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

SUPPLEMENTAL JOB AID – ACH (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 ACH activities.

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

Review Considerations:

- ✓ Policies and procedures that address the onboarding and ongoing monitoring of ACH customers and the origination and receipt of ACH transactions.
- ✓ Monitoring reports that address ACH activity (e.g., customer origination volume and value reports, return rate reports, exception reports that show anomalous activity or operational issues, Key Risk Indicator (KRI) / Key Performance Indicator (KPI) reports).
- ✓ Examination and other findings that affect ACH operations.
- ✓ Audit tracking reports with ACH issues identified and remediation status.
- ✓ ACH security requirements of Operators or third parties (e.g., FedLine Security and Resiliency Assurance Program documentation)

Items to Consider:

- ✓ Management, with the board's oversight, has identified the types of ACH customers and transactions for which the FI will provide origination services. For example, the FI may originate for Third-Party Payment Processors (TPPPs), or the FI will originate certain types of ACH transactions (e.g., international ACH transactions).
- ✓ A written framework (e.g., policies, procedures, customer analysis document), under which the FI reviews new customers for ACH origination including the frequency of review of customer relationships and activity (e.g., monthly, yearly).
- ✓ ACH monitoring reports, including those that address the FI's customers (including any TPPPs). Consider the following:
  - Trending over time for origination volume and value (by month, quarter, and year).
  - Return rates by overall returns and by return types (e.g., returns for unauthorized or administrative reasons), and exception reports.
  - Confirm process for appropriate levels of management review and escalation and frequency of reporting.

Potential Questions to Consider:

- ✓ Does the FI originate for TPPPs? If so, do ACH policies and procedures address TPPPs?
- ✓ Does the FI have regular training for its employees and customers on ACH responsibilities and operations? How does the FI communicate new NACHA Rules requirements to employees and customers, particularly those that affect ACH operations?
- ✓ Has the FI established control testing for ACH transactions?

Procedure 3-4 – Policies and Procedures

Introduction: Consider whether the FI's ACH policies and procedures reflect the complexity and volume of the FI's ACH 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 NACHA Rules, Operator, and third-party service provider (TPSP) requirements.

Review Considerations:
- ✓ ACH policies and procedures.
- ✓ ACH data and payment flow and process diagrams. If the FI does not have diagrams, use descriptions.
- ✓ Sample customer due diligence documents.
- ✓ Sample customer ACH credit analysis and risk rating summaries.
- ✓ Sample agreement/contracts between the ODFI and its Originator customers and between the ODFI and a TPPP (if the FI originates for TPPPs).

Items to Consider:
- ✓ Data flow diagrams, customer due diligence documents, and credit risk summaries align with existing policies and procedures.
- ✓ For ODFIs, exception-processing procedures, include steps to handle transaction activity that is outside of policy for customer ACH origination (e.g., origination greater than exposure limits). For RDFIs, processes are in place to return ACH entries within appropriate time frames.
- ✓ ACH policies and procedures are reviewed periodically (e.g., annually, when new products or technologies are implemented or other conditions occur that necessitate a review such as a new NACHA Rule) and include an established approval process.
- ✓ Agreements address types of ACH activity the FI allows to be originated, information security requirements for data transmission, customer exposure limits and other controls, roles, responsibilities, processes and procedures, and performance standards for customers.
- ✓ ACH agreements are consistent with the FI's policies and procedures and address current NACHA Rules.
- ✓ Policies and procedures are in alignment with the requirements of the ACH Operator(s), correspondent, or TPSP agreements/contracts.
- ✓ Policies and agreements address how the FI will engage with the TPPP (i.e., if the FI originates for TPPPs).
- ✓ Policies and procedures address authentication procedures and requirements (i.e., log on requirements), and return monitoring processes.

Potential Questions to Consider:
- ✓ What is the process the FI goes through to review policies and procedures when new ACH services are offered (e.g., same-day ACH)?
- ✓ What is the FI's process for evaluating new customers against policies and procedures, including any origination for TPPPs?
- ✓ What conditions trigger a review of ACH agreements or of policies and procedures?

Procedure 5 – Risk Assessment

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

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

Review Considerations:
- ✓ Risk assessments associated with ACH activities. These assessments can be stand-alone or ACH elements considered in a risk assessment with a broader focus.

Items to Consider:
- ✓ ACH risk assessment reflects the current operating environment and the services offered.
- ✓ Risk assessment incorporates any changes in channels by which ACH instructions are accepted, and any significant increases in ACH volume or new ACH products and services.
- ✓ Management reviews ACH activity holistically across business lines and activities.
- ✓ Management incorporates any additional risks related to any TPPP or direct access relationships into the FI's risk assessment.

Potential Questions to Consider:
- ✓ How does the FI conduct an ACH risk assessment? Does the FI conduct an internal assessment itself or contract with an external party to perform the ACH risk assessment?
- ✓ How does the FI assess the risk of new ACH products, services, or technology?
- ✓ Does the FI allow any customers to transmit ACH transactions directly to the ACH Operator without going through the FI's risk processes (i.e., direct access), and how are risks assessed?

Decision Factor 2 – Key Controls

Procedure 6-10 – Operational/Logical/Physical Controls

Introduction: Consider whether the FI's operational, logical, and physical controls are commensurate with the level of risk posed by the FI's ACH transactions.

Relevance: An adequate layered-control environment will mitigate risks from internal and external threats. Weak or inadequate controls could result in several types of risk, including the risk of the occurrence of events such as cyber-attacks, internal fraud, and ultimately customer and FI losses.

Review Considerations:
- ✓ User and privileged access reports for ACH.
- ✓ FI reports that show customer names and exposure limits, and ACH activity reports that show exceptions over exposure limits by customer.
- ✓ Management reports on ACH activity overall (key metric analysis) and by customers, returns and thresholds (e.g., total returns, returns for unauthorized reasons, and returns for administrative reasons).
- ✓ Relevant minutes from groups that discuss ACH issues, including exceptions.
- ✓ Screen shots or other documentation that show which key configuration options are offered by ACH Operator(s), correspondents, or TPSPs were chosen.
- ✓ Observe or interview ACH operations staff conducting activities such as logging in, authenticating, executing, and reconciling transactions.
- ✓ 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 from another vendor.
- ✓ Insurance coverage requirements for ACH.
- ✓ ACH receipt reports for RDFIs.
- ✓ Audit report findings related to operational, logical, and physical controls.
- ✓ Description or explanation of the allowable customer ACH transfer initiation channels (e.g., digital banking, text, telephone, and in-person).
- ✓ Customer transaction activity monitoring reports including those provided by third parties.
- ✓ Observe or interview ACH operations staff addressing security procedures and controls used to verify customers.
- ✓ Sample of ACH origination agreements, including any with TPPPs.

Items to Consider:

- ✓ Policies, procedures, risk assessments, and credit analyses concerning customer exposure limits.
- ✓ Consult with an IT examiner working on inventories to ensure there are no hardware or software issues relating to ACH.
- ✓ 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 who have access rights, those who can originate ACH files, and those that can approve ACH files. If the FI does not have sufficient staff to accommodate segregation of duties, look for other compensating controls in place (e.g., dual approvals).
- ✓ Verification that ACH customers' exposure limits are set over both a single- and multi-day basis and reviewed periodically.
- ✓ 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.
- ✓ Authentication procedures (e.g., password requirements, password controls, callbacks) used by the FI.
- ✓ Appropriate reconciliation processes are performed with independent data sources.
- ✓ Implementation of any NACHA rule changes that affect operations.
- ✓ ACH origination agreements are consistent with the FI's ACH policies and procedures.
- ✓ Adherence to allowable security procedures for ACH customers. Examples of these procedures include callbacks, biometrics, dual controls, IP address registration, and others.
- ✓ 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).
- ✓ ACH origination files are securely transmitted (e.g., encryption methods).
- ✓ Third-party origination system configurations are established, in place, and regularly reviewed.

Potential Questions to Consider:

- ✓ Are the FI's user access rights that affect ACH transactions established under the least privilege principle?
- ✓ How are customer exposure limits for ACH origination set, monitored, and adjusted over time? Do system settings reconcile with policies and procedures?
- ✓ Does the FI utilize minimum balance requirements for any set of customers as an additional control?
- ✓ What is the process the FI uses to adjust the initially set configuration options offered by the ACH Operator, correspondent, or TPSPs?
- ✓ What types of authentication and out-of-band processes are used by the FI? For example, texting of a code for access or phone calls to validate files sent to the FI.
- ✓ 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?
- ✓ How does the FI ensure the operational requirements within the NACHA Rules are being followed, including amendments to those Rules?
- ✓ Explain or show (by conducting a walkthrough) how the ACH data-flow diagrams align with controls in place. For example, an end user should have an adequate username and password.
- ✓ How often are established limits within policies reviewed against controls within ACH systems?
- ✓ How has the FI changed the standard configurations of third-party origination systems to align with FI security principles?
- ✓ 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 ACH origination files?

Procedure 11-12 – Payment Network Controls

Introduction: Consider whether ACH transactions are securely transmitted.

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

Review Considerations:
- ✓ Annual information security or Gramm-Leach-Bliley Act (GLBA) report to the FI's board
- ✓ ACH data flow diagrams or discussions about data flows

Note: In this section, examiners are looking at payment network controls that specifically affect the ACH 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 ACH:
  - 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 payments platforms (workstations and servers) that impact ACH transactions included in the most recent penetration tests and vulnerability assessments? Were any exceptions noted?
- ✓ What types of encryption are used to protect ACH activity?
- ✓ Does management perform social engineering tests?
- ✓ Does management provide ACH payments training 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 ACH transactions?
- ✓ How does the FI ensure a comprehensive hardware/software inventory includes ACH-related hardware and software?

Decision Factor 3 – Business Continuity Management

Procedure 13-14 – Business Continuity Management

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

Relevance: Failure to establish adequate business continuity plans and processes could result in the inability to react quickly when an incident or outage occurs that impacts ACH processing and, consequently, expose the FI to financial and reputational losses.

Review Considerations:
- ✓ Business continuity, disaster recovery, and incident response plans that relate specifically to ACH operations.
- ✓ FI testing reports for these plans.

Items to Consider:
- ✓ Business continuity plans include contingencies for personnel as well as systems.

- ✓ Incident response plans specifically address ACH 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 ACH transaction operations from alternative site(s)?
- ✓ Has the FI tested ACH transaction operations from the FI's alternative provider?

End of Supplemental Job Aid – ACH (INTERNAL ONLY)