FEDERAL RESERVE BANK
OF NEW YORK

At-Cir. No. 10339

March 19, 1990

FEDWIRE SECURITY GUIDELINES BROCHURE

To the Chief Operating Officer of Each Depository Institution
in the Second Federal Reserve District:

The Federal Reserve System has prepared guidelines to assist financial institutions in reviewing the adequacy of security and operational controls in their funds and securities transfer operations. These guidelines are incorporated in the enclosed brochure entitled **Fedwire Security Guidelines for Financial Institutions.**

The guidelines are offered for consideration when conducting reviews of your funds and securities transfer operations. While they refer specifically to Fedwire transfers, they have applicability to all wire transfer operations, and each institution should have procedures in place to meet its particular needs. We recognize that these suggestions may be implemented in different ways by different institutions, but we believe that the basic control principles can and should be adopted by all.

If you or members of your staff have any questions concerning security and control procedures, please contact Andrew Heikaus, Manager, Funds Transfer Department (212-720-5561) or Patricia Hilt-Lupack, Manager, Securities Transfer Department (212-720-5379).

CAROL W. BARRETT,
Vice President.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

FEDWIRE

SECURITY GUIDELINES

FOR

FINANCIAL INSTITUTIONS

FEDERAL RESERVE SYSTEM

DECEMBER 1989

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

INTRODUCTION

Currently, there is a trend toward the increased use of electronic transfer of funds. As a result, the opportunity for external and internal fraud or theft may also increase. Although the Federal Reserve System has incorporated safeguards in the design of the Federal Reserve Communications System (FRCS) Network and the Funds Transfer application, it is vitally important that each financial institution involved in funds transfer operations assumes the responsibility for examining its internal procedures in order to reduce risk.

This brochure has been prepared by the Federal Reserve System to assist financial institutions in reviewing the adequacy of their security and operational controls in this area. Recommendations have been separated into categories, each dealing with a specific aspect of funds transfer operations. The recommendations contained within this document are suggested guidelines which the Federal Reserve System strongly encourages you to adopt, however, we realize that operational limitations within your institution may require you to implement these recommendations using a phased approach as they become feasible.

It should be noted that the brochure has been prepared to assist in identifying responsibilities and is not meant to encompass all possible operational controls to avoid fraud or theft.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

I. PERSONNEL

1. Management responsible for sensitive positions should review screening and hiring procedures and practices.

2. Candidates for employment in sensitive positions should be subjected to extensive screening procedures, which may include requirements for periodic submission of statements of indebtedness, credit checks, written confirmation of both education and previous employment, fingerprinting, and a criminal records investigation through the FBI.

3. Employees in sensitive positions should be counseled on a regular basis regarding management's position on the control of the operation, handling of all data and equipment, and the employee's obligation to report immediately to management any knowledge of fraud or violations of operating procedures.

4. Whenever possible, longer-service employees should be assigned to work in the funds transfer unit.

5. Supervisory staff members should be attentive and alert to unusual behavior on the part of employees in the funds transfer unit.

6. Temporary or outside agency help should be excluded from working in the funds transfer unit.

7. Employees of the funds transfer unit should not have relatives employed in other units of the institution, such as data processing or accounting functions, which have a working relationship with the funds transfer unit.

8. Whenever possible, management should promptly reassign to another unit any funds transfer employees who have given notice of resignation.

9. Terminated employees should be released immediately and allowed no further access to the funds transfer facility.

10. If an employee resigns or is terminated, management should immediately recover from the employee identity cards, badges, or passes, and where necessary lock combinations or doors accessing the funds area should be changed. Management should also remove the employee's name from any authorization forms with the Federal Reserve Bank or a correspondent, including any signature or off-line authority. In the case of an on-line institution, it would also be appropriate to contact the local security officer in order to suspend the employee's User ID and ACF2 access.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

11. Formal training, emphasizing security, controls, and current trends in funds transfer activities, should be provided for all employees handling funds transfers. Up-to-date procedure manuals should be readily accessible to these employees, and periodic review of funds transfer procedures should be mandatory.

12. If possible, unannounced rotation of funds transfer employees should be instituted by management.

13. All employees should be instructed not to disclose sensitive transfer information and procedures.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

II. OPERATIONAL AND PROCESSING CONTROLS

1. At least two employees (dual control) should be present while the funds application is operational and funds transactions can be sent or received.

2. Management should segregate duties, to the extent possible, within the funds transfer operation. For example, receipt, entry, and verification functions should not be performed by the same employee.

3. The name of the employee responsible for or actually handling each step in processing a transfer should be recorded and maintained to ensure accountability.

4. The flow of work should proceed in only one direction to provide an adequate internal control environment.

5. Transfer requests should be verified before the transfers are actually executed.

6. Authentication procedures (e.g., codewords, passwords and/or callbacks) should be used when receiving funds transfer instructions over the telephone, particularly for those involving a third party. Ideally, all such requests should be received at a central point so that authentication procedures can be applied uniformally.

7. Before paying funds to customers, callback or other positive verification procedures should be used to confirm third-party transfer instructions or advices of receipt from correspondents.

8. To provide additional support to the institution in the event of disputes regarding instructions or dollar amounts, telephone conversations involving transfer requests should be recorded.

9. Before transfer instructions are acted upon, an employee should confirm that available funds are in the customer's account or that the transfer amount is within authorized credit limits.

10. Rejected transactions and all correcting and reversing entries should be subjected to supervisory review.

11. All transactions should be thoroughly documented to ensure that a proper audit trail exists.

12. All incoming and outgoing payment orders and message requests received in the funds transfer area should be (1) time stamped or sequentially numbered for control, (2) logged, (3) reviewed for signature authenticity, and (4) reviewed to determine whether personnel initiating funds have the authority to do so.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

13. If transfer requests are accepted after the close of business or with a future value, they should be properly controlled and processed.

14. All payment orders and message requests should be accounted for in an end-of-day proof to ensure that all requests have been processed.

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

16. A daily reconcilement of all funds sent and received over the system (CHIPS and Fedwire) should be performed. The reconcilement should indicate dollar amounts and number of transactions.

17. Retrieved messages should be clearly identified as copies so that they are excluded from accounting and settlement processes.

18. Continuous, unbroken hard copies of all transactions transmitted through a terminal connected to Fedwire should be retained.

19. Supervisors should be advised promptly of any irregularities involving transfers or procedures.

20. Extra attention to security and control procedures should be extended in emergency or unusual situations (e.g., major computer outages or power failures).

21. Adequate retention periods should be established for transaction records.

22. Care should be taken to assure that documents related to a funds transfer request are not disposed of inadvertently.

23. Confidential materials (e.g., expired codeword lists) should be destroyed in accordance with established procedures for destruction of such information.

24. Employees should be instructed to keep passwords confidential. Passwords should be changed periodically or, if compromised, immediately.

25. If codewords are used to originate transfers off-line, receipt of these codewords from the Federal Reserve Bank should be acknowledged immediately. Control should be maintained over codeword access to prevent unauthorized access.

26. Employees should be discouraged from answering questions or revealing operational information to those outside the funds transfer department.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

III. BALANCING AND ACCOUNTING CONTROLS

1. Institutions that receive telephonic advice from the Federal Reserve Bank of incoming funds transfers for credit to a third party should (1) verify the transfer by callback, or (2) wait for the paper advice to arrive from the Federal Reserve Bank before payment is made.

2. Institutions having a large volume of transfers should perform periodic balancing throughout the day to ensure that transfer requests, credit advices or other pertinent funds documentation has not been misplaced, overlooked, or discarded. The balancing procedure should include verification and control of incoming and outgoing sequence numbers to ensure that they are consecutive and unique, as well as confirmation that all batch acknowledgements for outgoing items are received.

3. Procedures should be in place to verify that the total number and dollar amount of funds transfer messages sent and received by Fedwire are in proof with summaries received from the Federal Reserve, at least on an end-of-day basis. To facilitate this proof, a log should be maintained of all transfer requests at point of receipt.

4. On the next business day after receipt, institutions should reconcile their funds transfer activity with the accounting entries on the daily reserve or clearing account statements. Exceptions should be reported to the individuals responsible for funds transfers at the Federal Reserve Bank in their District as soon as possible.

5. Institutions should provide advice copies of funds transfers to customers and encourage them to reconcile the advices on the day of receipt.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

IV. PHYSICAL SECURITY

1. The funds transfer operation should be located, if possible, in an enclosed, limited-access area.

2. Only persons having a business need should be permitted access to the funds transfer area.

3. Unauthorized persons should be challenged when they attempt to enter the funds transfer area.

4. If visitors are admitted into the funds transfer area, they should be required to sign in and out, continuously exhibit identification, and be escorted by an authorized employee at all times.

5. Vendor personnel should be barred from (1) having access to sensitive data and/or (2) unsupervised access to equipment.

6. The supervisor or designated equivalent should always be present in the terminal and message preparation area.

7. Sensitive data should be restricted from viewing by visitors.

8. Use of cameras in the funds transfer area should be prohibited unless specific written authorization has been provided by the appropriate personnel, for example, security, public relations, communications officials and funds management. Under no circumstances should the use of cameras be authorized to photograph or record pictures of terminal screens.

9. Terminals and other equipment and material used in the Fedwire operations should be secured at all times.

10. Security copies of software (computer programs) used to run data entry devices (PCs) should be stored in a secure manner.

11. Keys for sensitive equipment should not be removed from the funds area.

12. Employees should be trained in the proper steps to be taken in case of fire or other emergency situations.

13. Fire fighting procedures should be regularly tested and established evacuation plans reviewed periodically.

14. An adequate power supply should be available from a secondary source and regularly tested.

15. If possible, internal plumbing should be routed to avoid flooding of communications installations in the event of breakage or malfunction.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

V. LEGAL AGREEMENTS

1. Written agreements for all funds transfer operations between the financial institutions and its customers, hardware and software vendors, correspondent banks, maintenance companies, and the Federal Reserve Bank should be established and maintained. (agreements with the Federal Reserve Bank should specifically refer to pertinent operating circular(s) regarding wire transfer of funds, pursuant to subpart B of Regulation J.)

2. Agreements should fix responsibilities and accountability between the parties.

3. Agreements should clearly set forth the scope of the financial institution's liability.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

VI. AUDIT PROGRAMS

1. Funds transfer operations should be periodically reviewed on both an announced and unannounced basis.

2. All of the activities of funds transfer operations should be included in your institution's audit program.

3. Internal auditors should be trained in funds transfer operations and controls.

4. Full scope audits should require substantive testing or quantitative measurements in such funds transfer activities as (1) personnel policies, (2) operating procedures, (3) legal agreements, (4) physical security, (5) processing, (6) contingency plans, (7) message testing, and (8) balance verification and overdraft approval.

5. Internal and/or external audit reports to management should include appraisal of the internal control environment.

6. Management response to audit exceptions should indicate whether prompt and appropriate corrective action was taken.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis

VII. DISASTER RECOVERY PLANS

1. Formal disaster recovery plans should be devised, updated, and reviewed on a regular basis.

2. Disaster recovery plans should include the names of personnel to be notified in the event of an outage; hardware, software, and communications requirements; plans for intermediate storage of transactions; procedures for accepting messages from localities other than normal ones; accounting procedures to be followed; the maximum and minimum amounts which may be processed; and additional security measures.

3. Periodic testing using the back-up system and the disaster recovery plan should be performed with disaster recovery personnel to ensure successful operations in a disaster situation. A refresher course for disaster recovery personnel should be conducted on an annual basis.

4. In selecting a communications site, the following should be considered: topography; controlled access to communications, power, fuel, and water systems; proximity to sources of radio frequency interference; availability of fire and police services; controlled entry to the building; and controlled entry to and visibility of the computer complex.

5. Disaster Recovery plans should be distributed by management to all funds transfer personnel.

6. Sensitive information and equipment should be adequately secured before evacuation in an emergency and further access to the affected areas should be controlled by security personnel.

7. The disaster recovery installation should conform to building fire, and electrical codes.

8. Availability of the detailed site plan for the disaster recovery installation should be limited to authorized personnel.

Digitized for FRASER
http://fraser.stlouisfed.org/
Federal Reserve Bank of St. Louis