Federal Deposit Insurance Corporation

FRAUD Alert

FDIC

Summer, 1999 Volume 7, Number 2

Editor's Note:

This report was prepared by the Check Fraud Working Group, a subgroup of the interagency Bank Fraud Working Group. That working group includes representatives from the Federal Bureau of Investigation, the Department of Justice, Federal Deposit Insurance Corporation, Federal Reserve Board, Internal Revenue Service, Office of the Comptroller of the Currency, Office of Thrift Supervision, U.S. Postal Inspection Service, National Credit Union Administration, and U.S. Secret Service. The Check Fraud Working Group was convened to provide a forum to explore ways to combat check fraud perpetrated against federal financial institutions.

Check Fraud: A Guide to Avoiding Losses

Background

Check fraud is one of the largest challenges facing financial institutions. Technology has made it increasingly easy for criminals, either independently or in organized gangs, to create increasingly realistic counterfeit and fictitious checks as well as false identification that can be used to defraud financial institutions.

The scope of the problem can be shown by some recent statistics. According to the U.S. Department of the Treasury, Financial Crimes Enforcement Network's (FinCEN) 18 Month Analysis of the Suspicious Activity Reporting System (SARS), 43 percent[1] of suspicious activity reports filed between April 1996 and September 1997 related to check fraud, counterfeit checks and check kiting. Estimates are that financial institutions lost $1 billion to these check fraud related schemes during that time.

To protect the banking industry and its customers from check fraud, financial institutions need to become familiar with common check fraud schemes. This report describes some of these schemes and presents tactics for use in combating check fraud. It cannot offer a comprehensive description of all types of check fraud or check fraud schemes because the variations are limitless. While this report is a general guide, financial institutions should look to state and local laws for other guidance or limits. It can, however, get bankers, tellers, operations personnel, and security officers to think about the problem and how they can protect their institutions from check fraud.

Significant Terms

Some technical terms relating to checks and drafts[2] are worth defining.

Customer - a person with an account at the financial institution.

Drawee - a party, typically a financial institution, that is required to pay out the money when a check or draft is presented. The drawee is usually the payer financial institution.

[1] This figure does not include Bank Secrecy Act reported violations.

[2] In Credit Unions, these instruments are referred to as share drafts.

Telemarketing frauds can be successful when customers reveal confidential account information.

To protect against such frauds, *financial institutions should:*

- warn customers about them, either through direct mail or advertising in the financial institution.
- check a customer's file when a demand draft is presented to see if he or she has provided written authorization for the financial institution to pay those drafts.

Check Fraud by Gangs

Some gangs have become actively involved in check fraud. These gangs typically go after corporate accounts and have received a measure of notoriety because of their successes and failures.

Example 1: Gangs have traveled throughout the country cashing counterfeit payroll checks obtained by gang members in targeted corporations or financial institutions. They use sophisticated counterfeiting techniques to capture the company's logo and a company executive's signature by scanning them and to prepare payroll checks using account information from a company check or a bank insider. They use the same information and techniques to prepare false identification for the people who will cash the checks.

If insider information is not available, such gangs sometimes call the targeted company's accounts receivable department, tell them that they have funds to wire into the company's account, and get the company's financial institution account number to accomplish the transfer. The deposit, of course, never materializes. Such gangs move into a city or town around payday and cash the checks at local institutions which have check cashing agreements with the targeted corporation.

Example 2: A fictitious foreign company sends a letter to an individual or U.S. company claiming to have a large quantity of money that must be transferred out of the foreign home country immediately. The foreign company asks the targeted individual or company to help set up a financial institution account into which the money can be transferred. They offer a sizable commission, while asking for the target's checking account information. The foreign company's representative then uses the account information to withdraw money from the target's checking account using financial institution drafts.

Financial institutions should remember that, although the individual or U.S. company acted negligently, the financial institution may be liable for honoring the fraudulent drafts.

Gang frauds can be successful when customers are careless and financial institutions fail to secure account information.

To protect against such frauds *financial institutions should:*

- warn customers about such schemes.
- verify new employees' backgrounds.
- require proper identification from customers before cashing checks.
- be aware that gangs obtain account information from financial institution insiders who process checks, copy payee checks and use discarded receipts and/or statements.
- be aware that gangs will recruit account holders in good standing and request individuals to open accounts, or open fictitious accounts (to deposit checks).
- be aware that gangs will also obtain genuine identification issued by the state where they are negotiating the checks (be cognizant of the issuance date of the identification).

Preventative Measures

General Internal Controls

Strong organizational controls can reduce the likelihood of check fraud. A sound organizational strategy should require the financial institution to:

- monitor, classify, and analyze losses and potential losses to identify trends.
- report findings from monitoring activities to the audit, risk-management, and security divisions as well as to senior management.
- ensure communication among departments about check fraud concerns.
- assess operating procedures regularly and implement changes.
- target check fraud awareness training to specific check fraud schemes—how they occur, and how to prevent them.

Internal Controls to Prevent Check Fraud by Insiders

Unfortunately, dishonest financial institution employees can be involved in check frauds. Internal controls that can help prevent check fraud by financial institution insiders include:

- ensuring that account changes, such as adding names or changing addresses and/or other information, are authorized by the customer in writing, or in a way that guarantees that the customer is requesting the change.
- establishing special protections for dormant accounts, such as requiring extra approvals and mandatory holds and maintaining special security for signature cards.
- maintaining permanent signature cards for each account and keeping files and appropriate documentation for business accounts (e.g., a certificate of incorporation, recent federal tax return, etc.).
- separating duties to ensure that no one person in the financial institution, acting alone, can commit check fraud.
- ensuring that persons other than those who open accounts or prepare statements handle night depository, ATM, Automatic Clearing House (ACH), and mail deposits.
- ensuring that customer complaints and discrepancy reconcilements are directed to staff who are not account openers, tellers, or bookkeepers.
- conducting thorough and complete background investigations of new hires.
- holding the initial deposit checks when opening accounts with $50 or $100 deposits, for the time allotted per Regulation CC, or until they clear.

Education and Training

Alert and well-trained front line personnel, managers, and operations personnel are essential to effective check fraud prevention programs. Before beginning their positions, new employees should be trained in financial institution procedures concerning:

- what is acceptable identification.
- opening new accounts.
- cashing checks and accepting deposits.
- detecting counterfeit checks.
- cash-back transactions.
- back room operations.

Effective training and education are important in preventing check fraud losses. Suggested training for specific financial institution positions follows.

Teller Training

Financial institutions must emphasize to all tellers the importance of being alert to check fraud. One way to focus on preventing check fraud is to include a separate section on the subject in teller manuals. That section can emphasize typical check fraud schemes and warning signs. Some common warning signs include:

- A check that does not have a MICR line at the bottom.
- A routing code in the MICR line that does not match the address of the drawee financial institution.
- MICR ink that looks shiny or that feels raised. Magnetic ink is dull and legitimate printing produces characters that are flat on the paper.
- A check on which the name and address of the drawee financial institution is typed rather than printed, or that includes spelling errors.
- A check that does not have a printed drawer name and address.
- A personal check that has no perforated edge.
- A check on which information shows indications of having been altered, eradicated, or erased.
- A check drawn on a new account which has no (or a low) sequence number or a high dollar amount.
- A signature that is irregular-looking or shaky, or shows gaps in odd spots.
- A check printed on poor quality paper that feels slippery.
- Check colors that smear when rubbed with a moist finger. (This suggests they were prepared on a color copier).
- Checks payable to a corporation that are presented for cashing by an individual.
- Corporate or government checks which show numbers that do not match in print style or otherwise suggest that the amount may have been increased.
- Checks presented at busy times by belligerent or distracting customers who try to bypass procedures.
- Checks which have dollar amounts in numbers and in words which do not match.
- Items that are marked "void" or "non-negotiable," yet are presented for cash or deposit.

Guidelines to Consider When Cashing Checks

Although this list is not exhaustive, it provides a useful starting point when someone presents a check for payment.

☞**Properly identify customers,** either through personal recognition, or signature and personal picture identification. If in doubt, refer the customer to an account representative.

☞**Be careful when paying customers,** especially new customers, split checks for deposit and cash.

☞**Require two forms of identification and list them on the back of the check.** Carefully review the identification to ensure it is genuine. Be alert for an individual who tries to distract you while you are reviewing his or her identification.

☞**Be careful when accepting official checks drawn on another financial institution.** Such items are sometimes counterfeit. The date of issue may indicate possible fraud, e.g.—issued the same day or one day prior, especially if a payroll check is involved.

☞**Refer all questionable transactions to a supervisor** for a second opinion.

☞**Be sure the customer's account is open and has a positive balance.**

Remember: A financial institution may delay cashing a check for a reasonable amount of time to verify that a signature is genuine and to make sure that it has properly identified the person presenting it. A short delay may cause a criminal to leave the financial institution without the forged or altered check rather than risk being arrested.

New Accounts Representative Training

A significant amount of check fraud begins at the new accounts desk. A new accounts representative should remember it is possible that a new customer may be intending to defraud the financial institution. Financial institutions should monitor new accounts diligently and should reconcile promptly any discrepancies or problems they identify. The few extra steps it takes to become familiar with a customer can prevent significant losses.

New accounts representatives should be alert to the following signs that an account **may** be fraudulent. These situations may not indicate a problem, but should signal to the new accounts representative that further information may be required.

The new accounts representative should be alert when a new customer provides:

- a telephone number or exchange that does not match the address or that has been disconnected.
- a home address that is outside of the financial institution's geographic area, that is a major highway, or that is not a street mailing address. Such addresses include those identified by post office box, suite, or drawer identifiers.
- no employer name or an employee with no telephone number. This includes new customers who identify themselves as self-employed.
- no driver's license.
- identification with a birth date (particularly the year) that does not match the birth date on the new account application.
- information that is in any way insufficient, false, or suspicious.

Guidelines to Consider When Opening Accounts

Although the following list is not exhaustive, it provides some procedures a financial institution representative should consider when opening new accounts:

☞**Request two forms of personal identification.**
Acceptable identification includes:

- driver's license.
- U.S. passport or alien registration card.
- certified copy of birth certificate.
- government, company, or student identification card.
- credit card.

Note: Be aware that all forms of identification can be counterfeited.

☞**Request documents on corporate accounts.**
Such documentation may include copies of:

- state incorporation certificate.
- corporate resolution.
- recent corporate federal tax return.
- list of major suppliers and customers, with their geographic locations.

☞**Require complete information.**
The new account card should show street address, date of birth, driver's license number, and social security number or tax identification number.

☞**Verify information provided.**

- Compare the date of birth on the application with that on the driver's license, passport, or alien registration card.

- Check employment by telephoning the employer identified on the application.

- Look up the customer's name, address, and telephone number in the telephone directory.

☞**Check the new customer's banking history.**

Contact the financial institution(s) with which the customer reports having had prior relationships, if any, and ask for the customer's:

- type of account(s) and balances.

- listed address(es).

- taxpayer identification number.

☞**Use the address provided.**

Write a thank you letter to the new customer using the street address provided. If the letter is returned, the bank knows to investigate the account.

☞**Visually inspect business premises.**

Drive by the business address to verify it fits with the type of business reported.

New accounts representatives should refer all inconsistencies identified and any difficulties in the new account opening process to a supervisor.

Other Preventative Measures

Positive Pay

Positive pay allows a company and its financial institution to work together to detect check fraud by identifying items presented for payment that the company did not issue. In the usual case, the company electronically transmits to the financial institution a list of all checks it issued on a particular day. The financial institution verifies checks received for payment against that list and pays only those on the list. The financial institution rejects:

- checks not on the company's list.

- checks that exceed a specific dollar amount.

- checks that carry dates long past due (stale checks).

The financial institution investigates rejected checks to find out if the items are fraudulent or in error. The financial institution only pays exception items approved by the company.

Reverse Positive Pay

Reverse positive pay is similar to positive pay, but the process is reversed, with the company, not the financial institution, maintaining the list of checks issued. When checks are presented for payment and clear through the Federal Reserve System, the Federal Reserve prepares a file of the checks' account numbers, serial numbers, and dollar amounts and sends the file to the financial institution.

In reverse positive pay, the financial institution sends that file to the company, where the company compares the information to its internal records. The company lets the financial institution know which checks match its internal information, and the financial institution pays those items.

The financial institution then researches the checks that do not match, corrects any misreads or encoding errors, and determines if any items are fraudulent. The financial institution pays only the "true" exceptions, that is, those that can be reconciled with the company's files.

Fingerprints

Some financial institutions have seen a reduction in check fraud by inkless fingerprinting of non-customers who seek to cash checks. Generally, the program requires all persons presenting checks for payment, who do not have an account with the financial institution (i.e., non-customers), to provide a fingerprint or thumbprint.

The teller explains the process whenever a non-customer presents a check for payment. The teller will not accept the item if the person objects. A person who does not object to providing a fingerprint is

asked to ink his or her thumb on a small pad and place the imprint in the space between the memo line and the signature line of the check being presented.

If the financial institution later finds out the check was fraudulent or was altered, it can provide the check, with the fingerprint, to law enforcement officials.

Any financial institution that implements this type of plan should exercise care to ensure that it is not applied on a selective basis.

Electronic Check Presentment

Electronic check presentment (ECP) is an electronic/paper method of expediting check collection. Participating financial institutions exchange check payment information before physically presenting the checks for payment.

The depository financial institution captures payment information from the MICR line of incoming checks and immediately transmits the information electronically to the paying financial institution. Later, the depository financial institution sends the actual check according to its normal paper deadlines. During check posting, the paying financial institution identifies checks that should be returned and immediately notifies the depository financial institution.

ECP supporters believe that it speeds up processing, controls cost and reduces fraud by providing early notification of return items.

Data Sharing: Cooperation Between Check Manufacturers and Financial Institutions

In 1993, the American Bankers Association and the National Retail Federation sponsored an inter-industry task force known as the BankCheck Fraud Task Force to examine solutions to check fraud problems. The task force has developed a data sharing program for closed accounts. This program prevents people who have outstanding checks due to retailers from opening new accounts.

Participating financial institutions report all checking accounts closed for cause to a central database called ChexSystems.

ChexSystems transmits the closed account information to the shared check authorization network (SCAN) database.

Participating financial institutions use the SCAN information before opening new accounts to spot repeat offenders. A participating financial institution can also use MICR information from a check presented with the applicant's driver's license number to check the SCAN file for any previous fraudulent account activity.

Check Security Features

Check manufacturers help deter check fraud by making checks difficult to copy, alter, or counterfeit. Some useful security measures include:

Watermarks. Watermarks are made by applying different degrees of pressure during the paper manufacturing process.

Most watermarks make subtle designs on the front and back of the checks. These marks are not easily visible and can only be seen when they are held up to light at a 45-degree angle. This offers protection from counterfeiting because copiers and scanners generally cannot accurately copy watermarks.

Copy Void Pantograph. Pantographs are patented designs in the background pattern of checks. When photocopied, the pattern changes and the word "VOID" appears, making the copy nonnegotiable.

Chemical Voids. Chemical voids involve treating check paper in a manner that is not detectable until eradicator chemicals contact the paper. When the chemicals are applied, the treatment causes the word "VOID" to appear, making the item nonnegotiable. Checks treated with chemical voids cannot be altered without detection.

High Resolution Micro Printing. High resolution micro printing is very small printing, typically used for the signature line of a check or around the border, in what appears to be a line or pattern to the naked eye. When magnified, the line or pattern contains a series of words that run together or become totally illegible if the check has been photocopied or scanned with a desktop scanner.

Three-dimensional Reflective Holostripe. A holostripe is a metallic stripe that contains one or more holograms, similar to those on credit cards. These items are difficult to forge, scan, or reproduce because they are produced by a sophisticated, laser-based etching process.

Security Inks. Security inks react with common eradication chemicals. These inks reduce a forger's ability to modify the printed dollar amount or alter the designated payee because when solvents are applied, a chemical reaction with the security ink distorts the appearance of the check. This makes such items very difficult to alter without detection.

Sources

Check Fraud Prevention, *Bank Security Desk Reference,* Chapter 14, August 1995.

Check Fraud, *Fraud Prevention and Detection Series,* Bank Administration Institute (First National Bank of Chicago, 1989).

Check Fraud Prevention, American Bankers Association (1995),"1994 ABA Check Fraud Survey," American Bankers Association (1994).

Bruce P. Brett, "Information-based Strategies to Prevent Check Fraud," *Journal of Retail Banking,* Vol. XVII, No. 2, pp. 33-36 (Summer 1995).

J.D. Carreker, "Electronic Check Presentment: Capturing New Technology," *Bank Management,* pp. 33-40 (March/April 1995).

James Clark, "Taking Positive Steps Against Check Fraud," *TMA Journal,* Vol. 15, No. 2, pp. 53-56 (March/April 1995).

Dean Karkazis, "Using Technology Enhancements to Fight Check Fraud," *TMA Journal,* Vol. 15, No. 2, pp. 47-49 (March/April 1995).

John P. Mello, Jr., "You Must Protect Yourself," *CFO,* Vol. 11, No. 5, pp. 98-101 (May 1995).

Gary Robins, "Check Fraud Defense," *Stores* (April 1994).

Attn: Chief Executive Officer

FDIC
Federal Deposit Insurance Corporation
Washington, DC 20429-9990

OFFICIAL BUSINESS
Penalty for Private Use, $300.00

BULK RATE
MAIL
Postage & Fees
Paid FDIC
Permit No. G-36