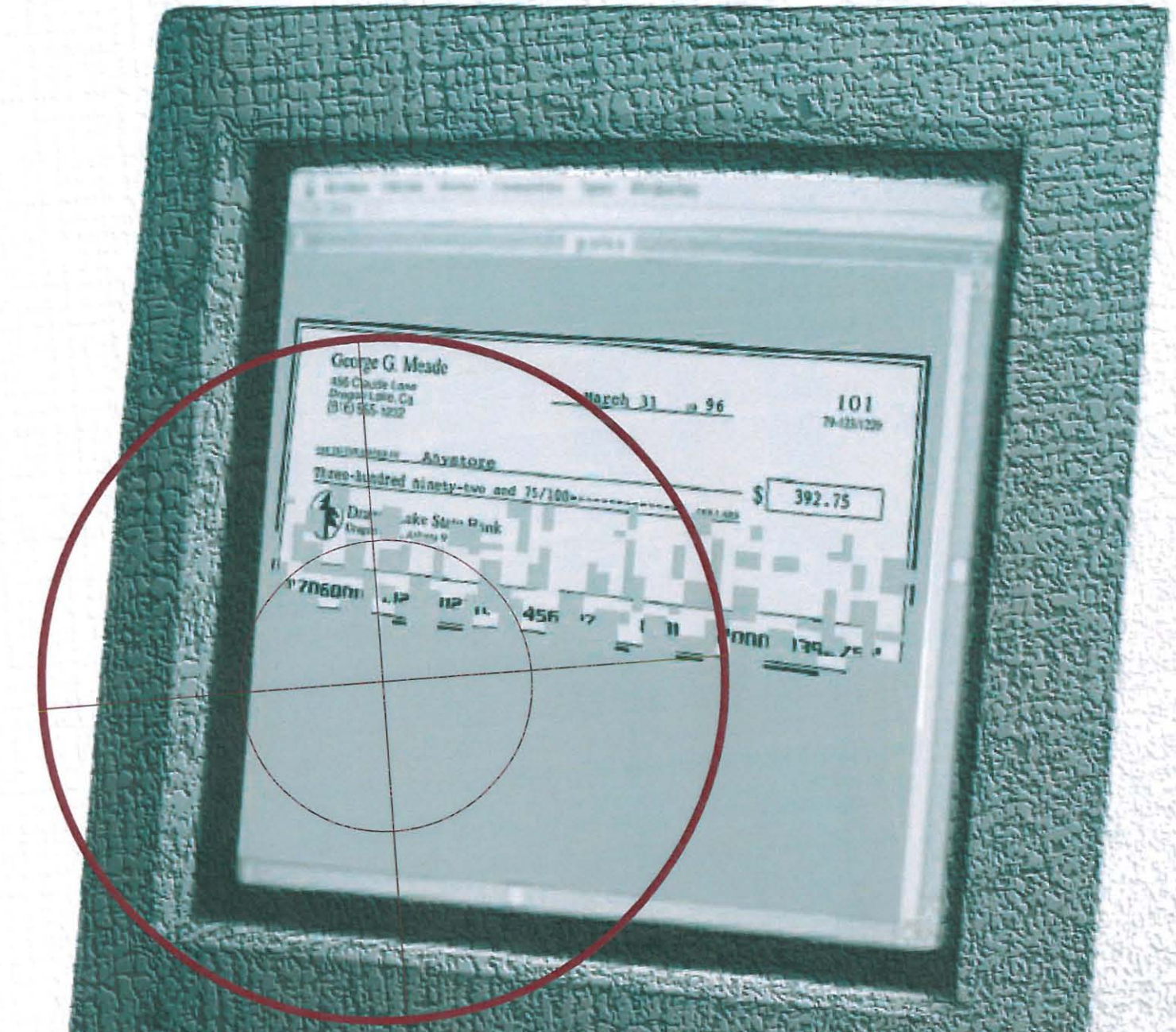


CHECK FRAUD

Federal Reserve System

FEDERAL RESERVE

FINANCIAL SERVICES

Check fraud affects every financial institution, every business, and every individual throughout the United States and around the world. Industry sources estimate that check fraud and counterfeiting costs our nation between $10 and $14 billion per year. Some observers are calling it the growth crime of the 1990s.

This brochure offers a look at the various forms of check fraud and what each of us can do to prevent it. If you have any questions or concerns, please contact your local Federal Reserve Bank.

Forms of check fraud

You and others in your institution may have come in contact with a number of types of check fraud. Here are some of the more common forms encountered today.

Forged signatures usually involve the use of legitimate blank checks, with a false imitation of the payor signature on the signature line. Many cases of forged signatures are perpetrated by a person known to the valid payor. "Employees gone bad" are one source of forged signatures. In other cases, signatures are forged on blank checks stolen from the mail while being shipped from the check printer to the account holder. The theft of blank check stock from the mail tends to increase following natural disasters when account holders have to replace destroyed check stock.

Forged endorsements often involve the theft of valid checks which are then endorsed and cashed or deposited by someone other than the payee. Marital partners involved in separation or divorce proceedings are a common source for forged endorsements. Forged endorsements can also appear on checks made payable to more than one party when one party endorses the check for all parties.

Counterfeit checks are the fastest growing source of fraudulent checks. Check counterfeiters use today's sophisticated color copiers to copy valid checks. Exact imitations of genuine checks can be created with readily available desktop publishing capabilities. Scanning a real check into a computer, and then using desktop publishing

software to change some of the check information, allows the counterfeiter to include many valid check components into the imitation. When this counterfeit check is printed on a high quality laser printer, extremely authentic looking "bad" checks can be created. Some of these counterfeit checks even include MICR (magnetic ink character recognition) line characters. As computer technology continues to become more widespread, this form of check fraud has the potential for explosive growth in the near future. Almost any kind of check can be counterfeited, including cashier's, payroll, government, and traveler's checks.

Altered checks are defined as valid check stock with certain fields changed. When the payee name is changed, payment is made to the wrong person. The courtesy and/or written amount can be increased, resulting in overpayment to the payee. Some checks have had the MICR line altered with bogus information (such as the routing/transit (ABA) number or the account number) to slow down the clearing/return process. Checks can be altered to include information that assists the criminal in negotiating the check. For example, bank officer approval stamps have been lifted from one check and included on another check of higher value.

Check kiting requires multiple bank accounts and the movement of monies between accounts. The check kiter takes advantage of the time required by a bank to clear a check. A check drawn on one bank is deposited in a second bank without having proper funds to cover the check. When the deposit is made, the bank grants the depositor a conditional credit, and will allow the customer to draw checks against uncollected funds. The customer then writes a check on the second bank and deposits it in the first bank to cover the original check. Unless detected, this process can continue indefinitely, covering one check written against insufficient funds with another check.

Third-party bill paying services are often misused to commit check fraud. The checks produced by these service providers do not include the payor signature. Instead, the signature line reflects something such as "signature on file." Unauthorized checks produced by third-party payment services are usually not detected until the customer reviews the monthly bank statement. By the time the customer identifies the unauthorized check, it is often too late to recover the funds, since the "24-hour window" (actually until midnight of the next banking day) for the timely return of checks has long since passed. These checks usually sail right through the check sorting operation, since they include good account information and sometimes even include good serial numbers. Too often, both business and individual account holders seem unaware of how their account information, given too freely to a requesting party, can be used for fraudulent purposes.

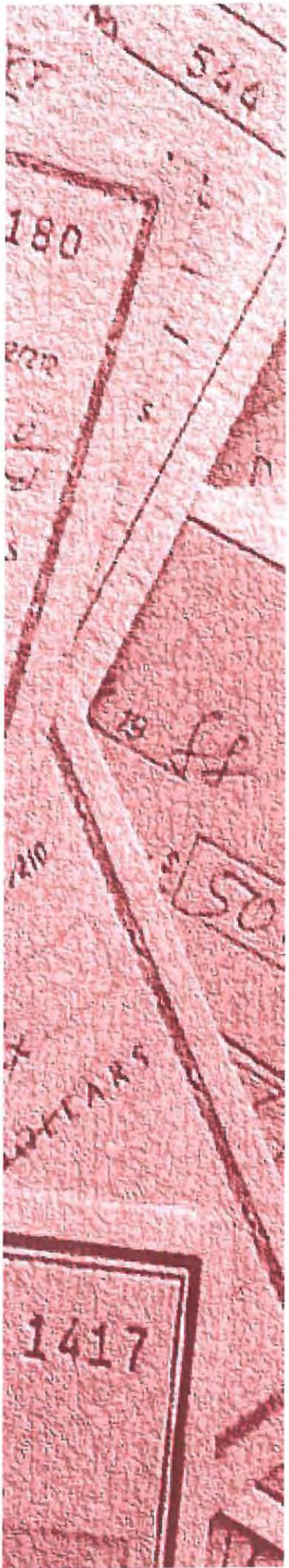
Demand drafts can be misused to commit check fraud. This practice involves the misuse of account information to obtain funds from a person's bank account without that person's signature on a negotiable instrument. Other terms for demand drafts are "preauthorized drafts" and "telephone drafts." While there are many legitimate business uses of demand drafts, such as quick-turnaround telephone transactions initiated by airlines and car rental companies, demand drafts have been used by deceptive telemarketers who obtain bank account information and withdraw unauthorized funds from consumers' bank accounts, without their realizing that such withdrawals are occurring.

The Federal Trade Commission has published a "Telemarketing Sales Rule," effective December 31, 1995, which is designed to offer some protection to consumers and banks against deceptive telemarketing practices. Among other things, the rule requires "verifiable authorization," such as written consent or express oral authorization which is tape recorded. While rules and laws help, consumers (and businesses) still need to use demand drafts cautiously and provide account information only to known reputable payees.

Other forms of check fraud

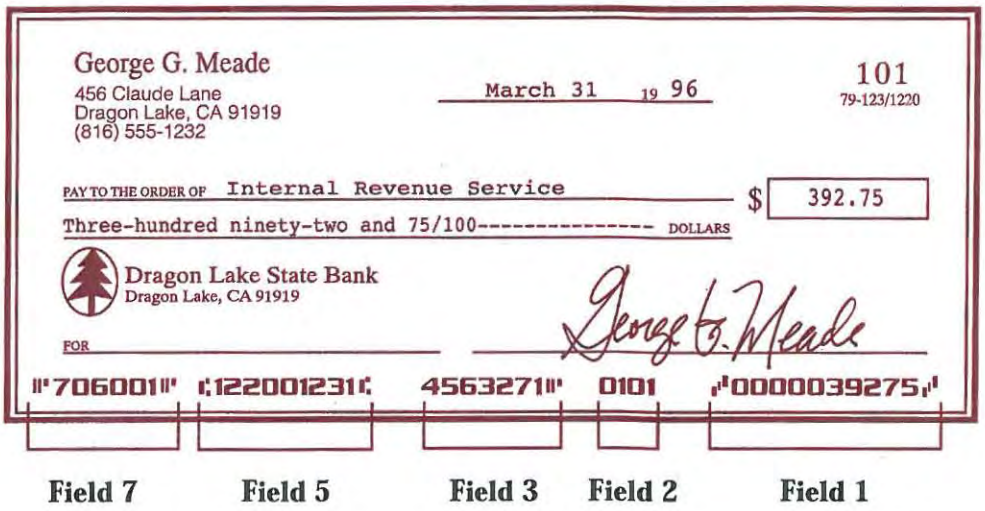
Check fraud has also been committed by individuals opening fraudulent bank accounts or making fraudulent deposits through the automatic teller machine (ATM) network. Others have ordered checks directly from check printers using bogus names, addresses, routing numbers, and account numbers. Still others have counterfeit money orders cashed by check cashing operations.

Another scheme involves the deposit of fraudulent checks, followed by quick funds withdrawal before actual check clearing. This form of fraud is actually made easier by the fact that most banks, for competitive reasons, make funds available sooner than required by Reg CC.



Elements of a check

Recognizing a fraudulent check is easier when you are familiar with the components that make up a good check. All parties who participate in check transactions should be aware of the following elements of a check:



Perforation- Look for at least one perforated side on the check.

Bank address- The address of the bank should correspond to the appropriate Federal Reserve District. For example, if you receive a check drawn on a bank in California, the routing/transit number generally should depict the Twelfth Federal Reserve District (12). Note, however, that some banks with offices in several Federal Reserve Districts are using a routing/transit number for one Federal Reserve District and a bank address in a different Federal Reserve District.

Federal Reserve District and Office- The first two digits of field 5, the routing/transit number in the MICR line, indicate the Federal Reserve District.

01 - Boston	07 - Chicago
02 - New York	08 - St. Louis
03 - Philadelphia	09 - Minneapolis
04 - Cleveland	10 - Kansas City
05 - Richmond	11 - Dallas
06 - Atlanta	12 - San Francisco

The third digit indicates the particular District office. As an example, in the Sixth District, the numbers and the offices are:

1 - Atlanta	4 - Nashville
2 - Birmingham	5 - New Orleans
3 - Jacksonville	6 - Miami

In the Tenth District, the numbers and the offices are:

1 - Kansas City	3 - Oklahoma City
2 - Denver	4 - Omaha

In the Twelfth District, the 12**20** in the example to the left would indicate the Los Angeles Office.

Bank ID number- Positions 5 through 8 of field 5 of the MICR line identifies the issuing bank. MICR symbols (⑆ , ⑆) surround the routing/transit number in the MICR line.

Account number- Field 3 in the MICR line identifies the customer's account number. A MICR symbol (⑈) follows the account number in the MICR line.

Serial number- Field 2 in the MICR line generally identifies the check number on personal checks. The serial number in the MICR line should match the serial number at the top right corner of the check.

Auxiliary number- Field 7 in the MICR line identifies the auxiliary number, generally on commercial checks only. The auxiliary number generally matches the number in the top right corner of a commercial check.

Fractional routing/transit number- The fraction on the top of the check should match the bank ID in the MICR line.

Signs of a bad check

There are a few key signs that can tip you off to a "bogus" check. The first is perforation. Most checks produced by check printing companies have at least one perforated edge. Although some companies produce their own legitimate checks using blank check stock and laser printers with MICR-printing capabilities, the lack of a perforation often is the first signal of a phony check.

Inconsistent routing and fractional routing numbers also can indicate a counterfeit check. Many check forgers alter the routing/transit number in the MICR line to gain additional clearing time while the check is misrouted to an incorrect, distant Reserve Bank or paying bank. Forgers also print an incorrect fractional routing number to further delay presentment of the item and print a bank location on the check that is inconsistent with routing/transit and/or fractional routing numbers.

What the Banking Industry can do

Education

A vital first step in limiting losses from check fraud is the thorough training of employees in your institution. Many fraudulent items can be detected by your tellers and cashiers during a cursory review. Once your personnel become familiar with the MICR line, fractional routing/transit (ABA) number, serial number, perforation, and typeface used by your institution, irregularities will be more apparent.

Fraudulent checks also can be detected by back room operations staff involved in the proof encoding process, reject repair, outgoing returns, and account reconcilement – if everyone is properly trained. For example, there is a certain level of MICR repair that is excessive and may signify a fraudulent check. Bank employees involved in the "new account opening" process should be aware of the amount of verification necessary to guard against new accounts that are fraudulent.

Networking

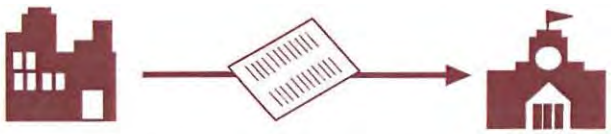
Many of the organized check fraud rings move from one part of the country to another and run the same check fraud scheme, hitting one financial institution and then another within that geographical area. Banks, credit unions, and savings and loans must share information with each other and with business and retail customers if the fraud is to be prevented. Check fraud is not a problem for financial institutions only. Everybody needs to be educated.

Positive pay programs

One proactive step you can take to combat check fraud is to implement positive pay programs. In these programs, presented checks are compared to a file of the checks that the bank has issued (issue file) that can be updated by corporate customers. When a presented item does not match the issued file, the bank will investigate the check's authenticity.

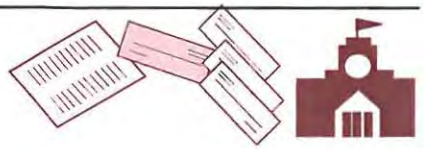
With a positive pay program in effect, banks approve checks for payment based on whether or not they *were* issued by their customer not on whether or not they *appear* to have been

1) Your customer provides you with check issue data (date, check number, amount).



2) Data for checks submitted for payment are automatically compared to the check issue data.

3) Exception items are identified and physically outsorted.



4) Your customer is notified of any "incurable" items so that a pay/no-pay decision can be made.

5) Items are paid or returned as directed by your customer.

issued by their customer. Some banks have chosen to eliminate the labor intensive signature verification process for customers in positive pay programs. It should be noted that a fraudulent copy of a check could be paid for a positive pay account if the fraudulent check clears before the valid check, but only one fraudulent copy of the check could be paid.

Transaction analysis software
With newly developed transaction analysis software, banks can check transactions against databases of closed accounts or accounts that are suspected of prior fraudulent activity. Automated signature verification systems are becoming more sophisticated in their ability to detect possible fraud suspects.

Check security features
As those who commit check fraud become more sophisticated, so must those who combat them. The following features are helping to make fraud more difficult.

Watermarks- Since watermarks are designed to be viewed at a 45-degree angle, scanners and photocopiers are not able to reproduce them.

Void pantographs- Pantograph technology protects documents from being illegally duplicated. When documents containing pantographs are copied, words like "copy" or "void" appear.

Warning bands- Warning bands call attention to the security features that protect the document.

Laid lines- Laid lines are unevenly spaced lines on the check that make it difficult to electronically cut and paste information on the check from a scanned image.

Chemically sensitive paper- Chemically sensitive paper reveals attempts at altering the paper with eradicator chemicals. When the eradicator comes in contact with the paper, the word "void" will appear.

Prismatic printing- Prismatic printing is designed to make it difficult to reproduce intricate colored backgrounds on color copies.

Micro printing- Micro printing is a group of words so small that it becomes unreadable and appears as a line when copied or scanned.

What your business customers can do

Educate your business customers about the importance of procedures and controls to deter dishonest employees from committing internal fraud. Your business customers should store check stock in secured, locked, and access-controlled environments. Keys and combinations should be changed periodically and inventories should be conducted on a regular basis by someone other than those who have regular access. Signature plates also should be controlled and stored separately from check stock.

Another deterrent to fraud is timely account reconciliation. Accounts should be reconciled *immediately* upon receipt of the bank statement, then reviewed and approved by a different person, preferably a member of management, to ensure accuracy and integrity. An important step in this process is to verify the authenticity of the authorized signer on the check.

You should also encourage your business customers to segregate staff responsibilities so that the same people do not retain custody of check stock, issue and sign checks, reconcile the bank statement, and process accounts payable. When these duties are not performed by separate and independent individuals, embezzlement may occur. By clearly defining and segregating staff responsibilities, the threat of unauthorized check issuance can be reduced.

Regular and frequent audits are necessary in a fraud prevention program and should be designed to validate specific fraud control procedures. Individuals conducting the audits should be knowledgeable about effective examination and fraud prevention procedures.

What the Federal Reserve Bank can do

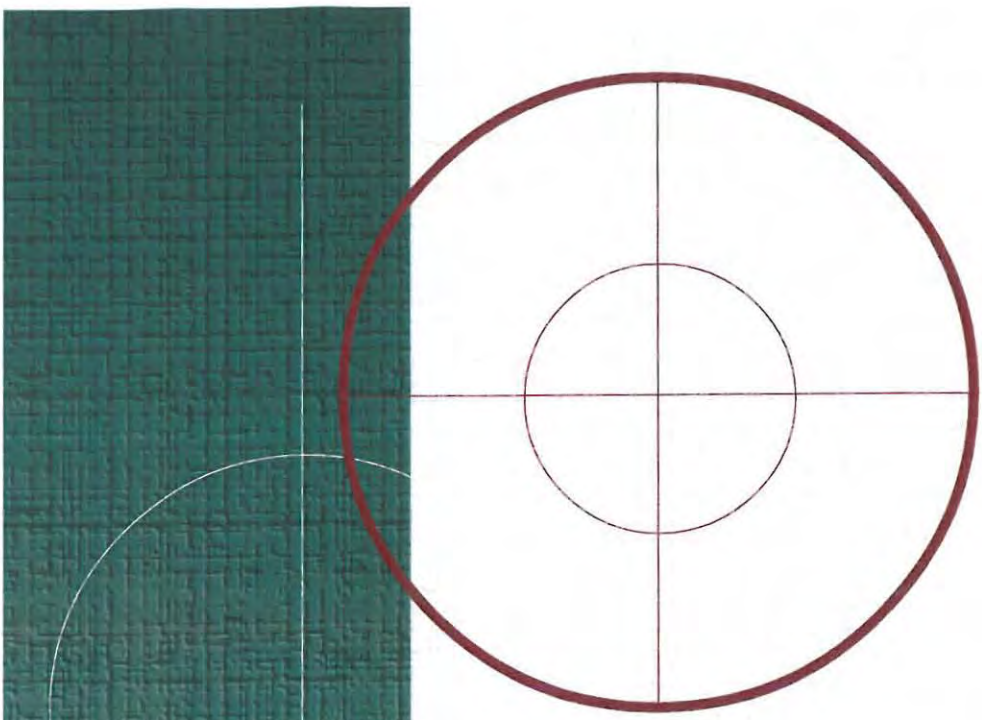
Your local Federal Reserve Bank offers alternative payment methods that can significantly reduce check fraud risk. Forms of Electronic Funds Transfer (EFT) such as Direct Deposit and Direct Payment using the Automated Clearing House (ACH) continue to expand as institutions and corporations implement payment systems to reduce their vulnerability to loss.

Electronic presentment

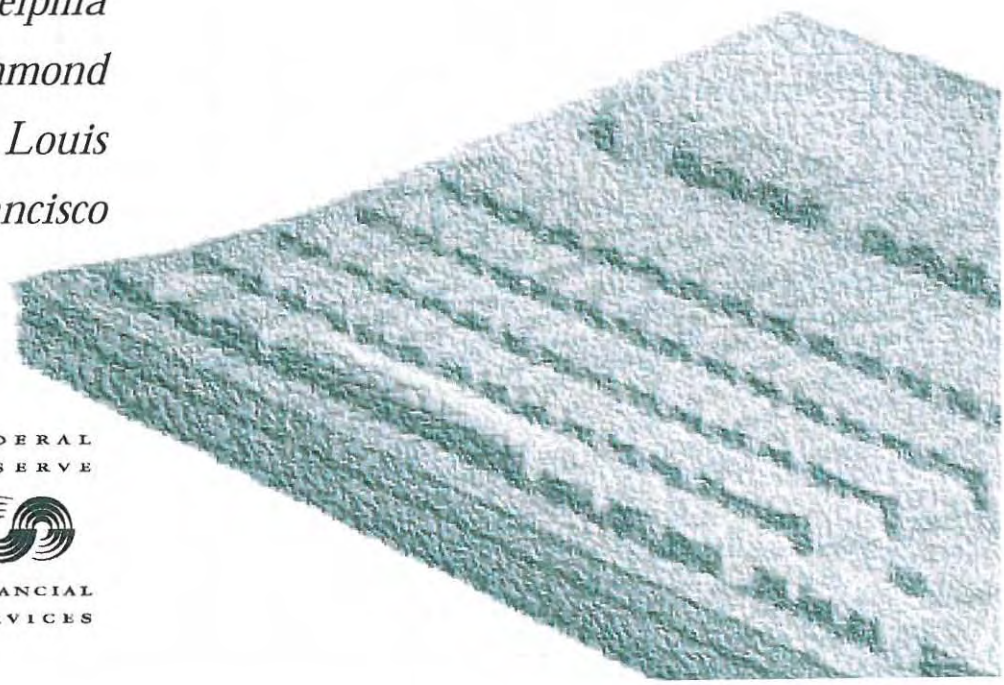
Some banks also are turning to various forms of Electronic Check Presentment (ECP) to combat some of the risks associated with paper payments. Receiving MICR line details from the Federal Reserve Bank allows a bank to obtain information on suspect accounts much sooner than conventional physical paper presentment. This process gives these banks an opportunity to put fraudulent items back into the return stream earlier. Image-enhanced ECP services offer additional opportunities for banks to enhance their ability to validate signature authenticity in a timely and accurate manner. Contact your local Business Development office to discuss ECP and image services available.

For more information

If you have questions about check fraud and the deterrents discussed here, please contact your local Federal Reserve Bank.



Atlanta
Boston
Chicago
Cleveland
Dallas
Kansas City
Minneapolis
New York
Philadelphia
Richmond
St. Louis
San Francisco



FEDERAL
RESERVE

FINANCIAL
SERVICES