FEDERAL RESERVE BANK OF DALLAS

DALLAS, TEXAS 75222

Circular No. 81-73
April 13, 1981

BOOKLET ON SECURITY AND
CONTROL OF FUNDS TRANSFERS

TO DEPOSITORY INSTITUTIONS USING THE
ELECTRONIC FUNDS TRANSFER FACILITY IN THE
ELEVENTH FEDERAL RESERVE DISTRICT:

Enclosed is a booklet which recommends ways to safeguard your funds transfer operation. It should assist the auditors in identifying funds transfer operations that may require special attention by your organization.

Security and control should be a continuing concern of those with responsibility for the electronic funds transfer activity because of the sensitivity of this function and the increasing volume and dollar amount of funds transferred.

The booklet should be very helpful to you in developing or enhancing your own review of the funds transfer activity for proper security and control. It should reinforce the importance of adequate safeguards and help your auditors focus on those areas which may need special attention.

Requests for additional copies of the booklet or any related questions may be directed to our Auditing Department, Ext. 6262.

Sincerely yours,

William H. Wallace

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.

Security and Control of Funds Transfer

Federal Reserve Bank of Dallas

INTRODUCTION

With the increasing volume and dollar amount of funds transfers between Federal Reserve Banks and depository institutions, and among depository institutions, there is an accompanying need for greater audit attention to these activities.

This booklet has been prepared for auditors by the Auditing Department of the Federal Reserve Bank of Dallas to highlight areas of concern and to suggest ways to safeguard funds transfer operations.

3

THE FUNDS TRANSFER SYSTEM

A prime responsibility of the Federal Reserve System is to provide for an elastic currency to ensure a regular flow of money and credit throughout the nation and help create conditions for stable economic development.

To help fulfill this responsibility, the Federal Reserve Communications System (FRCS) was established as a nationwide network connecting all twelve Federal Reserve districts. One of the purposes of the FRCS is to support the transfer of funds between depository institutions.

Depository institutions may send and receive funds transfer messages either in an off-line mode via telephone advice through the Federal Reserve office, or in an on-line mode using a terminal directly connected to the computer system of the Federal Reserve Bank.

Participation in funds transfer service in the Eleventh District is governed by the provisions of this Bank's Bulletin No. 6.

To ensure control and security for transfers of funds, the Federal Reserve Bank of Dallas provides authentication lists to most depository institutions. Code numbers are given by these institutions when requesting transfers.

For institutions not having authentication lists, a callback procedure is used to authenticate transfers. The institution is called immediately after receipt of a transfer request by the Federal Reserve Bank to verify that the request is genuine. Similarly, institutions are urged to call back to the Fed's wire transfer unit after receiving a notification of a transfer for its account.

For those institutions requesting third party transfers, a callback procedure is used to authenticate a random sample of the transfers.

4

AREAS OF VULNERABILITY

Although safeguards against unauthorized use were provided in the design of the FRCS network, it is important that each institution examine its own situation to be certain that all reasonable measures are being taken to reduce the risk of both human error and attempts to intentionally abuse the system.

There have been erroneous transfers, and there have been attempts, some of them successful, to execute fraudulent transfers. From these incidents, the following areas of possible vulnerability have been identified.

- Lack of message authentication procedures.
- Failure to maintain confidentiality of internal operating procedures.
- Clerical errors in giving or taking information over the telephone.

In addition, on-line institutions should be alert for:

- Failure to catch encoding errors at computer terminals.
- Misuse of terminals.
- Lack of contingency plan in the event of computer or terminal downtime or other eventualities.

Although some of these precautions may seem elementary, fraudulent transfers have in fact been made when recommended procedures have not been followed.

In one instance, a man called a Federal Reserve Bank, said he represented a depository institution, and asked the Fed to send a transfer to a third-party institution in another part of the coun-

try, for payment to a specified individual. After hanging up, the Fed employee taking the call realized that the caller had not used an authentication code, although the institution usually did.

Following normal procedures, the Fed employee called the institution and explained it had received a transfer request without a code number. The employee at the institution apologized for the apparent error, looked up the next valid code number, and gave it to the Fed employee. Now the Fed had a code to work with; when it was checked and found to be the proper number in the listing issued to the institution, the transfer was sent, and the institution suffered a loss—a loss that could have been avoided if only the institution employee had been alerted by the call from the Fed to check the institution's records and see whether the transfer request was legitimate.

In another instance, alertness succeeded in preventing a fraud.

In this case, a caller pretending to be a Fed employee advised an institution that it had an incoming transfer. The institution's employee, knowing all its transfer notifications were automatically received via computer terminal, called the Fed to inquire, thwarting the attempt. An off-line institution could foil a similar attempt by following callback procedures.

In a third case, failure to call the Fed back did allow a fraudulent transfer to take place. In this instance, a woman called an institution, saying she was a Fed employee, and advised the institution of an incoming transfer from a nonmember institution for payment to a third party. The institution didn't call to verify the transfer, nor did it become suspicious when no such transfer was included on the next day's statement.

The caller's husband was able to come in and pick up a cashier's check upon presentation of personal identification. The only positive note was that the institution was able to give the FBI the man's real name.

In three similar situations, another person with apparent knowledge of the proper procedures called an on-line institu-

tion, identified herself as working for a correspondent institution, and asked that a transfer be sent to a third institution for payment to a third party. The caller was able to furnish the correct correspondent account number, so the institution sent the transfer and the receiving institution paid out the money. A simple callback would, of course, have prevented this loss.

Finally, there was a case of such magnitude that it made the national press, yet it too could have been prevented.

The story began when an on-line institution retained a firm to install its computer interface system. Several weeks later one of the men who had worked on the installation—a consultant, as it turned out, not an employee of the computer firm—returned to the institution and told funds transfer personnel he was there to check out part of the system. An officer recalled seeing him earlier and, convinced his visit was legitimate, admitted him.

He spent some time in the room checking terminals, apparently noticing that employees kept each day's code word taped to their machines.

Later that day, the funds transfer unit received a call from a man who identified himself as an officer of the institution's international branch. He furnished the proper code and arranged for transfer of $10,200,000 through a New York bank to an account in a Swiss bank. The transfer went through, and the man traveled to Zurich and used more than $8 million of the funds to buy diamonds from a Soviet firm, leaving some $2 million in his bank account.

This fraudulent transfer could have been thwarted if the institution's officer had checked into his visitor's credentials more carefully. However, simply safeguarding the institution's codes would have been more effective. In addition, the institution's statement with the Fed, had it been balanced daily, would have permitted early detection of this fraud.

7

SUGGESTED CONTROLS

To aid you in a review of your funds transfer operations, control recommendations have been separated into several categories, each dealing with a particular aspect of the funds transfer operation. Those dealing with transfer requests, processing, proof, personnel, and general controls related to most institutions are discussed first, while the last section deals with a few controls applicable only to on-line institutions.

TRANSFER REQUESTS

1. Your customers should be positively identified.
2. Any unusual or suspicious telephone calls regarding transfer requests, or requests for information about procedures, should immediately be reported to your management and the Fed bank in your zone, giving as much detail as possible.
3. Telephone requests from outside your institution should be tape recorded and/or transfer data should be repeated back to the requesting individual to verify all information.
4. There should be a callback or authentication procedure, which should require that code words or numbers be used for each transfer.

PROCESSING

1. Transfer requests should be verified before transfers are executed.

2. There should be separation of duties among those employees receiving, verifying, and transmitting transfers.

3. Each employee participating in the transfer process should initial the transfer form or advice to designate that portion of the process which he or she has performed.

4. The flow of work should proceed in one direction only.

5. Account balances should be checked before sending transfers, to ensure that sufficient funds are available.

6. All outgoing transfers should be numbered sequentially to aid in control and reference.

7. Supervisors should be advised promptly of any irregularities in transactions.

8. All telephone transfer requests sent through your Fed office should be logged with (a) the time of each transfer, (b) the name of the Fed employee, and (c) the details of the transaction.

9. All transactions should be thoroughly documented for proper audit trail.

10. Messages received too late for processing should be logged and strictly controlled until they can be processed the next business day.

PROOF

1. For those institutions having a large volume of transfers, periodic balancing throughout the day is an excellent control. It will ensure that transfer requests, credit advices, or other documents have not been misplaced, overlooked, or discarded.

2. There should be procedures to account for all transfers in the end-of-day proof.

3. Institutions should reconcile transfer advices with reserve account entries on a daily basis, promptly reporting exceptions to the Federal Reserve Bank's Accounting Department.

4. Institutions receiving advice of a funds transfer over the telephone should verify the transfer (by callback) before payment is made.

PERSONNEL

1. Whenever possible, tenured, qualified employees should be selected for assignment to the funds transfer unit.

2. Vacancies in the unit should not be advertised in the newspaper.

3. Employees of the unit should not have relatives employed in any other unit of the institution which has a relationship with funds transfer, such as accounting or data processing.

4. Formal training, emphasizing security and controls, should be provided for all employees handling funds transfers:

   (a) each should have access to a current procedures manual, and

   (b) employees should review procedures frequently to keep current.

5. Management should promptly reassign funds transfer employees who have given notice of resignation.

6. Terminated employees should be released immediately.

GENERAL

1. The funds transfer operation should be located in an enclosed, limited-access area.
2. There should be a current list of employees authorized access to the funds transfer area, and access should be controlled.
3. Code and signature lists should be restricted to only those employees responsible for funds transfer operations, and should be secured during non-business hours.
4. Confidentiality of internal operating and control procedure manuals should be protected.
5. All employees should be cautioned not to disclose information regarding codes, callback procedures, or other sensitive transfer information.
6. At least two persons should be in the unit at all times during working hours.
7. There should be agreements in effect governing transfers between the institution, its customers, and correspondent institutions.
8. Funds transfer and auditing personnel should agree on a retention period for transactional records.
9. Wastepaper should be carefully inspected before it is taken from the work area to ensure that no actual transfers are present.

ON-LINE INSTITUTIONS

1. Access to terminals should be limited to personnel authorized to execute transfers.
2. Transfer requests should be checked carefully for errors before transmission.

3. An unbroken copy of all messages should be retained on terminals throughout the operating day, and then stored. This is best accomplished by the use of two-part paper.

4. Terminated or transferred employees' password authorization should be canceled promptly.

5. The total number and dollar amount of transfers should be reconciled promptly to the summary report of the day's transfers. This report is sent by the Fed at the close of business.

6. Telephone line cabinets should be in controlled-access areas.

7. Code lists, user manuals, and forms should be controlled at all times during business hours and secured at the close of business.

8. There should be a contingency plan in case of a computer malfunction at the Fed or an in-house malfunction:

   (a) operators should be able to recognize system failure by thorough familiarization with their equipment,

   (b) in notifying the Fed of terminal failure, operators should know who and where to call, and

   (c) the plan should denote how messages will be delivered and received during downtime.

AUDIT QUESTIONNAIRE

During audits and reviews of funds transfer operations, Fed auditors give attention to physical security, separation of duties, operating controls, effectiveness of procedures, and the selection and training of personnel.

If you have not done so recently, it is suggested that you conduct a review of the procedures in your funds transfer function to determine that adequate controls have been established and are being followed.

One tool used for auditing a funds transfer operation is a questionnaire such as the one that follows. If you currently use a questionnaire in your audits, the Wire Transfer Audit Questionnaire may provide additional questions to use.

The questionnaire employs a Yes/No answer style with questions worded so all "Yes" responses indicate satisfactory conditions, and "No" responses identify points of concern, with space allotted to describe the problem and symbols to indicate whether the answer is based on an inquiry "I," observation "O," or test "T."

If you do not presently use a questionnaire, you may find it to be a most useful audit tool. The questionnaire on the following pages can be adapted to best fit your situation.

WIRE TRANSFER AUDIT QUESTIONNAIRE

TRANSFER REQUESTS

QUESTION	Y/N	BY IOT	COMMENT/RESPONSE
1. Have employees been cautioned to positively identify customers?			
2. Are unusual or suspicious telephone calls immediately reported to the Federal Reserve accounting department?			
3. Are telephone requests tape recorded?			
4. When recorders are not used, is data repeated back to the caller to verify information?			
5. Are call-back procedures used on third-party requests?			

WIRE TRANSFER AUDIT QUESTIONNAIRE

PROCESSING

QUESTION	Y/N	BY IOT	COMMENT/RESPONSE
1. Are verification procedures used to validate transfer requests prior to final execution?			
2. Is there separation of duties in the receiving, verification, and transmitting of transfers?			
3. Does each employee initial transfer forms to designate process each performs?			
4. Is there a one-way work flow?			
5. Is customer account balance checked before making transfers?			
6. Are forms sequentially numbered on all outgoing transfers?			
7. Is supervisor promptly advised of any suspicious irregularities in transactions?			
8. Is a log kept of telephone conversations with Federal Reserve wire transfer unit?			

WIRE TRANSFER AUDIT QUESTIONNAIRE

PROCESSING (CONT.)

QUESTION	Y/N	BY IOT	COMMENT/RESPONSE
9. Are transactions documented for proper audit trail?			
10. Have procedures been initiated to control messages received too late for processing?			

WIRE TRANSFER AUDIT QUESTIONNAIRE

PROOF

QUESTION	Y/N	BY IOT	COMMENT/RESPONSE
1. Are transfers proved periodically during the day?			
2. Have procedures been initiated to account for all transfers in final proof?			
3. Are transfer advices reconciled to Reserve Account entries on a daily basis?			

WIRE TRANSFER AUDIT QUESTIONNAIRE

PERSONNEL

QUESTION	Y/N	BY IOT	COMMENT/RESPONSE
1. Are vacancies in the unit filled by tenured employees?			
2. Does institution refrain from using newspaper advertising to fill vacancies in the unit?			
3. Does institution have a policy restricting relatives of wire transfer employees from working in the accounting or data processing departments?			
4. Is there a formal training program emphasizing security and control?			
5. Upon giving notice of resignation, is an employee reassigned out of the unit?			
6. Are terminated employees immediately released?			

WIRE TRANSFER AUDIT QUESTIONNAIRE

GENERAL

QUESTION	Y/N	BY IOT	COMMENT/RESPONSE
1. Is the wire transfer unit in a limited access area?			
2. Is there a current list of employees authorized access to the area?			
3. Have procedures been instituted to control the following?			
a. Current code lists.			
b. Current signature file.			
c. Operating and control procedure manuals.			
4. Are employees made aware of potential vulnerabilities?			
5. Have employees been cautioned not to discuss internal operating procedures with customers or other outsiders?			
6. Is dual presence maintained at all times during operating hours?			

WIRE TRANSFER AUDIT QUESTIONNAIRE

ON-LINE INSTITUTIONS

QUESTION	Y/N	BY IOT	COMMENT/RESPONSE
1. Are terminals in a limited access area?			
2. Are generated hard copies of transfers checked for correctness of transmission?			
3. Is an unbroken copy of all messages retained on terminals throughout the operating day?			
4. Are total transfers proved to summary report once each day?			
5. Is there a current contingency plan?			
6. Are employees instructed on contingency plan?			
7. Are telephone lines in a controlled access area?			
8. Are test word lists, program initialization tapes, user manuals, and forms controlled at all times?			
9. Is a terminated or transferred employee's password canceled promptly?			

If you have any questions or comments, please contact the Auditing Department, (214) 651-6262.

To obtain a copy of Bulletin 6, "Wire Transfers of Funds," contact the Records Division of the Department of Communications, Financial and Community Affairs, (214) 651-6382.

Federal Reserve Bank of Dallas
400 South Akard Street
Dallas, Texas

[Mailing Address: Station K, Dallas, Texas 75222]