WIRE TRANSFERS

Core Analysis Decision Factors

Click on the hyperlinks found within each of the Core Analysis Decision Factors to reference the applicable Core Analysis Procedures.

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

C.1.	**Do management and the board effectively supervise wire transfer activities?** ***Refer to Core Analysis Procedures #2-5.***
C.2.	**Are operational, logical, and physical controls commensurate with the level of risk for wire transfer transactions?** ***Refer to Core Analysis Procedures #6-11.***
C.3.	**Are the business continuity, disaster recovery, and incident response programs appropriate for wire transfer activities?** ***Refer to Core Analysis Procedures #12-13.***

WIRE TRANSFERS
Core Analysis Procedures

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

References

- *Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook – Wholesale Payment Systems*
- *Federal Reserve Regulation J*
- *Federal Reserve Bank Operating Circulars*

Considerations and Background

For the purposes of this module, U.S. dollar wire payments (aka large-value payments or wholesale payments) include those payments that are settled through one of two wire operators -- Fedwire Funds Service or the Clearing House Interbank Payment System (CHIPS). Because CHIPS participation is limited to a small subset of the large, international financial institutions, this work program and job aid focuses on Fedwire Funds Service transactions.

Transactions in Fedwire are settled individually throughout the processing day. Settlement of funds is immediate, final, and irrevocable. Individual payments for any purpose and value (from $1 to $999,999,999.99) can be made by participating financial institutions (FIs) using Fedwire Funds Service, though in general, most participants use this payment rail for large-value, time-critical payments.

Fedwire Funds uses a propriety messaging system to send and receive electronic payment instructions from participants. FIs can access Fedwire Funds Service to send payments through one of two FedLine electronic access solutions -- FedLine Direct or FedLine Advantage. Low-volume financial institution participants can also initiate payments over the telephone.

Third-party messaging systems, most notably Society for Worldwide Interbank Financial Telecommunication (SWIFT), are often used by FIs to send U.S. dollar and international wire payment instructions to correspondent banks, who then originate on the financial institution's behalf. Many FIs also use core providers to connect to Fedwire Funds Service. This module covers transactions initiated by a FI directly or through its correspondent or other third party.

Examination Considerations

The Federal Reserve's Operating Circular 5 (Electronic Access) and Operating Circular 6 (Funds Transfers for Fedwire Funds Transfer Service) may be particularly useful to review. Examiners should also consider requesting a copy of the security and control procedures that financial institutions are expected to implement to comply with Federal Reserve requirements as part of the participation agreement. In January 2021, the Federal Reserve Banks implemented an annual FedLine Security and Resiliency Assurance Program ("Assurance Program"). As part of this program, organizations that use the FedLine Solutions must:

- Conduct an assessment of compliance with the Federal Reserve Banks' FedLine security requirements; and
- Attest to the Federal Reserve Banks that the assessment was completed.

If wire operations have not been reviewed at the FI for several years, examiners may find it beneficial to have the FI provide an overview of its wire operations at the start of the examination.

Preliminary Review

1. **Review items relating to the institution's wire activities, such as:**
   - **Prior examination reports and workpapers**
   - **Examination planning memoranda and file correspondence**
   - **Description of wholesale payment (wire) activities, including list of payment networks and messaging systems used (e.g., Fedline Direct, Fedline Advantage, CHIPS, SWIFT, other third-party service providers (TPSPs), bankers' banks), and related process flow maps/data flow diagrams**
   - **Organizational structure and institution personnel responsible for wire activities**
   - **Trends in volumes and dollar values of wire transactions in total and by customer**
   - **Customer risk ratings**
   - **Wire systems and staff wire exposure limits**
   - **Policies and procedures specific to wire activities, including fraud monitoring and incident response, Business Continuity Plan/Disaster Recovery (BCP/DR), Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT), and Office of Foreign Assets Control (OFAC) policies and procedures**
   - **Management and board reports that cover wire activities**
   - **Wire-related reports from operators, correspondents, or TPSPs used for business or risk management purposes. Specific to users of FedLine Advantage, the "Subscriber and Roles Report."**
   - **Federal Reserve Payments Analysis and Screening System (PASS) data shared among national regulators**
   - **Risk assessments of wire activities**
   - **Internal and external audit reports of wire activities, including associated audit tracking**
   - **Any attestations of compliance with requirements of wire service operators/messaging systems/TPSPs, (e.g., FedLine Security and Resilience Assurance Program), including supporting documentation and any internal and/or external audit reports that include reviews of attestations**
   - **Copy of contracts/service level agreements (SLAs) with TPSPs of wire-related products and services**
   - **The TPSP Reports of Examination that cover wire services products provided to the institution by the TPSP and, as available, the Shared Application Software Review (SASR) of the TPSP's wire product**

Board and Management Oversight

Risk Framework

2. **Consider whether the appropriate oversight structure and processes have been established, including:**
   - **Audit and management oversight**
   - **Framework for onboarding and periodic review of wire customers**
   - **Management information systems (MIS) and associated reporting practices for wire transfers**

- **Training programs for internal employees and customer education on wire transfers**
- **Information sharing through collaborative industry group participation (e.g., FS-ISAC (the Financial Services Information Sharing and Analysis Center))**

Policies and Procedures

3. Determine whether policies and procedures contain appropriate content based on the volume and complexity of wire operations. Consider the following:

- **Scope**
  - **Who can initiate and approve wire transfers/segregation of duties**
  - **Internal wire staff approval limits**
  - **Customer onboarding and ongoing credit and other monitoring**
  - **Customer agreement requirements**
  - **Customer limits**
  - **Customer credit lines/overdraft lines**
  - **Customer security requirements**
  - **Use of third parties**
  - **Change management processes**
  - **Business continuity and incident response**
  - **International wire transactions**
  - **Alignment with operator (FedWire Funds, CHIPS, SWIFT), correspondent, or TPSP requirements**
  - **FedLine Security and Resilience Assurance Program and SWIFT Customer Security Program documentation, as appropriate**
  - **Exceptions**
- **Review and approval practices for policies and procedures**

4. If the institution extends credit to customers intraday for payments, review the customer credit analysis and risk rating summaries of several customers, and confirm that the institution's analysis aligns with the current wire policies and procedures.

Risk Assessment

5. Evaluate the effectiveness of the risk assessment process specific to wire activities. Consider the following:

- **Credit risk**
- **TPSP risk**
- **Operational risk, including cyber risk**
- **Whether the risk assessment considers operator requirements**
- **How changes in the channels by which wire instructions are accepted or a substantial increase in wire volume are incorporated into the risk assessment**

Key Controls

Operational/Logical/Physical Controls

6. Assess operational, logical, and physical controls for the primary and back-up systems and processes used for wire transfers. Consider the following:

- **Segregation of duties among those who establish access rights, originate payment orders, and approve payment orders and any other combinations that could pose risk of fraud or other malfeasance**
- **Configuration and limit structure**
  - **Dollar limits, including for staff who enter or approve instructions, as well as for customers**
  - **Time-of-day restrictions for instruction input**
  - **Country-of-beneficiary restrictions**
  - **New beneficiary procedures**
- **Identity and access management**
  - **Authentication procedures and requirements**
  - **Privileged access management**
- **Adequacy of insurance relative to transaction limits**
- **Fraud detection and anomalous activity monitoring tools**
- **Physical and environmental monitoring and controls**
  - **Wire service equipment located in a secure location**
  - **Tokens secured when not in use**
  - **Hardware and software inventory**
- **Reconciliation using independent information sources**
- **Template management for recurring wire transfers**
- **Range of allowable customer wire transfer initiation channels**
- **Customer versus non-customer wire request procedures**
- **Customer agreements stipulating security procedures for wire customers**
- **Customer education provided on use and importance of security procedures and other controls in addressing fraud due to endpoint security risks**

7. Review available user reports (including as appropriate the FedLine Subscriber and Roles Report or third-party user access reports) to determine whether:

- **Segregation of duties is implemented to avoid conflicts of interest in role assignments**
- **Recent reports accurately reflect the staff authorized to access the relevant wire system service**
- **No individual authorized to send wire transfers has more than one set of credentials**
- **No terminated individuals are listed on the report**
- **Established wire limits are consistent with established policies and/or board approval**
- **Changes to wire configurations, including third-party origination configurations, process flows, and security control parameters, are regularly reviewed and follow a formal change management process**

- **The processes used for log on, authentication, and transaction execution conform with policy, which can be done by observing or interviewing wire operations staff**
- **Security procedures and controls are followed to verify customers, which can be done through document reviews, walk throughs, and conversations with wire operations staff**

8. Determine whether customer access to internet-based products or services requires authentication controls (e.g., layered controls, multi-factor) that are commensurate with the risk.

9. Determine whether customer service (e.g., call center) uses formal procedures to authenticate customers commensurate with the risk of the transaction or request.

Payment Network Controls

10. Assess network controls for primary and backup systems used for wire transactions. Consider the following:

- **Segmentation of wire systems from general network system, if possible**
- **Security monitoring for anomalous activities**
- **Hardware and software used for sending payments is included in vulnerability and patch management programs**

11. Determine whether customer transactions generating anomalous activity alerts are monitored and reviewed.

Business Continuity Management (BCM)

12. Evaluate whether wire activities are appropriately addressed in business continuity, disaster recovery, and incident response programs and practices. Consider the following:

- **Inclusion of contingencies for personnel as well as systems**
- **Inclusion of testing backup systems and alternative systems**
- **Alignment of service provider SLAs with BCM policy**

13. Confirm testing includes a range of scenarios that are high impact, but plausible.

End of Core Analysis

SUPPLEMENTAL JOB AID – WIRE TRANSFERS (INTERNAL ONLY)

Considerations and Background

Purpose: This job aid is provided only as a reference tool for examiners to consider in completing the Core Analysis Decision Factors. Examiners do not need to use this job aid and do not need to provide responses to the considerations below.

Decision Factor 1 – Board and Management Oversight

Procedure 2 – Risk Framework

Introduction: Consider whether management and the board have established an appropriate oversight structure and processes for wire activities.

Relevance: To identify, measure, monitor, and control wire risk, management and the board are responsible for establishing the FI's wire strategy and ensuring that processes are consistent with that strategy.

Review Considerations:

- ✓ Policies and procedures including those that address the onboarding and ongoing monitoring of wire customers and the origination and receipt of wire transactions.
- ✓ Monitoring reports, including second line risk management reports that address wire activity (e.g., customer origination volume and value reports, return rate reports, and exception reports that show anomalous activity or operational issues).
- ✓ Examination and other findings that affect wire operations.
- ✓ Audit-tracking reports with wire issues identified and remediation status.
- ✓ Any documentation associated with the FI's participation in collaborative industry groups that focus on controlling wire fraud/cyber-attacks (e.g., FS-ISAC).

Items to Consider:

- ✓ Management, with the board's oversight, has identified which types of wire customers and transactions (e.g., international wire-transactions) for which the FI will provide origination services.
- ✓ A written framework (e.g., policies, procedures, customer analysis document,) which the FI reviews new customers for wire origination including how often there is a review of customer relationships and activity (e.g., monthly, yearly).
- ✓ Wire-monitoring reports, including those that address the FI's customers, trends over time for origination volume and value (by month, quarter, year), and exception reports. Confirm process for appropriate levels of management review and escalation and frequency of reporting.

Potential Questions to Consider:

- ✓ Does the reporting threshold for management and the board align with the wire-risk assessment?
- ✓ Does the FI have regular training for its employees and customers on wire responsibilities and operations? How does the FI communicate new rules requirements to employees and customers, particularly those that affect wire operations?
- ✓ Has the FI established independent review of controls for wire transactions?

Procedure 3-4 – Policies and Procedures

Introduction: Consider whether the FI's wire policies and procedures reflect the complexity and volume of the FI's wire operations.

Relevance: Comprehensive policies and procedures support consistent operations and decision-making by articulating the FI's risk appetite, control structure, and the alignment with Operator and third-party service provider (TPSP) requirements.

Review Considerations:
- ✓ Wire policies and procedures.
- ✓ Wire data and payment flow and process diagrams. If the FI does not have diagrams, use descriptions.
- ✓ Sample customer due diligence documents.
- ✓ Sample customer wire-credit analysis and risk rating summaries.
- ✓ Sample agreement/contracts between the customer and the FI, and the FI and any TPSPs.
- ✓ Wire-security requirements of operators or third parties (e.g., Operating Circulars and FedLine Advantage Monitoring and Control Guidelines).
- ✓ Documentation supporting an assessment of security programs for Fedwire or SWIFT, as relevant, e.g., Security and Resiliency Assurance Program attestation documentation.

Items to Consider:
- ✓ Data flow diagrams, due diligence documents, customer due-diligence documents, and credit risk summaries align with existing policies and procedures.
- ✓ Wire exception-processing procedures include steps to handle transaction activity that is outside of policy for customer wire origination (e.g., origination greater than exposure limits).
- ✓ Wire policies and procedures are reviewed periodically (e.g., annually, when new products or technologies are implemented), include the date drafted/adopted, and include an established approval process.
- ✓ Agreements address types of wire activity that the FI allows to be originated, information security requirements for data transmission, customer exposure limits and other controls, roles and responsibilities, processes and procedures and performance standards for customers.
- ✓ Wire agreements are consistent with the FI's policies and procedures.
- ✓ Policies and procedures are in alignment with the requirements of wire operator(s), correspondent, or TPSP agreements/contracts.
- ✓ Policies and procedures address segregation of duties, authentication procedures and requirements (i.e., log-on requirements), and reconciliation.

Potential Questions to Consider:
- ✓ What is the process the FI goes through to review policies and procedures when there are significant changes to processes that affect wire transactions?
- ✓ What is the FI's process for evaluating new customers against policies and procedures?
- ✓ What conditions trigger review of wire agreements or of policies and procedures?

Procedure 5 – Risk Assessment

Introduction: Evaluate the effectiveness of the risk assessment process specific to wire activities.

Relevance: The risk assessment process helps the FI to identify and mitigate the risks associated with wire activities.

Review Considerations:
- ✓ Risk assessments associated with wire activities. These assessments can be a stand-alone, end-to-end wire risk assessment, or the combination of wire risk-assessment elements considered in IT, business line, or other risk assessments.

Items to Consider:
- ✓ Wire risk assessment reflects the current operating environment and the services offered.

- ✓ Risk assessment incorporates any changes in channels (e.g., digital banking, telephone, in-person) by which wire instructions are accepted, and any significant increases in wire volume or new wire products and services.
- ✓ Wire activities are reviewed holistically across business lines and activities.
- ✓ Wire risk assessment aligns with the operator security requirements.

Potential Questions to Consider:

- ✓ How does the FI ensure that the wire risk assessment comprehensively identifies the risks in the end-to-end wire transfer process?
- ✓ How does the FI assess the risk of new wire products, services, or technology?

Decision Factor 2 – Key Controls

Procedure 6-9 – Operational/Logical/Physical Controls

Introduction: Assess operational, logical, physical controls for the primary and backup systems used for wire transfers.

Relevance: An adequate layered control environment will mitigate risks from internal and external threats. Weak or inadequate controls could leave the FI vulnerable to cyber-attacks, internal fraud, operational outages, and other adverse events that ultimately result in customer and FI losses.

Review Considerations:

- ✓ Federal Reserve Subscriber and Roles Report for FedLine Advantage users and the FI's own reports listing internal users and privileged users for wire networks and applications.
- ✓ Federal Reserve Event Tracker Report and/or reports provided by TPSPs or correspondents that show configuration changes.
- ✓ FedTransaction Analyzer reports and dashboards.
- ✓ Interview or observe wire operations staff perform log on, authentication, execution, and reconcilement for types of wire transactions (e.g., domestic, foreign, recurring) originated by the FI.
- ✓ Management reports used to identify conflicts of interests in assigned user roles and responsibilities for FI staff involved in the end-to-end wire payments process, including privileged/administrative users.
- ✓ Documentation on the most recent reviews of user access rights for authorized wire users and privileged users.
- ✓ Management reports on wire activity overall (key metric analysis) and by customers.
- ✓ Screen shots or other documentation that show which key configuration options (e.g., transaction amount, time of day, country of beneficiary) offered by wire operator(s), correspondents, or TPSPs have been chosen.
- ✓ Documentation that shows user authorization limits for wire systems.
- ✓ Fraud detection and anomalous activity monitoring tools. These tools could be developed by the FI or may be an add-on module from a service provider or another vendor.
- ✓ Insurance coverage requirements for wire transactions
- ✓ Audit-report findings related to operational, logical, and physical controls.
- ✓ Description/explanation of the allowable customer wire-transfer initiation channels (e.g., digital banking, text, telephone, and in-person).
- ✓ Customer transaction activity-monitoring reports, including those provided by third parties.
- ✓ Walkthrough and/or conversations addressing security procedures/controls followed to verify customers sending wire transfers through each allowable initiation channel.
- ✓ Sample of wire origination agreements.
- ✓ FI reports that show customer names and exposure limits, and wire activity reports that show exceptions over exposure limits by customer.

Items to Consider:

- ✓ Policies, procedures, risk assessments, and credit analyses around customer exposure limits.
- ✓ Administrators (i.e., individuals who set up and delete users) do not have the ability to transact. Make sure that management reviews privileged access controls.
- ✓ Segregation of duties among those that have access rights, those who can originate wire transfers, and those who can approve wire transfers. If the FI does not have enough staff to accommodate segregation of duties, look for other compensating controls in place (e.g., dual approvals).
- ✓ Chosen wire-configuration options are in line with risk tolerances and policies and procedures, and that changes to wire configurations, including third-party origination configurations, process flows, and security control parameters are reviewed regularly, and follow a formal change-management process.
- ✓ Authentication procedures (e.g., password requirements, password controls, callbacks) used by staff accessing wire-related systems/applications.
- ✓ Appropriate reconciliation processes are performed with independent data sources (e.g., appropriate reports, records or logs not generated from the same systems).
- ✓ Templates for recurring wire transfers are managed appropriately.
- ✓ Wire origination agreements are consistent with the FI's wire policies and procedures.
- ✓ Adherence to allowable security procedures for wire customers. Examples of these procedures include callbacks, biometrics, dual controls, IP address registration, and others, as appropriate, based on initiation channel.
- ✓ Customer transaction-activity monitoring reports are reviewed for potential anomalous or fraudulent activity (e.g., account takeover, business email compromise, and other changes in trends).
- ✓ Wire transactions are securely transmitted (e.g., encryption methods).

Potential Questions to Consider:

- ✓ Are the FI's user access rights that affect wire transactions established under the least privilege principle?
- ✓ How are customer exposure limits for wire origination set, monitored, and adjusted over time? Do system settings reconcile with policy and procedures?
- ✓ What is the process the FI uses to adjust the initially set configuration options offered by the Federal Reserve, correspondent, or TPSP?
- ✓ What types of authentication processes are used for internal users (staff) to initiate a transaction? For example, tokens, call backs, passwords, secret codes.
- ✓ What reports does management review regarding activity flowing through TPSPs?
- ✓ Does the FI have insurance as a compensating control for possible losses? If so, how does the FI evaluate the adequacy of insurance relative to transaction limits?
- ✓ Explain or show (by conducting a walkthrough) how the wire data-flow diagrams align with controls in place.
- ✓ How often are established limits within policies reviewed against system-defined limits within the wire systems?
- ✓ Does the FI provide customer education on the use and importance of security procedures and other controls to address potential fraud?
- ✓ What kind of encryption is in place for transmission of wire transactions?

Procedure 10-11 – Payment Network Controls

Introduction: Consider whether wire transactions are securely transmitted.

Relevance: Secure networks will maintain the confidentiality and integrity of data and reduce the risk of financial loss related to wire transactions.

Review Considerations:

- ✓ Annual information security or Gramm-Leach-Bliley Act (GLBA) report to the FI's board.

- ✓ Wire data-flow diagrams or discussions about data flows.
- ✓ Available schematics illustrating security controls, including potential network segmentation, implemented on the FI's internal payments networks connected to Fedwire.
- ✓ List of outstanding vulnerabilities affecting the institution's internal payment network connected to Fedwire.

Note: In this section, examiners are looking at payment network controls that specifically affect the wire environment. Consult with an IT examiner responsible for overall review of network controls as appropriate.

Items to Consider:

- ✓ Annual information security reports address the following content and there are no identified weaknesses or incidents related to wire transfers:
  - Information security risk assessment
  - Vulnerability program and internal vulnerability assessments
  - Penetration testing is performed
  - Patch compliance
  - Configuration management program

Potential Questions to Consider:

- ✓ Are the wire-related systems (workstations and servers) included in the most recent penetration tests and vulnerability assessments? Were any exceptions noted?
- ✓ What types of encryption are used to protect wire activity?
- ✓ Has management provided social engineering tests or education to payments staff?
- ✓ Is fraud monitoring included in the payment transmittal software platform? Has management purchased or contracted with a third party to provide fraud monitoring? What fraud monitoring software is used, what have the configurations been set to, and what types of information is flagged to trigger alerts and anomalous detection? Has the software been configured to monitor all wire transactions?
- ✓ How does the FI ensure a comprehensive hardware/software inventory includes wire-related hardware and software?

Decision Factor 3 – Business Continuity Management

Procedure 12-13 – Business Continuity Management

Introduction: Consider whether the FI's business continuity and disaster recovery programs adequately address wire activities and operations.

Relevance: Failure to establish adequate business continuity plans and processes could result in the FI not being able to react quickly when an incident or outage occurs impacting wire processing, thereby exposing the FI to financial losses.

Review Considerations:

- ✓ Business continuity, disaster recovery, and incident response plans that relate specifically to wire operations.
- ✓ FI testing results for these plans.

Items to Consider:

- ✓ Plans include contingencies for personnel as well as systems.
- ✓ Incident response plans specifically address wire operations and are sufficiently detailed to enable timely action.
- ✓ Testing includes backup systems and alternative systems.
- ✓ Service provider service level agreements (SLAs) align with business continuity policy.

Potential Questions to Consider:

- ✓ Does the FI's testing include a range of scenarios that are high impact, but plausible?
- ✓ Has the FI tested wire transaction operations from alternative site(s)?
- ✓ Has the FI tested wire transaction operations from the FI's alternative provider?

End of Supplemental Job Aid – Wire Transfers (INTERNAL ONLY)