FEDERAL RESERVE BANK
OF NEW YORK

AT 9665

April 5, 1984

SECURITY OF FEDWIRE OPERATIONS

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

Over the past several months, we have noticed an increase in the number of attempts to make fraudulent funds transfers over electronic payments systems. The Federal Reserve's funds transfer service is an important service we offer to you, and through you, to your customers. It is essential that we each do our part to maintain the integrity of these payments.

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 funds transfer attempt, the local office of the Federal Bureau of Investigation should be notified immediately. If the fraud attempt involves a Fedwire transfer, this Bank should also be notified immediately.

It is also important that depository institutions ensure that precautionary measures are in place to guard against possible wire transfer fraud. Particularly because Fedwire transfers are irrevocable, we believe that procedures for processing transfers sent and received over Fedwire should be carefully and regularly reviewed to assure that appropriate security procedures are in place for both funds and securities transfer operations.

The suggestions printed on the following pages are offered for your consideration when conducting such reviews. 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, at our Head Office, Robert W. Dabbs, Manager, Funds Transfer Department (Tel. No. 212-791-8475), or H. John Costalos, Manager, Securities Transfer Department (Tel. No. 212-791-5986); or, at our Buffalo Branch, Robert J. McDonnell, Operations Officer (Tel. No. 716-849-5022).

JORGE BRATHWAITE,
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 periodically.
   - 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*
   - Confirm that incoming transfer messages from the Federal Reserve are received in proper sequence.
   - 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*
   - Segregate, to the extent possible, the duties and responsibilities of employees in your wire transfer operations. The functions that should be clearly segregated are origination, receipt, customer verification, message testing, transmission, error correction, and reconcilement.
   - Ensure that employees receive periodic training concerning the importance of security and control measures and that penalties for non-compliance 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).

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 used in your Fedwire operations are secured 24 hours a day.

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 Services Function
April 3, 1984