Electronic Funds Transfer Risk Assessment

Examiners should evaluate the above-captioned function against the following control and performance standards. The Standards represent control and performance objectives that should be implemented to help ensure the bank operates in a safe and sound manner, and that the entity's objectives are carried out. Associated Risks represent potential threats to the bank if the standards are not achieved and maintained. The Standards are intended to assist examiners in analyzing important functions that may warrant additional review. All of the following Standards may NOT need to be considered at every bank. Conversely, these do NOT represent all of the control and performance standards needed for every bank. Examiners should continue to use their judgement when assessing risk.

Standards	Associated Risks
MANAGEMENT AND CONTROL	
Written policies and procedures are in place that address personnel, physical security, data security, operations, credit risk, and disaster recovery.	The risk of fraud increases if policies and procedures are not established. Unauthorized loans may result if transfers are completed with provisional (uncollected) funds. The bank may exceed its legal lending limit. The possibility of fraudulent transfers and losses increases due to errors or omissions.
Auditors review the funds transfer function and report findings to the directorate.	Board may not be informed of risks in the funds transfer area.
Management provides for adequate controls including segregation of duties, dual control, and accounting.	Unauthorized transfers may occur.
The bank maintains adequate fidelity and business insurance for funds transfer activities.	Bank may incur substantial losses due to errors, omissions, or fraud. Settlement losses will impact liquidity and capital if there is inadequate insurance coverage.
Adequate contingency and disaster plans exist.	Funds transfers may be disrupted or incomplete. Security and confidentiality may be breached.
PERFORMANCE	
Management and bank personnel adhere to written policies and procedures.	Risk of fraud, errors, and omissions increases if employees do not adhere to policies and procedures. Credit risk may increase if overdrafts are allowed and not controlled. Board approved objectives and controls may not be met.
Management evaluates and controls settlement risks (if using a system other than Fedline).	Payments received through the Clearing House Interbank Payment System (CHIPS) are provisional, and credit exposure exists if funds are released prior to settlement. If one participant fails to settle, it could disrupt the settlement for other participants. As a result, the

Standards	Associated Risks
.	system's settlement fails (liquidity risk). One participant's failure to settle could deprive other participants of the funds they need to settle (systemic risk).
Management monitors its payment systems position and limits its credit exposure in the system and from customers and correspondents. Management establishes and monitors reasonable limits for daylight or overnight overdrafts.	Inadequate monitoring of payment systems increases the chance of systemic risk. Excessive volumes of daylight and overnight overdrafts increase credit risk. Officers may exceed established limits.

Electronic Funds Transfer Risk Assessment

Core Analysis Decision Factors

Examiners should evaluate Core Analysis in this section for significance and to determine if an Expanded Analysis is necessary. Negative responses to Core Analysis Decision Factors may not require proceeding to the Expanded Analysis. Conversely, positive responses to Core Analysis Decision factors do not preclude examiners from proceeding to the Expanded Analysis if deemed appropriate.

Do Core Analysis and Decision Factors indicate that risks are appropriately identified, measured, monitored, and controlled?

Core Answer: General Comment:(If any)

Core Analysis Decision Factors

C.1. Are policies, procedures, and risk limits adequate?

C.2. Are internal controls adequate?

C.3. Are the audit or independent review functions adequate?

C.4. Are information and communication systems adequate and accurate?

C.5. Do the board and senior management effectively supervise the electronic funds transfer area?

Lead Regulator: Examination Start Date: 03/09/2001

Electronic Funds Transfer Risk Assessment

Expanded Analysis Decision Factors

This section evaluates the significance and materiality of deficiencies or other specific concerns identified in the Core and Expanded Analyses.

Do Expanded Analysis and Decision Factors indicate that risks are appropriately identified, measured, monitored, and controlled?

Expanded Answer: General Comment:(If any)

Expanded Analysis Decision Factors

E.1. Are deficiencies immaterial to management's supervision of electronic funds transfers?

E.2. Are deficiencies immaterial to the bank's overall condition?

Electronic Funds Transfer Risk Assessment

Consider the following procedures at each examination. Examiners are encouraged to exclude items deemed unnecessary. This procedural analysis does not represent every possible action to be taken during an examination. The references are not intended to be all-inclusive and additional guidance may exist. Many of these procedures will address more than one of the Standards and Associated Risks. For the examination process to be successful, examiners must maintain open communication with bank management and discuss relevant concerns as they arise.

This section is intended to determine the adequacy of Electronic Funds Transfer (EFT) activities of the bank. Although these applications should operate outside the Information System (IS) environment, they are highly dependent on computer operations. The procedures are created so that they may be implemented separately as part of either the IS or safety and soundness examinations. Examiners should refer to Chapters 18 and 19 of the FFIEC IS Examination Handbook for additional guidance.

PRELIMINARY REVIEW

1 Review previous examination reports, earlier work papers, and file correspondence for an overview of previously identified EFT concerns.

2 Review the most recent audits and internal reviews to identify scope and noted deficiencies.

3 Review management's actions to correct examination and audit deficiencies.

4 Discuss with management recent or planned changes in EFT activities.

5 Review management reports to determine the nature and volume of current activity.

6 Review the minutes of management committees that oversee EFT activity. Review for content and follow-up of material matters.

POLICIES AND PROCEDURES

7 Determine if policies and procedures are adequate for the type and volume of funds transfer activities. Determine if formal guidance addresses the following broad areas of concern:

7 A Separation of duties for funds transfer personnel including originating, receiving, testing, and approving functions; authorizing dollar limits; and preparing data entry.

7 B Clearly defined security procedures over payment orders and controls over source documents.

7 C Organizational reporting controls.

7 D System testing.

7 E Maintenance of a physically secure environment.

7 F Personnel hiring and dismissing.

7 G Implementation of a comprehensive disaster recovery program.

7 H Credit standards and overnight and daylight overdrafts limits.

7 I Customer originated activities conducted through electronic banking systems.

INTERNAL CONTROLS

8 Evaluate management's procedures to prevent, detect, and respond to policy exceptions.

Funds Transfer Requests

9 Review the bank's procedures for validating transfer requests, including those received via telex, on-line terminals, telephone, fax, or written instructions. Determine procedures provide for adequate security.

10 Determine if more than signature verification (tests, call backs) are required on written requests.

11 Determine if management maintains a current record of authorized signers for customers who use the bank's funds transfer services. The following items reflect prudent controls:

11 A The record includes authorized sources of funds transfer requests (telephone, memo, fax).

11 B The bank advises its customers to limit the number of authorized signers.

11 C Customer authorization lists limit the amount one individual is authorized to transfer.

12 Ascertain if customer signature records are maintained under dual control or are otherwise protected.

Payment Processing and Accounting

13 Review the daily reconcilements of incoming and outgoing funds transfer activities, including both the dollar amount and number of messages. Determine if appropriate controls are in place, such as:

13 A Independent end-of-day reconcilements for messages sent to and received from intermediaries (Federal Reserve Bank, servicers, correspondents, and clearing facilities).

13 B System activity reconcilements to transfer request source documents.

13 C Daily supervisory review of funds transfer and message reconcilements.

13 D Daily activity balancing is performed separate from the receiving, processing, and sending functions.

13 E Daily reconcilements account for pre-numbered forms.

13 F Federal Reserve Bank, correspondent bank, and clearing house statements used for funds transfers are reconciled and reviewed daily in another area of the bank (accounting or correspondent banking) to ensure they agree with the funds transfer records.

14 Determine that the person reviewing rejects and exceptions is not involved in receiving, preparing, or transmitting funds.

Physical and Data Security

15 Determine if access to funds transfer area or terminal is restricted to authorized personnel.

16 Determine if management implements appropriate controls over funds transfer equipment, such as:

16 A Physical or software locks that prohibit access by unauthorized personnel.

16 B Automatic time-out or time-of-day controls to regulate terminal and other hardware access after normal working hours.

16 C Password suppression on terminal screens.

Credit Evaluation and Approval

17 Review the procedures in place to prohibit transfers of funds against accounts that do not have collected balances or preauthorized credit availability.

18 Determine if daylight or overnight overdrafts are allowed and controlled.

Incoming Funds Transfers

19 Determine if incoming payments not received over a secure system (Fedline), such as book entry transfer requests received via telex or phone, are authenticated prior to processing.

20 Determine if the bank maintains separation of duties over receiving instructions, posting to a customer's account, and mailing customer credit advices.

21 Determine if management maintains audit trails from receipt through posting to a customer's account.

22 Determine if management issues customer advices in a timely manner.

Contingency Plans

23 Determine if management has properly planned for contingencies and review the reasonableness of the plan in relation to the volume of activity. Determine if the contingency plan incorporates appropriate safeguards, including:

23 A A back-up system in the event of equipment failures and line malfunctions.

23 B A method for sending and receiving transfers if forced to operate at a different site.

23 C Procedures to ensure data is recovered by the opening of the next day's processing.

23 D A requirement for supervisory approval for using back-up equipment.

23 E A requirement that the plan be distributed to all funds transfer personnel.

23 F Periodic testing of the back-up systems.

23 G Procedures and controls to prevent the inadvertent release of test data into the production environment.

24 Determine if procedures for backup and off-site storage of critical information and inventory control on hardware and software are in force.

FEDLINE Electronic Funds Transfer

This type of transfer activity will be the most common type of funds transfer in community banks. Although some of the keystrokes are provided as examples, the examiner should not obtain the information identified directly from the terminal. Rather, the examiner should request this information from the bank. Refer to chapter 19 in the FFIEC Information Systems Handbook.

25 Obtain a screen print of the miscellaneous security settings screen (option #99 on Local Administrator (LA) menu). Determine if the miscellaneous security settings are set correctly and if the following controls exist:

25 A User ID is suspended after three or less invalid log on attempts.

25 B User changes his or her password every 30 days or less.

25 C Verification rule is set to E or U.

25 D Override and release rule is set to E or U.

25 E Timeout interval is set to 10 minutes or less.

26 Review a User-ID Status Report (option #60 on LA menu - type "all" to get all users) and a User or Access Report (option #65 on LA menu - press enter key for all users). Determine if the user or access report reflects:

26 A Employees assigned as Local Security Administrators have the proper LA application security set up, and are excluded from funds transfer applications and the host communication function.

26 B No one user has more than one user ID.

26 C No more than two staff members assigned as local security administrators.

26 D Appropriate rotation of the funds transfer supervisor or manager function.

26 E No one other than the local security administrators have the LA application.

27 Review a screen print of the verify fields screens (option #93 on Funds Transfer (FT) menu of manager to determine if the structured, structured draw down, and non-structured screens show an "x" in the amount field.

28 Review a screen print of the verify threshold screen (option #96 on FT menu of manager) to determine if the threshold screen reflects that the threshold is set at 0.00, or
confirm that a threshold greater than 0 is approved by the board and noted in the minutes.

29 Determine if the master user ID password is stored in a sealed envelope in a secure location in case the local security administrators are unavailable.

30 Determine if the Fedline configuration diskette is stored in a secure location and available only to the local security administrators.

31 If the Fedline terminal has a power-on password option, determine if the following controls are in place:

31 A The password is activated.

31 B Password access by the local security administrator is restricted.

32 Determine if the contingency plan contains a requirement for keeping a copy of the current version of the Fedline software available and periodically making a static file backup of the Fedline software.

Wholesale Electronic Funds Transfer Systems (FTS)

(Note: These procedures generally apply to larger banks that initiate large dollar transfers. Refer to Chapter 18 in the FFIEC IS Examination Handbook.)

33 Review flowcharts or narratives of the bank's overall FTS to determine the degree of automated interface, linkage to functions not supported by the FTS, and separation of duties or functions. Review this information as it relates to any of the following systems used by the bank:

33 A Fedline.

33 B CHIPS or other local payments system.

33 C SWIFT (Society for Worldwide Interbank Financial Telecommunications).

33 D Telex.

33 E Internal transfers (book entry).

33 F Customer networks.

33 G Internal networks.

34 Review the adequacy of security procedures in place for both outgoing and incoming payment orders for each step of the FTS process.

34 A Payment order origination such as message testing for fax, telephone, letters, or memos.

34 B Data entry.

34 C Payment order execution or release.

34 D Telecommunication lines.

34 E Physical security.

35 Review a sample of contracts authorizing the bank to make payments from a customer's account.

36 Determine if the contracts and disclosures adequately set forth responsibilities of the bank and the customer, primarily regarding the provisions of UCC Article 4A relating to authenticity and timing of transfer requests.

AUDIT OR INDEPENDENT REVIEW

37 Determine that the audit or independent review program provides sufficient coverage relative to volume and nature of EFT activities. Independent review efforts should address all areas of EFT business, including:

37 A Payment order origination (funds transfer requests).

37 B Message testing.

37 C Customer agreements.

37 D Payment processing and accounting.

37 E Personnel policies.

37 F Physical and data security.

37 G Contingency plans.

37 H Credit evaluation and approval.

37 I Incoming funds transfers.

37 J Bank Secrecy and Office of Foreign Assets Control (OFAC) issues, if applicable.

37 K Federal Reserve's Payment System Risk Program issues.

INFORMATION SYSTEMS AND COMMUNICATION

38 Determine if management reports provide sufficient information in relation to the nature and volume of EFT activities.

39 Evaluate the accuracy and timeliness of information provided to the board and senior management.

MANAGERIAL EFFECTIVENESS

40 Assess compliance with board policies and guidelines.

41 Determine the adequacy of bank documentation of EFT activities, including the sufficiency of record retention practices.

42 Analyze compliance with laws and regulations, including requirements of the Bank Secrecy Act and Financial Recordkeeping.

43 Assess the adequacy of management's response to audit exceptions and recommendations.

44 Determine if the funds transfer area maintains Office of Foreign Assets Control (OFAC) identification and reporting capabilities.

45 Determine the adequacy of insurance coverage for each EFT operation and the overall EFT environment. (Note: Standard blanket bonds do not cover funds transfer operations. Banks typically obtain a special rider for funds transfers. However, the special rider does not normally provide coverage if telephonic requests for funds are honored.)

Electronic Funds Transfer Risk Assessment

Generally, procedures used in the Expanded Analysis should target concerns identified in the Core Analysis and Decision Factors. Expanded procedures associated with Core Analysis and Decision Factors of no concern need not be used. The flexible guidelines specified for the Core Analysis also apply here.

The following procedures should be implemented for Fedline as well as Wholesale EFTs if inadequate monitoring, audits, or controls exist.

POLICIES AND PROCEDURES

1 Investigate why the policy and procedure deficiencies identified in the Core Analysis exist. Possible reasons for policy deficiencies may include the following circumstances:

1 A Management overlooked these issues.

1 B Management is unfamiliar with prudent electronic funds transfer guidelines and procedures.

1 C Management is unwilling to create or enhance policies and procedures.

2 If poor compliance with policies and procedures exist, determine the reasons. Possible reasons are detailed below:

2 A Lack of awareness of policies' existence.

2 B Disregard for established policies.

2 C Misunderstanding the intent of policy guidelines.

2 D Poor internal communication of subsequent revisions in policy and procedures.

3 Determine if management commits to and supports proper controls and monitoring to ensure policy guidelines are followed in the future. Determine if proposed controls, if any, are reasonable.

INTERNAL CONTROLS

Funds Transfer Requests

4 Determine if the funds transfer function maintains a current list of bank personnel authorized to initiate transfer requests.

4 A Ascertain if the bank limits the number of employees who initiate or authorize transfer requests.

4 B Determine if authorized employee signature records are kept in a secure environment.

5 Review a sample of funds transfer requests. Determine if management uses standard, sequentially numbered forms or some other authentication system.

5 A Determine if funds transfer requests include the following items:

5 A1 The account title and number.

5 A2 A sequence number.

5 A3 The amount to be transferred.

5 A4 The person or other source initiating the request.

5 A5 The time and date.

5 A6 Authentication (call backs, fax, personal identification numbers).

5 A7 Paying instructions.

5 A8 The name of the bank personnel authorizing the transfer and the dollar amount.

6 Review the bank's procedures for recording all incoming and outgoing transfer requests.

6 A If calls are recorded, determine if the bank advises its customers in written contracts, by audible signals, or by informing the caller that telephone calls are being recorded.

7 Determine if transfer requests are recorded in a log, or another bank record, before execution.

7 A Determine if the funds transfer function maintains sequential control for requests it processes.

7 B If requests are not sequentially accounted for, determine if there is an unbroken copy of all messages received via telex or other terminal printers kept throughout the business day.

7 C Determine if someone not connected with equipment operations reviews sequence records and unbroken copies of messages.

8 Determine if incoming and outgoing messages are time stamped or sequentially numbered.

Test Keys

9 Determine if all messages and transfer requests that require testing are authenticated by using test keys. The following controls should be in place:

9 A Test keys are verified by someone other than the person receiving the transfer request.

9 B Test key formula incorporates a variable (sequence number). The requirement should be stated in an agreement between the bank and the customer.

9 C Only authorized personnel are permitted in the test key area or allowed access to terminals used for test key purposes.

10 Review test key files to determine if management keeps the files current.

10 A Determine if files containing test key formulas are maintained under dual control or otherwise protected.

10 B Determine if management maintains a list of those persons having access to test key files.

11 Determine if the bank has procedures in place for issuing and canceling test keys.

11 A Determine if the responsibility for issuing and canceling test keys are assigned to someone who is not responsible for testing the authenticity of transfer requests.

Payment Processing and Accounting

12 Determine if the funds transfer department verifies that work sent to and received from other bank departments agree with its totals.

13 Determine if key fields are re-verified before transmission and messages are released by someone other than the individual originally entering the message.

14 Ascertain if transfer requests accepted after the close of business, or transfer requests with a future value date, are properly controlled and processed.

15 Determine if open-statement items, suspense accounts, receivables or payables, and inter-office accounts related to funds transfer activity are controlled outside of the funds transfer operations. Determine if the following controls exist:

15 A Management prepares periodic reports on open-statement items, suspense items, and inter-office accounts.

15 B Reports include agings of open items, the status of significant items, and the resolution of prior significant items.

15 C Corrections, overrides, open items, reversals, and other adjustments are reviewed and approved by an officer.

16 Determine if all general ledger tickets, or other supporting documents, are initialed by the originator and supervisory personnel.

Personnel

17 Determine if screening procedures are applied to personnel hired for sensitive positions in the funds transfer area. Management should be implementing the following controls:

17 A New employees working in sensitive areas are closely supervised.

17 B Temporary employees are either prohibited from working in sensitive areas or closely supervised. (Note: The number of temporary employees allowed in sensitive areas should be limited.)

18 Determine if the bank requires statements of indebtedness for employees working in sensitive areas.

19 Review procedures governing personnel-related issues. Determine if the following control activities exist:

19 A Employees are subject to unannounced rotation of duties.

19 B Relatives of employees are precluded from working in the bank's bookkeeping, audit, data processing, or funds transfer requests departments.

19 C Employees are required to take a minimum number of consecutive days as part of their annual vacation.

19 D Employees who have given notice of resignation or have been notified of pending termination are re-assigned from sensitive areas.

Physical and Data Security

20 Determine if the following controls exist to protect access to the funds transfer area:

20 A Visitors are identified, required to sign in, and accompanied at all times.

20 B Written authorization is required for employees who remain in the funds transfer area after normal working hours, and security guards are informed of the employee's presence.

20 C Bank terminal operators and others in the funds transfer operations are denied access to computer equipment or programs.

20 D Computer personnel are prohibited from accessing bank terminals or test key information used for funds transfers.

20 E Supervisory approval is required for terminal access at other than authorized times.

20 F Employees are prohibited from taking keys for sensitive equipment out of the funds transfer area.

Credit Evaluation and Approval

21 Determine if management establishes customer limits for daylight and overnight overdrafts. Management should complete the following tasks:

21 A Ensure limits include groups of affiliated customers.

21 B Monitor funds transfer requests during the business day to ensure that proper approval is granted before making payments that exceed limits.

21 C Review and periodically update customer limits.

22 Determine if management makes payments in anticipation of receiving funds that day to cover the daylight overdraft. Determine if the following controls over daylight overdrafts exist:

22 A Payments are approved by officers with appropriate credit authority.

22 B Daylight exposures are limited to amounts expected to be received that same day.

22 C Daylight overdraft limits are established after considering other types of credit facilities for the customer.

22 D A daylight record is kept for each customer showing the following information:

22 D1 Opening collected and uncollected balances.

22 D2 Transfers in and out of the account.

22 D3 Collected balance at the time payments are released.

23 Determine if any overnight overdrafts exceed established limits:

23 A Assess why the overdraft exceeded limits.

23 B If a control failure caused the overdraft, determine if the following procedures were followed:

23 B1 The cause was properly documented.

23 B2 Adequate follow-up to obtain the covering funds in a timely manner.

24 Determine if a person with appropriate credit authority approves payments that exceed established daylight and overnight limits.

25 If the bank is a participant of a net settlement system (CHIPS), determine if bilateral-lateral credit limits are set based on a formal credit analysis. The limits should be reviewed by an appropriate level of management.

Payment System Risk

26 If the bank incurs overdrafts in its Federal Reserve account, determine if it completed the payment system risk program (selected an appropriate net debit cap).

27 If the bank has selected a de minimis or self-assessment net debit cap, evaluate the adequacy of records supporting the bank's program and accuracy of the de minimis or self-assessment rating.

FEDLINE Electronic Funds Transfer

28 Determine why management has elected to deviate from recommended security settings and controls and assess the adequacy of compensating controls.

29 Determine if appropriate compensating controls are active where the master user ID password has not been isolated and stored in a secure location.

Information Technology Standards

30 Determine if standards exist for the following activities:

30 A Software and hardware acquisitions, including the following information:

30 A1 Cost benefit analysis.

30 A2 Programming standards.

30 A3 Documentation standards.

30 A4 Ownership of programs, spreadsheets, etc., developed on the bank's time and equipment.

30 A5 Escrow of source code of critical, tailor-made funds transfer software to ensure the bank can continue to maintain software in the event the vendor fails.

30 B Micro computer use including the following controls:

30 B1 Use of the output or data.

30 B2 Restrictions on personal and non-job related use.

30 B3 Use of personal equipment and software.

30 B4 Use of unauthorized software.

30 B5 Modification of the hardware and software.

30 B6 Copying or piracy of the software.

30 B7 Requirements for file backup.

Other

31 Review agreements that are in effect concerning funds transfer operations between the bank and its customers, correspondent banks, systems provider (Federal Reserve, CHIPS), servicers, and hardware and software vendors. Determine if the agreements contain the following information:

31 A Responsibilities of and accountability between all parties.

31 B Security procedures as defined by UCC Article 4A.

31 C Requirement that the bank obtain written waivers from customers who chose security procedures that differ from what the bank offers.

31 D Cut-off times for receiving, processing, and canceling or amending payment orders.

MANAGERIAL EFFECTIVENESS

32 Determine why previously identified deficiencies remain uncorrected.

33 Determine the reasons for poor compliance with policy guidelines, accounting standards, or applicable regulations.

34 Assess the adequacy and viability of management's corrective commitments.

Electronic Funds Transfer Risk Assessment

Impact Analysis reviews the impact that deficiencies identified in the Core and Expanded Analysis and Decision Factors have on the bank's overall condition. Impact Analysis also directs the examiner to consider possible supervisory options.

1 Determine if credit risk resulting from funds transfers will adversely impact overall asset quality and if the risk is included in determining the adequacy of the loan loss reserve.

2 Decide if the weaknesses identified in this area will negatively impact liquidity, earnings, or capital.

3 Determine the need for administrative and enforcement actions, formulate specific recommendations, and advise appropriate supervisory officials on the nature of the concern

4 Discuss the possibility of administrative and enforcement actions with senior management and the board of directors.