Deconstructing the ACH Audit: How Do I Minimize My Risk In ACH

Presented by:
Andrew Barlow, AAP, NCP  
EVP, WACHA-The Premier Payments Resource

Jen Wasmund, AAP, CTP, NCP  
Enterprise Payments Risk Manager, Capital One
Disclaimer

- NACHA owns the copyright for the NACHA Operating Rules & Guidelines
- This material is derived from collaborative work product developed by NACHA — The Electronic Payments Association, its Direct Financial Members 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
- This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein
As the NACHA Operating Rules continue to evolve, creating faster and smarter payments, is your annual audit keeping pace? Organizations have traditionally relied on Appendix Eight to guide their audit activities, but as payments have become more complex, so has the relationship between compliance and risk management. Join our speakers for analysis of real-life stories from the field, analyzing the risks that exist below the surface of your ACH audit report. Attendees will walk away with actions they can quickly implement to enhance their ACH audit to ensure their organization employs a risk-based methodology to properly review their ACH activities.
Agenda

- ACH Audit
- Who is responsible
- General Rules
- Rights and Responsibilities of ODFIs, Their Originators and Third-Party Senders
- Rights and Responsibilities of RDFIs
- Federal Government Payments
ACH Audit—More than ACH Rules

- NACHA Operating Rules
- 31 Code of Federal Regulations 210
- Regulation E
- Regulation CC
- Uniform Commercial Code 4A
- Office of Foreign Assets Control (OFAC)
- OCC 2006-39, ACH Risk Management
- FFIEC-IT Handbook, Retail Payment Systems
Risk Based Audit or Risk Assessment

- A risk based audit--A risk-based approach will seek to identify higher risks with the greatest potential impact to my operations and focus on those risks through sampling and testing.

- A risk assessment--analyzes what can go wrong, how likely it is to happen, what the potential consequences are, and how tolerable the identified risk may be.
Who has to complete an ACH Audit

- Receiving Depository Financial Institutions (RDFI)
- Originating Depository Financial Institutions (ODFI)
- Third-Party Service Providers
- Receiving Point
- Sending Point
- Any entity that performs a function of ACH Processing on behalf of a Participating RDFI or ODFI
- Third-Party Senders
Article One-General Rules
Retention of ACH Data

- Retain all ACH record documentation for six years
  - Entries
  - Returns
  - Audits

- Must be able to accurately reproduce any electronic data

- Must retain data from previous mergers and acquisitions
Risk Assessment

- Must conduct, or have conducted, an assessment of the risks of its ACH activities

- Implemented a risk management program on the basis of such an assessment
Security Requirements

- Commercially Reasonable level Encryption for all entries received over the internet

- Participating DFI and Originators/Third-Party Senders have established, implemented and updated security policies, procedures and systems with respect to initiation, processing and storage of Entries

- In 2020, some Non-financial institution Originators, Third-Party Service Providers and Third-Party Senders will have to protect account number when stored electronically
Article Two—Rights and Responsibilities of ODFIs
Binding Agreements

- Has an agreement been executed with each company and financial institution for whom the financial institution originates binding them to US law and the ACH Rules?

- Has the agreement been reviewed by legal counsel?

- Has the agreement been updated for regulatory and rule changes?
Security Procedures for File Transmission

- Verify that your ACH agreement has language detailing the security procedures to receive ACH files/entries from your originators
  - Is this comprehensive?
  - Has it been updated as systems and processes have changed?
  - Have both parties agreed that these procedures are commercially reasonable?
Exposure Limits

- Review internal procedures to determine that exposure limits are established for each Originator.
- Exposure limits should be reviewed periodically.
- Entries initiated by Originators are to be monitored relative to the exposure limits across multiple settlement dates.
- The restrictions on types of SEC code of originated entries must be enforced.
- Procedures for monitoring limits and what happens if established limits are exceeded.
Authorizations

- Review authorizations for each type of debit entry originated
  - Is it clear and understandable?
  - Is a copy made available to the receiver?
  - Is there revocation language documented?
  - Is the authorization retained for two years from the termination of the authorization?
  - Can the authorization be provided to the RDFI within 10 Banking days?
Notifications of Change

- Review records to ensure changes specified within the Notification of Change are made within six days or before the next entry is initiated.
Return Entries

- Review records to ensure entries are not Reinitiated improperly.
  - An entry can be Reinitiated only if:
    - The entry was returned for insufficient or uncollected funds
    - The entry was returned for stop payment and Reinitiation has been separately authorized by the receiver; or
    - The originator has taken corrective action to remedy the reason for the return
  - Verify if the entry is being Reinitiated, the Company Entry Description field is changed to “RETRY PYMT”
Identity Verification

- Verify the ODFI has utilized a commercially reasonable method to verify the identity of each Originator or Third-Party Sender that enters into an Origination Agreement with the ODFI.

- Verify that when an ODFI has a relationship with a Third-Party Sender rather than with an Originator directly, also verify that the Third-Party Sender has utilized a commercially reasonable method to establish the identity of each Originator that enters into an Origination Agreement with the Third-Party Sender.
ODFI Reporting Requirements

- Verify the ODFI has reported information on each originator or TPS if you have been requested to by the national association
  - 0.5% Unauthorized Return Rate
  - Are you tracking returns?
ODFI Requirements of Originators and Third-Party Senders

- Verify that the ODFI has kept Originators and Third-Party Senders informed of their responsibilities under these rules. This section also applies to your financial institution for your own origination.
Third-Party Senders

- Require Third-Party Senders to provide proof of completion of a Rules compliance audit to its Participating DFI to fulfill request from NACHA

- Verify that the Third-Party Senders have provided a detailed list of all underlying merchants to the ODFI

- Verify the Third-Party Sender(s) have a Third-Party Sender agreement
Originator Obligations – WEB Credits

- Standard Entry Class Code
  - WEB
- Company Name Field
  - P2P Service Provider Name
- Company Identification
  - P2P Service Provider ID Code
- Company Entry Description
  - Identifies as Person to Person (P2P)
- Individual Identification Number
  - Sender’s Name
Originator Obligations – WEB Debits

- Commercially Reasonable Fraud Detection System
- Commercially Reasonable Verification of the Receiver’s Identity
- Commercially Reasonable Verification of Routing Numbers
- Annual Audit Requirements
  - Must have adequate levels of:
    - Physical security to protect against tampering, theft or damage;
    - Personnel and access control to protect against unauthorized access; and
    - Network security to ensure secure capture, storage, and distribution
Originator Obligations

- TEL Obligations
  - Verify for TEL entries the Originator is complying with:
    - Authorization requirements
    - Verification of identity of receiver
    - Verification of routing numbers
  - Single vs Recurring
    - Single: Recording or Notice
    - Recurring: Recording AND Notice
Article Three—Rights and Responsibilities of RDFIs
Credit Availability

- PPD credit entries made available to the RDFI by 5:00 p.m. the banking day prior to settlement date, are available to the Receiver for withdrawal no later than the opening of business on the settlement date.
  - Effective 9/20/2019--Credit entries that are not Same-Day credits, made available to the RDFI by 5:00 p.m. the banking day prior to settlement date, are available to the Receiver for withdrawal no later than the opening of business on the settlement date.
- Same Day Credits must be posted in accordance to Subsection 3.3.1.2.
- Debit entries are not posted prior to the settlement date.
Account Statement Content

- Verify that the RDFI sends or makes available as part of the account statement for consumer customers information from transactions as dictated by the ACH Rules and Regulation E
  - Verify your system has been updated to comply with all current ACH rules and SEC codes
Exception Handling

- Verify that returned entries (including debit entries to a corporate account returned as unauthorized) are received by the RDFI’s ACH Operator by its deposit deadline for the return entry to be made available to the ODFI no later than the opening of business on the second banking day following the Settlement Date of the original entry.

- Verify that dishonored return entries received by the RDFI are handled appropriately, and that contested dishonored return entries and corrected returns are initiated in a timely manner. Verify that the RDFI utilizes Return Reason Codes and Contested Dishonored Return Reason Codes that accurately describe the reason for the return.
Stop Payments

- Verify that the Stop Payment Orders are acted upon appropriately
  - Recurring Payment
  - Stop Instructions 3 banking days prior to debit
  - Single payment or Non-consumer payment
  - RDFI needs Reasonable time to act on Stop order
  - Stop one payment or all future payments based on consumers intent (Reg E)
- Verify that the reason for stop payment is not an error resolution entry
Written Statement of Unauthorized Debit

- Review records and procedures to ensure that signed Written Statement of Unauthorized Debit (WSUD) forms are obtained from consumers before returning entries for Return Reason Codes R05, R07, R10, R37, R51 and R53
- Returned in appropriate time frames
- Made available to ODFI upon request
International ACH Transactions

- Verify all received International ACH Transactions (IAT) entries are scrubbed against the Office of Foreign Asset Control (OFAC) lists
  - This should be done prior to posting entries to accounts

- Verify all IAT entries returned to the ODFI are rescreened against OFAC lists
Federal Government Payments
Reclamations and Deceased Accountholders

- Verify there are written procedures for steps to be taken upon learning of death of accountholder?
  - DNE Processing
  - Constructive knowledge of death
  - All benefit payment/all accounts
  - Front line staff
- Verify appropriate use of R14 (Death of Rep Payee) and R15 (Death of Beneficiary or Account Holder)
QUESTIONS
Contact information

Andrew Barlow
abarlow@wacha.org

Jen Wasmund
jennifer.wasmund@capitalone.com