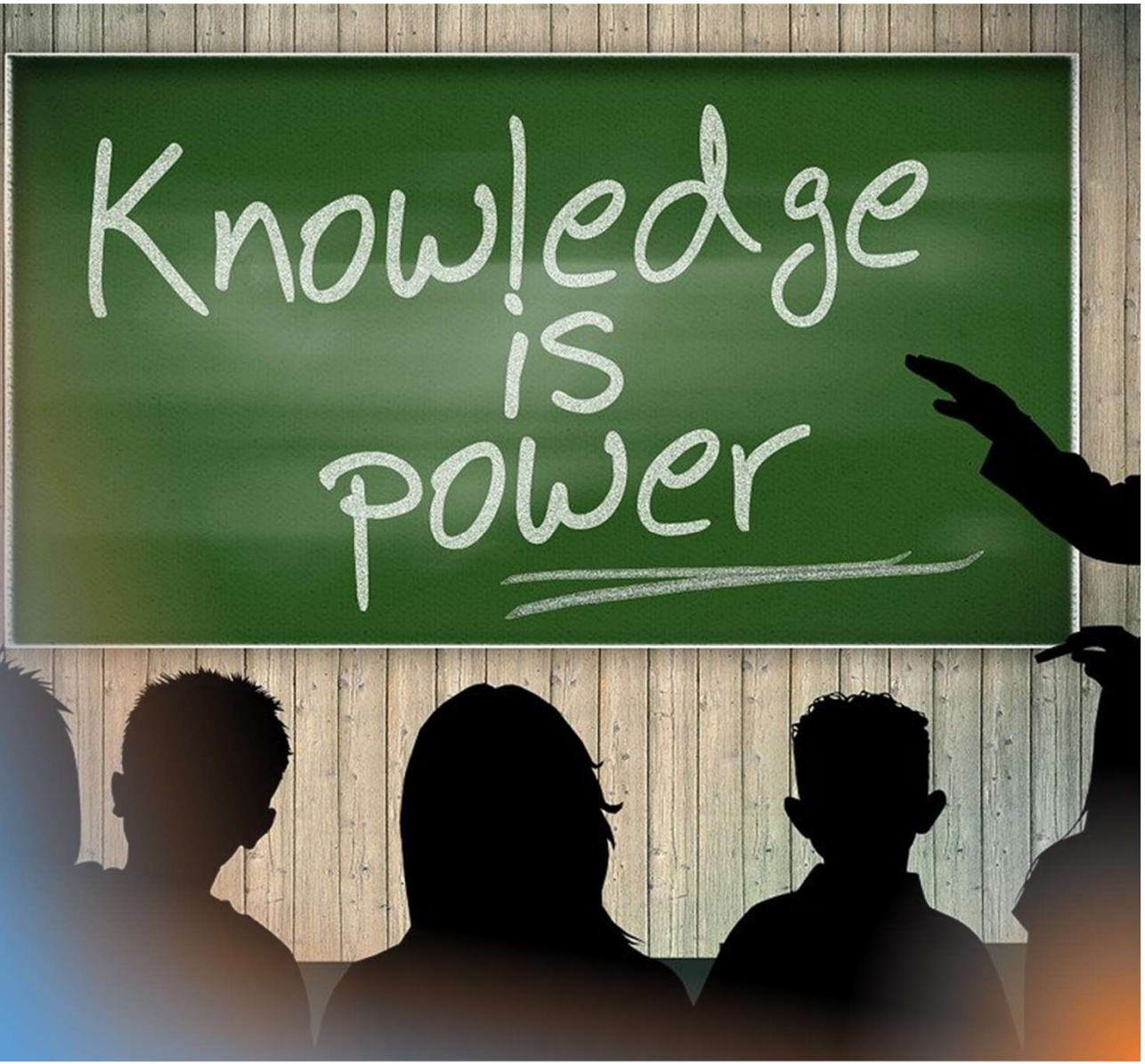


Knowledge is Power: Preparing for your ODFI Audit

Presented by:

Macha/PAR – Everything Payments - Everywhere

Jessica Lelii, AAP, APRP, NCP

www.macha.org

jlelii@macha.org

DISCLAIMER

Macha, through its Direct Membership in Nacha, is a specially recognized and licensed provider of ACH education, publications and support.

Payments Associations are directly engaged in the Nacha rulemaking process and Accredited ACH Professional (AAP) program.

Nacha owns the copyright for the Nacha Operating Rules & Guidelines.

The Accredited ACH Professional (AAP) and Accredited Payments Risk Professional (APRP) is a service mark of Nacha.

This material is derived from collaborative work product developed by Nacha and its member Payments Associations and is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This material is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein.

No part of this material may be used without the prior written permission of Macha/PAR.

ACH Audit Requirement

- All participating DFIs must conduct an audit of their compliance with the ACH Rules
- Participating DFIs must retain proof of completion for six (6) years
- Nacha may request proof of completion of an audit, at any time
  - DFI will have ten (10) banking days to provide documentation
  - Failure of a Participating DFI to provide proof of completion of an audit may be considered a Class 2 Rules Violation

2024 Nacha Operating Rules & Guidelines

Section VI-Special Topics

Chapter 56 Rules Compliance Audits

What?

Nacha Operating Rules	31 Code of Federal Regulation 210	Uniform Commercial Code 4A	OFAC (Office of Foreign Assets Control)
FFIEC Examination Handbook-Retail Payment Systems	Regulation E	Regulation CC	The Green Book

When?

The Rules Compliance Audit must be conducted by December 31 of each calendar year

Why?

REQUIREMENT OF THE NACHA RULES

AVOID FINES

IMPROVE OPERATIONAL EFFICIENCIES AND LOWER PROCESSING COSTS

ENHANCE ACH QUALITY AND CUSTOMER SATISFACTION

MANAGE RISK AND MINIMIZE LOSS

How?

- The Rules do not prescribe a specific methodology
- RDFIs should rely on guidance from their auditors for specific auditing practices and procedures

Audit Methods

Interview Personnel

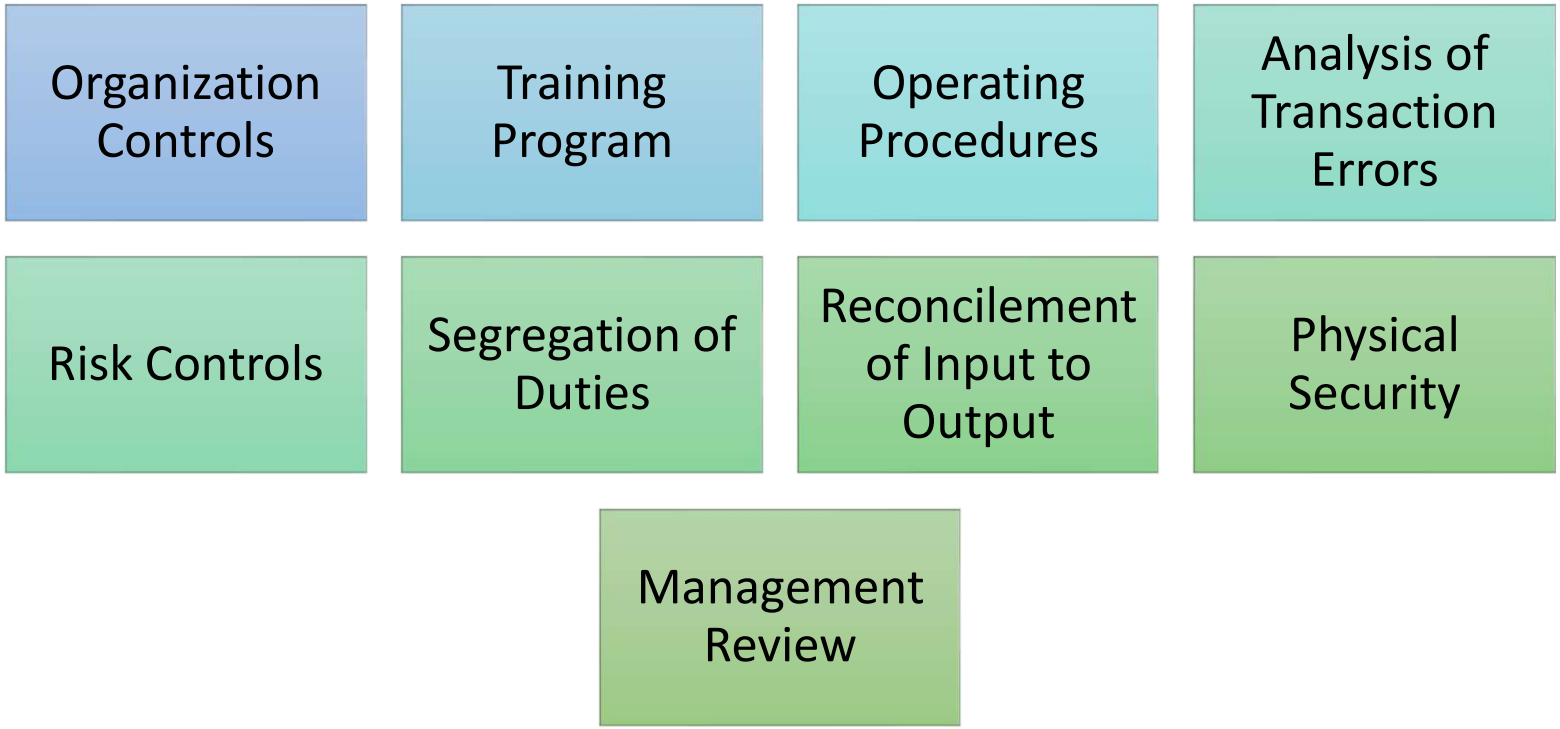
Sampling

- Random data samples
- May wish to cluster transactions by common characteristics before selecting samples so that you are certain to address all audit requirements

Testing

- Follow transactions
- Follow procedures

Internal Controls



ACH Audit Checklist

- Account Disclosures
- ACH Policies
  - Receipt
  - Origination Risk
  - OFAC
- Written Procedures
  - Do procedures accurately reflect your policies?
- Organizational Chart of Chain of Command for ACH Department
- Number of Employees involved in processing ACH
  - Dual control

ACH Audit Checklist

- Core Processing System/Internal Software updates
- Balancing reports and daily statements
- Rules violations
- Mergers or Acquisitions
- ACH Operator (FRB or EPN)
- Operator Advice

ACH Audit Checklist

- Third-party processor
- Staff training
  - AAP
  - APRP
- Physical access controls and passwords
- Contingency/Disaster Recovery Plans
- Record Retention

ACH Origination Audit Checklist

- How many Originators?
- Origination delivery system
- ACH Agreements
- Originator/Third-Party Sender education
- Processing schedule/Holiday schedule

ACH Origination Audit Checklist

- Do you originate…
  - Loan payments
  - Business to Business transfers
  - Consumer to Consumer transfers
    - P2P
    - A2S
  - Consumer to Business transfers
    - Bill payment

ACH Origination Audit Checklist

- Do you have exposure limits?
  - How often are they reviewed?
- Do you allow online initiated ACH transfers?
  - What are your transaction limits?
- How do you authenticate online banking users?
- Do you allow online account opening?
  - How are the accounts funded?

Audit Verification

Reference: Article One, Subsection 1.2.2

- Verify that an audit was completed in the previous year
- Verify that issues raised during the previous audit were corrected
- Audit reviewed by board of directors?

ODFI Rules Compliance

Verification of Originator/Third-Party Sender Identity

Reference: Article Two, Subsection 2.2.1

Does the ODFI use a commercially reasonable method to verify the identity of the Originator or Third-Party Sender that enters into an Origination Agreement with the ODFI?

If a Third-Party Sender relationship exists, does the Third-Party Sender use a commercially reasonable method to verify the identity of each Originator?

Origination Agreements

Reference: Article Two, Section 2.2.2.1, 2.2.2.2, 2.5.8.3

Do Origination Agreements:

- bind the Originator or Third-Party Sender to the Rules?
- authorize the ODFI to originate entries on behalf of the Originator or Third-Party Sender?
- expressly prohibit entries that violate laws of the United States?
- address any restricted types of entries?

Origination Agreements

Reference: Article Two, Section 2.2.2.1, 2.2.2.2, 2.5.8.3

Do Origination Agreements:

- address termination or suspension of the agreement?
- address the ODFI's right to audit the Originator's or Third-Party Sender's compliance with the Agreement and the Rules?
- address IAT entries?
  - Allocation of gains losses and the assumption of risk for foreign exchange conversion
  - Rights and responsibilities of the ODFI regarding erroneous entries
  - Compliance with foreign laws or payment system rules regarding authorization

Sending Point Agreements

Reference: Article Two, Subsection 2.2.2.3

Has the ODFI entered into an agreement with a Sending Point that transmits entries on the ODFI's behalf to an ACH Operator?

ODFI Risk Management

Reference: Article Two, Subsection 2.2.3 – 2.2.4

Does the ODFI:

- perform due diligence on Originators and Third-Party Senders?
- assess the risk of each Originator's and Third-Party Sender's ACH activity?
- establish, implement and periodically review exposure limits?
- establish and implement procedures to monitor return activity across multiple settlement dates?

ODFI Risk Management

Reference: Article Two, Subsection 2.2.3 – 2.2.4

Does the ODFI:

- enforce restrictions on the types of entries that may be originated?
- enforce exposure limits?
- obtain approval of Direct Access Debit Participants from the ODFI's board of directors, committee of the board of directors, or its designee?

Prenotifications

Reference: Article Two, Subsection 2.6

Does the ODFI transmit Prenote Entries in accordance with the requirements of the Rules?

Does the ODFI ensure that live entries are not initiated when a prenote is returned?

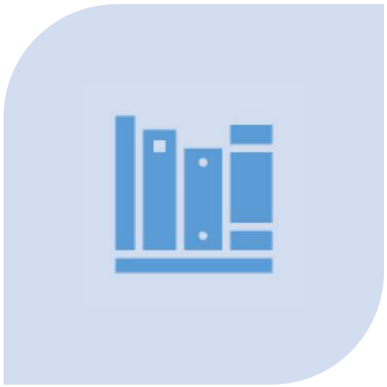
Return Processing

Reference: Article Two, Subsection 2.13.1, 2.13.6.1, 2.13.6.3

Does the ODFI:

- accept return entries and extended return entries that are timely and comply with the Rules?
- transmit dishonored return entries within five banking days after the settlement date of the return entry?
- accept contested dishonored return entries?
- use return reason codes in an appropriate manner?

Reinitiation of Returned Entries



REFERENCE: ARTICLE TWO, SUBSECTION 2.13.4

DOES THE ODFI TRANSMIT REINITIATED ENTRIES IN ACCORDANCE WITH THE REQUIREMENTS OF THE RULES?

Notifications of Change

Reference: Article Two, Subsection 2.12.1 – 2.12.2

Does the ODFI:

- provide information relating to NOCs and corrected NOCs to the Originator or Third-Party Sender within two banking days of the settlement date of the NOC or corrected NOC?
- provide information relating to NOCs and corrected NOCs for CIE and credit WEB entries to any Originator initiating such entries on behalf of a consumer Originator?
- transmit refused NOCs within 15 days of receipt of an NOC or corrected NOC?

Proof of Authorization

Reference: Article Two, Subsection 2.3.2.7, 2.5.18.6, 2.3.3.3

Does the ODFI:

- provide to the RDFI, upon request, the original, a copy, or other accurate record of the consumer receiver's authorization within 10 banking days of receipt of the request, without charge?
- provide to the RDFI, upon request, contact information for the Originator (including at minimum the Originator's name and phone number or email address) within 10 banking days of receipt of the request, without charge?

Proof of Authorization

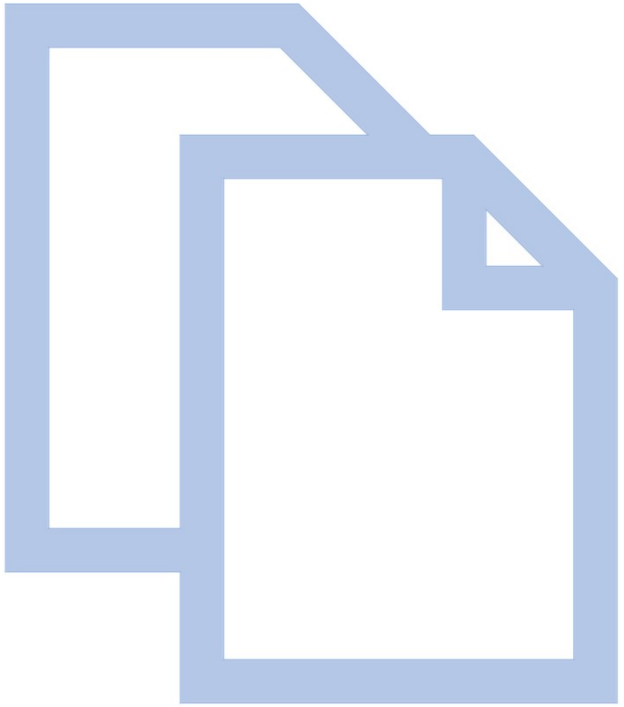
Reference: Article Two, Subsection 2.3.2.7, 2.5.18.6, 2.3.3.3

When the ODFI agrees to accept the return of an entry in lieu of providing proof of authorization, does the ODFI:

- provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within 10 banking days of providing the confirmation to the RDFI?
- provide the RDFI with the original, copy, or other accurate record of the consumer receiver's authorization within 10 banking days if the RDFI submits a subsequent written request for proof of authorization?

Copies of Source Documents (ARC and BOC)

- Reference: Article Two, Subsection 2.5.1.5 and 2.5.2.5
- Does the ODFI provide a copy of the front of the receiver's eligible source document used to initiate the ARC or BOC entry within 10 banking days upon receiving written request?



UCC4A

Reference: Article Two, Subsection 2.3.3.2

Does the ODFI provide the Originator with proper notice to ensure compliance with UCC Article 4A with respect to ACH transactions for non-consumer entries?

Reversals

Reference: Article Two, Section 2.8 – 2.9

Does the ODFI transmit reversing files and reversing entries in accordance with the requirements of the Rules?

Periodic Statement

Reference: Article Two, Subsection 2.5.4.2 and 2.5.17.8

- Does the ODFI provide or make available to the Originator all required information with respect to the consumer account of the Originator of a CIE entry or credit WEB entry?

Return Rate Reporting

- Reference: Article Two, Subsection 2.18.2
- Does the ODFI report return rate information on an Originator or Third-Party Sender, when requested to do so by Nacha?

Direct Access

Reference: Article Two, Subsection 2.18.1

Has the ODFI:

- registered its Direct Access status with Nacha?
- provided required statistical reporting for a Direct Access Debit Participant?
- notified Nacha of any changes to the information previously provided with respect to a Direct Access Debit Participant?

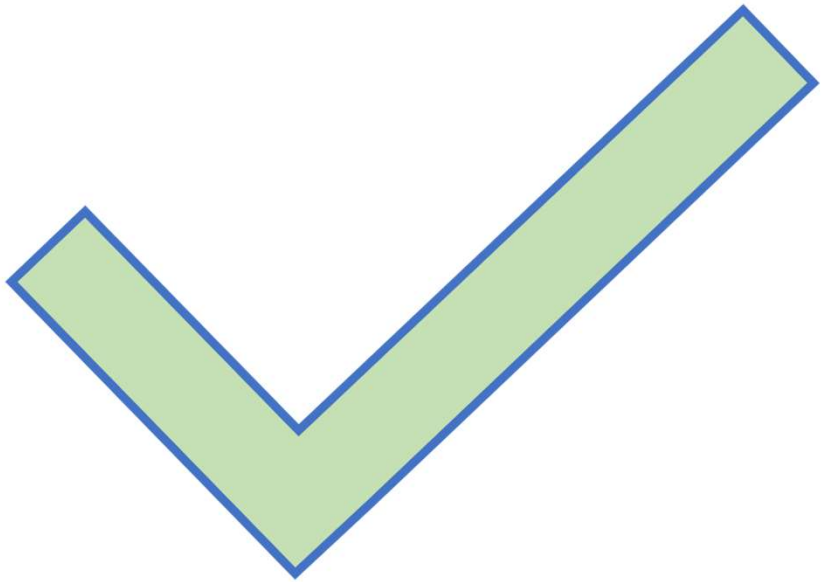
Third-Party Sender Registration

Reference: Article Two, Subsection 2.18.3

Has the ODFI:

- registered its Third-Party Senders with Nacha and updated, as necessary, any such registrations? Or…
- stated to Nacha that it has no Third-Party Senders?

Other Considerations

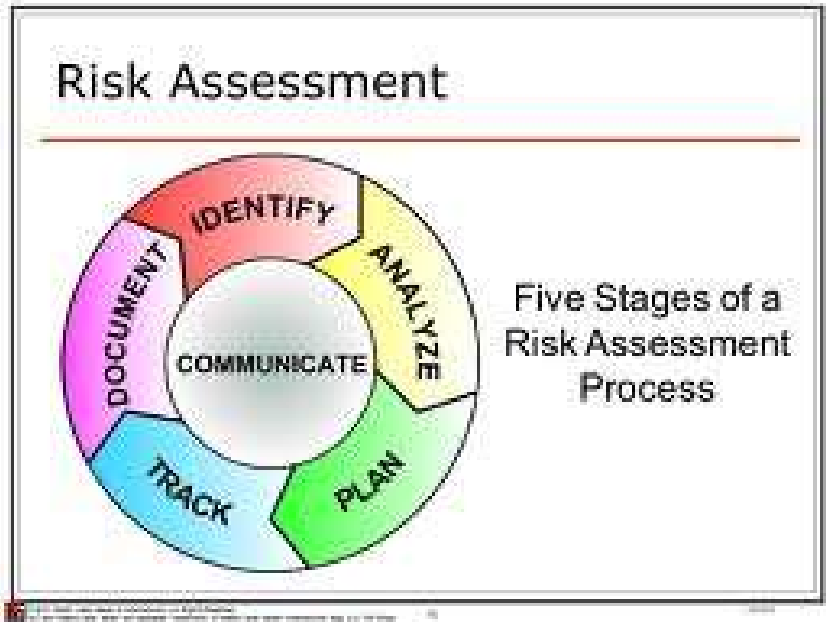


ACH Risk Assessment

- Reference: Article One, Subsection 1.2.4
- All participating DFIs and Third-Party Senders must –
  - conduct, or have conducted, an assessment of the risks of its ACH activities
  - implement, or have implemented, a risk management program based on their risk assessment
  - comply with the requirements of its regulator(s) with respect to their risk assessment and risk management program

ACH Risk Assessment

- Have your risk assessment and risk management program been reviewed by your board?
- How often do you re-assess?
- Have all identified areas of risk been addressed?



Data Security

Reference: Article One, Section 1.6

Each non-consumer Originator, participating DFI, Third-Party Service Provider and Third-Party Sender must establish, implement and update security policies, procedures and systems.

These policies, procedures and systems must:

- protect the confidentiality and integrity of Protected Information
- protect against anticipated threats or hazards to security or integrity of Protected Information
- protect against unauthorized use of Protect Information that could result in substantial harm to a natural person

Large volume, non-FI Originators must protect DFI account numbers by rendering them unreadable when stored electronically.

Data Security

Reference: Article One, Section 1.7

Banking information related to an entry transmitted via an unsecured electronic network must use Commercially Reasonable level Encryption

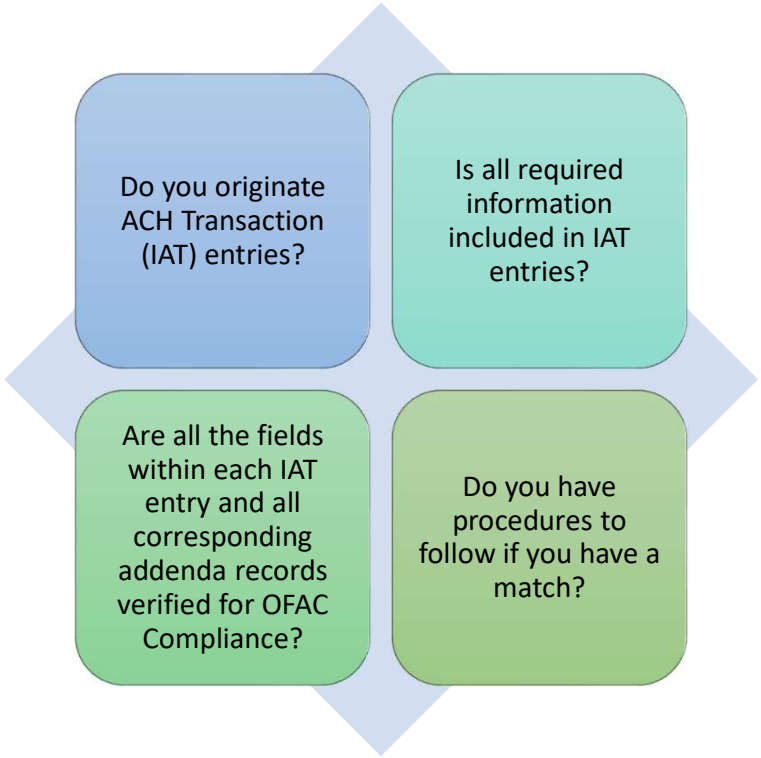
Network Administration Fees

Reference: Article One, Section 1.13

Has the financial institution paid all annual and per-entry fees to the National Association?

The Schedule of Fees is part of the Rules and is established by the Board of Directors of the National Association.

International ACH Transactions (IAT)



Regulation E – Error Resolution

Regulation E provides rules that protect consumers regarding errors in electronic transactions.

If a consumer claims that an error has occurred, the financial institution is required to take action by:

INVESTIGATING the error

Providing a RESOLUTION to the consumer

COMMUNICATING the resolution to the consumer

Regulation E – Error Resolution Log

Resolution process for each error should be logged

ACH Unauthorized/Improper returns should be logged

Written Statement of Unauthorized Debit (WSUD)

Notice of Final Credit for those transactions requiring a WSUD

Macha PAR

Questions

AAP™
Accredited
ACH Professional

APRP™
Accredited Payments
Risk Professional

Continuing Education Credits

Knowledge is Power:
Preparing for your ODFI Audit
September 2024

This session is worth 1.8 credits

(keep this slide for your records)

Macha PAR