FEDERAL RESERVE BANK
OF DALLAS

WILLIAM H. WALLACE
FIRST VICE PRESIDENT
AND CHIEF OPERATING OFFICER

March 10, 1988

DALLAS, TEXAS 75222

Circular 88-21

**TO:** The Chief Operations Officer of
financial institutions in the
Eleventh Federal Reserve District

**SUBJECT**

**Funds Transfer Fraud**

**DETAILS**

Please be alert for possible attempts at offline funds transfer fraud. The fraudulent transfers may involve a telephone call supposedly from another office of the same financial institution initiating a pay upon presentation of proper identification (PUPID) transfer. The persons involved may pose as a funds transfer operator at a main office or a correspondent and advise a branch office or respondent that a PUPID transfer has arrived.

Financial institutions should take appropriate precautions when handling funds transfers. Please review the telephone verification procedures that you have established for your funds transfer operations. If you do not use telephone callback verification with other offices or correspondents, we suggest you implement such procedures immediately. Institutions should use caution when accepting notifications of incoming transfers by telephone. Procedures for processing transfers sent and received over Fedwire should be carefully and regularly reviewed to assure that appropriate security measures are in place.

The following suggestions are offered for your consideration when conducting reviews of your funds and securities transfer operations. 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.

## Recommendations in Connection With Safeguarding the Integrity of Fedwire Transfers

### 1. Operational controls

- Employ authentication procedures (e.g., testwords and callbacks) 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 callback or other positive verification procedures to confirm third-party transfer instructions to or advices of receipt from correspondents before paying funds to customer.

- Change testword and other authentication mechanisms (e.g., encryption keys) on an appropriate schedule.

- Record telephone conversations involving transfer requests, to provide additional support to your institution in the event of disputes regarding instruction 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, and activities of coworkers. They also should be cautioned not to discuss internal procedures with anyone outside your funds or securities area.

### 2. Balancing and accounting controls

- Verify that the message accountability sequence numbers on transfers sent and received are unique and consecutive.

- Confirm that acknowledgments 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 the Dallas Fed 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 funds 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.

**MORE INFORMATION**

For more information, please contact Larry C. Ripley at (214) 651-6118 or Jonnie K. Miller at (214) 651-6290.

Sincerely yours,

William H. Wallace