ELECTRONIC FUNDS TRANSFER RISK ASSESSMENT

Core Analysis Decision Factors

Examiners should evaluate the Core Analysis in this section to determine whether an Expanded Analysis is necessary. Click on the hyperlinks found within each of the Core Analysis Decision Factors to reference the applicable Core Analysis Procedures.

Examiners are reminded that wire activity can have an impact on other examination areas such as Bank Secrecy Act/Anti-Money Laundering, Asset Quality, Liquidity, and Sensitivity to Market Risk. Examiners reviewing Electronic Funds Transfer (EFT) have an opportunity to observe such things (not all inclusive) as suspicious activity, loan participation activity, borrowing activity, brokered deposits and other inflows and outflows. When observed, appropriate information should be shared with examiners reviewing those respective areas.

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

C.1.	**Are policies, procedures, and risk limits adequate?** ***Refer to Core Analysis Procedure #8.***
C.2.	**Are internal controls adequate?** ***Refer to Core Analysis Procedures #9-34.***
C.3.	**Are the audit or independent review functions adequate?** ***Refer to Core Analysis Procedure #35.***
C.4.	**Are information and communication systems adequate and accurate?** ***Refer to Core Analysis Procedures #36-37.***
C.5.	**Do the board and senior management effectively supervise the electronic funds transfer area?** ***Refer to Core Analysis Procedures #38-43.***

ELECTRONIC FUNDS TRANSFER RISK ASSESSMENT

Core Analysis Procedures

Examiners are to consider the following procedures but are not expected to perform every procedure at every bank. Examiners should complete only the procedures relevant for the bank's activities, business model, risk profile, and complexity. If needed, based on other identified risks, examiners can complete additional procedures. References to laws, regulations, supervisory guidance, and other resources are not all-inclusive.

Preliminary Review
1. Review previous examination reports, earlier work papers, and file correspondence for an overview of previously identified electronic funds transfer (EFT) concerns.
2. Obtain an organizational chart and flowchart for the EFT area and determine key job responsibilities and workflows. *Note: If the institution is subject to Sarbanes-Oxley (SOX), review the SOX information pertaining to the wire transfer function (e.g. SOX narratives, flow charts, and internal controls).*
3. Review the most recent audits and internal reviews of EFT activities to identify scope and noted deficiencies.
4. Review management's actions to correct examination and audit deficiencies.
5. Discuss with management recent or planned changes in EFT activities.
6. Review reports to determine the type and volume of wire activity. Ascertain if any alternative systems were implemented to supplement/replace wire transfer systems (e.g., ACH remittance programs).
7. Review the minutes of management committees that oversee EFT activity. Review for content and follow-up of material matters.

Policies and Procedures
8. Determine whether policies and procedures are adequate for the type and volume of funds transfer activities. Consider whether policies and procedures address the following: • **Acceptable methods of wire requests (in-person, phone, fax, e-mail, E-Banking);** • **Customer versus non-customer wire requests;** • **Use of wire transfer request forms;** • **Use of wire transfer agreements for recurring wire customers;** • **Collected funds versus uncollected funds;** • **Credit standards and overnight and daylight overdrafts limits;** • **Callback requirements;** • **Use of customer confirmations and advices;** • **Maintenance of wire log;** • **Office of Foreign Assets Control (OFAC) compliance;** • **Separation of duties for funds transfer personnel including originating, receiving, testing, and approving functions; authorizing dollar limits; and preparing data entry;** • **Clearly defined security procedures over payment orders and controls over source documents;** • **Record retention;** • **Exception reporting;** • **Organizational reporting controls;** • **Maintenance of adequate blanket bond coverage;** • **Internal audit coverage;** • **Board reporting requirements;** • **System testing;** • **Network security;** • **Incident response;** • **Personnel hiring and dismissing;** • **User security reviews; and** • **Implementation of a comprehensive business continuity, contingency planning, and disaster recovery program.**
Internal Controls
9. Evaluate management's procedures to prevent, detect, and respond to policy exceptions.
FUNDS TRANSFER REQUESTS
10. Review the bank's standard form of agreement or other written agreements with its customers, correspondent banks, and vendors. Determine whether those agreements are current and clearly define the liabilities and responsibilities to all parties.

11. Review the bank's procedures for validating transfer requests, including those received via on-line terminals, telephone, fax, E-Banking systems, or written instructions. Determine procedures provide for adequate security. For banks that allow customers to submit requests via E-Banking products, determine whether appropriate authentication measures are in-place (refer to the FFIEC Supplement to *Authentication in an Internet Banking Environment*: FDIC: FIL-50-2011; FRB: SR 11-09).
12. Determine whether more than signature verification (tests, callbacks) are required on written requests. Verify that any callback procedures utilized by the institution comply with actual callback requirements (if any) stated in the blanket bond coverage.
13. Determine whether management maintains a current record of authorized signers for customers who use the bank's funds transfer services. The following items reflect prudent controls: • **Recurring wire transfer customers should be required to have current signed wire transfer agreements on file that outline duties and responsibilities of both the customer and the institution.** • **The record includes authorized sources of funds transfer requests (telephone, memo, and fax).** • **The bank advises its customers to limit the number of authorized signers.** • **Customer authorization lists limit the amount one individual is authorized to transfer.**
14. Ascertain if customer signature records are maintained under dual control or are otherwise protected.
15. Determine whether procedures are in place to prohibit transfers of funds against accounts that do not have collected balances or preauthorized credit availability.
16. In situations where payments are to be made against uncollected funds and intraday overdrafts in excess of established limits, ensure that they are referred to appropriate authority for approval.
17. In situations where payments are made against uncollected funds and in excess of established limits, ensure that timely and appropriate steps are taken to obtain covering funds.
18. Evaluate management's compliance with OFAC regulations.

19. Determine whether the Outgoing Wire Log is appropriately completed and documented. Consider the following: ***Note: Logs typically include customer-initiated and bank-purpose wires.***

- **Originator name,**
- **Originator account number,**
- **Dollar amount of transaction,**
- **Beneficiary name,**
- **Beneficiary account number,**
- **Counterparty institution,**
- **Counterparty location, and**
- **Domestic or foreign.**

PAYMENT PROCESSING AND ACCOUNTING

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

- **Independent end-of-day reconcilements for messages sent to and received from intermediaries (Federal Reserve Bank, servicers, correspondents, and clearing facilities);**
- **System activity reconcilements to transfer request source documents;**
- **Daily supervisory review of funds transfer and message reconcilements;**
- **Daily activity balancing is performed separate from the receiving, processing, and sending functions; and**
- **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.**

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

22. Ensure that suspense items or adjustment accounts are appropriately accounted for, reviewed for abnormal fluctuations, and do not contain unusual or stale items.

CREDIT EVALUATION AND APPROVAL

23. Determine if there are well-documented, periodic credit reviews of funds-transfer customers and ensure that they are completed by credit personnel who are independent of account officer and operations staff.

24. Ensure that limits on intraday and overnight overdrafts are reasonable in view of the organization's capital position and the creditworthiness of the respective customers.
INCOMING FUNDS TRANSFERS
25. Determine whether incoming payments not received over a secure system are authenticated prior to processing.
26. Determine whether the bank maintains separation of duties over receiving instructions, posting to a customer's account, and mailing customer credit advices.
27. Determine whether management maintains audit trails from receipt through posting to a customer's account.
28. Determine whether management issues customer advices in a timely manner. (Prudent practices would indicate advices sent for incoming as well as outgoing wires)
29. Determine whether the Incoming Wire Log is appropriately completed and documented. Consider the following: • **Beneficiary name,** • **Beneficiary account number,** • **Dollar amount of transaction,** • **Sender name,** • **Sender account number,** • **Counterparty institution,** • **Counterparty location, and** • **Domestic or foreign.** ***Note: Ensure logs include customer-initiated and bank-purpose wires.***
BUSINESS CONTINUITY AND DISASTER RECOVERY *(To the extent possible, leverage off the work of Information Technology examiners.)*

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

- **A back-up system in the event of equipment failures and line malfunctions,**
- **A method for sending and receiving transfers if forced to operate at a different site,**
- **Procedures to ensure that data is recovered by the opening of the next day's processing,**
- **A requirement for supervisory approval for using back-up equipment,**
- **A requirement that the plan be distributed to all funds transfer personnel,**
- **Periodic testing of the back-up systems, and**
- **Procedures and controls to prevent the inadvertent release of test data into the production environment.**

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

FEDLINE ELECTRONIC FUNDS TRANSFER

Note: This type of transfer activity will be the most common type of funds transfer in community banks. Refer to the FFIEC IT Examination Handbook on Retail Payment Systems and the FedLine Advantage workprogram.

WHOLESALE ELECTRONIC FUNDS TRANSFER SYSTEMS (FTS)

Note: These procedures generally apply to larger banks that initiate large dollar transfers. Refer to the FFIEC IT Examination Handbook - Wholesale Payment Systems.

32. 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:

- **FedLine,**
- **CHIPS (Clearinghouse Interbank Payment System) or other local payments system,**
- **SWIFT (Society for Worldwide Interbank Financial Telecommunications),**
- **Internal transfers (book entry),**
- **Customer networks, and**
- **Internal networks.**

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

- **Payment order origination such as message testing for fax, telephone, letters, or memos;**
- **Data entry;**
- **Payment order execution or release;**

- **Telecommunication lines; and**
- **Physical security.**

34. Review a sample of contracts authorizing the bank to make payments from a customer's account and determine whether 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

35. Determine whether the audit or independent review program provides sufficient coverage relative to volume and nature of EFT activities. Independent review efforts should address relevant areas of EFT business, such as:

- **Adequacy of and compliance with policies and procedures;**
- **Payment order origination (funds transfer requests);**
- **Message testing;**
- **Customer agreements;**
- **Payment processing and accounting;**
- **Personnel policies;**
- **Physical and data security;**
- **Contingency plans;**
- **Credit evaluation and approval;**
- **Incoming funds transfers;**
- **Outgoing funds transfers;**
- **Accuracy and completeness of wire logs;**
- **Bank Secrecy and OFAC issues, if applicable;**
- **Federal Reserve's Payment System Risk Program issues;**
- **Adequacy of blanket bond coverage, as well as compliance with any requirements of this insurance coverage for things such as callbacks;**
- **Evaluation of metrics utilized by management to measure the transactional risk inherent in the wire transfer function; and**
- **Appropriateness of board reporting of wire activity that is commensurate with level of risk.**

Information Systems and Communication

36. Determine whether management reports provide sufficient information in relation to the nature and volume of EFT activities and that it is sufficient for the directorate to assess the organization’s inherent risk in EFT activities. Consider the following:

- **Identification of customers with large intraday and overnight overdrafts;**
- **Drawings against uncollected funds or in excess of established credit limits;**

- **Credit evaluation and approval;**
- **Total and average number of wires;**
- **Total and average dollar amount of wires;**
- **Volume of incoming vs. outgoing wire activity;**
- **Volume of domestic vs. international wire activity;**
- **Location of international activity;**
- **Volume of customer-initiated vs. bank-purpose wire activity; and**
- **Trend of wire activity (e.g., number, dollar, average).**

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

Managerial Effectiveness

38. Assess compliance with board policies and guidelines.

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

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

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

42. Determine whether management has properly planned for contingencies and has developed reasonable contingency plans and safeguards that are commensurate with the volume of EFT activities.

43. 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.) Assess compliance with any requirements of the blanket bond coverage such as callback requirements.

End of Core Analysis. If needed, Continue to the Expanded and Impact Analyses.