PaymentsFirst
Service • Education • Support

Audit and Risk Assessment
Module 5

Disclaimer

NACHA DIRECT MEMBER
Regional Payments Associations℠

This material is derived from collaborative work product developed by NACHA — The Electronic Payments Association and its member Regional Payments Associations.

This material is not intended to provide any warranties or legal advice, and is intended for educational purposes only. NACHA owns the copyright for the *NACHA Operating Rules & Guidelines*.

The information in this document and discussed during this presentation is the exclusive property of PaymentsFirst. It may not be copied, disclosed, or distributed, in whole, or part, without the express, written permission of PaymentsFirst.

Anti-Trust Laws

- PaymentsFirst is a not-for-profit organization and we closely adhere to all applicable laws and regulations.
- In accordance with Anti-Trust laws, we may not play any role in competitive decisions of members or their employees.
- During discussions with competitors and within the presentation materials we will and we ask participants to refrain from any discussion regarding pricing of products and services.

ACH Risk Assessment

- Participating DFIs must
  - Conduct assessment of the risk of ACH activities
  - Implement risk management program
  - Comply with requirements of Regulators

ACH Risk Assessment

- The Rules are not prescriptive regarding the following
  - Frequency of when risk assessment is conducted or reviewed
  - Content of risk assessment
  - Who is responsible (internal or external) for completing the assessment
  - How risks may be rated or evaluated
- If your regulator has not provided direct guidance to your program, you may wish to review documents from your regulatory agency or from the Federal Financial Institution Examinations Council

ACH Risk Assessment

- Federal Financial Institution Examinations Council
  - A formal interagency body empowered to prescribe uniform examination principles including the following entities
    - Board of Governors of the Federal Reserve System (FRB)
    - Federal Deposit Insurance Corporation (FDIC)
    - National Credit Union Administration (NCUA)
    - Office of the Comptroller of the Currency (OCC)
    - Consumer Financial Protection Bureau (CFPB)
  - Additional input is gathered from the State Liaison Committee and other state or association level supervisory groups

ACH Risk Assessment

- Regulatory resources to consider when planning to conduct your assessment
  - OCC 2006-39: https://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html
  - FFIEC Retail Payment Systems Booklet: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems.aspx
  - Related guidance documents from the FFIEC or your primary regulator

ACH Risk Assessment

- Purpose and overview
  - Assessments should be designed in accordance with the risk tolerances and preferences of the organization's highest levels of oversight (Boards of Directors, Supervisory Committees, etc.)
  - An institution may choose to accept certain amounts of risk due to their goals and objectives or may identify areas where risk must be reduced by the application of controls

ACH Risk Assessment

- Risk tolerance
  - How much risk your institution is willing to accept in your ACH program
- Risks
  - Parts of your ACH program that could cause harm or loss (financial or reputational) to your financial institution if not managed properly, often evaluated by the probability and severity of the occurrence
- Controls
  - Policies, procedures or other safeguards put into place to reduce the amount of risk posed to your institution

ACH Risk Assessment

- Your institution can develop your own rating system
  - Check with other departments or your compliance are to see if you have a standard rating scale or guide
    - Numbering system
    - Letter grades

ACH Risk Assessment

- Rating and reports should identify potential gaps in risk management that could indicate the need for additional controls
  - Remember each organization's risk tolerance will be different
  - Work with other colleagues and departments in your company to determine what yours is as you approach ACH Risk Assessments

 11

ACH Audit Requirements

- Governed by Appendix Eight of the *NACHA Operating Rules*
- Audit performed under the direction of
  - audit committee
  - audit manager
  - senior level officer
  - independent examiner or auditor

 12

ACH Audit Requirements

- Must be completed on an annual basis by December 31
- Proof of audit must be retained for six years
- NACHA may request proof of audit completion
  - Failure to produce satisfactory proof of audit may results in an enforcement action against the organization
  - No specific form of proof of audit is required (e.g. summary letter, audit committee minutes or memo, full audit report)

ACH Audit Requirements

- Appendix Eight is divided into four subsections
  - 8.1 – General Audit Requirements
  - 8.2 – Requirements for all DFIs
  - 8.3 – Requirements for RDFIs
  - 8.4 – Requirements for ODFIs
- Third-Party Senders' audit requirements may vary from relationship to relationship depending upon what functions they are performing on behalf of an ODFI

ACH Audit Requirements

- Receiving Depository Financial Institutions
  - Audit Requirements: 8.1, 8.2 & 8.3
- Originating Depository Financial Institutions
  - Audit Requirements: 8.1, 8.2, 8.3 & 8.4
- Third-Party Senders
  - Audit Requirements: 8.1, 8.2 8.4 items
    - 8.2.e, 8.4.l and 8.4.m do not apply for TPSs

ACH Audit Requirements

- Third-Party Service Provider on behalf of an RDFI (Receiving Point)
  - Audit Requirements: 8.1, 8.2 & 8.3
    - 8.2.e does not apply for Receiving Points
- Third-Party Service Provider on behalf of an ODFI (Sending Point)
  - Audit Requirements: 8.1, 8.2 & 8.4
    - 8.2.e does not apply for Sending Points
- Third-Party Service Provider on behalf of an Originator (but who is not a Third-Party Sender)
  - Audit Requirements: N/A

ACH Audit Requirements

- Appendix Eight includes certain testing functions that may be some of the most common areas on which an organization should focus
  - Not designed to limit the scope of a full audit of compliance with the Rules
  - May not be inclusive of every rule

ACH Audit Requirements

- General audit requirements also include references to areas beyond the *NACHA Operating Rules* which an institution may wish to review (not inclusive or required, but could include)
  - OFAC Compliance
  - ACH business continuity plans
  - Compliance with 31 CFR 210
  - ACH risk management policies

ACH Audit Requirements

- While Appendix Eight also does not include lists of how to categorize findings, exceptions where the institution has violated any Rules should be documented and summarized in accordance with the organization's audit policy and procedures
  - Sound business practice is to work to resolve any exception areas to prevent repeat findings in future audits
  - Rules do not require findings be fixed but external examiners, regulators or a Board of Directors may require the organization to build an action plan to remediate findings

Questions?

PaymentsFirst

www.paymentsfirst.org

866-993-3753

