FEDERAL RESERVE BANK OF NEW YORK

NEW YORK, N.Y. 10045-0001

AREA CODE 212-720-5000

April 28, 1999

To: FEDLINE ® SECURITY ADMINISTRATORS

From: Mark Harris, Staff Director
Fedwire Network Services Staff

Subject: Encryption enhancement

Triple DES Security Enhancement

The Federal Reserve Bank recognizes the critical importance of protecting data transmissions to and from depository institutions. One of the mechanisms to protect data transmissions used by the Federal Reserve Bank is encryption, where information is scrambled with a secret key shared between the Federal Reserve Bank and your depository institution. Currently, FedLine terminals use a security architecture with encryption technology known as the Data Encryption Standard (DES). The Federal Reserve conducts ongoing reviews of opportunities to strengthen its security techniques. After extensive analysis, the Federal Reserve has selected an improvement to the current DES that can be used by most FedLine terminals. This security improvement uses Triple DES encryption to increase the level of protection to encryption keys transmitted at the beginning of a session between the Federal Reserve Bank and depository institutions. These keys will be encrypted under Triple DES, making it more difficult to unscramble them.

Because of the increased security Triple DES provides, all FedLine dial and leased-line terminals using Jones Futurex 300 series boards will be converted from DES to Triple DES encryption. If your institution uses a different encryption board or method, you may wish to contact your local Federal Reserve Bank to discuss alternatives for security improvements. **Note: (IBM PS2 Series machines use Jones 526 Boards which do not accommodate this upgrade).**

Implementation Process

The Triple DES conversion for the Jones Futurex 300 Series is scheduled to begin in April 1999 and will continue through the end of August 1999. All affected FedLine PC's are being scheduled for conversion within these dates. Conversion to Triple DES requires manual entry of your encryption key, which involves a "dual-custody" approach. Two designated individuals at your institution each will receive half of the key via secure mail. Both halves of the key must be entered on your conversion date to ensure that your FedLine connectivity is not disrupted.

Security Administrator

As a part of this effort we want to ensure that we have current Security Administrator information on file. In addition to containing your Triple DES cutover date, the enclosure contains the current Primary and Alternate security administrator information that is on file for your institution. Triple DES keys will be delivered to these administrators unless otherwise instructed by your institution. If this Security Administrator information has changed, we ask you complete the enclosed Security Administrator card and mail it to:

Fedwire Network Services Staff
33 Liberty Street
New York, NY 10045
Attn: Mark Harris

Year 2000 Readiness Disclosure

With the upgrade to Triple DES, the FedLine software remains unchanged, and no changes will be made to the hardware used for the FedLine product. The Federal Reserve has successfully completed rigorous Y2K readiness testing of all components of the Triple DES upgrade. This upgrade does not affect date-sensitive code or date-dependent processing routines; rather, it provides an updated driver for use by the encryption board and other utility files needed to enable Triple DES encryption. The FedLine software is not being changed; therefore, further Y2K testing of the Triple DES upgrade is at the discretion of your institution's management and Y2K readiness policies. Should your institution decide to retest, please contact your Federal Reserve FedLine contact for scheduling. If your institution's Y2K change limitation policies restrict your ability to implement Triple DES, or if your institution has not yet tested FedLine for Y2K readiness, we urge you to contact your FedLine contact immediately. For more information on Federal Reserve System Y2K century date change (CDC) testing, refer to *CDC Bulletin No. 6*, available on the Federal Reserve System's CDC web site (http://www. frbsf.org/fiservices/cdc/).

Triple DES Conversion

Keys will be loaded to your FedLine at 3:00 p.m. the day of your scheduled cutover. In the event that we are not able to convert your FedLine to Triple DES, we will provide to you a "fallback" set of single DES keys. **Please note**: **minimum FedLine version 2.50.55 is required for this installation.**

Conversion Date

Enclosed you will find cutover dates for each one of your FedLine terminals. Please indicate if these dates are acceptable to your institution. We request confirmation of these dates at least two weeks prior to your conversion date. If the cutover dates are not acceptable please indicate "no" and complete the comments section of the attachment and we will contact you to determine dates that are mutually convenient. Please complete and fax the form to the Fedwire Network Services Staff at 212-720-6281 or contact the Customer Service Staff at 212-720-5802.

Approximately two weeks prior to your cutover you will receive the following materials:

- A set of Triple DES keys for each terminal
- A set of “FALLBACK ” Single DES keys
- Installation Instructions
- Triple DES patch

For Additional Information

If you have questions or concerns regarding the FedLine Triple DES encryption conversion, please contact Mary Freudenberg at 212-720-5987 or Stanley Rozanski at 212-720-5138.

Enclosure