AUTOMATED CLEARING HOUSE

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 Automated Clearing House (ACH) activities?** ***Refer to Core Analysis Procedures #2-5.***
C.2.	**Are operational, logical, and physical controls commensurate with the level of risk for ACH transactions?** ***Refer to Core Analysis Procedures #6-12.***
C.3.	**Are the business continuity, disaster recovery, and incident response programs appropriate for ACH-related activities?** ***Refer to Core Analysis Procedures #13-14.***

AUTOMATED CLEARING HOUSE
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 – Retail Payment Systems*
- *National Automated Clearing House Association (NACHA) Operating Rules*
- *ACH Operations Bulletins*
- *Interagency Guidance on Third-Party Relationships: Risk Management (FDIC: FIL-29-2023; FRB: SR 23-4)*

Considerations and Background

An ACH is an electronic network for the exchange of payment instructions among financial institutions (FIs), typically on behalf of customers. ACH transactions are payment instructions to either debit or credit a deposit account. ACH transactions are batch-processed, value-dated electronic funds transfers between originating and receiving FIs. ACH transactions can either be credits, originated by the account holder sending funds (payer), or debits originated by the account holder receiving funds (payee). NACHA is responsible for the administration, development, and enforcement of the NACHA Operating Rules and sound risk management practices for the ACH Network.[1]

FIs can support ACH activities in a number of ways. ACH transactions are either originated by an Originating Depository Financial Institution (ODFI) or received by a Receiving Depository Financial Institution (RDFI). Any FI that is an ODFI must also be an RDFI. ACH transactions are cleared and settled between the ODFI and RDFI in batches through one of the two ACH Operators—either the Federal Reserve Bank (FRB) or The Clearing House's Electronic Payments Network (EPN). ACH transactions are either credit (push) transactions or debit (pull) transactions that can be cleared and settled same-day or in one or two business days.

FIs may contract with third-party service providers (TPSPs) to facilitate ACH activities. Such third parties may include commercial businesses of all types, payment processors, non-bank financial technology organizations (fintechs) and other third-party deposit providers that may generate significant ACH payment activity to move funds. ODFIs are responsible for all ACH payment activity initiated by their customers (including any nested relationships), and like any other third party relationship the use of such entities does not diminish or remove banking organizations' responsibility to ensure activities are performed in a safe and sound manner and in compliance with applicable laws and regulations. Agreements that detail and set expectations of each party are central to managing payments risk.

[1] **See www.nacha.org for further information on NACHA.**

Preliminary Review

1. Review items relating to the institution's wire and ACH activities, such as:

- **Prior examination reports and workpapers**
- **Examination planning memoranda and file correspondence**
- **Description of ACH activities, including ACH operator used (i.e., Electronic Payment Network (EPN) or Federal Reserve ACH), and process flow maps/data flow diagrams**
- **Organizational structure and institution personnel responsible for ACH activities**
- **Customers, type of transactions (i.e., Standard Entry Class (SEC) codes), volumes and dollar values of ACH transactions, and reports that monitor baseline and trending ACH activity, including originations and returns**
- **Customer risk ratings and ACH origination exposure limits**
- **Policies and procedures specific to ACH 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 ACH activities**
- **ACH-related reports from ACH operators, correspondents, or TPSPs used for business or risk management purposes**
- **ACH data shared among national regulators such as Federal Reserve Payments Analysis and Screening System (PASS) data and EPN ODFI origination and return data**
- **Risk assessments of ACH activities**
- **FedLine Security and Resilience Assurance Program documentation, as applicable**
- **Internal and external audit reports of ACH activities, including associated audit tracking**
- **Copy of contracts with TPSPs, including third-party payment processors (TPPPs) of ACH-related products and services and accompanying service level agreements (SLAs)**
- **Documentation that addresses recent or planned changes in ACH activities, including new products and use of new technologies**
- **The TPSP Reports of Examination that cover ACH services products provided to the institution by the TPSP and, as available, the Shared Application Software Review (SASR) of the TPSP's ACH product**

Board and Management Oversight

Risk Framework

2. Consider whether the appropriate oversight structure and processes have been established, including:

- **Audit**
- **Framework for onboarding and periodic review of ACH customers and third parties, including TPPPs**
- **Monitoring reports for ACH**
- **Training programs for internal employees and customer education on ACH**
- **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 ACH operations. Consider the following:

- **Scope**
  - **Segregation of duties**
  - **Acceptable methods of ACH originations**
  - **Customer onboarding and ongoing credit and other monitoring**
  - **Customer agreement requirements**
  - **Customer security requirements for transfer of information**
  - **Customer exposure limits**
  - **Use of third parties, including TPPPs**
  - **Direct access by customers to the ACH operator**
  - **Originator return monitoring processes**
  - **ODFI services performed**
  - **Same-day ACH**
  - **For RDFIs, funds availability for customers**
  - **Change management processes**
  - **Customer credit lines**
  - **Business continuity and incident response**
  - **Alignment with NACHA Rules requirements**
  - **International ACH transactions**
  - **Alignment with Operator (Federal Reserve, EPN), correspondent, or TPSP requirements**
  - **Exceptions**
- **Review and approval practices for policies and procedures**
- **ODFI contracts/agreements**

4. Review the ACH credit analysis and risk rating summaries of several customers. Confirm the institution's analysis aligns with the current ACH policies and procedures.

Risk Assessment

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

- **Credit risk**
- **TPSP risk**
- **Direct access risk**
- **Operational risk, including cyber risk**
- **How changes in the channels by which ACH instructions are accepted or a substantial increase in ACH volume are incorporated into the risk assessment**

Key Controls
Operational/Logical/Physical Controls

6. Determine whether operational, logical, and physical controls are commensurate with the level of risk for ACH transactions. Consider the following:
• **Segregation of duties among those who establish access rights, originate ACH files, and approve ACH files**
• **Limit structure for ACH operations staff**
• **Configuration options offered by ACH operator, correspondent, or TPSP**
• **Time-of-day restrictions for instruction input**
• **Identity and access management**
  o **Authentication procedures and requirements**
  o **Privileged access management**
• **Adequacy of insurance relative to transaction limits**
• **Fraud detection and anomalous activity monitoring tools**
• **Hardware and software inventory**
• **Reconciliation using independent information sources**
• **NACHA Rules operational requirements**
• **Processes and monitoring, including management reports on ACH origination and returns and thresholds, including for unauthorized reasons**
• **Process in place to analyze RDFI transactions (e.g., key metrics)**
• **Range of allowable customer ACH transfer initiation channels**
• **Customer agreements stipulating security procedures for ACH customers**
• **Variety of security procedures used**
• **Customer exposure limits (single and multi-day)**
• **Customer education provided on use and importance of security procedures and other controls in addressing fraud due to endpoint security risks**
• **Customer transaction activity monitoring provided by third parties**

7. Assess whether changes to ACH configurations (including third-party origination configurations), process flows, and security control parameters are regularly reviewed and follow a formal change management process.
8. Interview or observe ACH operation staff perform log on, authentication, and execution of a transaction. Determine whether processes conform with policy.

9. 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.
10. 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
11. Assess network controls for primary and backup systems used for ACH transactions. Consider the following: • **Security monitoring for anomalous activities** • **Hardware and software used for sending payments is included in vulnerability assessments and patch management programs**
12. Determine whether customer transactions generating anomalous activity alerts are monitored and reviewed.
Business Continuity Management (BCM)
13. Evaluate whether ACH 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**
14. Confirm testing includes a range of scenarios that are high impact, but plausible.
End of Core Analysis