Federal Financial Institutions Examination Council

FFIEC

FedLine FED

AUGUST 2003

IT Examination Handbook

TABLE OF CONTENTS

INTRODUCTION

The FedLine Booklet is another in the series that comprises the Federal Financial Institutions Examination Council (FFIEC) *IT Examination Handbook* (*IT Handbook*). This booklet replaces Chapter 19 of the 1996 Federal Financial Institutions Examination Council (FFIEC) *Information Systems Examination Handbook.* It addresses the risks, risk management practices, and mitigating controls necessary to establish and maintain an appropriate operating environment for the FedLine Funds Transfer (FT) application. FedLine is the Federal Reserve Bank's proprietary electronic delivery channel for financial institution access to Federal Reserve financial services, and includes DOS-based FedLine and FedLine for the Web.[1] FedLine for the Web is available to financial institutions for access to financial services deemed low-risk by the Federal Reserve but does not currently offer access to high-risk payment-related applications such as funds transfer. Future updates to this booklet will incorporate the risk considerations and controls associated with the FedLine for the Web environment, including high-risk payment applications such as funds transfer, as the Federal Reserve introduces these additional features for financial institution use.

FedLine is a stand alone, PC-based hardware and software package providing financial institution access to accounting, Automated Clearinghouse (ACH), book-entry securities, cash, check, treasury services, and Fedwire funds transfer applications. These applications allow for the creation and transmission of payment messages, account balance monitoring, and other functions performed via encrypted dial-up sessions with the Federal Reserve Bank's host computer.[2]

Using the FedLine FT application exposes a financial institution to certain operational (transaction) risks that the institutions must appropriately control. Funds transfer messages provide for the immediate availability of funds to the credited account once sent from the FedLine PC and processed at the Federal Reserve Bank's host computer.

FedLine incorporates three security measures designed to protect against unauthorized access to FedLine applications and Federal Reserve communication networks:

- Assignment of access levels needed to perform local FedLine functions;
- Restricted access to Federal Reserve host computer systems; and
- Controlled use of hardware-based data encryption.

[1] ® FedLine, DOS-based FedLine, FedLine for the Web, and Fedwire are registered servicemarks of the Federal Reserve Banks. References to FedLine refer specifically to DOS-based FedLine, unless otherwise noted.

[2] Refer to Appendix D for a complete list of FedLine applications and corresponding codes.

Appropriate physical and logical access controls should be established to ensure only authorized staff can create, verify, and send funds transfer instructions on behalf of the financial institution and its customers as well as guard against inadvertent errors or omissions. The operational risk inherent in generating and sending fraudulent funds transfer messages, potentially targeting the institution's available cash balances, and transferring them to accounts beyond the control of the financial institution, exposes the financial institution to significant credit, liquidity, legal, and compliance risks.

Federal Reserve Operating Circular No. 5 sets out the terms and conditions under which a financial institution may access certain financial services and under which a financial institution may send data to or receive data from a Federal Reserve Bank by means of electronic connection(s).[3] Federal Reserve Operating Circular No. 6 sets out the terms and conditions under which a financial institution can transmit and receive funds transfers through Fedwire, including responsibilities for information security, business continuity, and related administrative information.[4]

The guidance in this booklet primarily targets operational (transaction) risks related to funds transfers. Management, however, should also understand the indirect impact this funds transfer system could have on other risk areas within the institution.

The booklet is organized within three general sections. The first section describes the operational (transaction risks) associated with the use of the FedLine PC and FT application and the specific risk management practices and controls needed to mitigate these risks.

The second section includes recommended FedLine security settings available to the financial institution to support processing only authorized funds transfer messages and to minimize processing potentially unauthorized messages due to fraud, errors, and omissions. Although the recommended security settings provide specific information useful to both financial institution management and examination field staff, the recommended security settings are appropriate within the context of the size and complexity of the financial institution including its specific operating environment, staffing levels, and funds transfer activity. Financial institutions and examiners should use the recommended settings as a guide to evaluate the related controls. Differences may be the result of the institution choosing alternate mitigating controls designed to meet its particular operating environment and capabilities.

The third section includes examination procedures, a glossary of terms, and references to information including specific FedLine applications, codes, and access levels. Please

[3] Refer to http://www.frbservices.org/, "Reference Guides and Operating Circulars," for Federal Reserve Bank Operating Circular No. 5, Electronic Access.

[4] Refer to http://www.frbservices.org/, "Reference Guides and Operating Circulars," for Federal Reserve Bank Operating Circular No. 6, "Funds Transfers Through Fedwire."

refer to the *IT Handbook's* "Information Security Booklet" and "Business Continuity Planning Booklet" for additional details on information security access controls and business continuity planning respectively. Additional information concerning Fedwire funds transfer, including the Federal Reserve's Payment System Risk (PSR) policy, balancing functions, credit limits, collected balances, and transferee identification can be found in the *IT Handbook's* "Wholesale Payment Systems Booklet."

OPERATIONAL (TRANSACTION) RISK MANAGEMENT

Action Summary

A financial institution should evaluate the physical, administrative, logical, procedural, and business continuity risk management practices associated with its funds transfer operation, and assess its ability to process only authorized funds transfer messages. Because FedLine is typically a high-priority system, financial institutions should integrate consideration of FedLine into their risk assessment, control, monitoring, and testing processes for security, business continuity, and vendor management. Management should ensure appropriate risk assessments are conducted to assess financial institution performance in meeting the standards set forth in the Federal Reserve's Operating Circulars, Nos. 5 and 6, and internal policies and procedures established to conduct funds transfer services.

Financial institutions are responsible for developing the appropriate physical, administrative, logical, and procedural safeguards necessary to mitigate funds transfer operational (transaction) risk when using the FT application.[5] At a minimum, institutions should consider implementing the suggested controls and safeguards described below. Although financial institutions may implement the suggested controls differently depending upon the nature of their activities, each institution should demonstrate an effective control environment. Appropriately defined and assigned FT and Local Administration (LA) application access levels support effective separation of duties. The institution should also implement, monitor, and test the effectiveness of the logical access controls as part of its information security program. Financial institutions should also develop, implement, and test business continuity plans appropriate for their level of funds transfer activity.

PHYSICAL SECURITY CONTROLS

The physical security controls described in this section focus on preventing unauthorized staff and customer access to the FedLine PC and printer. Financial institution management should periodically assess the overall physical security risks associated with the use of the FedLine PC and printer and determine the specific physical security risks present when using the FT application. The risk assessment should focus on the financial institution's funds transfer operation and include an analysis of any risks resulting from build-

[5] Refer to Federal Reserve Operating Circular No. 6, Appendices A, "Funds Transfer Security Procedures," and A-1, "Funds Transfer Security Procedure Agreement," for a discussion of financial institution responsibilities.

ing and office configuration limitations. The assessment should also include an analysis of any risks associated with controlling physical access to FedLine software and other critical information.

ACCESS TO THE FEDLINE PC

Weak physical security controls could result in the unauthorized use of, or tampering with, the FedLine PC and printer, thereby jeopardizing the integrity of the PC platform, FedLine software, or funds transfer messages entered for transmission to the Federal Reserve. Failure to properly secure the financial institution's wire room or the work area designated for the operation of the FedLine PC and printer could create vulnerabilities due to unauthorized staff or customer access.

Institution management should locate the FedLine PC and printer in a physically secured area that prevents access to unauthorized staff and customer access. Therefore, institutions should avoid operating the FedLine system from an area designated for customer transactions. Financial institutions should consider locating the FedLine PC and printer in a locked room with restricted and monitored access. Placing the PC in an open staff area during normal business hours may also be acceptable if the institution can demonstrate that appropriate monitoring is conducted and that the PC is properly secured (e.g., locked cabinet or PC enclosure) during non-business hours. Ultimately, financial institution management should establish a level of physical security appropriate to its operating environment.

ACCESS TO FEDLINE SOFTWARE AND OTHER CRITICAL INFORMATION

Unauthorized access to FedLine software and other critical information (e.g., encryption material, master local user ID and password, configuration diskette, PC power-on password, printer log) potentially compromises the availability and integrity of funds transfer operations. In the event of an equipment failure, power outage, or declared disaster, this risk may increase.

Management should secure these materials under lock and key, and restrict access to authorized staff on a need-to-know basis. Management should also ensure that complete back-ups of these materials are stored securely offsite. These materials include:

- *Configuration Diskette* – Used in conjunction with the local Federal Reserve Bank office in case authorized users are locked out of the system or there is a need to re-configure the system.
- *Encryption Material* – Refers to information pertaining to the encryption implementation and Federal Reserve Bank supplied encryption keys. FedLine encryption keys are unique to each FedLine PC.

- *PC Power-on Password (if available on PC used for FedLine)* – Requires the use of a password before the FedLine PC will activate. The Local Security Administrator (LSA) should not have access to the PC power-on password, and a procedure should be established defining its use and the circumstances under which the LSA can gain access. This procedural control can prevent the LSA from potentially entering unauthorized funds transfer messages while the FedLine PC is not being monitored. If the PC power-on password is not available, the institution should carefully monitor access to the FedLine PC during business hours, and physically secure the FedLine PC after business hours to prevent unauthorized LSA access.

- *Master Local User ID (Master ID) and Password* – The master ID and password shipped with FedLine. The LSA uses the master ID and password to initially establish access to FedLine and is required to immediately change the default password for production use. The master ID and password should be stored in a secure location (e.g. safe deposit box in the vault). It is important to remember that the master password may be needed in an emergency or other situation in which the LSA is unavailable and LA application functions need to be performed. The master ID and password should be changed by the LSA or back-up or alternate LSA immediately after it is used in an emergency situation and stored securely for future use.

ADMINISTRATIVE CONTROLS

The administrative controls described in this section are primarily designed to ensure that the financial institution has appropriately assigned the role of LSA and back-up or alternate LSA. The LSA and back-up LSA perform critical roles in defining and maintaining an effective, efficient, and secure funds transfer operation. As such, assigned staff members should be trusted and *not* responsible for day-to-day payment and computer-related operations. The financial institution should also establish procedures for the periodic review of the FedLine printer log (Printer Recap Report), and is responsible for maintaining the FedLine PC at current release levels.

LOCAL SECURITY ADMINISTRATOR

The use of FedLine requires the financial institution to designate an LSA. The LSA, using the LA application, is responsible for establishing and maintaining application access levels for all financial institution users, including those assigned the FT application. The LSA is a privileged user who could bypass authorized access levels and security settings, resulting in the sending of unauthorized funds transfer messages.

Financial institutions should generally limit the number of employees with LSA access to two staff members, and periodically monitor their activities. In larger institutions, senior

management should carefully evaluate and justify the existence of more than two staff members with LSA responsibilities.

As privileged FedLine users, the LSA and back-up or alternate LSA have the authority to bypass established funds transfer internal controls. Compensating controls, including prompt reconcilement and accounting procedures, timely FedLine printer log (Printer Recap Report) reviews, and distinct job descriptions that promote effective separation of duties, should be established to mitigate potentially fraudulent actions on the part of the LSA and back-up LSA. If the LSA or back-up LSA uses the FedLine PC, operations staff should be present to monitor their actions, where practical.

The LSA acts as the primary contact with the Federal Reserve Bank for FedLine software updates and host-communication and encryption-related activities. The LSA is primarily an administrative role. The LSA is responsible for adding new users, deleting old users, and changing authorized user access levels as their responsibilities change. The LSA, in order to perform these functions, is required to use the LA application, "Entry/Update" access level. Since this access gives a user privileged access to the FedLine application, institutions should only assign LA application access to the LSA and LSA back-up.

The LSA duties are inconsistent with any role in the daily operations of the FedLine application. To ensure the ability to restrict and monitor FedLine activity, any staff member assigned access to the LA application, which allows entry and update capabilities, should not have access to either the FT or Host Communications (HC) applications. Even with this restriction in place, an unauthorized funds transfer message could be created and transmitted if personnel with the LA application, "Entry/Update" access level, have unmonitored access to the FedLine PC and Federal Reserve Bank host computer access. It is essential that the financial institution carefully evaluate assigned access levels and monitor physical access to the FedLine PC. The designated LSA, back-up LSA, and any other staff assigned the LA application with "Entry/Update" access level should not have a role in the daily operation of any FedLine business applications, particularly the FT application.[6]

FEDLINE PRINTER LOG

The financial institution should have the appropriate procedures for controlling and reviewing the FedLine printer log (Printer Recap Report), which automatically logs *all* FedLine activity to an attached dedicated printer. Failure to maintain and adhere to such procedures allows potentially unauthorized and fraudulent activity to occur undetected for extended business periods.

[6] Refer to *Appendices E and F*, "FedLine Access Levels for the Funds Transfer (FT) Application" and "FedLine Access Levels for the Local Administration (LA) Application".

The printer log, designed for continuous feed paper, should not exhibit unexplained breaks, and should be reviewed periodically, and at each cycle/date rollover, by staff other than the LSA to confirm only authorized LSA and FT activity has taken place. The recommended retention period for the FedLine PC printer log is five (5) years. The log can serve as an invaluable resource for reviewing changes made to the FedLine environment.

FEDLINE PATCH MANAGEMENT

Failure to maintain the FedLine computer at current software release levels or to apply all patches and program changes issued by the Federal Reserve Banks potentially exposes the financial institution to processing errors due to noncompliance with program updates reflecting Federal Reserve and clearinghouse processing and format changes.

The LSA should establish the appropriate procedures to maintain the FedLine PC at current release levels, and to ensure the implementation of Federal Reserve-supplied patches and authorized program changes as required. The "Browse Patch Status" (refer to the "Examination Procedures", Appendix A, Objective 2, Work Step 8) provides a history of all upgrades performed on the FedLine PC. In addition to ensuring the application of appropriate patches and maintenance upgrades, it is also important to ensure the back-up and implementation of all patches and upgrades to FedLine PCs used at any alternate processing sites.

LOGICAL ACCESS CONTROLS

The logical access controls described in this section focus on preventing inappropriately assigned access levels within the FT application to staff working in the wire room or funds transfer operation. Inappropriately assigned access levels provide the opportunity to transmit unauthorized funds transfer messages. This risk is greater if message verification is not appropriately set to ensure adequate separation of staff duties between those initiating and those responsible for verifying and sending funds transfer messages. Staff, whether or not assigned to the wire room, may also have inappropriately assigned access levels within the LA application that could allow them unauthorized access to the FT application. This control deficiency could enable the creation and transmission of unauthorized funds transfer messages.

Each staff member should only have one local user ID assigned. Staff with more than one local user ID could bypass established verification requirements by using the first ID to enter funds transfer messages and using the second ID to perform verification and transmission.

FEDLINE ACCESS LEVELS

Appropriately assigned FT and HC application access levels support effective separation of duties and should be designed to prevent the sending of unauthorized funds transfer messages. Access assigned to staff responsible for the financial institution's wire room or funds transfer operation should be based on a "least privilege" basis, reinforcing the concept of only authorizing the level of access needed to perform a particular job function. The institution should require staff independent of the wire room or funds transfer operations to periodically review and evaluate the assigned FT access levels.

Staff assigned to the FT application are responsible for creating and updating funds transfer messages and normally require the "Entry/Update" access level. Staff responsible for transmitting authorized funds transfer messages normally require the "Verify/Transmit" access level. Some staff members will also require access to the HC application, and should be assigned the appropriate HC application "Entry/Update" or "Verify/Transmit" access levels depending upon their responsibilities. In addition, message verification should be set to ensure an adequate separation of duties between staff initiating funds transfer messages and those responsible for verifying and sending funds transfer messages.

Staff assigned the "Entry/Update" and "Verify/Transmit" access levels within the FT application should not also be assigned the FT "Supervisor" or "Managerial" access levels. The FT application "Supervisor" and "Managerial" access levels permit the user to bypass the verification requirement, and should only be activated by the LSA in response to unique processing situations. If activated, the LSA should monitor the actions performed by FT staff assigned these access levels and deactivate them when processing is complete. While the "Supervisor" access level is needed to perform required functions in other FedLine applications such as "Startup/Shutdown Control," it is not normally needed for the FT application.

HOST COMPUTER ACCESS

Having "Entry/Update" and "Verify/Transmit" access to the HC application is not sufficient by itself to allow for the transmission of authorized funds transfer messages to the Federal Reserve Bank's host computer. To transmit authorized FT messages the individual must also possess a valid Federal Reserve Bank host user code and password permitting the transmission of funds transfer messages to the host Fedwire funds transfer application. The LSA, working with the respective Federal Reserve Bank, is responsible for establishing staff host user codes and passwords. The LSA is also responsible for ensuring ongoing host access is needed, and host user codes no longer required are de-activated or deleted. The LSA should maintain an accurate "Host User Code" list defining active staff host user codes, and financial institution management should be able to certify the accuracy of the list if requested by examination staff on-site (refer to the "Examination Procedures", Appendix A, Objective 2, Work Step 9).

FEDLINE ACCESS REPORTS

The "User-ID Status" and "User/Access" reports (refer to the "Examination Procedures", Appendix A, Objective 2, Work Steps 4 and 5) should be used to verify the logical access controls granted to staff assigned to the wire room or funds transfer operation. Examiners should verify that staff members using FedLine on a daily basis do not have the LA application listed under their local user ID on the "User/Access" report. The "**" on the listing indicates access has been granted to all applications listed on the menu, *except for the LA application*. If a staff member has access to the LA application, it will be listed specifically on the "User/Access" report, and should be questioned as to the need for this level of access.

In addition, examiners should review the FedLine "Users Guide" that should be made available to examiners on-site for more detailed information on available reports and screen snapshots that will assist in verifying assigned access levels.

PROCEDURAL CONTROLS

The procedural controls described in this section focus on the financial institution policies and procedures used to process funds transfers. These procedures may not provide the appropriate level of control and supporting documentation for the movement of funds into or out of customer and institution accounts. Inadequate policies and procedures used to prepare funds transfer source documents, verify debit and credit transactions affecting customer and institution accounts, noncompliance with the Office of Foreign Asset Control (OFAC) verification procedures, and lack of independent funds transfer processing and balancing functions, create the potential for fraudulent funds transfer activity.

FUNDS TRANSFER POLICIES AND PROCEDURES

Financial institutions should have funds transfer policies and procedures addressing both the processing of funds transfer messages within the wire room and the related standards for creating and maintaining source documents for the movement of funds into and out of customer and institution accounts. Policies and procedures should include documentation describing all interfaces between the FedLine FT application and other backroom and customer-related banking processes, and should address the controls relating to crediting, debiting, and reconciling customer and institution account balances.[7] Policies and procedures should also document institution specific compliance requirements to address federal and state regulations including OFAC verification procedures.

[7] Financial institutions may rely on third-party software products that include a funds transfer module. Depending on the use of such third-party funds transfer products, an evaluation of these products may be warranted when reviewing the FedLine environment and FT application.

INFORMATION SECURITY PROGRAM

The financial institution's information security program should include an effective risk assessment methodology supporting an evaluation of the risks relating to performing high-risk activities such as funds transfer and other payment-related activities. Risk assessments based on a periodic review of high-risk activities such as funds transfer should be used to develop effective standards for adequate separation of duties, physical security, and logical access controls based on the concept of "least privilege".

INTERNAL AND EXTERNAL AUDIT

Periodic independent reviews of the funds transfer operation, including all pertinent internal policies and procedures, should be conducted by the financial institution's internal auditors, or included as a part of the external audit. Financial institution audits should verify the effectiveness of the funds transfer control environment and identify funds transfer deficiencies for correction.

BUSINESS CONTINUITY PLANNING

The inability to restore funds transfer services in a timely manner can expose a financial institution to increased operational (transaction), liquidity, or credit risks resulting from the lack of system availability. Typically, funds transfer operations are critically important in managing the financial institution's assets. Unscheduled system outages can reduce the institution's ability to manage its operations effectively and could adversely affect the institution's customers and counter-parties. Failure to prepare and test business continuity plans capable of restoring funds transfer service to levels commensurate with the financial institution's business requirements can result in significant risk to the institution.

An institution's business continuity plan should document the ability to restore wire transfer operations and quickly recover any potentially lost funds transfer transactions in the event of a system outage. In most emergencies, the institution can initiate off-line funds transfer message transactions by contacting the local Federal Reserve Bank office via telephone. Generally, this contingency arrangement is sufficient if the institution does not generate large funds transfer message volumes. If a disaster or other type of emergency is declared, and the off-line funds transfer procedure is invoked, authorized funds transfer operations staff will require access to specific encryption code words needed to complete the off-line funds transfer process.[8]

[8] Refer to Federal Reserve Operating Circular No. 6, Appendix A-1, "Funds Transfer Security Procedures, Section 3.0, Off-line Security Procedure."

For financial institutions generating larger funds transfer volumes, back-up FedLine PCs should be included at the institution's back-up business and information processing facility, and tested periodically to ensure connectivity with the Federal Reserve.

The institution should also have business continuity plans in place for equipment failure (e.g., encryption device, modem, or PC failure). These plans should include establishing an inventory of spare encryption boards, modems, and other hardware components. The institution can also contact its Federal Reserve Bank to arrange for next-day shipment of replacement hardware and software components.

Business continuity plans should include creating a back-up copy of the current FedLine configuration diskette. The back-up diskette should be stored in a secure off-site location along with the encryption material, PC power-on password, and master ID. Additionally, the institution should periodically make a static file back-up of the FedLine applications ("Back-Up Static Files" function in the "Miscellaneous Support" application) that includes customized financial institution-specific information (e.g., frequent ABA numbers, user IDs, and recurring funds transfer-related information).

RECOMMENDED SECURITY SETTINGS

Action Summary

Financial institutions should evaluate the recommended FedLine PC and FT application security settings described in this section. The recommended settings should be used as a guide to assess the financial institution's overall control environment. Where there are differences, the examiner should determine whether they are the result of oversight or chosen due to alternate mitigating controls designed to meet the institution's particular operating environment and capabilities. Although the recommended settings support the implementation of separation of duties and logical access controls needed to reduce the potential transmission of unauthorized funds transfer messages, *each institution must carefully assess its environment and applicability of the settings*.

Note: Management should institute change control procedures to ensure institution security settings are restored to approved levels should the FedLine PC hardware or software components be updated or otherwise altered due to malfunction or routine maintenance.

MISCELLANEOUS SECURITY SETTINGS

The LA application, "Entry/Update" function screen 99, allows the LSA to establish the following local administration access options applicable to all FedLine applications, including the FT application.

USER ID SUSPENDED AFTER XX CONSECUTIVE BAD PASSWORD RETRIES

This setting specifies the maximum number of consecutive invalid sign-on attempts before the local user ID is suspended. This prevents an unauthorized person from trying to guess the password of a legitimate user by limiting the number of invalid password attempts.

The recommended setting is "3".

USER MUST CHANGE PASSWORD EVERY XX DAYS

This setting specifies the maximum number of days that operators can use their password before they must change it.

The recommended setting is "30".

VERIFICATION RULE

This rule sets the message verification requirement. This rule can prevent the origination of unauthorized, and potentially fraudulent, messages by requiring more than one person's involvement the generation of funds transfer messages. The following options are available:

- *N – No restriction (Very high risk)* – This option allows the operator entering or updating a message to also verify the same message. There is no dual control for funds transfers if this option is chosen.
- *U – Verifying operator cannot be the last operator who updated the transfer*. This option prevents the last operator who entered or updated a transfer from verifying that same message. It would allow the original operator to verify the transfer if it was changed by a second operator.
- *E – Verifying operator cannot be operator who entered or updated the transfer*. This option prevents any operator who entered or updated a transfer from verifying that same transfer.

Note: Settings "E" and "U" will only apply if the "Verify Thresholds" parameter is appropriately set to $0.00 (or threshold amount approved by the Board of Directors and noted in the minutes) for both accountable and non-accountable messages (see "Verify Thresholds under Update Funds Application Attributes"). This rule will affect all message types requiring verification including funds transfers, large dollar check returns, and Treasury, Tax, and Loan (TT&L) transactions.

The recommended setting is "E," however "U" is acceptable.

OVERRIDE AND RELEASE RULE

This field indicates the level of restrictions placed on overriding or releasing transfers. This potentially allows users to bypass verification. Only operators with the "Supervisory access" level have the ability to perform the "Override" function. The following options are available:

- *N – No restriction on "Override" or "Release"* – Any operator with the supervisor function access level can override or release the verification of a transfer regardless of any previous processing

performed with the exception of messages that have a status of "Queued for Transmission (TQ)" or "Marked for Correction (MC)."

- *U – Limited restriction on "Override" or "Release"* – The operator overriding or releasing the transfer cannot be the operator who last updated the message.
- *E – Full restriction* – The operator overriding or releasing the transfer cannot be the operator who entered or updated the message.

The recommended setting is "E," however "U" is acceptable.

USER ID WILL BE SIGNED OFF AFTER XXX MINUTES OF INACTIVITY

This timeout parameter minimizes the amount of time a terminal remains active if a user forgets to signoff. It causes the system to revert to the FedLine sign-on screen after a specified amount of time during which no keystrokes have been entered at the PC (can be set between 0 – 999 minutes of inactivity).

The recommended setting is "10" minutes.

SUPPRESS THE CHECK FOR POSSIBLE KEYBOARD EAVESDROPPING

This feature allows the FedLine PC to detect whether another application program is operating in memory simultaneously with the FedLine software. If another program is detected, the FedLine PC will issue a warning message that another program has been detected and will suspend operation. The following options are available:

- *No* – Not suppress monitoring for possible keyboard eavesdropping.
- *Yes* – Suppress monitoring for possible keyboard eavesdropping.

The recommended setting is the default value "No."

CYCLE-DATE ROLLOVER'S PRINT-DELETE OPTION

The cycle-date rollover process automatically deletes all unsent messages that were queued for transmission since the last cycle-date rollover. Prior to their deletion from the FedLine PC, each message is listed in the cycle-date rollover report. The user may choose from two report options.

- *Full* – The complete details and unabbreviated content of all unsent messages are included in the cycle-date rollover report.

- *Summary* – The details and content of each unsent message are condensed into a single line summary and listed in the cycle-date rollover report. In the event that full message details are subsequently needed, it would then be necessary for the FedLine operator to revert back to the paper audit report produced at the time of the transaction.

The recommended setting is the default value "Full."

UPDATE FUNDS APPLICATION ATTRIBUTES

The FT application," Managerial" function screen 96, allows the LSA or staff assigned the FT "Managerial" access level to update the funds transfer application attribute parameters for verification thresholds, duplication of reference fields, and holding accountable messages from transmission.

VERIFY THRESHOLDS

The "Verify Thresholds" field sets the specific dollar amount threshold requiring verification for all outgoing accountable and non-accountable funds transfer messages. Accountable funds transfer messages are payment orders with an "Input Message Accountability Data (IMAD)" key assigned at the time staff verifies them and queues them for transmission (TQ status). Non-accountable funds transfer messages are administrative in nature rather than payment orders. These messages are service messages that typically do not contain funds transfer dollar amounts. However, non-accountable messages may contain instructions modifying or correcting prior messages designated accountable, including modifying dollar amounts, routing, and account numbers.

Verification refers to designated fields that must be re-keyed by a second operator. If the institution should decide to set the verification level at any amount greater than $0.00, the board of directors should approve the amount and not their approval in the board minutes. An amount of $99,999,999,999.99 in the "Accountable" and "Non-Accountable" threshold fields indicate that there is no requirement for verification by a second operator.

Note: The "Verification Threshold" settings for accountable and non-accountable messages cannot be blank. The system requires a numeric value or it displays an error message.

The recommended verification threshold setting is $0.00 for both accountable and non-accountable messages, requiring the verification of **all** funds transfer messages by a second operator.

OK TO DUPLICATE A REFERENCE FIELD

The "OK to Duplicate a Reference" field allows the system to automatically check for reference numbers. The reference field can be used to cross-reference FT messages to their corresponding source documents when initially entered or updated. Depending on the setting selected, this edit check can prevent the creation of duplicate transfer records from the same source document. The following options are available:

- *N* – Not okay to duplicate a reference field (check for duplicate reference numbers).
- *Y* – OK to duplicate a reference field.

The recommended setting is the default value "N."

AUTOMATICALLY HOLD ALL ACCOUNTABLE MESSAGES FROM TRANSMISSION

The "Hold Accountable Messages" field provides an enhanced control option, typically only used for an emergency or contingency situation, which the LSA sets to automatically hold all accountable funds transfer messages from transmission (including those with verified status). During normal operations, verified accountable messages should be sent to the Federal Reserve Bank host computer automatically for processing. Holding all accountable messages may create a backlog of valid funds transfer messages until released by authorized staff. Depending on the volume of funds transfer activity, automatically holding all verified accountable messages may not be operationally feasible and should only be used after carefully considering the potential effect on operations. Staff members assigned "Supervisor" access level within the FT application are authorized to invoke the "Message Status Override" function to release the held messages. The following options are available:

- *No* – Do not hold accountable messages. Messages are automatically queued for transmission.
- *Yes* – Hold accountable messages, requiring staff with "Supervisor" access level within the FT application to perform the message status override function to release messages for transmission.

The recommended setting is the default value "No."

UPDATE VERIFY FIELDS

The FT application, "Managerial" function screen 93, allows the LSA or staff assigned the FT "Managerial" access level to update the verification fields applicable for the FT application.

VERIFICATION FIELDS

The LSA, or other staff assigned FT managerial access designates specific funds transfer message fields that require verification by a second operator, by placing an "x" in each field requiring verification. Verification can range from requiring verification for all fields to not requiring verification of any field. If the fields do not have an "x," the second operator does not have to re-key any information, however a second operator would still have to provide sight verification before releasing for transmission to the Federal Reserve Bank.

The recommended verification fields setting should be verification of the dollar amount field, at a minimum. However, the financial institution can strengthen dual control with each additional field requiring verification so it should also consider requiring the verification of account number, routing number, etc.

APPENDIX A: EXAMINATION PROCEDURES

The FedLine "Examination Procedures" are used to determine the adequacy and effectiveness of the logical, physical, administrative, and procedural controls, as well as business continuity planning, over the institution's implementation of FedLine and use of the FT application. The procedures evaluate the effectiveness of the financial institution's FedLine funds transfer internal controls environment and the related risk management processes.

The analysis for determining the examination procedures and testing to be performed should be based on the examiner's assessment of the risks and risk management practices relating to the financial institution's use of the FedLine FT to support its funds transfer activity, including transaction volume, and individual transaction dollar amounts. This assessment should include consideration of formal policies and procedures established to provide funds transfer services, as well as an assessment of the effectiveness of the financial institution's underlying internal control environment including information security and business continuity.

A financial institution is exposed to significant operational (transaction), credit, and liquidity risks when processing funds transfers on behalf of its internal activities and in providing this service to its customers. Depending on the complexity of the funds transfer activity, the financial risks, operational (transactional) risks, and compliance risks may require an integrated team approach that includes the knowledge and skills of safety and soundness examiners, IT examiners, and compliance specialists. Refer to the *IT Handbook's* "Information Security Booklet" and "Business Continuity Planning Booklet" for additional information regarding examination procedures that focus more specifically on security and business continuity planning.

Examiners can incorporate the procedures in either an IT or safety and soundness examination targeting the FedLine application in the scope. The procedures need not be used in their entirety and all of the work steps need not be performed. However, the examiner should perform sufficient procedures to arrive at a conclusion regarding the quality of risk management practices governing the funds transfer function.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the scope and objectives of the examination of the FedLine FT application. Examiners need not perform every examination procedure or include every objective in developing the examination strategy.

1. Review past documents for comments relating to the FedLine FT application. Consider:

   - Regulatory reports of examination.
   - Internal and external audit reports.
   - Supervisory strategy documents, including risk assessments.
   - Examination work papers.
   - Correspondence.

   While reviewing this documentation, consider the implication of the findings for the institution's internal control environment as it relates to FedLine FT. More specifically, assess:

   - Internal controls including logical access, data center, and physical security controls.
   - Compliance with Federal Reserve System Operating Circulars, Nos. 5 and 6.

2. Obtain an inventory of any computer hardware, software, and telecommunications protocols used to support the wire room or funds transfer operation in addition to the FedLine PC.

3. Identify during discussions with financial institution management:

   - A thorough description of the funds transfer activity performed in-house, including activity volumes by dollar and number of transactions and the scope and complexity of operations.
   - A thorough description of any outsourced funds transfer-related services, including the use of third-party software products that generate funds transfer messages in addition to FedLine. Determine the financial institution's level of reliance on these services.

- Any significant changes in the funds transfer operation since the last examination, particularly the introduction of any new funds transfer services.

- A description of all reports and logs used by management to verify appropriate staff access to the FT application.

4. Review the financial institution's response to any funds transfer issues raised at the last examination. Consider:

   - Adequacy and timing of corrective action.

   - Resolution of root causes rather than specific issues.

   - Existence of outstanding issues.

Objective 2: Obtain information needed for the examination using FedLine reports and screen prints.

1. Obtain the financial institution's FedLine user documentation, including the FedLine "Users Guide" and "Local Security Administrator Guide," for more detailed information on security settings and controls.

2. Obtain the financial institution's FedLine PC printer log (Printer Recap Report) for a one-week time period in advance of the on-site examination.

3. Obtain a screen print of the "Miscellaneous Security Settings" screen (option #99, LA "Entry/Update" access level).

4. Obtain a "User-ID Status Report" (option #60, LA "Inquiry" access level, type ALL to get all users).

5. Obtain a "User/Access Report" (option #65, LA "Inquiry" access level, press ENTER key for all users).

6. Obtain a screen print of the "Update Funds Application Attributes – Funds Transfers" screen (option #96, FT "Managerial" access level).

7. Obtain a screen print of the "Update Verify Fields – Funds Transfers" screen (option #93, FT "Managerial" access level).

8. Obtain a screen print of the "Browse Patch Status" screen (option #80, "HD Non-Restricted" access level).

9. Obtain the active staff "Host User Code" list from the LSA (the LSA should certify the accuracy of the list).

Objective 3: Determine the level of physical security surrounding the financial institutions' wire room, or work area designated for the operation of the FedLine PC.

1. Verify whether there is a designated work area supporting the prevention of unauthorized staff and customer access, including the use of a locked room, locked cabinet or PC enclosure, or similar measure restricting access to authorized staff only. Note: Financial institutions may also consider placing the PC in an open staff area during normal business hours if it can be demonstrated that appropriate mitigating controls exist.

2. Verify whether the FedLine software and other critical information necessary to maintain funds transfer operations in the event of an equipment failure, outage, or declared disaster is appropriately controlled, including securing the following material, under lock and key restricting access to authorized staff only on a need-to-know basis:

    - *Configuration Diskette* – Used in conjunction with the local Federal Reserve Bank office.
    - *Encryption Material* – Refers to information pertaining to the encryption implementation and Federal Reserve Bank supplied encryption keys. FedLine encryption keys are unique to each FedLine PC.
    - *PC Power-On Password* – Requires the use of a password before the FedLine PC will activate.
    - *Master Local User ID (Master ID) and Password* – The master ID and password shipped with FedLine.

Objective 4: Evaluate the control environment and security settings for the FedLine PC and the FT application.

1. Verify that the miscellaneous security settings are set correctly (refer to Objective 2.3), including:

    - User ID suspended after "3" or less tries.
    - User must change password every "30" days or less.
    - Verification rule set to "E" or "U."

- Override and release rule set to "E" or "U."
- Timeout interval set to "10" minutes or less.
- Suppress the Check for Possible Keyboard Eavesdropping set to "N."
- "Cycle/Date Rollover's Print Delete Option" set to "Full."

2. Review the User ID Status Report and Host User Code list (refer to Objectives 2.4 and 2.9), and:

    - Verify staff not assigned more than one user ID per individual.
    - Verify the accuracy of the status report when compared to staff currently assigned access to the FT application.
    - Verify staff assigned host user codes require host access, and confirm access to the HC application is appropriate.

3. Review the User/Access Report (refer to Objective 2.5), and:

    - Verify staff members assigned LA application access are not assigned FT application access.
    - Determine, when more than two staff members are assigned to the LSA role, if the institution has the appropriate documentation justifying this approach.
    - Determine if any funds transfer operations staff is not assigned FT application Supervisor or Managerial access.
    - Determine if there is adequate separation of duties for funds transfer operations staff members assigned FT application access.

4. Review the "Update Funds Application Attributes – Funds Transfer" screen (refer to Objective 2.6):

    - Verify "Accountable Threshold" set to 0.00 (if greater than 0.00, verify this amount has been approved by the board of directors and noted in the board minutes).
    - Verify "OK to Duplicate a Reference Field" is set to "N" (if set to "Y," review the financial institution's procedure for avoiding entering duplicate reference number information).

- Verify "Automatically Hold All Accountable Messages From Transmission" is set to "N" (if set to "Y," evaluate the financial institution's ability to process funds transfer messages in a timely manner).

5. Review the "Update Verify Fields - Funds Transfer" screen (refer to Objective 2.7):

   - Verify that an "X" is entered for the dollar amount field.

   - Determine through discussion or review of written policies whether the financial institution requires other fields to be verified by reviewing for an "X" is entered for these fields.

6. Verify that the "Master User ID" password has been changed from the original password, re-established under dual-control, and stored in a sealed envelope in a secure location in case the LSA or back-up is not available.

7. Verify that the FedLine configuration diskette is stored in a secure location and available only to the LSA.

8. Verify "Encryption Material" is stored in a secure location, and is accessible to only the LSA and LSA back-up designee.

9. Determine whether the FedLine PC has a power-on password option. If it does, verify that it is activated and is not given to staff assigned the LA access level without a legitimate need to know. If it does not, evaluate the institution's ability to control staff members assigned the LA access level access to the FedLine PC, including monitoring the FedLine PC during business hours, and physically securing the FedLine PC after business hours.

10. Review the help desk (HD) application's "Browse Patch Status", refer to Objective 2.8, and determine whether the FedLine PC is maintained at current release levels and that all Federal Reserve supplied patches and authorized program changes are applied as required.

Objective 5: Evaluate financial institution procedural controls for both the processing of funds transfer messages within the wire room or funds transfer operation and related standards for the movement of funds into and out of specific customer and institution accounts.

1. Evaluate the policies, procedures, and supporting documentation describing interfaces between the FedLine FT application and other internal banking processes, including:

- Adequacy of procedures for generating and storing source documents used to process funds transfers, including the appropriate documentation, reference/control numbers, and authorizations.

- Adequacy of procedures for reconciling completed funds transfer transactions with customer and institution accounts.

- Compliance with regulatory requirements, including OFAC verification procedures.

- Adequacy of procedures for using third-party funds transfer software products, if applicable, in conjunction with FedLine, including source document preparation, authorization, reconcilement, and record retention.

2. Evaluate the financial institution's information security program, including:

   - Documented separation of duties principles, particularly for high-risk areas.

   - Defined physical security and logical access control standards, including specific controls for high-risk business activities such as funds transfer.

   - Defined risk assessment methodology, including assessing high-risk activities such as funds transfer and other payment-related functions.

3. Evaluate whether the financial institution's internal and external auditors:

   - Periodically perform independent assessments of the wire room or funds transfer operation, including evaluating internal policies and procedures.

   - Verify the effectiveness of the wire room or funds transfer operation control environment and business continuity preparedness.

4. Evaluate whether the financial institution's policies and procedures for the FedLine printer log (Printer Recap Report) include:

   - Adequate procedures to ensure the integrity of the printer log, including appropriate approvals for any breaks in the log printer paper.

   - Adequate procedures for an independent periodic management review (not by the LSA or back-up) of the printer log, including the cycle/date rollover and any changes to assigned access levels, security settings, and the addition or deletion of FedLine users.

   - A five (5) year printer log retention policy.

Objective 6: *Evaluate the effectiveness of the institution's business continuity planning and disaster recovery capability relating to funds transfer operations.*

1. Evaluate the institution's ability to send and receive funds transfers in the event of an equipment failure.

2. Evaluate the institution's methodology for sending and receiving transfers if required to operate from a different location, including availability of back-up FedLine PCs.

3. Evaluate the institution's testing of business continuity plans related to the wire room or funds transfer operation.

4. Determine whether the institution keeps a back-up copy of the encryption material, PC power-on password, and master ID and password stored off site at a secure location. Evaluate whether staff access to these materials is on a need to know basis.

5. Determine whether the institution has established an inventory of spare encryption boards, modems, and other PC-related hardware. Evaluate whether these components are stored securely off site and readily available in the event of a device failure.

6. Determine whether the institution keeps a back-up copy of the most current version of the FedLine software on diskette and stored off site at a secure location. Review whether these back-ups include FedLine software patches as they are issued.

7. Determine whether the institution periodically generates a static file back-up of all FedLine financial institution-specific information and stores it off site at a secure location (Note: static file back-ups should be performed for all FedLine PCs and stored off site).

CONCLUSIONS

Objective 7: Discuss corrective action and communicate findings.

1. From the procedures performed:

   - Document conclusions related to the quality and effectiveness of the security controls and business continuity planning relating to the wire room or funds transfer operation and FedLine FT application.

   - Determine and document to what extent, if any, the examiner may rely upon funds transfer review procedures performed by internal or external audit.

2. Review your preliminary conclusions with the EIC regarding:

- Violations of law, rulings, regulations, and third-party agreements.
- Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination.
- Potential impact of your conclusions on composite and component URSIT ratings.

3. Discuss your findings with management and obtain proposed corrective action, including time frames for correction, for significant deficiencies.

4. Document your conclusions in a memo to the EIC that provides report-ready comments for all relevant sections of the FFIEC Report of Examination and guidance to future examiners.

5. Organize work papers to ensure clear support for significant findings and conclusions.

APPENDIX B: GLOSSARY

Authentication	The process of verifying the claimed identity of an individual user, machine, software component, or any other entity.
Clearance	The process of transmitting, reconciling, and in some cases, confirming payment orders or financial instrument transfer instructions prior to settlement.
Encryption	A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key. Refer to the *IT Handbook's* "Information Security Booklet" for more information.
Federal Reserve Banks	The Federal Reserve Banks provide a variety of financial services, including funds transfer, book-entry securities, ACH, and clearing and settling checks drawn on depository institutions located in all regions of the United States.
FedLine	FedLine is the Federal Reserve Bank's proprietary electronic platform providing a common electronic delivery channel for financial institution access to Federal Reserve financial services including Fedwire funds transfer.
Fedwire	The Federal Reserve System's nationwide real-time gross settlement electronic funds and securities transfer network. Fedwire is a credit transfer system, and each funds transfer is settled individually against an institution's reserve or clearing account on the books of the Federal Reserve as it is processed and is considered a final and irrevocable payment.
Finality	Irrevocable and unconditional transfer of payment during settlement.
OFAC	The Office of Foreign Assets Control (OFAC), within the U.S. Department of the Treasury, administers and enforces economic and trade sanctions against targeted foreign countries, terrorism-sponsoring organizations, and international narcotics traffickers based on U.S. foreign policy and national security goals.
Payment	A transfer of value.

Reserve Account	A noninterest earning balance that depository institutions maintain with the Federal Reserve Bank or with a correspondent bank to satisfy the Federal Reserve's reserve requirements. Reserve account balances play a central role in the exchange of funds between depository institutions.
Reserve Requirements	The percentage of deposits that a financial institution may not lend out or invest and must hold either as vault cash or on deposit at a Federal Reserve Bank. Reserve requirements affect the potential of the banking system to create transaction deposits.
Settlement	The final step in the transfer of ownership involving the physical exchange of securities or payment. In a banking transaction, settlement is the process of recording the debit and credit positions of the parties involved in a transfer of funds. In a financial instrument transaction, settlement includes both the transfer of securities by the seller and the payment by the buyer. Settlements can be "gross" or "net." Gross settlement means each transaction is settled individually. Net settlement means that parties exchanging payments will offset mutual obligations to deliver identical items (e.g., dollars and EUROs), at a specified time, after which only one net amount of each item is exchanged.

APPENDIX C: LAWS, REGULATIONS, AND GUIDANCE

LAWS

- 12 USC 248 (i), (j), and (o), 342, 360, 464, and 4001-4010: Federal Reserve Act

FEDERAL RESERVE BOARD

REGULATIONS

- 12 CFR Part 210, Subpart B, Funds Transfer Through Fedwire (Regulation J)

APPENDIX D: FEDLINE APPLICATIONS AND CODES

Code	FedLine Application
**	All Applications
AA	Automated Auction
AH	Automated Clearing House
AS	Accounting Services
BA	Book-Entry Securities
CA	Check Adjustments
CH	Check Services
FT	Funds Transfers
HC	Host Communications
HD	Help Desk
LA	Local Administration
MS	Miscellaneous Support
RA	Local Reserve Account
RR	Reporting and Reserves
SB	Savings Bonds
SS	Startup/Shutdown Control
TI	Treasury Investment Program
TT	Treasury Tax and Loan

APPENDIX E: FEDLINE ACCESS LEVELS FOR THE FUNDS TRANSFER APPLICATION

Inquiry access level grants access to the following functions:

- Activity status report.
- Browse incoming message.
- Browse outgoing message.
- Local terminal totals.
- View and print recurring templates.
- Reprint FT incoming and outgoing wires.
- View recurring templates.

Entry/Update access level grants access to the following functions:

- Create a message – Enter a transfer.
- Derive a reversal – Reverse a previously received transfer.
- Export a message file – Copy selected funds transfers onto diskette.
- Import a message file – Copy funds transfers created using another processing system into FedLine.
- Update a message – Change detail information in a transfer.

Verify/Transmit access level grants access to the following functions:

- Group release – Change status of a group of transactions for immediate release.
- Release transfers for transmit – Change status of transfer marked "held" to release.
- Verify a message – Verify a previously entered transfer.

Assistant Supervisory access level grants access to the following functions:

- Add recurring template – Create new template.
- Delete recurring template – Delete template.
- Update recurring template – Modify template.

Supervisor access level grants access to the following functions:

- Group override – Change status of a group of messages held from transmission.
- Message status override – Allows the status of a transfer to be changed (bypasses verification).
- Modify screen defaults – Allows modification of default data of the create screens which are automatically inserted whenever you create a message.
- Re-send message – Allows re-sending of a previously transmitted message that may have been lost by the receiver or rejected by the host.

Managerial access level grants access to the following functions:

- Resynchronize host – Re-sequence transfer ID application sequence numbers on host mainframe.
- Update key verify fields – Select fields in transfer fields entry that must be verified.
- Update FT application attributes – Specify dollar amount attributes of outgoing transfers that require verification.

APPENDIX F: FEDLINE ACCESS LEVELS FOR THE LOCAL ADMINISTRATION APPLICATION

Nonrestricted access level grants access to the following functions:

- Change Patch Date.
- Export a Patch.
- Implement a Patch.

Inquiry access level grants access to the following functions:

- Application/Function Report.
- Browse a User Profile.
- Display Session Parameters.
- Display Terminal Parameters.
- User-ID Status Report.
- User/Access Report.

Entry/Update access level grants access to the following functions:

- Add a User Profile.
- Back Off A Patch.
- Delete a User Profile.
- Miscellaneous Security Settings.
- Set FedLine Site Identifier.
- Set Session Parameters.
- Set Terminal Parameters.
- Update a User Profile.
- Update Application Attributes.

Supervisor access level grants access to the following functions:

- Crypto Key Maintenance.
- Install an Application.
- Remove an Application.
- Select Default Applications.

Managerial access level grants access to the following functions:

- Import a Patch.