FEDERAL RESERVE BANK OF DALLAS

DALLAS, TEXAS 75222

Circular No. 80-124
June 19, 1980

FEDERAL RESERVE SYSTEM BOOKLET ON
PROTECTING WIRE TRANSFER OPERATIONS

TO THE CHIEF EXECUTIVE OFFICER OF
THE MEMBER BANK ADDRESSED IN THE
ELEVENTH FEDERAL RESERVE DISTRICT:

Security.

This issue is uppermost in the minds of all chief executives and those with responsibility for protecting the institution's valuables or controlling the daily operations.

But, no matter how much attention we, as part of the senior management of our individual banks, give to security--not to mention the funds we devote to control vulnerabilities--there is always someone giving as much attention, or more, to finding the one weak link which will make their intrusion plans successful.

Moreover, the ratio of intrusion at financial institutions to the volume of funds and securities handled daily by financial institutions nationwide presents a false and dangerous sense of security.

Attached is a small brochure which I believe may help in reducing the chance of a fraud being perpetrated against your institution, particularly in the area of funds and securities transfer.

"By The Way" does not contain all the answers; neither does it intend to imply that if all the suggestions are adopted your institution will be totally secure. However, I hope "By The Way" will help you focus on those practices which need more attention, especially if your institution uses any funds transfer services.

Improved security will benefit you and your customers directly.

Please take five minutes today to read "By The Way", published by the Federal Reserve Subcommittee on Communications, and ask your operation and security officers to do likewise. Five minutes is a small price to pay for greater security.

Requests for additional copies of "By The Way" or any related questions may be directed to Richard D. Ingram, Ext. 6333, at the Dallas Office, Larry Wilson, Ext. 210, at the El Paso Office, Vernon L. Bartee, Ext. 45, at the Houston Office, or Rene Gonzales, Ext. 421, at the San Antonio Office.

Sincerely yours,

Robert H. Boykin

First Vice President

Enclosure

Banks and others are encouraged to use the following incoming WATS numbers in contacting this Bank: 1-800-442-7140 (intrastate) and 1-800-527-9200 (interstate). For calls placed locally, please use 651 plus the extension referred to above.

BY THE WAY

MAY 1980

Conference of First Vice Presidents
Committee on Communications and Payments
Subcommittee on Communications
Federal Reserve System

Look At Your Banking Floor: Fraud, Theft May Be Lurking

Look around your banking floor.

Many employes are on telephones transferring or receiving funds for customers.

By the way, how do you know that?

Listen to that conversation over there. Now you can be sure the funds are being moved. The transfer clerk just issued the code word validating the transaction.

By the way, how many others on the banking floor—employes and customers—heard that code word? How do you know the funds movement was authorized, and the correct amount was moved to the right account?

And, over there, that businessman who has been staying at the hotel down the street, and who told you some funds would be coming to your bank for him; nice fellow. Not likely to be involved in a fraud.

By the way, how do you know that?

The point is your bank is vulnerable to funds transfer fraud and could suffer a loss.

Among the largest commercial banks it isn't uncommon for each bank's assets to be turned over, through the funds transfer mechanism, one or more times a day.

Did you know that?

Almost all those funds and securities—more than $64 trillion in 1979—were moved through direct terminal or computer links between commercial banks and the Federal Reserve System.

Nevertheless, a sizable portion of funds and securities are moved via telephone, teletype and similar equipment, from commercial banks to the Federal Reserve and on to other banks. In 1979, about $5 trillion of funds and securities were moved in this manner, through

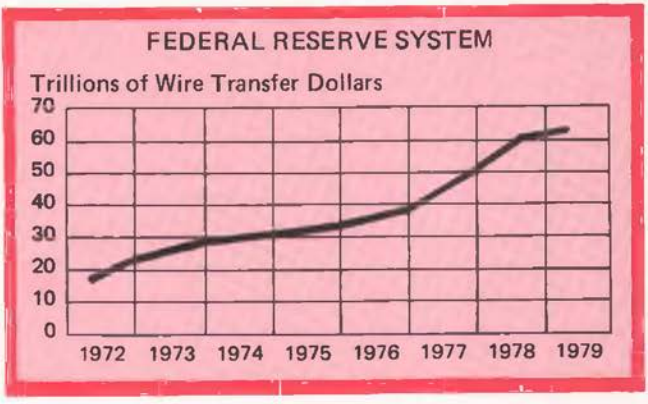
3.5 million transfer requests—or about 14,000 transfer requests, valued at $20 billion, every business day.

By the way, what are you doing to ensure fraud isn't perpetrated on your bank?

Clearly, an impregnable money transfer security-system has never been devised.

Furthermore, the most complete security plan probably isn't. If procedures are too stringent they won't be followed, rendering the plan even more vulnerable than less secure arrangements.

But, to ignore security, or make security less than top priority is to invite intrusion: there is always someone giving top priority in their intrusion plan to penetrating your security system.



If you think because your bank is relatively small, and in a relatively small city or community, it isn't likely to be a target, you are wrong.

Your bank may be a target, right now. From the viewpoint of a criminal, your bank might be easier to defraud than a larger bank, which has sophisticated protection equipment, numerous guards and considerable other resources to invest in security.

Regardless of the institution's size, one thing is clear: the growth in the dollar volume of funds and securities

transferred equals greater vulnerability. Thus, the number of attempts to defraud may increase, requiring greater awareness on the part of all concerned. Further, the growth in dollar volume is likely to continue, as investors, more active than ever before, move funds from one market instrument to another, seeking a higher rate of return on investments.

Put simply: the relatively low ratio of the frequency of intrusion attempts to the dollar volume of transfers provides a false sense of security. ■

Various Safeguards Available To Deter Transfer Fraud

There are a number of safeguards you can put into place to help deter a funds transfer fraud. Clearly, the amount of money allocated to security and the availability of resources and personnel will be a major factor in deciding which of these safeguards are instituted.

*Formally designate responsibility for security. Make sure there are regular meetings between those security officers and senior management, including directors. All aspects of security—from programs aimed at increasing awareness of employes to new equipment and controls—should be scrutinized.

*Make certain that employes strictly observe the established procedures, and provide for unannounced checks of daily work by the auditing staff or other designated supervisors or officers.

*If possible, institute unannounced rotation of employes and change all codes on a random basis.

*Require that employes responsible for funds and securities transfer take at least five (10 is desirable) consecutive business days of vacation during the year.

*Change authentication and authorization codes frequently. Keep such information secure, and don't allow it to be visible or used within earshot of persons not authorized to have access to the information.

*Be sure there is an end-of-day proof of funds and securities transfers against original instructions and the verification is conducted by someone other than the employe handling the original transfer.

*Reconciling statements immediately for early detection of incorrect information facilitates quick correction before there is extensive harm, and serves an important role in detecting fraud. The criminal is left with little time in which to complete the action. Immediate notification of the crime will help catch the thief.

*Install tape recording devices on telephones used in handling money transfer requests. The recording equipment should be under the supervision of an officer-in-charge, or the security officer. Copies of these tapes often are helpful to investigators in tracking individuals making fraudulent requests. Tapes are useful in voice analysis and may provide relevant background noises. The tapes also aid in resolving disputes which occassionally occur concerning instructions.

*Retain message copies for at least 30 days to help resolve questions.

*Avoid placing new employes or employes who have been transferred from other

areas into a sensitive area involving funds or securities transfers.

•Ensure equipment is inoperative, inaccessible and protected during nonbanking hours. Secure authentication codes, authorization codes, supplies and procedure manuals when not in use.

•Restrict access to equipment to authorized personnel only.

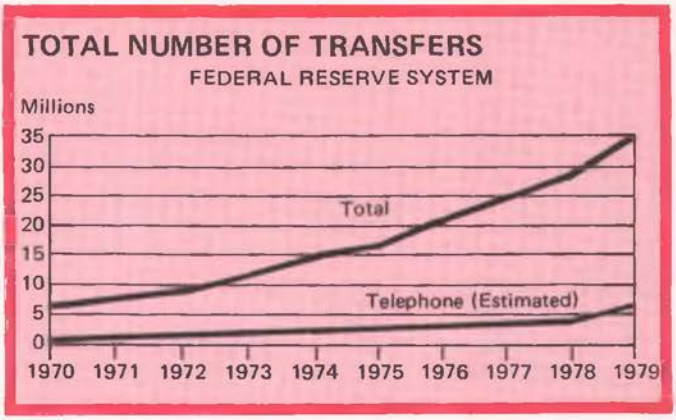
•Be suspicious of strangers, repairmen, workmen, vendors, meter readers and similar persons. Keep them out of transfer areas unless authorized and accompanied at all times by an authorized employe.

•Make sure when receiving instructions to credit a third-party account, code words are verified to ensure the call is coming from a Federal Reserve Bank, or follow the call-back procedure established by your Reserve Bank.

•Never pay out funds or deliver securities directly without validating the originator of the call.

•Before funds or securities transfer requests, received by telephone, are delivered to a customer, always verify and validate the entire transaction with the originating institution.

•Before requesting a local Reserve Bank or branch to send a securities transfer, employes should confirm that the securities are on deposit at the Reserve Bank or branch, or arrange to have the securities delivered with the request.



*Be certain that employes are aware that any attempted security breach must be challenged and reported immediately to the designated security officer.

*When telephoning the local Reserve Bank or branch, be sure the information is correct, particularly the name of the receiving bank. If possible, check first with the originator of the transfer, check a bank directory, or ask the local Reserve Bank to contact the Reserve Bank responsible for the area in which the receiving bank is located. This can be accomplished quickly through the wire transfer department of your Reserve Bank.

By the way, if you think most of these suggestions are just more paperwork, or something which simply requires lip service, ask some of your banking colleagues who thought funds and securities transfer fraud couldn't happen to them—until it did.

Nobody expects theft, but every bank locks the vault door at the close of business. ■

Alert Fed, FBI, Police To Suspected Fraud, Intrusion

A banker suspecting an attempted funds or securities transfer fraud, or an intrusion, should immediately contact the local office of the Federal Bureau of Investigation, as well as the Federal Reserve Bank or branch which serves the bank.

The communications security officer, or designated representative, should coordinate contact with the FBI, local police and Federal Reserve.

The telephone number of the regional office of the FBI, as well as the name of the agent-in-charge, should be kept within easy access of the senior officers of the bank, as well as supervisors in the transfer area.

At the time the FBI is contacted, the communications officer should ascertain whether the FBI or the bank will inform the local police department.

The local Federal Reserve head office or branch should be informed as soon as possible. If the attempted or actual fraud involves a transfer made through the Federal Reserve, the Reserve Bank should be immediately informed so an effort can be made to halt the funds or securities transaction.

All information regarding the transaction should be directed to the officer at the Reserve Bank head office or branch responsible for funds and securities transfers.

The regional bankers association also should be advised as soon as possible, enabling a circular to be dispatched warning area bankers.

To avoid the possibility of slander, information provided should be reviewed with legal counsel. Such a review shouldn't delay the alert.

Procedures should be reviewed regularly by the bank's attorney, in concert with security officers and

appropriate supervisory personnel, to ensure timely notification of authorities.

To ensure the correct persons at Reserve Banks or branches are informed of attempted or actual transfer frauds, procedures regularly should be discussed with bank relations representatives. ■

Accurate Information Is Key To Safely Speeding Transfers

The key to ensure funds and securities move promptly and safely from or to your bank through the Federal Reserve is to provide accurate information and to ensure adherence to established procedures.

While that sounds obvious, incorrect information is occasionally received by the Reserve Bank, causing the processing of transfers to be slowed, or misrouted. Although the Federal Reserve attempts to confirm information before transferring funds or securities, the commercial bank is ultimately responsible for providing the correct information.

When calling the Federal Reserve with a transfer, the commercial bank employe should:

- Provide the full name and town or city of the sending bank, and the full name and town or city of the receiving bank;
- Provide the American Bankers Association routing numbers of the sending and receiving banks. The ABA routing number of each bank is listed in Rand McNally & Co.'s "American Bankers Association Key to Routing Numbers," as well as Polk's "World Bank Directory."
- Provide his or her full name, telephone number and appropriate authentication

codes or other similar information. It is wise to review the wire transfer rules from time-to-time. If you have a question regarding the wire transfer rules, consult the bank relations representative of your Reserve Bank or branch during the regular visits to your bank. Similarly, bankers should review with these Reserve Bank representatives any problems encountered in transferring funds or securities, including any threats of intrusion.

*Provide the full name, address and telephone number of the person or corporation receiving the funds or securities. If the receiving bank is to be notified to expect a transfer, include the telephone number. If the funds are corporate funds or securities, the name of the authorizing official (such as the treasurer) should be recorded by the commercial bank on its records, should a question arise.

*Ensure proper authorization through verification, such as calling the individual or corporation, using a previously prepared list of telephone numbers and names, to confirm the request, before calling the local Reserve Bank or branch. Know your customer and keep authorization lists up-to-date.

- Special attention should be given when unusually large or small sums (relative to previous transactions made by the person or corporation) are involved; when a new or seldom used account is involved; or when a "new" person makes the funds or securities transfer request.

Special attention also should be given when providing the dollar amounts. Numbers should be stated as "one million, two hundred and fifty thousand dollars and twelve cents," and repeated one digit at a time: 1 comma 2 5 0 comma 0 0 0 point 1 2.

When transferring securities, employes providing instructions to the Reserve Bank must at the outset specify the transfer involves securities.

In addition to providing the total dollar amount of the securities (at face value) as a group in the manner suggested, as well as the full name and city or town location of the sending bank and receiving bank, the ABA numbers and the appropriate transfer authentication codes, the sending bank should:

- Provide a full description of the securities, including kind (United States Treasury bills, bonds or notes), interest rate, maturity, dollar amount (at face value), and "CUSIP" number of each security;

- Inform the Federal Reserve if the securities are to be delivered against payment;

- Provide the delivery date.

Finally, every transaction should, on a daily basis, be given a unique number. This number, the code word or other similar information, and ABA routing numbers should be given to the Federal Reserve at the time the telephone call is initiated, depending upon the Reserve Bank or branch requirements.

The "CUSIP" number, the standard numbering system for securities, is printed on each security, and is listed in Standard & Poor's Corp.'s "The CUSIP Directory." ■

Bank Regulators Are Source For Security Assistance

Bankers seeking assistance in planning or improving security measures should contact their local Reserve Bank or branch, the regional office of the Comptroller of the Currency, the Federal Deposit Insurance Corp., or the state banking authority.

The Federal Reserve is responsible for Regulation "P" which covers various aspects of security, particularly for the public banking area of state member banks. In addition, the Reserve Bank will soon be making available a newly published booklet entitled "The Security Gap." The booklet will be available through the bank relations or public information departments and from the funds and securities transfer officers of your local Reserve Bank or branch.

To determine how the local Reserve Bank or branch can be of further assistance, contact the bank relations office, the security officer, or the officer-in-charge of the funds or securities transfer areas.

State banking authorities also are responsible for bank protection. Likewise, the Comptroller and the FDIC have a variety of rules on protection. Various other government agencies, such as the FBI, may be able to provide general assistance. ■

Reviewing Transfer Rules May Prevent Costly Errors

Knowing the Federal Reserve's rules of funds and securities transfer may help prevent a bank from suffering a costly and embarrassing error.

Officers and employes should periodically review all bulletins, circulars, regulations and agreements regard-

ing transfers and assign an individual to promptly circulate changes throughout the depository institution.

Specifically, an officer of the bank should examine the circulars sent by the local Reserve Bank or branch to ensure all correspondence is being received on a timely basis and that the appropriate person at the bank is on the Reserve Bank's mailing list. Problems should be called to the immediate attention of the bank relations personnel. Changes in positions should be forwarded to the Reserve Bank or branch in writing.

Regular review should be made of Federal Reserve Regulation "J," Subpart "B," which governs wire transfers of funds; the operating "circular" or "letter" which covers the procedures for wire transfer of funds and the schedule of time limits for those transfers; and the operating "circular" which covers transactions in marketable U.S. Treasury and agency securities.

Senior management, including the security officer, the legal officer and the audit staff, should regularly review internal operating procedures to ensure new procedures or new equipment haven't compromised existing security arrangements. ■

Going "On-Line" To Fed Can Aid Commerical Bank

Commercial banks which make 10 or more funds and securities transfers a day with the Federal Reserve should consider becoming an "on-line" bank.

Being directly linked through terminals to the Federal Reserve enables the bank to receive notice of credits more quickly than those banks which are "off-line." As a result, banks are more certain of giving their customers timely credit and may employ funds more quickly.

In addition, "on-line" banks can make transfers far more quickly than those banks using telephones, which,

in heavy periods, are subject to delays. When the transfer time is significant, being "on-line" could be important to the bank and the customer. And too, "on-line" banks receive a daily "total debit" and "total credit" report enabling a speedier and more timely proof of current transactions.

In some cases, the terminal is a status symbol and has been of benefit in generating new business. This new service quickly becomes an important cost-justified benefit to the community served by the bank. Similarly, the service assists in daily money management responsibilities.

In addition, the likelihood of misrouting information is reduced, since there is little chance for the wrong number to be dialed and the information to be given to someone who might misuse the data.

For additional information on becoming an "on-line" bank, discuss your situation with the wire transfer management staff or the bank relations representative at your local Reserve Bank or branch.

Requirements for becoming an "on-line" bank vary from Reserve Bank to Reserve Bank. In addition, there is a training and installation period prior to conversion to "on-line" status. ■

By the way, are the safeguards in your bank adequate, and will they immediately identify a discrepancy, or intrusion of your operation?

Reserve System Concerned About Preventing Weak Links

The visibility and importance of the Fedwire has increased significantly during the past decade, as the volume of funds and securities transferred for bank customers has grown.

This visibility has been broadened through speeches, newspaper and magazine reports and the movement of personnel among financial institutions.

The Conference of First Vice Presidents of the Federal Reserve System is deeply concerned about any weak link in the security chain: what happens in one area can deeply influence what happens in your bank.

"By The Way" was written to share the Federal Reserve System's concern for security and to bring it to your attention. The bank relations, wire transfer, and other representatives of your Reserve Bank or branch would be pleased to discuss these matters in depth with you at mutually convenient times.

Additional copies of **"By The Way"** are available from the bank relations, wire transfer or public information department of your local Reserve Bank or branch.

Conference of First Vice Presidents
Committee on Communications and Payments
Subcommittee on Communications

Do You Have A Weak Link?

Printed at the Federal Reserve Bank of Philadelphia