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