FEDERAL RESERVE BANK OF NEW YORK

Atl. Cir. No. 10218

January 7, 1988

SECURITY OF FEDWIRE OPERATIONS

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

The purpose of this notice is to encourage depository institutions to review periodically their funds and book-entry securities transfer operations to ensure that adequate precautionary measures are in place to guard against possible wire transfer fraud. Fedwire transfers often involve large sums of money, and cannot be retrieved unilaterally by the sender. Thus, procedures for processing transfers sent and received over Fedwire should be carefully and regularly reviewed to assure that appropriate security measures are in place.

Nationwide data suggest that various methods have been used to attempt fraudulent transfers. Examples include: gaining unauthorized access to computer rooms, terminals, or testwords; collusion with bank or customer personnel; and impersonating correspondent bank personnel, Federal Reserve Bank personnel, or corporate or respondent bank customers. If your institution detects a fraudulent wire transfer attempt, regardless of whether or not the attempt is successful, the local office of the Federal Bureau of Investigation should be notified immediately. If the fraud attempt involves a Fedwire transfer, the Funds Transfer Department or the Securities Transfer Department of this Bank should also be notified immediately.

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

If you or members of your staff have any questions concerning Fedwire security and control procedures, please contact Andrew Heikaus, Manager, Funds Transfer Department (Tel. No. 212-720-5561), or Patricia Hilt-Lupack, Manager, Securities Transfer Department (Tel. No. 212-720-5379).

CAROL W. BARRETT,
Vice President.

Recommendations in Connection With Safeguarding the Integrity of Fedwire Transfers

1. *Operational controls*

   - Employ authentication procedures (*e.g.*, testwords and call-backs) when receiving funds and securities 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 uniformly.
   - Use call-back or other positive verification procedures to confirm third-party transfer instructions to or advices of receipt from correspondents before paying funds to customers.
   - Change testword and other authentication mechanisms (*e.g.*, encryption keys) on an appropriate schedule.
   - Tape-record telephone conversations involving transfer requests, to provide additional support to your institution in the event of disputes regarding instructions or amounts.
   - Retain unbroken monitor copies or hard copies of all transactions transmitted through terminals connected to Fedwire.
   - Confirm that available funds are in a customer's account or that the transfer amount is within authorized credit limits before transfer instructions are implemented.
   - Devote extra attention to security and control procedures in emergency or unusual situations (*e.g.*, major computer outages or power failures).
   - Subject rejected transactions and all correcting and reversing entries to supervisory review.
   - Above all, caution all employees involved to be alert to unusual or suspicious requests for information, changes in instructions from customers, activities of coworkers, etc. They should also be cautioned not to discuss internal procedures with anyone outside your funds or securities areas.

2. *Balancing and accounting controls*

   - Verify that the message accountability sequence numbers on transfers sent and received are unique and consecutive.
   - Confirm that acknowledgements are returned for all outgoing messages.
   - Verify that the total number and dollar amount of funds and securities 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, maintain a log of all transfer requests at the point of receipt.
   - Reconcile differences on daily reserve or clearing account statements promptly and report any discrepancies to this Bank immediately.
   - Provide advice copies of funds and securities transfers to your customers and encourage reconcilement of these advices by your customers on the day of receipt.

3. *Personnel*

- Establish appropriate segregation of duties, to the extent possible, within the wire transfer operation. For example, receive, entry and verification functions should *not* be performed by the same person for the same message.
- Ensure that employees receive periodic training concerning the importance of security and control measures and that penalties for noncompliance with operating procedures are published and enforced.
- Rotate personnel assigned to the communications area; enforce vacation requirements; and consider increasing supervision of these employees, if appropriate.
- Review the appropriateness of hiring practices with respect to employees having access to computer rooms and communications terminals.
- Reassign employees who have given notice of resignation or who have been given notice of termination.
- Monitor closely the activities of all outside personnel who are on your institution's premises (*e.g.*, consultants, programmers, repairmen).
- Direct employees to keep user-id passwords confidential and to change their passwords periodically.

4. *Physical security*

- Ensure that only individuals who have a business need are permitted access to computer rooms, communications lines, telephone panel boards, terminals, operating instructions, test-code formulas, encryption keys, testword lists, forms, passwords, computer files, and programs.
- Ensure that terminals and other equipment and material (*e.g.*, encryption keys, testwords) used in your Fedwire operations are secured 24 hours a day.
- Ensure that security copies of software (computer programs) used to run data entry devices (PCs) are stored in a secure manner.

5. *Legal agreements*

- Establish and maintain written agreements for all customers making funds or securities transfer requests, particularly for those customers who initiate transfer requests by telephone, terminals, or other means that do not provide for signed authorization. These agreements should clearly set forth the scope of your institution's liability.

6. *Audit programs*

- Include all of the activities of your institution's funds and securities transfer operations in your institution's audit program.

Prepared by:
Federal Reserve Bank of New York
Electronic Payments Function
January 1988