distribution of checks and other MICR-encoded documents.

The benefits of imaging over microfilming are quality, transportability, availability and timeliness. The capturing financial institution can keep an archival copy of every document processed. A copy of a customer's check can be included in the statement mailing. Checks drawn on other financial institutions can be exchanged with those financial institutions in lieu of physical documents. Check imaging reduces the risk inherent in the payments system by considerably reducing the time in which checks are presented and paid.

Responsibilities in the New Environment

Financial institutions have new responsibilities in the new environment, including:

- Serving the needs of the business community and individuals by providing a secure process wherein financial transactions are completed in an environment that ensures their privacy and security.
- Ensuring that the financial portion of e-commerce activities are completed expeditiously and with audit trails that allow the transaction to be undone in response to account-holder direction, and in accordance with the Uniform Commercial Code and Federal Reserve Bank regulations.
- Ensuring the privacy of account holders and the security of the accounts they own.

Banks have always had a fiduciary responsibility to their customers to protect those financial assets with which they have been entrusted. That responsibility has been further broadened to include non-financial assets such as personal information. "The Privacy provisions of the Gramm-Leach-Bliley Act of 1999, and the newly proposed rules to implement the statute recognize the unique commercial value of the personal information acquired by banks…and other financial institutions in opening and maintaining accounts."[7] The challenge that privacy presents for financial institutions is to get sufficient information about individuals in order to authenticate them as owners of accounts or transactions while respecting their right to privacy. The answer may well lie within the financial institution itself and the processes it develops to authenticate an individual prior to opening an account with them, or with third party providers that provide authentication without violating an individual's right to privacy.

Challenges of the New Environment

The Growth of Check Fraud

Check Fraud has increased to an estimated $2.2 billion according to the ABA Deposit Account Fraud Survey Report for the year 2000[8]. This number includes $679 million in actual losses and $1.5 billion in losses avoided. The leading causes of those

[7] Clark, Barkley, Get Ready for the New Privacy Rules Governing Account Information Held by Financial Institutions, *Clark's Bank Deposits and Payments Monthly*, Volume 8 Number 7 [January, 2000], Arlington, Virginia: A.S. Pratt & Sons Group

[8] American Bankers Association (2000). Op Cit.

losses include forged maker signatures and counterfeit checks, debit cards, identity theft and Internet based transactions. Clearly there are many challenges to banks and their customers in the new environment. The business paradigm is evolving into one where accounts are opened remotely and transactions are originated through a paperless, electronic medium.

In particular, the new Internet driven economy is fraught with uncertainty for financial institutions. "Uncertainty means that decision makers do not have sufficient information about environmental factors and they have a difficult time predicting external changes… Characteristics of the environmental domain that influence uncertainty are the extent to which the external domain is simple or complex and the extent to which events are stable or unstable."[9] In this new business environment, banks will encounter a new breed of criminal, one who is intelligent, better organized and more sophisticated in the use of technology for criminal purposes. Future attacks against banks and their customers will come from members of organized crime enterprises who will subvert technology to steal existing identities or create new ones. Then, using the anonymity promised by the Internet, these perpetrators will steal money, goods and services from innocent bank customers and unsuspecting merchants and service providers. Major organized crime groups such as the American and Sicilian Mafia, the Russian Mafiya, the Japanese Yakuza, South American drug cartels, and Nigerian groups have all developed an expertise for suborning the Internet to advance their criminal enterprises. Generally, these criminal organizations are motivated by greed. Their objective is simply to accumulate wealth (and the power that goes with it) through illegal but profitable means. However, there has arisen a more insidious opponent. Islamic Terrorist organizations such as Al-Qaeda, have been judged responsible for committing such atrocities as the recent suicide attacks on the Pentagon and the World Trade Center. These organizations are known to have developed expertise in identity theft and using that expertise to not only hide undercover operatives, but also to defraud American financial institutions of funds that are used to finance future acts of terrorism.

The challenge created by terrorist groups such as Al-Qaeda goes beyond utilizing stolen identities to commit theft. In the days following the attacks on the World Trade Center and the Pentagon, investigators were increasingly frustrated in their attempts to identify those responsible for the atrocities. "The fact that a legion of detectives can't conclusively decide who those 19 men were indicates just how difficult it is – even in our database-friendly times – to pin down something so slippery as one's identity. Identity theft, which was seen as an irritating consequence of modern life before Sept. 11, is now seen as a potential threat to national security."[10]

[9] Daft, R.L. (1998). Essentials of Organization Theory and Design. (p.52).Cincinnati, Ohio: South-Western College Publishing

[10] Manjoo, F. (2001, October 1). Another Thing To Fear: Identity Theft. http://www.wired.com/news/ (2001, October 1).

Identity Theft

Identity theft is defined under 18 USC 1028 as occurring when someone impersonates a legitimate customer in order to defraud a financial institution. The law, passed by Congress in1998, targets those who use the identity of another. The following year, Congress passed another law making it a crime to used trickery to obtain personal financial information of another person. For those who want to impersonate another person without their knowledge or consent, there are several methods of obtaining information about an individual and compromising their identity:

- theft of their personal belongings,
- tapping into their computer through a "worm" virus, or
- obtaining the information from employees of a financial institution or a credit bureau.

The seriousness of this problem has reached the highest levels of government where senior officials have expressed their concerns. "Some law enforcement officials and regulators say identity theft has become one of their most pressing problems. The Federal Office of the Comptroller of the Currency recently estimated that there are half a million victims of identity theft per year in the United States. What makes this problem particularly irksome for banks and other financial institutions is that identity theft presents some significant challenges to their fiduciary responsibility to execute duly authorized financial transactions for their customers. As these financial institutions migrate their financial services onto the Internet, customer authentication becomes problematic. Signatures are no longer a practical method of identifying customers, so the financial institution is relegated to using other means of authentication.

Internet Fraud

"The Internet has become the new frontier of fraud. The very attributes that make it so attractive as a means of communication and commerce also make it attractive to con artists. They have taken advantage of the low cost of communication that it affords, the capacity to reach a worldwide audience, and the fact that it is difficult to distinguish whether information and the source of that information is legitimate or not."[11]

Of particular concern to banks is that payment in both fraudulent telemarketing and Internet-related transactions is most commonly made by check or money order. These checks, which contain financial information about the payor are often sold, via the Internet, to other cyber criminals who will then use that financial information to create counterfeit checks drawn against the victim's account. Another concern for banks is that consumer confidence in the Internet is critical to the growth of legitimate electronic commerce. One of the challenges for banks is to provide an Internet environment that is safe for the legitimate customer. Crucial to that security is the bank's ability to correctly authenticate the originator of Internet-based transactions as well as to continue supporting

[11] Report from the National Consumers League to the U.S. Department of Justice Concerning Telemarketing and Internet Fraud, January 10, 2000.

those transactions, such as checks, that support Internet transactions in an off-line environment.

If banks do not rise to that challenge, it will have a detrimental effect on consumer confidence. An erosion of that confidence will have a serious impact on the growth of legitimate electronic commerce. The challenges for the financial industry, law enforcement, and consumer protection groups are to provide the appropriate balance between consumer privacy rights and the need for concerted and cooperative actions against the perpetrators of online fraud.

Current Successful Strategies

The Authentication Challenge

The fraud problem starts with the conflicting policies of maintaining individual privacy and knowing the customer. Banks in particular must endeavor to satisfy both these policies while affording delivery channels to the customer that are efficient and easy to use.

Utilizing software-based solutions that are currently being used by banks to prevent fraud in their "older" financial services such as credit card, EFT or even check and deposit processing can facilitate resolution of the dilemma. These systemic solutions can be divided into two broad categories, those that validate identities and those that authenticate transactions.

Physical Identity Authentication Strategies

Signature verification is the most common method used by financial institutions and their merchant clients to authenticate an individual's identity. However, signature verification is a technique that requires practice and diligence. It also requires a valid signature for comparison. As such signature verification at the merchant's site is neither practical nor effective. The back offices of financial institutions are the best places to verify signatures; however, those back offices are beset by two challenges:

- the volume of checks being presented for payment is too large for a bank to consider validating signatures on every item presented for payment; and,
- the proliferation of inexpensive optical scanning devices makes unauthorized signature replication a very easy method for creating counterfeit items.

The presentation of such identification cards as drivers' licenses, social security cards, etc. are not an effective means of customer authentication. Websites are available on the Internet that provide counterfeit identity cards to any requestor without demanding any proof of that person's true identity.

In summary, presentation of physical identity, though still used, is the least effective method for authenticating an individual.

Computer-Based Identity Authentication Strategies

Identity Validation Systems

In the category of identity validation, there are systems that have been used to validate the identity of a new customer who is seeking to open either a credit card account or a demand deposit (checking) account with the bank. Prudent banking practices dictate that some validation of the new customer's identity be done; to a small bank that may mean a few well-placed (but discrete) phone calls, to a large bank that can mean one of several automated identity validations. Two of the more popular systems are:

- FraudFinder® (e-Funds Corporation)
- Early Warning® (WJM Technologies)

FraudFinder® leverages data available through DebitBureau® a comprehensive source of debit data and utilizes neural-net modeling to pinpoint information most likely to be fraudulent. Early Warning® compares new account data with national databases of social security numbers, driver's license numbers, addresses, telephone numbers, and employer information. The system validates addresses, cross check telephone numbers to zip codes, ensure that the social security numbers align with the dates of birth, and, in some states, compare the drivers license numbers to a file of valid numbers.

In addition, many banks also do a credit check on new customers, as there is a direct correlation between a customer's credit worthiness and the potential of that becoming a fraud problem. These identity validation systems are transferable to the validation of Internet customers. Sound fraud prevention argues in favor of asking the same information of any new customer regardless of how they open an account. In addition, many banks will send a "welcome" letter to the address of record thus further establishing that the given address exists and is valid for the individual so named.

Physical Transaction Authentication Strategies

Transaction Validation Through Laser Ink Application

The application of laser ink detection ("LID") methodology is designed to minimize the problem of counterfeit checks. The concept is that an invisible ink is applied to valid check stock for legitimate customers. The ink is detectable to a reading device that uses a laser light beam that is keyed to a specific intensity. The light beam "excites" the ink, which reflects light back to the LID detection device. The device is attached to a high-speed sorting device that will pass information to a special sorting program. The program will read the file of accounts that are known to have LID ink on their checks. Checks that are supposed to have LID ink but do not will be sent to a specific sorter pocket where they will be manually researched and returned, if necessary. Thus, the detection of the ink validates the check stock as part of a high-speed sorting process.

The advantage of this type of strategy is that it provides a "passive" detection against fraudulent items. The customer has to do nothing except order the LID ink on his check stock. Further enhancements of this methodology include the possibility of sharing information among banks about which accounts print checks containing LID ink. This information could be shared by leveraging existing methodologies such as the shared fraud databases discussed in the previous section. Participation in a sharing forum such as that would provide depositing banks with information needed to identify potential counterfeit items more quickly and take measures to prevent losses.

Two Dimension Bar Codes

The application of two dimension bar codes provides protection against fraud on the face of the check. The bar coding may appear either embedded in existing design on the check (e.g. a corporate logo) or as a separate visible field on the face of the check. In either example the bar code contains the account number, payee name, dollar amount of the check and date the check the check was written. By applying PKI technology, the account owner or an authorized representative encodes the information onto the bar code format using a private key. The same information can be decoded using a public key made available to any depositing bank. Using Public Key Infrastructure ("PKI") technology provides authentication of the account holder as the originator of the document. Also, decoding and then comparing the information in the bar code to that which is on the check validates that the check information has not been altered.

Automated Signature Verification

Technology is approaching a more robust solution to the problem of signature verification. This solution is known as automated signature verification. This technology is use in a number of banks overseas and has established footholds here in the United States. One of the most promising applications has been developed by SoftPro that is based in Newark, Delaware and Boeblingen, Germany. Using existing image technology, combined with sophisticated application software, SignPlus is a complete signature verification solution, with the capacity to maintain a current, dynamic database for all account signatory information, and automatically verify transactional signatures both at the back office and at the teller line.

Computer-Based Transaction Authentication Strategies

Positive Pay

Positive Pay is a fraud prevention product offered by financial institutions to their corporate clients who issue large volumes of checks. One of the earliest and most successful fraud prevention strategy, this process requires the check issuer to send an "Issue" file to the paying bank. The bank then automatically compares the information on the check to that which is on the "Issue" file. Discrepancies will result in the check being separated for manual review and, if required, customer confirmation

Account Behavior Analysis

One method of authenticating transactions is by using software programs that monitor the "account behavior" for both the credit and the debit transactions and maintain historical files at the account level. Two software companies at the forefront of these types of fraud prevention solutions are Carreker Corporation and Sterling Software.

Sterling Software provides Vector Detect, an automated system designed to reduce check fraud losses by detecting counterfeit and forged checks. The system creates customer transaction profiles against which every on-us check is automatically evaluated, so your financial institution is protected on a daily basis from check fraud schemes.

Carreker Corporation's FraudLink® series are rules-based programs designed to detect aberrations from the normal (or "rules") patterns beyond thresholds established by the user department. FraudLink On-Us® is a mainframe-based fraud detection platform solution that can identify potentially fraudulent check items as they pass through the bank, either at the teller station or in the back office. With user-defined rules, it provides the flexibility to respond quickly to current fraudulent trends.

Shared Fraud Databases

Transactions can also be validated through access to shared databases that contain account information. These databases provide a depositing bank with information to identify potentially fraudulent items and take precautionary steps such as placing a hold on the account of deposit. One example of a shared database provider is Primary Payments Systems Inc. ("PPS"). The success of their database is that it contains account information from most major banks and many of the smaller banks throughout the country. To use this type of database, a depositing bank captures information from the MICR line of the check and sends it to a database provider such as PPS. The provider compares the supplied information to the information about that account that it has on its database. The provider then sends back to the bank information as to whether the account is a valid, open account, and whether this account has a history of fraudulent transactions. Using this information, the depositing bank can take precautionary steps such as placing a hold on the account of deposit or even refusing to accept the check as a cash item.

Securing the Future of the Financial Industry

Historical Framework

The rise of mercantilism began in the 16th century and lasted for approximately 200 years. Mercantilism is the European economic theory and practice that promoted governmental regulation of a nation's economy for the purpose of augmenting state power at the expense of rival national powers. The tremendous growth in trade that evolved from the newly discovered American continents fueled mercantilism's ascent. Mercantilism was an enormous change in the dynamics of the world's economies and represented a tremendous challenge to the businesses and financial institutions of that

day. Throughout the British Empire in particular, financial institutions rose to that challenge by facilitating international commerce through creation of paper-based financial instruments that were to be used as settlement for goods or services. Merchants, even those from different countries accepted these items with complete faith that the financial institutions upon which they were drawn would honor them. It wasn't until the mid-18th Century, almost 150 years after the beginnings of the use of paper instruments that British law ratified these practices through the momentous decision rendered in the case of Price v. Neal.

Challenges to Existing Authentication Standards

The economic and commercial environment facing today's financial institutions challenges those institutions as they have never been challenged before, even during the era of mercantilism. The advent of the information age has been heralded by the availability of inexpensive, user-friendly computers that put an array of automation tools in the hands of business users and their customers. This electronified power enables the entire breadth of a financial institution clientele, from the largest corporation to the individual consumer to be provided computer-based, Internet-driven products and services. This new service paradigm does not come without sacrifice. The customer signature has been toppled from its place as the basis for customer authentication of a financial document. Signatures are too easily compromised by today's modern technology. Scanners, copiers and computer art programs provide a counterfeiter with the tools to replicate not only the signature but also the very document itself. Those same tools also provide the malefactor with the apparatus needed to create phony drivers' licenses, passports and other paraphernalia that assists in the impersonation.

Regulations such as the UCC provide little guidance, they are too vague to address the specific issues surrounding customer authentication. The Check Truncation Act defines the Image Replacement Document and describes its usage and acceptance. Privacy legislation is aimed at protecting the individual's privacy, but it fails to address the financial institutions' needs to share information about names, addresses and other information that has been used in fraud schemes.

Banks and financial institutions have endeavored to enlist technology to support fraud reduction efforts. For example, the 2000 ABA survey shows the vast majority of banks with assets over $5 billion are using rules-based technology to support their signature verification process. The technology platforms use rules to measure account activity patterns and identify those items that are more likely to be fraudulent. Interfaces to the banks' sorting programs help to separate the suspect items for manual verification. This verification, also known as "check review" is more thorough than the old process of verifying signatures because check review includes inspection of the physical properties of the check (e.g. color, location of corporate logo and print fonts) in addition to signature verification.

Banks cannot look to the courts for immediate support of these new processes. The legal system addresses issues specific to certain cases and, courts arrive at

contradictory conclusions. Also common law, as determined by court findings, lags behind the immediate issues of the modern business environment. The case of Price v. Neal was not adjudicated until long after paper instruments were created to facilitate the global trade economy that arose in the 16th Century.

The Information Age has arrived and with it the Information Economy. The new Economy is making more and more demands upon financial institutions for their services. Clearly, those demands will be met, if not by financial institutions then by other service providers. One of the obvious examples is that of the "screen aggregators". These Internet companies specialize in providing an interface to multiple web sites for the consumer so that only one login is needed. It is a very convenient service for the consumer and a very important one for the aggregator who is now privy to a wealth of financial information about consumer preferences – where they shop, where they bank, and what are their buying habits and spending patterns. In response to this threat, many of the larger banks are offering 'aggregation" services to their account holders.

Recommendations

The financial institutions and their business partners must continue to seek and develop new solutions to the issue of customer authentication and transaction validation. Some of the applications are very effective when used by one institution. However, many of these applications, though effective as a singular institutional solution, may become many times more powerful when adopted as an overall industry approach to solving the issues of customer authentication and transaction validation providing:

- they become a standard for the financial industry; and,
- information about which banks use them and how they are used are made available to the financial industry.

The more information that the originating merchant or a depositing financial institution has about a customer or a financial transaction, the more effective each will be in combating authentication fraud. In addition to those successful strategies that financial institutions are currently using, the financial services industry must look to further standardization of their fraud strategies and more effective information sharing that will result in a more united approach to fraud solutions.

New Standards for Identity Authentication

Every financial institution has information about its account holders. That information can be used to authenticate a customer whenever a customer interacts directly with a financial institution to open a new account or to originate a transaction using the financial institution's on-line services. In those examples, a financial institution can take advantage of the proximity of the communication to validate the customer's identity by utilizing of one of the following:

- what the person knows – a combination of both "in wallet" information such as social security number or "out of wallet" information such as the name of an old pet;

- what the person has – a token that generates random numbers and is synchronized with the authentication program or a private key that encrypts the transaction so that only a corresponding public key can decrypt it; and,
- who the person is – utilizing biometrics to confirm an identity by comparing physical characteristics to those on file.

There are two levels at which identity can be established, using information about the customer that the financial institution has on file, or using information about the customer that has been established by other financial institutions and shared through a common database.

An example of this type of information sharing is BioPay®, a database that is accessed by fingerprint. The database record contains information about the customer and may also include a photo of the individual and also of the check stock the individual uses.

The New Fraud Risk Paradigm

If financial institutions are going to continue upholding their fiduciary responsibility to their customers, they need to employ new standards for customer authentication. Technology has made simple verification of the signature on a document to be ineffective in authenticating a financial transaction. Similarly, the ease of obtaining false identification by using the Internet to probe both legitimate and illegitimate sources has rendered the more common forms of establishing identification (i.e. driver's license, passport, etc.) obsolete. New standards must be developed for authenticating customers and their transactions. These standards will rely heavily on technology solutions to what has been a technology problem, the creation of false documents to support the commission of fraud. The previous sections have provided examples of technologies that can be adopted as industry standards. However, there is no "silver bullet" to the authentication problem in the payment system. Like cancer, there are many variations, and each one requires its own unique solution.

Each financial institution will find an approach to effective risk management that addresses the weaknesses in its customer authentication and transaction validation processes. The corporation's own internal organization structure and corporate culture will influence the risk management solution. Generally, however, the steps taken toward an effective risk reduction program are:

- Centralization of fraud loss reporting to identify the scope of the problem on a corporate basis;
- Strengthening of internal controls and procedures currently in place;
- Development and implementation of new technologies to enhance fraud management effectiveness; and,
- Joining industry forums and forming partnerships to maintain a "leading edge" approach to fraud solutions.

Joining industry forums and creating partnerships is the most important part of solving the fraud issue on an industry-wide basis. Individuals intent on committing fraud

rely on the fact that financial institutions depend on their own devices to address fraud; hence, they are often able to perpetrate the same fraud on different financial institutions, often using the same false documents to create the same false identity.

The organized crime groups described earlier in this document are known to share information about the latest technology available to commit fraud, which institutions are easier targets and what are the current most effective scams. While fraud against financial institutions may never go away completely, the solution to controlling fraud risk must be found by addressing the problem on an industry-wide basis.

The information sharing can take several forms and all of these forms will be needed to continue to minimize the risk to the payments system for losses from fraud:

- Sharing account and transaction history information;
- Sharing best practices and successful strategies; and,
- Sharing information about fraudulent activity.

Controlling fraud, particularly that fraud associated with falsified customer identity, can be more effective if it addressed at the origination of the payment process whether that is at a merchant or a financial institution.

Authentication is no longer the sole province of the paying institution. In the new financial services paradigm, it is responsibility of all participants in the payments system.

References

Carrubba, Paul A. (1993). The Banker's Guide to Checks, Drafts, and Other Negotiable Instruments. Burr Ridge, Illinois: Irwin Professional Publishing.

Daft, R.L. (1998). Essentials of Organization Theory and Design. Cincinnati, Ohio: South-Western College Publishing

Nichols, R.K., Ryan, D.J., and Ryan, J.J.C.H. (2000). Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, New York: McGraw-Hill.

Richards, J.R. (1999). Transnational Criminal Organizations, Cybercrime, and Money Laundering. Boca Raton, Florida: CRC Press LLC.

American Bankers Association (2000). ABA Deposit Account Fraud Survey Report. Washington, D.C.: American Bankers Association

Clark, Barkley, Get Ready for the New Privacy Rules Governing Account Information Held by Financial Institutions, *Clark's Bank Deposits and Payments Monthly*, Volume 8 Number 7 [January, 2000], Arlington, Virginia: A.S. Pratt & Sons Group

On-Line References

The Federal Reserve Board, Draft Check Truncation Act.
www.federalreserve.gov/PaymentSystems/truncation/actprin.htm. (June 2, 2002)

Manjoo, F. (2001, October 1). Another Thing To Fear: Identity Theft.
http://www.wired.com/news/. (October 1, 2001).

Anon., January 10, 2000. Report from the National Consumers League to the U.S. Department of Justice Concerning Telemarketing and Internet Fraud.
http://www.fraud.org/welcome.htm. (September 22, 2002)

About the Author

Edward J. Potter (potterej@msn.com) has recently founded a consulting firm to advise the financial services industry on how to manage their fraud-related operational risk. He has started this endeavor after a 25-year career with JP Morgan Chase where he was responsible for developing fraud detection and prevention strategies with global and domestic business areas within the bank.

Ed has been chairing the JP Morgan Chase Bank Fraud Committee since 1995. That Committee has been tasked with developing enterprise-based solutions to risk from payments systems fraud. The success of the Committee is evidenced in that the Bank has traditionally had one of the lowest amounts of fraud losses among peer banks. He has also chaired the Banking Industry Technology Secretariat (BITS) Successful Strategies Subcommittee and was a member of the Fraud Reduction Steering Committee. Additionally, he chaired the New York Clearing House Check Fraud Committee and was a member of the American Bankers Association Deposit Account Fraud Committee.

Ed frequently speaks about fraud to financial institutions and their corporate clients. He is currently working with BITS to assess the impacts of the Check Truncation Act, the National Automated Clearing House ("NACHA") Point of Sale program, and other electronification initiatives on the existing risk management platforms in financial institutions. He received his undergraduate degree from Villanova University and is a recent graduate of Utica College where he has earned a Master of Science in Economic Crime Management.