PaymentsFirst
Service • Education • Support

Risk Management / Compliance
Module 4

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.

Types of Risk

- Credit Risk
- Exposure Risk
- Operational Risk
- Fraud Risk
- Systemic Risk
- Compliance Risk

Security Requirements

- Non-Consumer Originators, Participating DFIs and Third-Party Service Providers must
  - Protect confidentiality and integrity of Protected Information until destruction
  - Protect against anticipated threats
  - Protect against unauthorized use

 5

Data Breach

- NACHA Board of Directors Interim Policy Statement on ACH Data Breach Requirements
  - Loss, theft or unauthorized access of consumer data by or from any ODFI or Originator or Third-Party Service Providers using the ACH Network

 6

Credit Risk

- Occurs when a party to a transaction cannot provide the necessary funds, as contracted, in order for settlement to occur

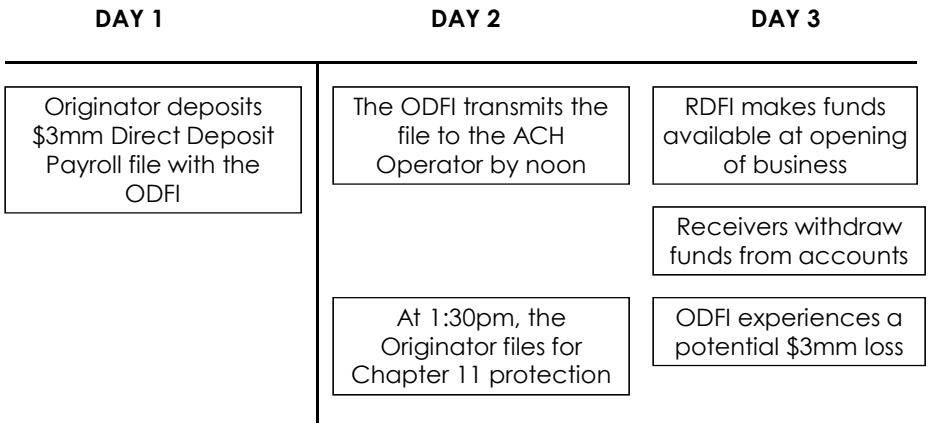
 7

ODFI Credit/Exposure Risk

- ODFI Credit origination
  - Risk is the Originator will fail to fund the ODFI for credits
  - ODFI is exposed from the time the ACH File is transmitted until the ODFI receives funding from the Originator/Third-Party Sender
- ODFI Debit origination
  - ODFI is exposed to risk from the time the funds from the debit entries are released to the Originator/Third-Party Sender until the statute of limitations expires under applicable state law
  - NACHA Operating Rules allow for ease of return via the Network within the 60-day timeframe

 8

Exposure Risk – Next-Day Credit File



Same Day ACH Credit File

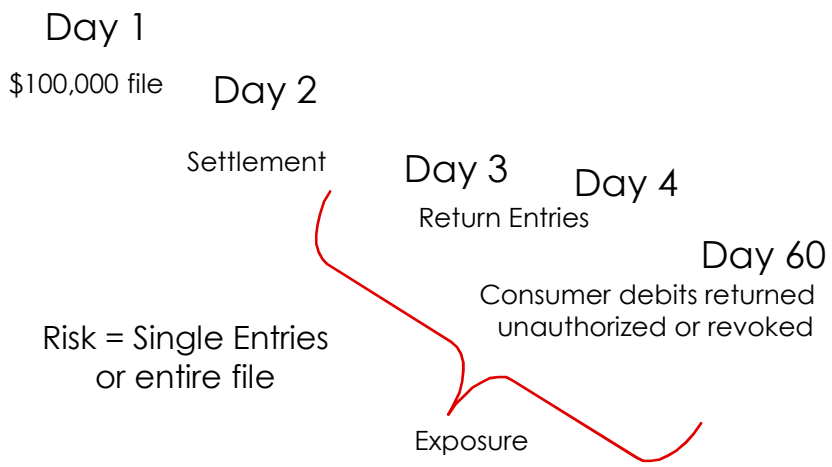
- Credit File of Same Day ACH Entries
  - Effective Entry Date of October 18
  - Submitted to the ACH Operator within Same Day ACH processing window
  - File contains four Entries
    - 2,000.00
    - 20,000.00
    - 1,000.00
    - 6,000.00
- Settlement of the Credit Entries will occur on October 18

Same Day ACH Credit File

- Effective entry date stays the 18th, the settlement date will be the 18th. Suggested changes:
- Offset Debit File
  - Settlement Date is October 18 right? Wait!
    - Although debits are eligible for processing, the total offset debit exceeds the per entry limit of $25,000
  - Settlement for the debit will occur after October 18 regardless of when the Debit File is sent on October 18
    - The Settlement Date for the debit will be pushed to the next eligible settlement window
- Risk alert
  - Credits will settle before the funding Debit File
  - Funds may not be available for debits despite final settlement of credits

PaymentsFirst

Exposure Risk - Debit File



PaymentsFirst

ODFI Credit/Exposure Controls

- Determine creditworthiness and exposure limits for Originators and Third-Party Senders and review periodically
- Assess the nature of the Originator's and Third-Party Sender's activity and the risk it represents
  - Through prefunding, ODFI may significantly reduce credit risk
- Monitor the Originator's and Third-Party Sender's origination and returns across multiple settlement dates

ODFI Credit/Exposure Controls

- Establish clear policies and procedures to deal with "over limit" transactions
- Perform ACH Rules Compliance Audit annually
- Address in Originator and/or Third-Party Sender agreement
  - Restrictions on the types of ACH transaction that may be originated
  - Right to terminate or suspend
  - Right to audit

RDFI Credit/Exposure Risk

- RDFI credit receipt
  - Risk is related to the time of settlement finality granted by the ACH Operator
  - Reduced by Same Day ACH
- RDFI debit Return
  - Failure to meet return time frames may result in a loss for the RDFI

Operational Risk

- Occurs when a transaction is altered or delayed due to an unintentional error
  - Hardware failure
  - Software failure
  - Telecommunications failure
  - Power failure
  - Human error
  - Staffing problems
  - Disaster or civil unrest

Operational Risk Controls

- Maintain systems
  - Hardware
  - Software (update software versions and patches as needed)
- Personnel
  - Employ skilled staff
  - Continuous training
  - Cross-train

Operational Risk Controls

- Processing
  - Account for Files
    - Balance Files after each step of processing
  - Authenticate Originator or Third-Party Sender
  - Establish and comply with processing schedules
  - Use positive acknowledgements for transmitted Files
  - Monitor key dates
  - Reconcile dollar amounts and item counts
  - Maintain audit trails

Operational Risk Controls

- Contingency
  - Alternative telecommunications; protect operations with uninterruptible power supply
  - Develop and test disaster recovery plan
    - Protect data
    - Restrict access
    - Back up copies
    - Provide offsite storage

Fraud Risk

- Occurs when a payment transaction is initiated or altered in an attempt to misdirect or misappropriate funds by any party to the transaction
  - Outside parties
  - Intruders
  - Combination of both

Who Commits Fraud?

- Employees
  - Dissatisfied, disgruntled, desperate or dishonest
- Interlopers
- Originators/Receivers
  - Dishonest or unscrupulous

Fraud Risk Controls

- Physical security
- Data security
- Application security
- You tell me…provide some examples of each of these three

Fraud Risk Controls

- Operational controls
  - File and dollar controls for each processing step
  - Ability to reconstruct series of events to analyze the transaction
  - Out of band transaction verification
  - Out of band alerts for unusual activity
  - Require dual control

Fraud Risk Controls

- Educate Originators
  - Initiate ACH payments under dual control
  - Restrict functions for computer workstations and laptops used for online banking and payments
  - Monitor and reconcile accounts daily
  - Install commercial, up-to-date anti-virus and firewalls on all computers
  - Never access bank accounts at Wi-Fi hotspots (airports, Internet cafes, etc.)

Systemic Risk

- Occurs when one funds transfer system participant is unable to settle their commitments causing others to fail
- ACH Operators have established risk management procedures which help minimize the possibility of systemic financial institution failures due to ACH settlement

 25

Systemic Risk Controls

- ACH Operators monitor
  - File controls and dollar controls
  - ACH activity according to funding capabilities of ODFI
  - Finality
    - Reserve Bank next-day settlement is final for ACH credits and debits as of 8:30 a.m. ET
    - Two Same Day settlement windows added at 1:00 p.m. ET and 5:00 p.m. ET

 26

Compliance Risk

- Occurs when a party to a transaction fails to comply, either knowingly or inadvertently, with *NACHA Operating Rules*, applicable regulations, U.S. law and state law

Compliance Risk Controls

- Compliance constitutes the actions necessary for a financial institution to meet the requirements imposed
- ACH participants must be familiar with rules and regulations, including but not limited to
  - *NACHA Operating Rules*
  - EFTA and Regulation E
  - Regulation CC
  - Regulation D
  - 31 Code of Federal Regulations (CFR) Parts 203, 208, 210, 370
  - Uniform Commercial Code Articles 3, 4 and 4A
  - Bank Secrecy Act/Anti-Money Laundering
  - Right to Financial Privacy Act
  - OFAC
  - Federal Reserve Bank Operating Circulars

Additional Risk Considerations

- Ancillary Risk - Consequence of not managing previously discussed risks
  - Reputation Risk
  - Cross-Channel Risk
  - Counterparty Risk
  - Third-Party Relationships
  - Direct Access
  - High return rates
  - Remotely-Created Checks
  - Certain business types

Reputation risk

- The risk of adverse publicity and the possible resulting litigation or loss of business from an incident, event, or problem.

Cross-Channel Risk and Controls

- Cross-channel risk should be monitored to watch for fraud and credit exposure across various payment systems used by a single entity
- Exposure may occur as a result of
  - Individuals perpetrating fraud from external sources (e.g. corporate account takeover)
  - Internal fraud or intentional misuse of multiple payments system by the entity itself
- To reduce these risks, organizations should be aware of activity on payment systems beyond ACH to identify anomalies

Counterparty Risk

- Counterparty Risk is reduced by more frequent settlement
  - Financial institutions will have less exposure to potential settlement failure by another financial institution

Direct Access

- Originator, Third-Party Sender, or a Third-Party Service Provider transmits credit or debit Entries directly to an ACH Operator using an ODFI's routing number and settlement account
- ODFI warrants all transactions that enter the Network under its routing number
  - Transactions bypass ODFI monitoring & review

 33

Direct Access Controls

- Direct Access approval required by FI's Board or Board-level committee for new debit participant customers
  - Although not required by the *NACHA Operating Rules*, it is highly recommended that Direct Access credit relationships be approved by Board or Board-level committee

 34

Direct Access Registration

- Each ODFI must register its Direct Access Debit Participant status with NACHA
  - Acknowledge no Direct Access Debit Participants
  - Provide information about each Direct Access Debit Participant
    - Must report volume and return rate activity on a quarterly basis
- Must report any change in status, including terminations, to NACHA

Return Rate Levels

- Administrative Return Rate
  - The rate at which an Originator's or Third-Party Sender's debit Entries are returned for administrative reasons as calculated in accordance with the Rules
    - R02
    - R03
    - R04
- Administrative Return Rate Level
  - 3%

Return Rate Levels

- Overall Return Rate
  - The rate at which an Originator's or Third-Party Sender's debit Entries, excluding RCK Entries, are returned, regardless of reason, as calculated in accordance with the Rules
- Overall Return Rate Level
  - 15%

Return Rate Levels

- Unauthorized Entry Return Rate
  - The rate at which an Originator's or Third-Party Sender's debit Entries are returned on the basis that they were unauthorized as calculated in accordance with the Rules
    - R05
    - R07
    - R10
    - R29
    - R51
- Unauthorized Entry Return Rate Threshold
  - 0.5%

Return Rate Levels - Definition

- Calculation processes are the same two options that exist currently in 2.17.2

Method One

$$\frac{\text{\# of debits returned for 60 days or two months}}{\text{Total \# of debit Entries within the File(s) the original Entries were sent}}$$

Method Two

$$\frac{\text{\# of debits returned for 60 days or two months}}{\text{Total \# of debit Entries originated for the proceeding 60 days or two months}}$$

Calculations are computed for each Originator or Third-Party Sender

Return Rate Levels - Definition

- All rates apply to debits only, calculated over a 60-day or two month period
  - RCKs are exempt from the overall return rate level
- Threshold vs. levels will be handled differently by the Rules Enforcement Panel

Thresholds vs. Levels

Violation of the Unauthorized Entry Return Rate Threshold

- NACHA will notify the ODFI of a potential threshold violation at which time the ODFI will be required to provide requested information within 10 Banking Days
- If the ODFI determines the threshold was exceeded, a plan and timeline to reduce this activity within 30 days must be provided
- Once reduced, unauthorized Return activity must remain below the threshold for 180 days
- Failure to respond to, reduce or maintain the unauthorized Return activity may constitute a Class 2 Rules Violation

41

Thresholds vs. Levels

Violation of the Administrative or Overall Return Rate Levels do not follow the same pattern of activity

- Levels are designed to be more forgiving and exceeding a level may not require action to reduce the level or other steps as exist with the threshold process
- Instead, exceeding a level will result in a brand new inquiry process overseen by an industry review panel appointed by NACHA

42

Inquiry Process

- Requests for return rate information related to the Administrative or Overall Rates require a response within 10 Banking Days
  - ODFIs have the ability to respond and explain why the rate is above the 3% or 15% respectively
  - The industry review panel may determine the activity is acceptable and close the case or it may direct the ODFI to reduce the return rate(s)

 43

Inquiry Process

- Responses to a request for return rate information on a Return Rate Level do not state how much or what type of supplemental information should be included to justify activity
- The industry review panel will evaluate information across certain review criteria
  - Length of time in business, time as customer of FI
  - Total Originator/TPS volume and Return volume
  - Rules Violations, RDFI complaints, UDAAP complaints
  - Regulatory or legal investigation or actions
  - Third-Party Sender audit completion, if applicable

 44

Inquiry Process

- Additional considerations may be given to the type of industry and trends displayed by similar Originators
- Remember
  - An inquiry doesn't automatically mean a Rules violation, but you have to make your case!

High Return Rate

- Occurs when the rate of unauthorized returns rises above reasonable ratio
- Risk to confidence in ACH Network and loss to ODFI
- *NACHA Operating Rules* contain reporting requirement
  - Written request from NACHA when suspect that unauthorized return rate threshold exceeds .5%
  - Requires mitigation plan if exceeds .5%

Return Rate Levels

- Returns that exceed the rates will not automatically be a Rules violation
- Should be a trigger to review the Originator's or TPS's origination activity

High Return Rate Controls

- Know Your Customer (KYC)
- Know Your Customer's Customer (KYCC)
- Verify company following proper authorization policy
- Monitor return volume and ratio by company
- Originator training/education

Remotely-Created Check (RCC)

- Regulation CC defines RCC as a check that is not created by the paying bank and does not bear a signature
- FIs should note that a shift from ACH to RCC could indicate a potential problem with Originator

Risk Specific to Products

- Internet-Initiated/Mobile Entries (WEB)
  - Unique risk issues inherent to Debit Entries
    - Open, fast, anonymous
- Telephone-Initiated Entries (TEL)
  - Potential for misuse through origination of unauthorized payments
    - May be originated as a result of deceptive practices
    - Anonymity when no prior existing relationship

Internet-Initiated/Mobile Debit Entry Risk Controls

- Authentication
  - Used to verify Receiver identity
  - Must be commercially reasonable
  - Varies based on relationship with Receiver (new, existing, single, recurring)
- Verification of routing number
  - Minimize exceptions
  - Verify RDFI routing number validity using commercially reasonable method

Internet-Initiated/Mobile Debit Entry Risk Controls

- Fraudulent Detection System
  - Screening reduces potential for fraudulent Entries
  - Factors vary based on Entry value, type, relationship
  - Must be deployed regardless of payment size or type
- Annual security audit
  - Originator/Third-Party Sender must conduct annually
  - Ensure Entry & Receiver information security
    - Physical security – theft, tampering and damage
    - Personnel security – unauthorized access and use
    - Network security – secure capture, storage and distribution

Telephone-Initiated Entries Risk Controls

- Verification of identity of Receiver
  - Utilize commercially reasonable method
    - Database, directory, etc.
    - For example: name, address, phone number, account profile information
- Verification of routing number
  - Minimize exceptions
  - Verify RDFI routing number validity using commercially reasonable method

 53

Questions?

PaymentsFirst

www.paymentsfirst.org

866-993-3753

 54