



ODFI Roles and Responsibilities

PRESENTED BY:

MACHA/PAR

262-345-1245 OR

800-453-1843

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) 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

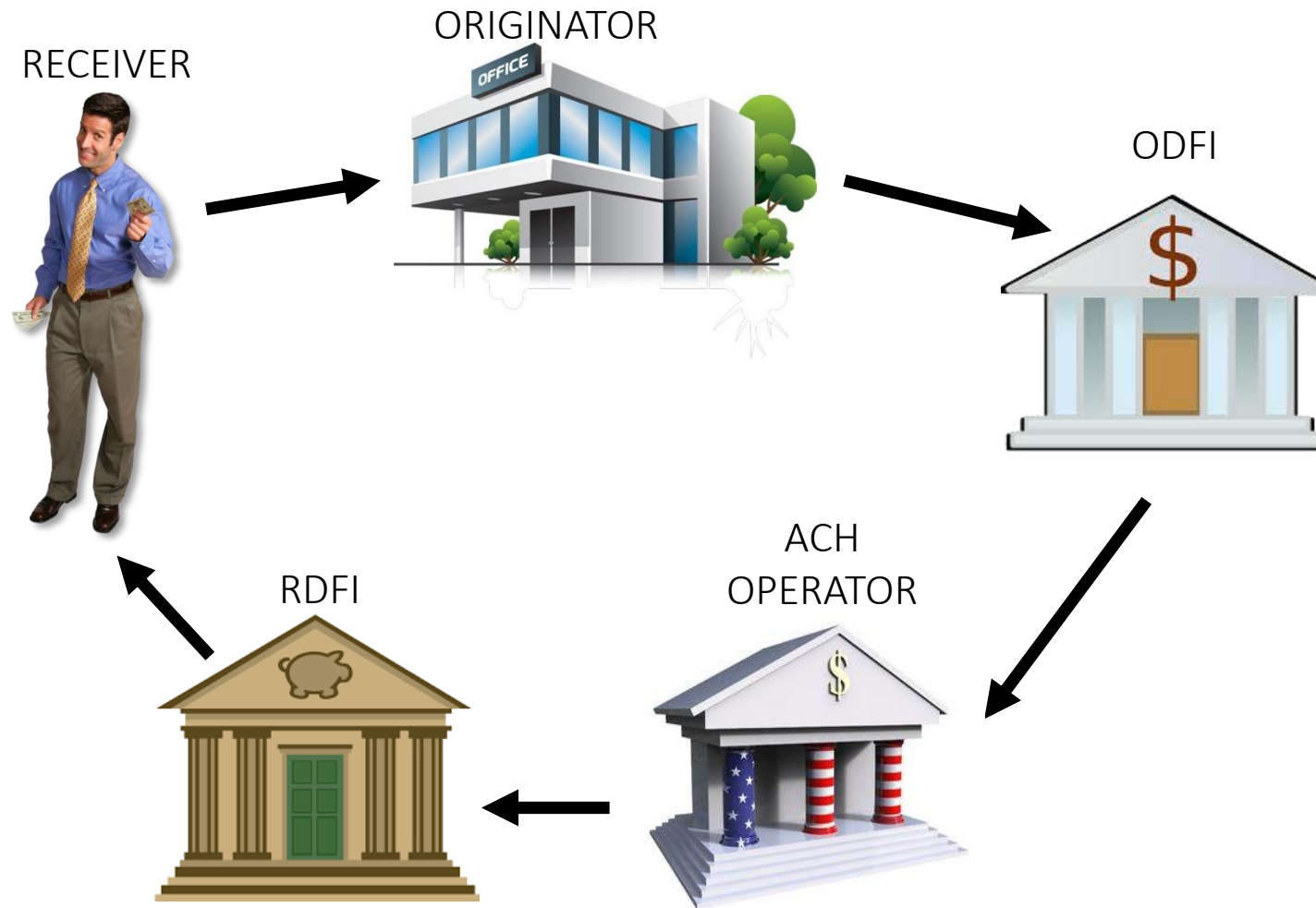
© 2024 Macha/PAR All rights reserved



Agenda

- ACH Transaction Flow
- ODFI Warranties
- ACH Risk Assessment
- ACH Origination Policy
- Agreements
- Third-Party Service Providers
- Third-Party Sender
- Third-Party Sender Registration
- Direct Access Registration
- ACH Contact Registry
- Exposure Limits
- Authorization
- Prenotifications
- Micro-Entries
- Effective Entry Date vs. Settlement Date
- Same-Day ACH
- ACH Originations
- Risk Management
- ACH Files
- Reversals
- Notifications of Change
- ACH Returns
- Reinitiated Entries
- Stop Payments
- Security Considerations

ACH Transaction Flow



ODFI Warranties

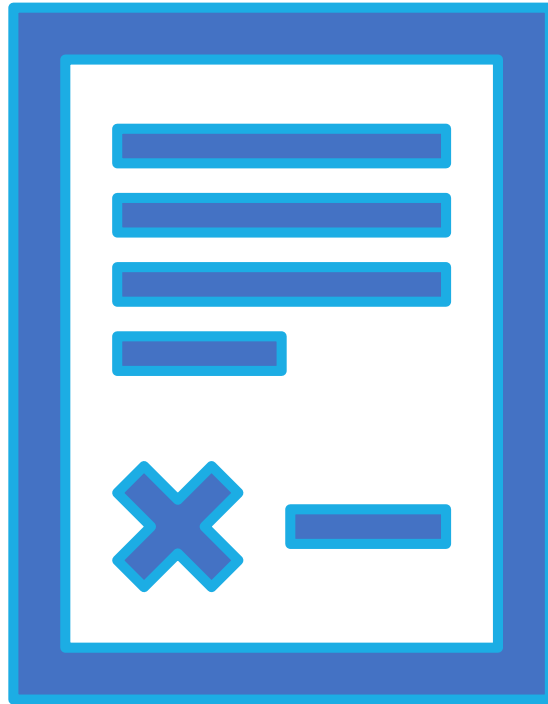
Article Two of the ACH Operating Rules

- Authorization by Originator and Receiver
- Timeliness of Entries
- Compliance With Other Requirements
- Revocation of Authorization
- Termination of Authorization by Operation of Law
- Transmission of ACH information via unsecured electronic networks



ODFI Warranties

- Verification of Identity of Originator/Third-Party Sender
- PIN Requirements
- Transmittal of Required Information
- Reclamation Entries
- Sending Points
- Audits/ACH Risk Assessments
- SEC code requirements



ODFI Warranties

Liability for Breach of Warranty

Simply...Each ODFI breaching any of the preceding warranties shall:

- Indemnify every other ACH participant and all claim, demand, loss, liability, or expense, including attorney's fees and costs that result directly or indirectly from the breach of warranty or the debiting or crediting of the entry to the Receiver's account.
- This indemnity also includes, in the case of a consumer account, the failure to comply with the EFTA or Regulation E.
- Pay any and all fines from ACH rules violations



ACH Risk Assessment

The Rules requires all participating DFI's, Third-Party Senders and Nested Third-Party Senders to conduct a risk assessment of their ACH activities, and to implement risk management programs based on the results of such assessments, in accordance with the requirements of their regulator(s)

ACH Risk Assessment



Assess the nature of risk associated with ACH activity;



Perform appropriate know-your-customer due diligence;



Establish controls for Originators, third-parties, and direct access to ACH Operator relationships



Have adequate management, information and reporting systems to monitor and mitigate risk

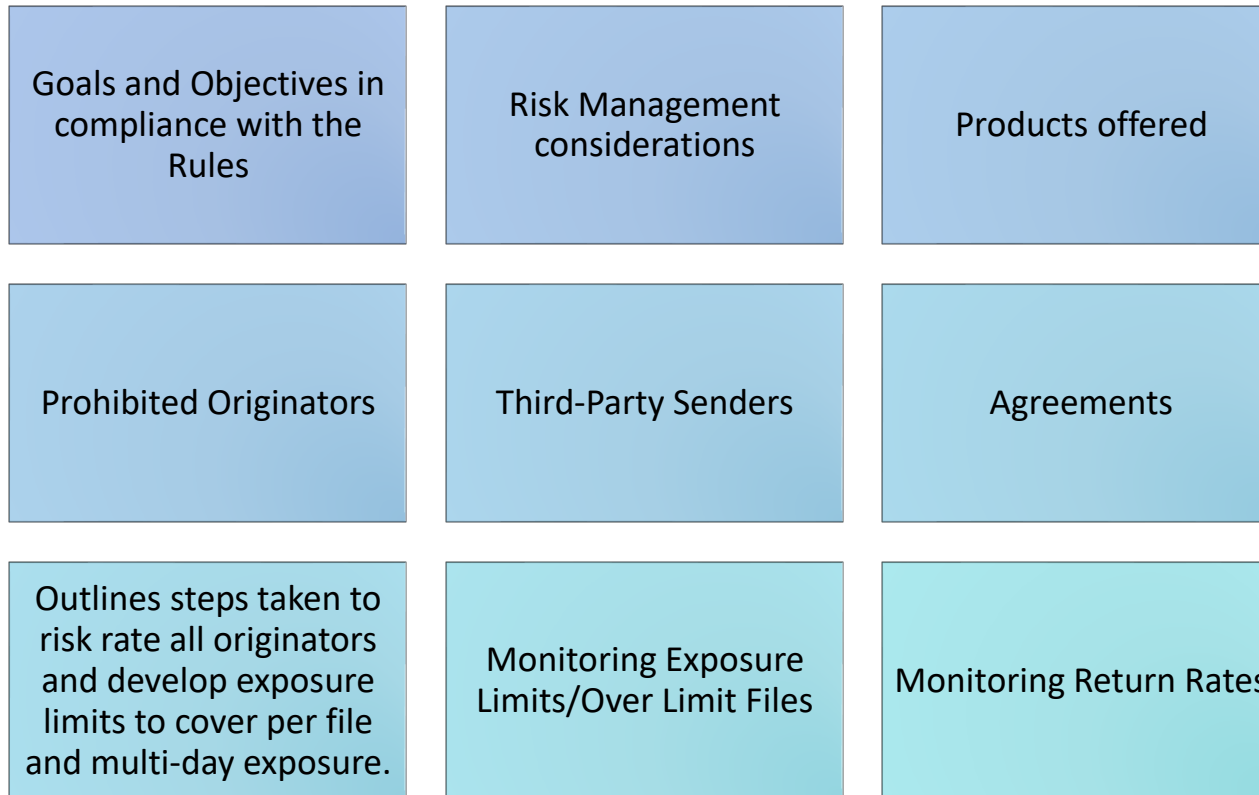
With that Said.... The FFIEC Guidance Says to...

Mitigate Fraud Risk through proper due diligence for all originators and strict adherence to **ACH** and **credit policies**

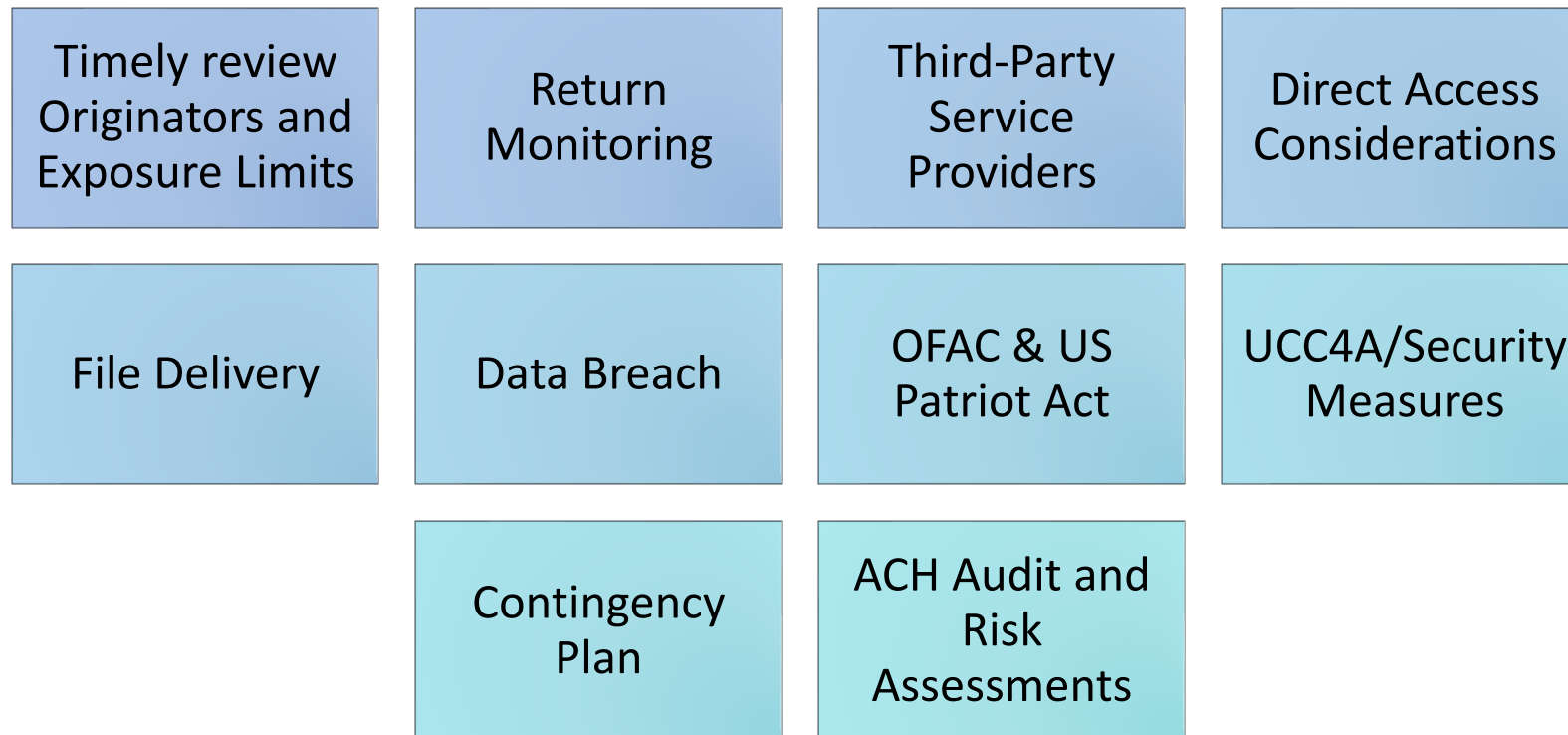
Manage Credit Risk by establishing **policies, procedures** and **limits** that acknowledge the risks originators bring to an ACH operation

Clear **policies and procedures** need to establish the proper control of these highly automated activities to manage the Operational Risk

ACH Origination Policy



ACH Origination Policy, (cont.)



Presenting.....



Sunset University

Joe's Gym



Smart Bank

Main Street CPA





Sunset University

A school of higher education who pays the professors on a weekly basis

Originator of Credit Entries

A payroll processing company called Main Street CPA processes the university's weekly payroll

Smart Bank is the ODFI



Main Street CPA

A payroll processing company

Forwards payroll files to the ODFI
on behalf of the Originators



Joe's Gym

A fitness center/spa who bills their members on a recurring monthly basis and converts checks received to ACH entries

Originator of Debit Entries

All ACH files are created by the staff of Joe's Gym

Smart Bank is the ODFI



Smart Bank

Smart Bank is an ODFI

Initiates debit entries from customers' accounts at other FI's to make loan payments at Smart Bank

Initiates debit or credit entries to customers' accounts at other FI's for deposit account transfers

Agreements



Originator/ODFI
Agreement



Third-Party Sender
Agreement



Third-Party Processor
Agreement



Agreement with the
ACH Operator

Originator/ODFI Agreements

The Originator and ODFI have entered into an agreement under which the Originator agrees to be bound by the ACH Rules and acknowledges that entries will not be initiated that violate the laws of the United States and OFAC

Originator/ODFI Agreements

DEFINES PARAMETERS OF RELATIONSHIP BETWEEN PARTIES

- Transmittal of Entries and Security Procedures
- Company Representations, Warranties and Agreements
- Financial Institution Obligations
- Company's account
- Exposure Limits
- Due Diligence
- Cancellation, Amendment of Entries
- Rejection of Entries
- Provisional Credit Notice
- Reversals
- Notice of Returned Entries and Notifications of Change
- Entries Returned as Unauthorized
- Return rates not to exceed Nacha's requirements
- Periodic Statements
- Fees
- Liability
- Rules Enforcement
- Inconsistency of Name and Account Number
- Rules Compliance Review-Right to Audit
- Miscellaneous – How to Terminate Agreement

Originator/ODFI Agreement Attachments

Delivery of Files

- Location
- Format
- Acknowledgement
- Timing
- Exposure Limits
- Notice by FI
- SEC Codes supported

Security Procedures

Fees (outlined in detail)

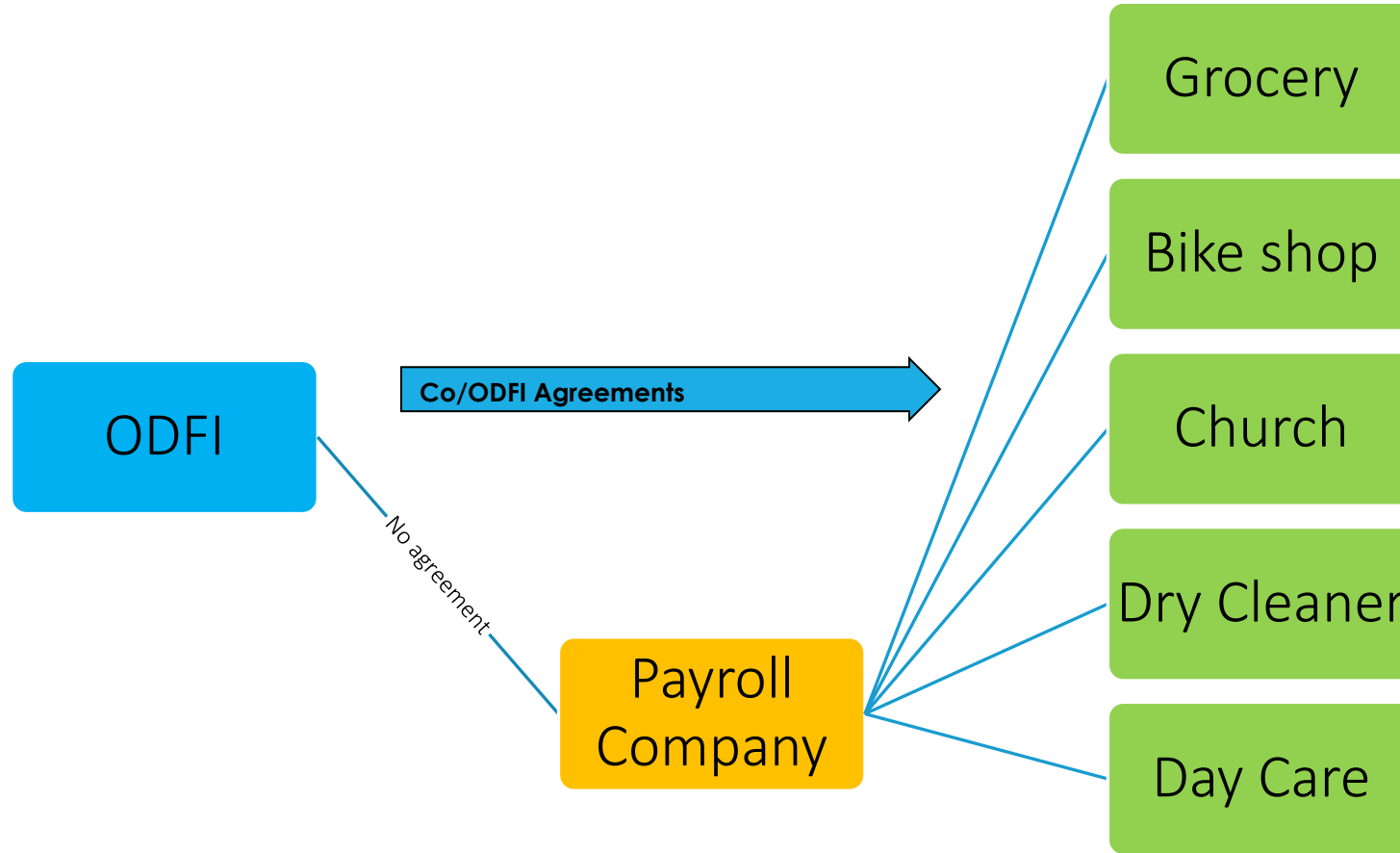
Authorized Representatives



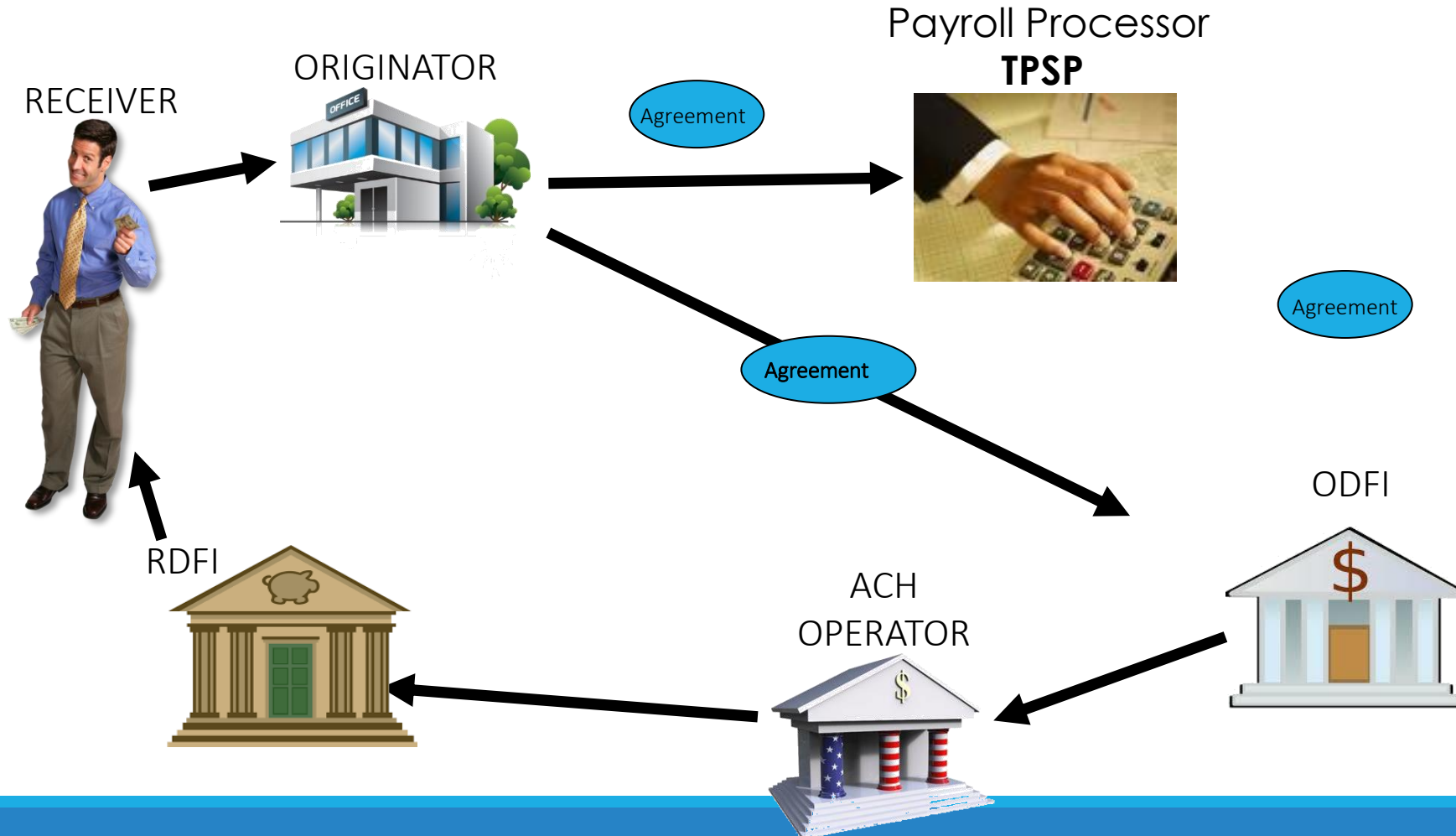
Third-Party Service Provider

An Organization that performs any functions on behalf of the Originator, ODFI or RDFI (not including the Originator, ODFI or RDFI acting in such capacity for such entries) related to the processing of entries, including the creation of the files or acting as a Sending Point or Receiving Point on behalf of a participating DFI. An Organization acting as a Third-Party Sender is also a Third-Party Service Provider.

Third-Party Service Provider



ACH Transaction Flow with Third-Party Service Provider





Liability

The Originating Depository
Financial Institution is **LIABLE** even
if a third-party service provider is
used!

Definition of a Third-Party Sender



A type of Third-Party Service Provider that acts as an intermediary in Transmitting Entries between an Originator and an ODFI, including through Direct Access, and acts on behalf of an Originator or another Third-Party Sender



A Third-Party Sender must have an Origination Agreement with the ODFI of the Entry



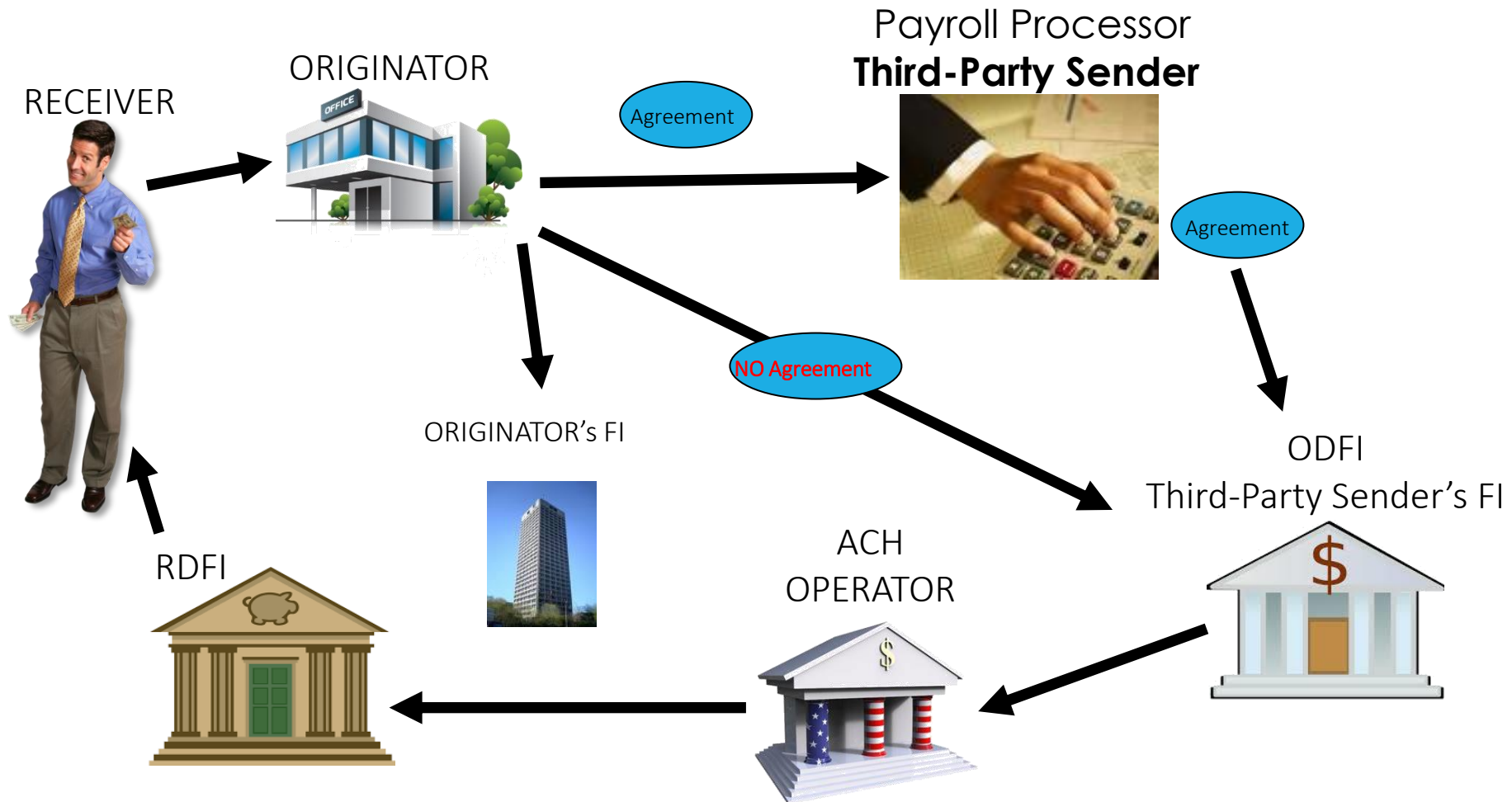
A Third-Party Sender is never the Originator for Entries it Transmits on behalf of another Organization

However, a Third-Party Sender of Entries may also be an Originator of other Entries in its own right.

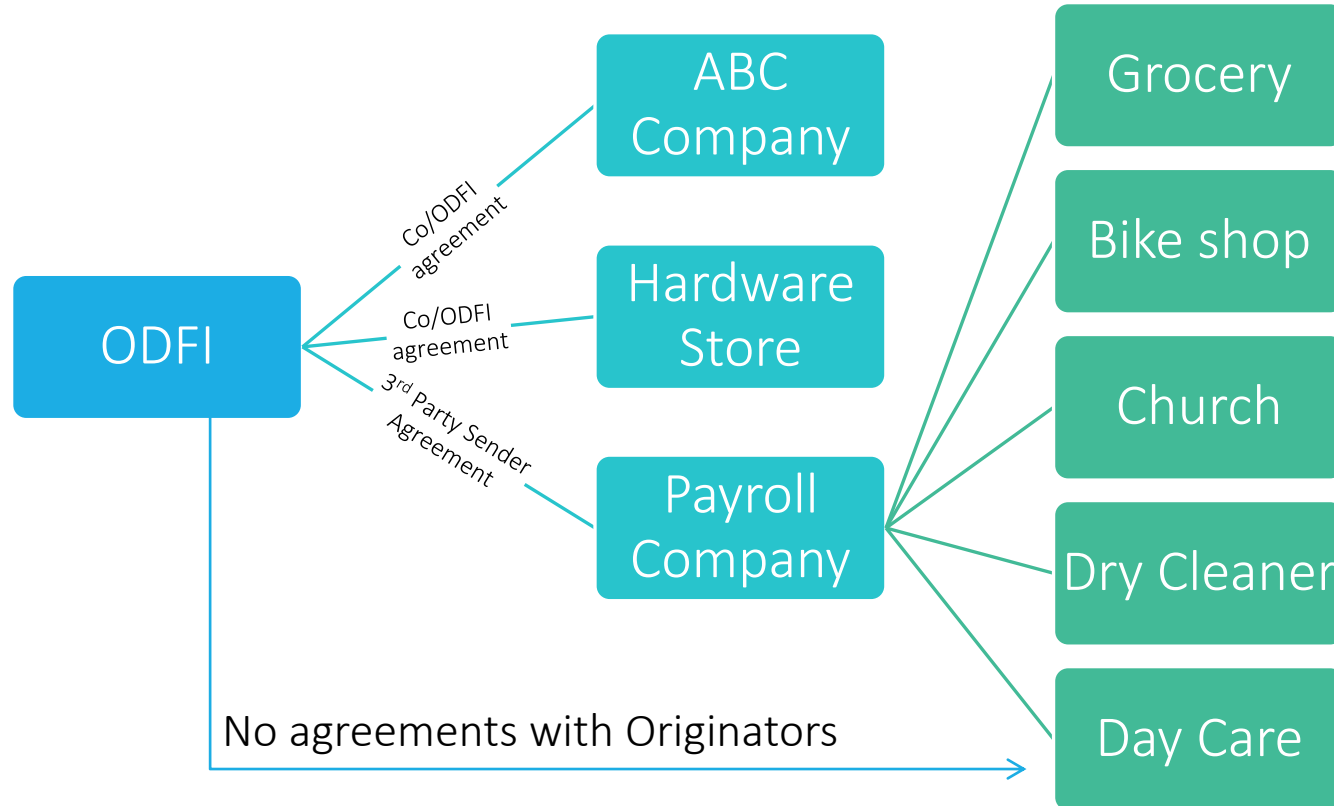
Why Use a Third-Party?

- Business/Corporate Originators
 - Outsourced business process-part of this being the ACH entry origination
 - Payroll
 - Receivables (Property Management)
- Originating Institutions
 - Initiates entries on behalf of the Originator and transmits to the TPS's ODFI
 - Simplifies the onboarding and processing process
 - Allows rapid growth without doing all the work

ACH Transaction Flow with Third-Party Sender



Third Party Sender



Third-Party Sender Risk Management

THE MOST IMPORTANT ITEM!!

- Know Your Customer

Due Diligence

- Company financials
- Payment history
- List of customers being processed
- Company principles and Beneficial ownership

Third-Party Sender Risk Management

- Payment velocity
- Normal Dollar value of files
- Return and other exception statistics
- Credit bureaus, BBB, D&B, etc.
- Nature of the businesses being processed for
- Written policy on onboarding and terminating Originators

Nested Third-Party Senders

- Definition: a Third-Party Sender that has an Origination Agreement with another Third-Party Sender to act on behalf of an Originator and does not have a direct agreement with the ODFI itself.
- Requirements of Origination Agreements to address Nested TPS
- ODFI required to attest in Risk Management Portal if Nested relationships exist
- ODFI warranties for chain of Nested TPS

Explicit requirement:

- Third-Party Senders and Nested Third-Party Senders must complete a Risk Assessment of their ACH Activity

Only applies if you **are** an Originating Depository Financial Institution and you **have** Third-Party Sender Relationships

Risk Assessments for Third-Party Senders

No Standard				
Credit, Operational, Fraud, Compliance, Reputational	ODFI Requirements – Article One & Two of Rules	CDD, Exposure Limits, Originator Authorization process, data security, ACH entry specific Rule	Guidance issued by financial institution regulators	PCI, TPPP industry groups, FFIEC & Third-Party Payment Processors

Contracts

What needs to be in there?

- Abide by the Rules – and Section 2.16 dealing with Third-Party Senders
- FI Liability and the Third-Party Sender's Liability
- Every transaction is appropriately authorized, and those authorizations can be reproduced when requested
- The Company Name field will be filled with the name of the ultimate originator
- The FI has the right to review the customer list of the Third-Party Sender on a regular basis
- FI's right to refuse to process for a specific customer
- The Third-Party Sender will manage and maintain exposure limits for all their Originators
- Attachments on security, pricing (and how you get paid), authorized signers, etc.

Contracts (cont.)

- Requirement that they share data the FI asks for to do your due diligence
- That the FI will or will not process transactions for nested Third-Party Senders
- Termination
- FI's right to audit
- SEC codes FI will process
- That they will have a disaster recovery plan
- AND.... How Returns, NOCs, and unauthorized transactions will be processed and delivered

Updating – clause allowing the FI to update with XX days notice

Third-Party Sender Registration- Who Must Register?

This rule applies to all ODFI's



Every ODFI will be required to either:

Register its Third-Party
Senders

State that it has no
Third-Party Senders

Similar to Direct Access
Registration

Third-Party Sender Registration

Provide at time of Registration

- ODFI's name and contact info
- TPS Name
- TPS business location
- Routing numbers used in TPS's originations
- Company IDs used by the TPS

Must be registered within 30 days of the first ACH Entry originated

Rule places an obligation on TPS's to provide ODFI's with any registration information needed

Third-Party Sender Registration

ODFI will be required to provide updated information within 45 days of a change with the following information

- Any of the registration info OR
- When a TPS relationship has ended



Third-Party Sender Registration

Supplemental information may be requested due to risk events, defined as cases in which it [Nacha] believes a Third-Party Sender in the ACH Network poses an escalated risk of:

- Financial loss to one or more Participating DFIs, Receivers or Originators,
- Violation of the Rules or applicable legal Requirements, or
- Excessive Returns

Third-Party Sender Registration

This additional information must be supplied within 10 banking days:

- DBAs
- Tax ID Number
- Street address
- Website
- Name and contact information for TPS contact person
- Names and titles of TPS's principals
- Approximate number of Originators
- Statement of the types of transactions processed – credits, debits, or both

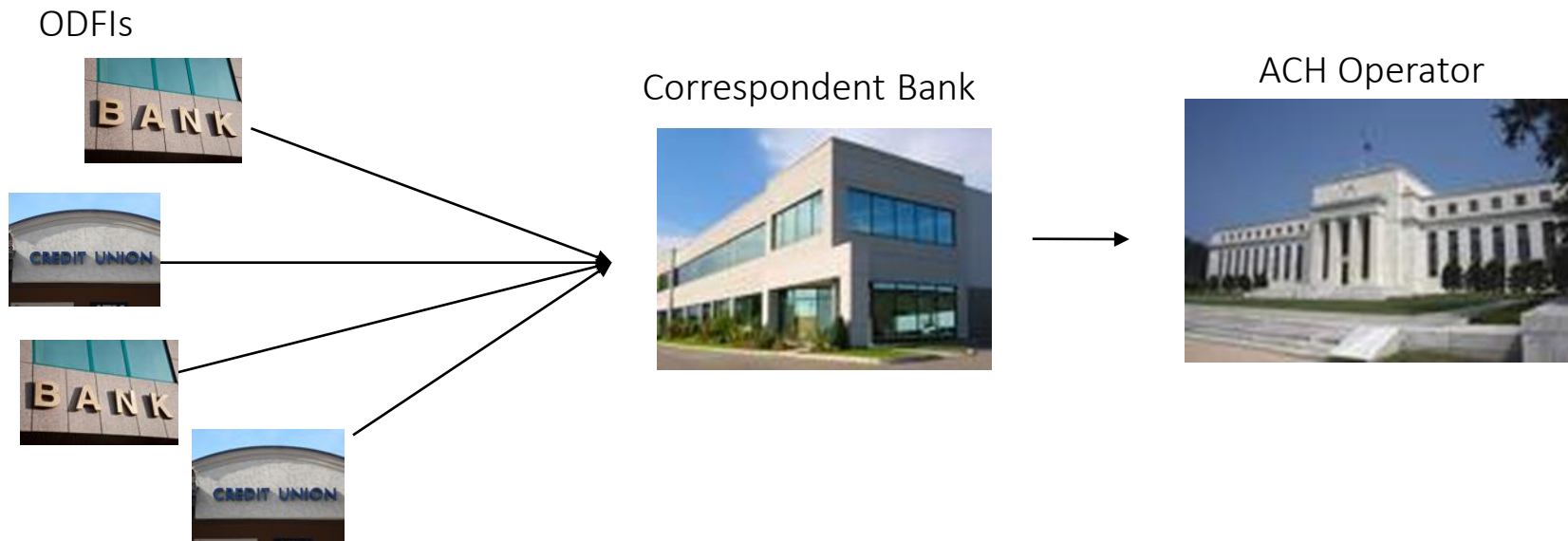
Direct Access Defined for Registration Purposes

Direct Access is a situation in which an Originator or a Third-Party (either a Financial Institution's Third-Party Service Provider or an Originator's Third-Party Sender) transmits debit ACH files [transactions] directly to an ACH Operator using a financial institution's routing number and settlement account

Direct Access Registration Exclusions

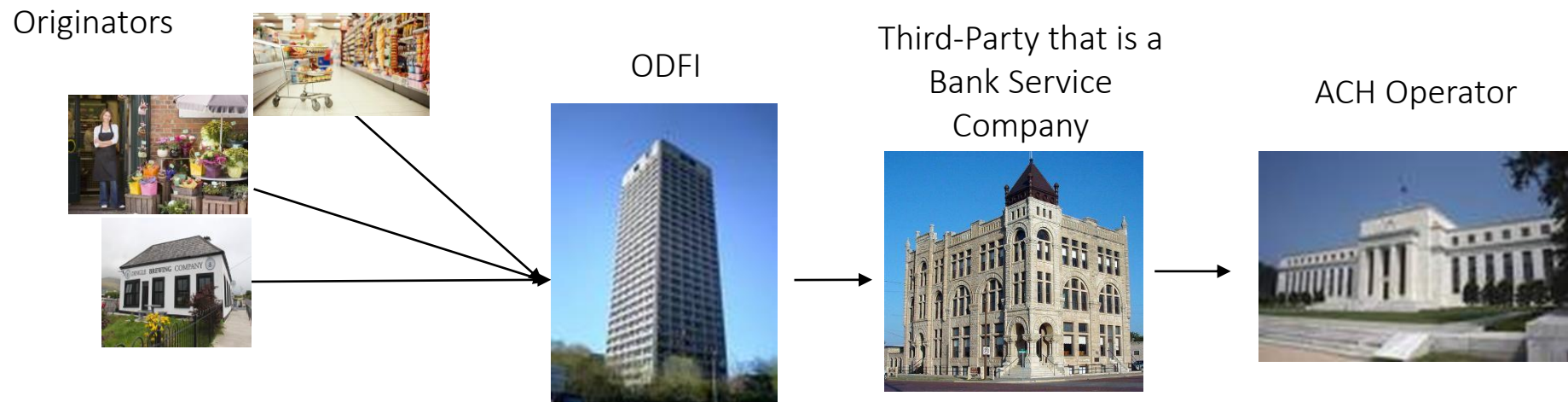
Direct access registration excludes:

- financial institutions that transmit files using another financial institution's routing number or settlement account (correspondent/respondent relationships)



Direct Access Registration - Exclusions

- Direct access registration excludes:
 - Third-Parties that transmit ACH files solely on behalf of the financial institution and do not have direct agreements with Originators (and are not themselves Originators)



ACH Contact Registry

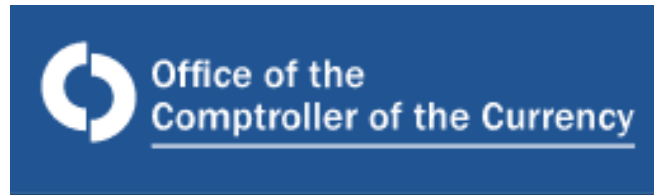
- All participating DFIs must register specific contact information in the ACH Contact Registry.
- Contacts must include personnel or departments responsible for:
 - ACH Operations
 - Fraud and/or Risk Management
- Participating DFIs must provide:
 - the name, title, email address, and phone number for at least one primary and one secondary contact person, or
 - general department contact information that includes an email address and a working telephone number.
- Participating DFIs may register additional contacts at their discretion.

ACH Contact Registry

- ACH Contact Registry is found in Nacha's Risk Management Portal.
- Participating DFIs must update the registration information within 45 days of any changes to the previously provided information.
- Registered DFIs must verify all registration information at least annually.
- Failure to register could result in a Rules Enforcement proceeding and a Class 2 Rules Violation.

Setting Exposure Limits

ODFI is required to set, monitor and periodically review exposure limits in accordance with the ACH Rules and OCC and FFIEC Guidance



Formal Guidelines for Establishing Exposure Limits



There are NONE!!!!



It is up to the ODFI to implement an effective risk management system and control of this system.

NACHA Rules on Exposure Limits

Article 2 subsection 2.2.3

- ...the ODFI must:
 - Assess the nature of the Originator's or Third-Party Sender's ACH Activity and the risk it presents
 - Establish, implement, and periodically review and set exposure limit for the Originator or Third-Party Sender
 - Establish and implement procedures to:
 - Monitor the origination and return activity across multiple settlement dates
 - Enforce restrictions on the types of entries that may be originated
 - Enforce exposure limits





Exposure Limits
should be relative to
the file amounts

Example:

- Originator qualifies for a \$100,000 exposure limits
- Estimated amount of each file is \$25,000



What should this originator's
exposure limit be?

Setting Exposure Limits



Monitoring Exposure Limits

When a file is over the established limit:

- Who is authorized to make decisions and/or release or suspend the file?
- What procedures are followed?
 - Procedures to handle suspended files
 - Procedures to temporarily increase an exposure limit
 - Log of file suspensions and return items

Monitoring and Reporting

- Monitor activity for consistency
- Consider establishing activity thresholds beyond which additional reviews may be necessary, such as:
 - Excessive over-limit files
 - Rapid increases in number of transactions and/or dollar value
 - Changes in the debit/credit mix
 - Increases in the number and/or percent of overall returns
 - Track the number of requests for proof of authorization for originated transactions
 - Proper use of SEC codes
 - OFAC

Originator Education

Comply with the ACH Rules

Effective Date vs Settlement Date

SEC Codes

Authorization requirements

Record retention

Origination Software

OFAC

Consumer Authorization for PPD Debit Entry

Must be recognizable as credit or debit authorization

Signed or Similarly Authenticated

- Written authorization is optional for credit

Clearly state terms of authorization

- Single, Recurring, or Subsequent Entries
- Amount or method of determining the amount
- Timing (start date, number of Entries, frequency, end date)
- Receiver's name and account to be debited
- Date of authorization

Terms and instructions on revoking authorization for electronic payment

Consumer to receive a copy

Changes to Original Authorization



Change in Date

The company must notify the receiver 7 days prior to the date of the debit



Change in Dollar Amount

The company must notify the receiver 10 days prior to the date of the debit

If the Receiver authorized a specific date range– no notice required

Authorization for CCD and CTX

Trading Partner Agreements

- Agreements between entities that spell out exactly how the transactions will be executed



Authorization Requirements

ARC

- Notice to Receiver plus receipt of source document = Authorization

BOC

- Notice to Receiver plus receipt of source document = Authorization

POP

- Written Authorization

RCK

- Notice = Authorization

TEL- Oral Authorization

- Recorded OR Written Notice for a Single Entry
- Recorded AND Written Notice for a Recurring Entry
 - Copy of authorization for recurring must be sent to Receiver

WEB

- Authorization obtained over internet

Notice Obligation

- “When you provide a check as payment, you authorize us either to use the information from your check to make a one-time electronic fund transfer from your account or to process the entry as a check transaction. “ (phone # for BOC)
- **Language per Regulation E and the ACH Rules

Authorization for all ACH Entries

Originator is responsible for authorization

- Securing
- Retention

Must retain for 2 years after termination or revocation of authorization



Single Entry Origination

Used for consumer-to-consumer payments

Always authorized by the person whose account is being debited

Examples:

- Smart Bank pulls money from Cardinal Credit Union for Jason's loan payment. (Jason signs authorization)
- Smart Bank sends money from Lynn's savings account to her daughters checking account at Cardinal Credit Union. (Lynn signs authorization)

Prenotification



Optional for the Originator



Zero dollar



Initiated a minimum of 3 banking days before live entry



RDFI must verify prenote information

If Information is incorrect

- Return
- Send Notification of Change (NOC)

ODFI Action on Prenotes

An Originator should be informed by the ODFI when a prenote is returned

Originator should research the problem according to the return reason code and make necessary corrections prior to transmitting subsequent entries

If the ODFI receives a Notification of Change (NOC) on a prenote, the ODFI must transmit the required NOC information to the Originator within 2 days

The Originator must make the changes within 6 banking days or prior to initiating another entry

Micro-Entries

- A credit or debit Entry used by an Originator for the purpose of verifying a Receiver's account or an individual's access to an account
- A credit Micro-Entry must be in an amount of less than \$1.00 and one or more debit Micro-Entries must not exceed, in total, the amount of the corresponding credit Micro-Entries
- The Company Entry Description field must contain "ACCTVERIFY"
- The Company Name must be readily recognizable to the Receiver and be the same or similar to the Company Name that will be used in future Entries
- Credit Micro-Entries and the corresponding debit Micro-Entry offsets (if used) must be simultaneously sent for settlement at the same time
- An Originator using Micro-Entries may initiate future Entries to the Receiver's account as soon as the Originator's process for validating the amounts of the Micro-Entries has been completed

Micro-Entries

- ODFIs are not required to review or inspect files to enforce compliance
- An Originator of Micro-Entries must conduct commercially reasonable fraud detection on its use of Micro-Entries, including monitoring of forward and return volumes of Micro-Entries
 - Monitoring forward and return volumes, at a minimum, establishes a baseline of normal activity
 - Establishing a baseline of normal activity allows for the detection of anomalous activity

Effective Entry Date vs. Settlement Date

Banking Day

- A day the Federal Reserve Operates
 - Not Saturday, Sunday or Legal Holidays

Effective Entry Date

- Assigned by Originator

Settlement Date (Julian Date)

- Determined by the ACH Operator
- Date the funds are settled between Fed and the Financial Institution
- Post Same Day Credit Entry based off this

Effective Date vs. Settlement Date Scenario

Sunset University sends a payroll file with an effective date of Monday, January 18. However, that is Martin Luther King day, and the Federal Reserve Bank does not process files that day as it is a Federal holiday. The Federal Reserve Bank will insert the settlement date of Tuesday, January 19 as the settlement date.



Same Day ACH



ACH transactions can be submitted on the same day

Based on transmission windows set by FRB



Mandatory receipt for RDFI



Optional Origination for ODFI

(effective March 19, 2021)

Same Day Eligible Forward Items

Transmission Deadline ¹	Target Distribution ²	Settlement Schedule ³
10:30 a.m. ET (1030 ET)	Noon ET (1200 ET)	1:00 p.m. ET (1300 ET) – current day
2:45 p.m. ET (1445 ET)	4:00 p.m. ET (1600 ET)	5:00 p.m. ET (1700 ET) – current day
4:45 p.m. ET (1645 ET)	5:30 p.m. ET (1730 ET)	6:00 p.m. ET (1800 ET) – current day

Future Dated Forward Items

Transmission Deadline ¹	Target Distribution ²	Settlement Schedule ³
10:30 a.m. ET (1030 ET)	Noon ET (1200 ET)	8:30 a.m. ET (0830 ET) – future business day ⁴
2:45 p.m. ET (1445 ET)	4:00 p.m. ET (1600 ET)	8:30 a.m. ET (0830 ET) – future business day ⁴
4:45 p.m. ET (1645 ET)	5:30 p.m. ET (1730 ET)	8:30 a.m. ET (0830 ET) – future business day ⁴
8:00 p.m. ET (2000 ET)	10:00 p.m. ET (2200 ET)	8:30 a.m. ET (0830 ET) – future business day ⁴
2:15 a.m. ET (0215 ET)	6:00 a.m. ET (0600 ET)	8:30 a.m. ET (0830 ET) – future business day ⁴

Before Originating Same Day ACH: Some Risk Considerations

Develop an overall strategy for offering Same Day ACH

- Should Same Day be offered to all or select Originators?
 - Not all customers may be suitable for same-day origination
 - Not all FI products may be suitable for same-day origination
- Determine how to identify those Originators or transaction types permitted to use Same Day ACH
- Consider customer's profile (i.e., business model) when offering Same Day ACH
 - Current credit limits and risk rating
 - Prefunding and exposure
 - Authentication methods

Review Files or have processes in place to determine compliance with Same Day eligibility rules

- Ensure proper use of Effective Entry Date
- Other indicators (Descriptive Date, Company Discretionary Data)

Late Delivery Example

Joe's Gym executes a file with an effective date of Wednesday, February 10 and transmits it to Smart Bank by 9 AM on February 10.

What will the settlement date of this file be?

If Smart Bank offers Same Day ACH, what would be the settlement date?



Credit vs. Debit Entries

Credit entries may be submitted to the ACH Operator 2 days prior to settlement date

Debits entries may be submitted to the ACH Operator 1 day prior to settlement date

- Sunset University processes CREDIT entries and may submit those 2 day prior to settlement date
- Joe's Gym processes DEBIT entries and may submit those 1 day prior to settlement date

How do you receive files from your Originators?



**CD/Thumb
Drive/other
storage device**

Drop off at FI



Secure E-mail



**Internet/Treasury
Management
System**



VPN-Modem



**3rd Party
processor**

Prior to Submission....

Items which need to be addressed prior to file submission

- Security Procedures for transmitting files
 - ID-Passwords (treasury management system)
 - Transmittal letter from authorized user
- Security procedures for delivered files
 - Transmittal letter from authorized user
- Where are File Limits set and checked
 - Prior to transmission
 - Treasury management systems/internet banking
 - At ODFI

Delivery of ACH Files



It is the responsibility of the ODFI to release entries at the proper time



Many ODFI's use the effective entry date to control the release of the file



If the file is received prior to the release date, the ODFI “warehouses” the file until the release date

Sunset University

Sunset University sends all the payroll information to Main Street CPA to prepare the ACH File and transmit it to the ODFI on their behalf.

Sunset University does send a transmittal letter to Smart Bank, the ODFI, which contains the amounts and item counts of debits, credits and the total of the files. This document also contain the effective entry date and an authorized signature.

The ACH file itself is sent to Smart Bank by Main Street CPA via a secure website.



Joe's Gym



Joe's Gym creates the monthly ACH billing file on its accounting software and uploads it to the treasury management system at Smart Bank, the ODFI.

Prior to being able to upload the file, an authorized user must sign into the system with ID, password and token number.

The file limits are set in the treasury management system and once the ACH file is uploaded, the limits are checked. If the file amount is above the limit, the user will be unable to submit the file.



Types of Risk



Credit (Exposure) Risk

Operating Risk

Fraud Risk

Reputational Risk

Systemic Risk

What is ACH Credit Risk?

The risk that a party to a transaction will be unable to provide the necessary funds for settlement to occur

- Losses due to Credit Risk typically result from the failure or bankruptcy of a company
- ODFIs are responsible for controlling credit risk
 - Develop and implement credit monitoring and control procedures

ACH Credit Risk



ODFI exposure (for credit entries)

- Period of time between the initiation of ACH credit file until the company funds the account
- Amount of risk based on total amount of the file
 - Up to 2 days

Origination of ACH Credit File - Sunset University

Day One	Day Two
ACH credit file is sent from Sunset University to Smart Bank totaling \$15,000	Smart Bank's account is charged by the Federal Reserve Bank - \$15,000
Entries are effective on Day Two	Smart Bank debits Sunset University's account for \$15,000
Smart Bank processes file and delivers to the ACH Operator	RDFI's credit the receivers' accounts
ACH credits are delivered to the RDFIs by the ACH Operator	
THE ODFI'S CREDIT RISK EXPOSURE IS \$15,000	

Origination of ACH Credit File - Multi-day/Multi-file

Day One	Day Two
ACH credit file is sent from Sunset University to Smart Bank, totaling \$10,000 (file 1)	ACH credit file is sent from Sunset University to Smart Bank totaling \$5,000 (file 2)
Entries are effective on Day Four	Entries are effective on Day Three
Smart Bank warehouses the items from File 1 and forwards them to the ACH Operator on Day Two	Smart Bank forwards items from File 1 and File 2 to the ACH Operator today
	ACH Credits are delivered to the RDFIs from the ACH Operator today
	No settlement for any items has yet occurred

Quiz

What amount of risk do you see on day 1?

- None
- \$10,000
- \$15,000

What amount of risk do you see on day 2?

- None
- \$5,000
- \$10,000
- \$15,000



Origination of ACH Credit File - Multi-day/Multi-File

Day Three	Day Four
ACH credit file is sent from Sunset University to Smart Bank totaling \$2,000 (file 3)	Smart Bank's account is charged by the Federal Reserve Bank - \$12,000 (total of file 1 and 3)
Entries are effective on Day Four	Smart Bank debits Sunset University account for \$12,000
Smart Bank processes file and delivers transactions to the ACH Operator today	
Smart Bank's account is charged by Federal Reserve Bank \$5,000 (for file 2) and Smart Bank debits Sunset University account \$5,000 (for file 2)	

Quiz

What amount of risk do you see on day 3?

- None
- \$10,000 (until final posting)
- \$15,000 (until final posting)
- \$17,000 (until final posting)

What amount of risk do you see on Day 4

- None
- \$10,000 (until final posting)
- \$12,000 (until final posting)
- \$17,000 (until final posting)



Credit Risk – ACH Debits

ODFI Exposure

- Date funds available to originator until debits can no longer be returned by RDFIs
 - 2 Banking days (24 hrs)
 - Up to 60 days from settlement
 - Unauthorized could be returned as ODFI warrants authorization
- Amount of risk based on amount of returned ACH debit
 - NOTE: Statute of Limitations – 7 years for most states where the ODFI would still be liable

Origination of ACH Debit File - Joe's Gym

Day 1	Day 2	Day 3	Day 4
ACH debit file sent from Joe's Gym to Smart Bank	Smart Bank credits Joe's Gym account for the total amount of the ACH File	RDFI returns ACH debit due to NSF funds in the Receiver's Account	Smart Bank received ACH debit return
Smart Bank delivers file to the ACH Operator	ACH Debit is received by RDFI		Smart Bank charge back the returned ACH Debit to Joe's Gym
ODFI'S EXPOSURE			

Origination of ACH Credit File

Day One	Day Two	Day Three
ACH credit file is sent from Sunset University to Smart Bank totaling \$15,000	Sunset University files for Bankruptcy	Smart Bank's account is charged by the Federal Reserve \$15,000
Entries are effective on Day Three		RDFIs credit Receiver's accounts
Smart Bank processes file and delivers transactions to the ACH Operator		
ACH credits are delivered to the RDFI's by the ACH Operator		
WHO IS LEFT HOLDING THE \$15,000 DEBIT?		

SDA Origination Risk Considerations

With multiple settlements each day, the ODFI's exposure may change throughout the day

- Established exposure limits for the Originator will not change, but the amount of exposure to risk throughout the day could change for the Originator or FI due to multiple settlement windows
- If an ODFI employs intraday real time settlement capabilities, they should consider how use of Same Day Entries may impact credit exposure limits

With the increased speed of Same Day Entries, the importance of commercially reasonable authentication methods and security around file delivery is increased

- Types of entries to monitor more closely may include account openings, A2A, and P2P

Use of Prenotifications and responses to Prenotifications will enable better quality of Entries and serve to mitigate risk

- This is true for Same Day Entries as well as non-Same Day transactions
- For example, a payroll Entry or bill payment containing an incorrect Receiver account number can be remedied more quickly if response is sent same-day

What is Operational Risk?

In the ACH payment system, operating risk is the risk that the exchange of ACH transactions will not be completed accurately or on time because of an operational failure at some point in the exchange process



PC Failure



Disasters



Power Outages

Operational Failure

An operational failure is any disruption in normal processing including:

- Failure/Unavailability of Computer Hardware or Software,
- Disruptions in telecommunications equipment
- and/or
- Advertent loss, alteration, or duplication of ACH data

Operational Risk Examples



Hardware, software, telecommunications and power failure



Human error

late returns
timeliness of reconciliation
aged items
out of balance conditions



Staffing problems

lack of training
sick or vacationing staff

Operational Risk Example

Power Outage

- A thunderstorm results in a loss of electricity to 140,000 customers, including a small community bank
- Smart Bank does not have a contingency plan or a back-up location
- It takes power crews three days to restore power to the area

Result:

- Smart Bank is unable to transmit Sunset University's payroll file because they had no electricity and no back-up plan
- Who is liable?

Operational Risk Controls

Reliable equipment, regular maintenance, adequate backup

Detection and correction of “bugs” in software

Diagnostic tools, backup modes of transmissions

UPS systems, backup procedures in event of power failure

Good supervision, cross-training, audits

Disaster recovery plans

Corruption of ACH Data

- File Accountability and Balancing
- Secure Storage
- Limited Access
- Backup Copies
- Audit Trails



Any disruption in ACH processing can imperil the accurate and timely processing of ACH entries



Repeated disruptions can undermine the credibility of the ACH payment system



Review ACH operations:

identify areas of risk
take steps to reduce risk to an acceptable level

Summary – Operational Risk

What is Fraud Risk?

The risk that ACH data will be compromised through:

- introduction of false transactions
- alteration of valid transactions
- alteration of data that controls the routing or settlement of valid ACH transactions



Causes of Fraud Risk

Fraudulent activities are usually the work of:

- disgruntled or dishonest employees
- outside parties (such as intruders or interlopers)
- combination of both where two or more individuals are acting in collusion.

Fraud can also be committed by an organization

Employee Fraud

An employee at Cardinal Credit Union scans a recurring file before forwarding it to the Operator and locates a large credit transaction destined for Smart Bank where the employee has a checking account under a false name. The employee alters the file by placing his account number in the transaction.

The next morning, the employee drives to Smart Bank and wires the money to his account in the Cayman Islands. Later that morning, the intended Receiver realizes that the expected transaction was not posted. The Originator requests reimbursement for the transaction from Cardinal Credit Union for the payment that was misappropriated by their employee.



Key-logging Example

Sunset University's payroll clerk is logged into the payroll software for the Main Street CPA. Prior to working with the payroll, she had been browsing the web and a keylogging program was inadvertently installed on her computer. This keylogging program then recorded all of the strokes she used to enter payroll information. Now the keylogger has the both Sunset University and the professor's account information.

Tools to Combat Fraud Risk

Sound personnel practices

Good physical security for computer, communications and ACH Operations areas

Effective data security

Rigorous control of all changes

Operational controls as used to reduce Operational risk

Summary – Fraud Risk

All participants in the ACH payment system should be on alert for fraudulent activity by their customers and within their organizations.

Reduce chances that improper activities go unnoticed, manage your fraud risk:

- detect fraudulent activity promptly
- maintain audit trails for all ACH transactions

What is Reputational Risk?



Risk that actions or events that take place involving your institution will affect your reputation

What is Systemic Risk?



The risk that the inability or unwillingness of one participant in a clearing and settlement network to settle its commitments will cause other network participants to be unable to settle their commitments

Such a chain of events could undermine confidence in the nation's payments system and therefore systemic risk of serious concern

Identify the Risk Type

When an originator's payroll was delivered to the ODFI for transmission, the ODFI employee accidentally deleted the file.

An originator sent six CCD payments to suppliers with a file value of \$557,000. The company's availability on their \$3 million line of credit is \$300,000. Their payments on the line of credit have been received 10-15 days late six of the past eight months.

Identify the Risk Type

An ODFI employee adds a payment to her own checking account to a company payroll she is transmitting.

The computer used to transmit origination files crashes due to memory limitations and the employee in charge of the transmission doesn't notice that the batch wasn't completed.

Identify the Risk Type

An ODFI transmitted tax payments for a company on Thursday. The sales officer at the ODFI learned the next morning that the company filed for bankruptcy.

Both employees responsible for ACH exception processing called in sick on the same day. The task is not completed that day as a result.

Your financial institution does not balance its Federal Reserve account

Identify the Risk Type

A new rule reduced the time to send corrected returns and your financial institution is unaware of the rule change

A foreign bank, with offices in the US, closes down all operations due to economic hardship in the country of their headquarters. Even US offices suspend operations, including ACH processing and settlement

Commercially Reasonable Security Procedures



Authorized signature and call back procedures



Transmittal letter



Other methods used to verify authenticity of payment information

IDs
Password
Encryption
Token

Sunset University

Sunset University does send a transmittal letter to Smart Bank, the ODFI, via fax which contains the amounts and item counts of debits, credits and the total of the files. This document also contains the effective entry date and an authorized signature.

Smart Bank has a file verification procedure. They sign off on the transmittal letter and fax it back to Sunset University.



Joe's Gym

Prior to being able to upload the file, an authorized user must sign into the system with ID, password and token number, or other form of multi-factor authentication



Balanced Files vs. Unbalanced Files

Balanced Files

- Contain both debit and credit items
- Can only send one day prior to settlement

Unbalanced Files

- Contain only debits or credits
 - Payroll file – only CREDITS – can send 2 days prior
 - Payments file – only DEBITS – can send 1 day prior
- Internally post debit (payroll) or credit (payments)

File Reject or Batch Reject?

Which reject level will you choose?

Specific errors will always cause the entire ACH file to reject

- Mandatory field errors in the file header or file control record
- Incorrect immediate origin or destination information
- Out-of-balance entry hash total, block count

File Level Reject – the entire ACH file will reject even if the error is specific to one batch

Batch Level Reject – when there is only a batch level error, only the batch with the error will reject (instead of the entire ACH file)

Rule of Thumb: If you have the ability to recreate at the batch level – choose the batch level reject option.

File or Batch Rejection

File Reject

- File cannot be read
- Invalid sending point
- Mandatory field errors
- Invalid characters
- Invalid immediate destination or origin routing number
- Out of balance condition (\$ amounts/hash totals)

Batch Reject

- Invalid SEC code
- Mandatory field errors
- Invalid characters
- Out of balance format condition
 - ODFI/Trace numbers



Operator Rejects

These return reason codes mean your entry was NOT processed!

- R13 – Invalid ACH Routing Number
- R18 - Improper Effective Entry Date
- R19 - Amount Field Error
- R25 - Addenda Error
- R26 - Mandatory Field Error
- R27 - Trace Number Error
- R28 - Routing Number Check Digit Error
- R30 - RDFI Not Participant in Check Truncation
- R32 - RDFI Non-Settlement
- R34 - Limited Participation DFI
- R35 - Return of Improper Debit Entry
- R36 - Return of Improper Credit Entry

Example

Sunset University has a new professor who will receive his payroll via direct deposit. The payroll file containing the new entry is sent with an effective entry date of March 18.

The payroll file is released to the ACH Operator by Smart Bank, the ODFI, on March 16.

On March 16, Smart Bank receives a rejected entry with a return code of R13 Invalid ACH Routing number.

Smart Bank contacts Sunset University to inform them of the return.

Sunset University then must contact Main Street CPA to find and fix the problem. Main Street CPA finds that 2 digits in the routing number of the entry were transposed.

The entry is corrected, and the entry is resent to Smart Bank on March 18. Will the new professor get paid on March 18?

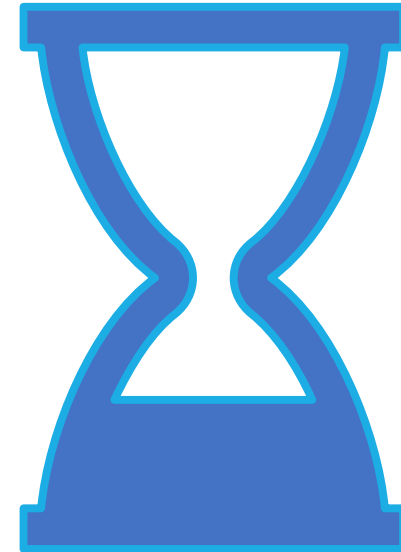
Reversals

Time frame

- Must originate reversal within 5 banking days following settlement date of the erroneous entry
- Files must be transmitted within 24 hours of discovery

ODFI Request for Return

- RDFI not obligated to comply if funds are not available



Erroneous

Duplicate

Unintended amount

Unintended receiver

Wrong date

- A credit entry sent too late
- A debit entry sent too early

The PPD credit is

- For funds related to a receiver employment
- The value of the entry is fully included in a check delivered at or prior to separation from employment
- The entry was transmitted prior to the delivery of the check

Notification of Change (COR) (NOC)

Optional non-dollar entry initiated by an RDFI

- Identifies that the entry has been received by the RDFI
- Indicates specific information that is incorrect
- Provides the correct information so the Originator may make the change
- Can be used on prenote or live dollar entry

Incoming Notification of Change Entries

Notifications of Change

ODFI Responsibilities

- NOC to Originator within 2 banking days

Minimum Information to be included

Originator Responsibilities

- Change needs to be made within 6 banking days or before initiation of next entry (whichever is later)

Refused/Corrected Notification of Change



Refused Notification of Change

Created by the ODFI to refuse a Notification of Change entry containing incorrect or incomplete information

- 15 days



Corrected NOCs

RDFI may transmit corrected NOC within 5 banking days

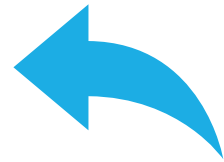
General Returns

Available to the ODFI on the morning of the second banking day following the settlement date of the original entry

Where does the ODFI find incoming return items?

How does the ODFI notify the Originator of the returns?

Incoming Return Entries



Returns

Understanding the Return Codes

Dishonored Returns

Re-initiation of Entries



ODFI Responsibilities

Information to Originator

Dishonoring returns

Software Exception processing capabilities

Reinitiating Return Entries

If the entry has been returned for insufficient or uncollected funds it may be reinitiated up to two more times

The entry must be reinitiated within 180 days after the settlement date of the original entry

If returned for Stop Payment, Authorization Revoked, Unauthorized or Improper Entry, it cannot be reinitiated unless the entry has been authorized by the receiver or the ODFI has taken action to remedy the reason for the return

Reinitiated Entries

Must be a separate batch

Contain “RETRY PYMT” in the Company Entry Description field

Used for all SEC Codes

The company name, company identification and amount fields must be identical to the original entry

Stop Payment Rule

For Consumer Accounts

- Does not impact non-consumer accounts

If stop pay applies to more than one payment, the order remains in effect until ALL entries are stopped

Implementation ODFI

Inform your originators

Dual meaning of R08 return code

- Does R08 now mean one entry or all future entries?

If Originators receive returns R08

- Best consideration
 - Turn off future debits
 - Contact the Receiver for clarification

Return Rate Monitoring



Returns should be logged and return rates monitored

NACHA is allowed to request information about an Originator from an ODFI when NACHA believes that the Originator's return rate for unauthorized reasons exceeds 0.5%

ODFIs must then implement plans to reduce an Originator's unauthorized return rate to less than 0.5 % within 30 days after contacted by NACHA and maintain for 180 additional days



NACHA may initiate enforcement proceeding if:

ODFI fails to provide complete & accurate information within required timeframe;

ODFI fails to reduce Originator/Third Party Sender return rate within 30 days after contacted by NACHA; or

ODFI fails to maintain return rate below 0.5% for 180 additional days

Monitoring Return Entries



**Unauthorized return rate =
0.5%**

R05, R07, R10, R11, R29 & R51

Will be charged
\$4.50 PER ENTRY



Overall return rate = 15%



**Administrative return rate =
3%**

R02, R03 & R04

Dishonored Returns

ODFI May Dishonor a Return if:

- It can substantiate that the RDFI failed to meet the time deadlines for the return entry
- The return entry contained incorrect or erroneous information



Dishonored Returns

Time frame –

ODFI must transmit within Five Banking Days after the Settlement Date of the Return Entry

Return Reason Codes –

- R61, R62, R67, R68, R69, & R70



R69 – Field Errors

ODFI determines the return entry has incorrect information in one or more of the fields listed below

In the Addenda Information field – indicates the error(s) - if multiple indicators are used, separate by asterisks

- 01 Incorrect DFI Account Number
- 02 Incorrect Original Entry Trace Number
- 03 Incorrect Dollar Amount
- 04 Incorrect Individual ID #/Individual ID
- 05 Incorrect Transaction code
- 06 Incorrect Company Identification Number
- 07 Invalid Effective Entry Date

Contested/Corrected Dishonored Return



RDFI may dispute a Dishonored Return Entry

- within Two Banking Days

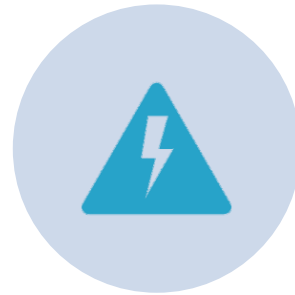
ODFI must accept Contested/Corrected Dishonored Return

The ODFI may not contest a contested entry received from an RDFI by reinitiating the entry

Request for Authorization



AT THE REQUEST OF THE RDFI, THE
ODFI MUST PROVIDE A COPY OF THE
AUTHORIZATION WITHIN 10 BANKING
DAYS OF THE WRITTEN REQUEST



CANNOT CHARGE



HOW WILL YOU GET A COPY OF
AUTHORIZATIONS FROM YOUR
ORIGINATORS?

Limitations on Warranty Claims

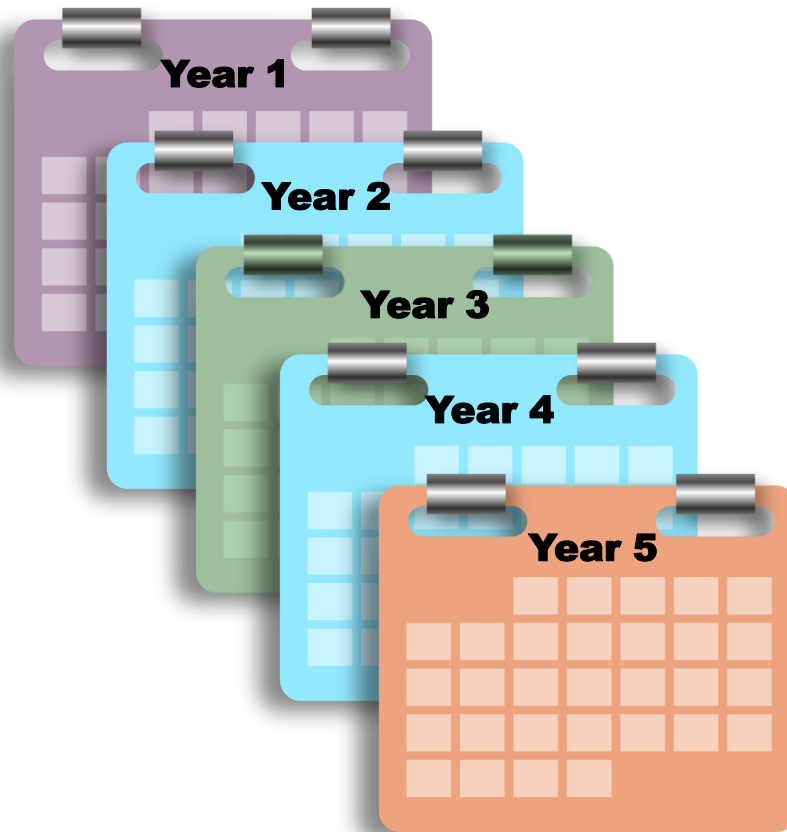
ODFI warrants that:

- An Entry is properly authorized; &
- Authorization has not been terminated

Non-Consumer Account	Consumer Account
1 year from Settlement Date of unauthorized Entry	2 years from Settlement Date of unauthorized Entry <i>PLUS</i> 95 calendar days IF <u>more than 2 years</u> has <u>elapsed</u>

Limitations on Warranty Claims

Consumer Dispute Beyond 2 Years

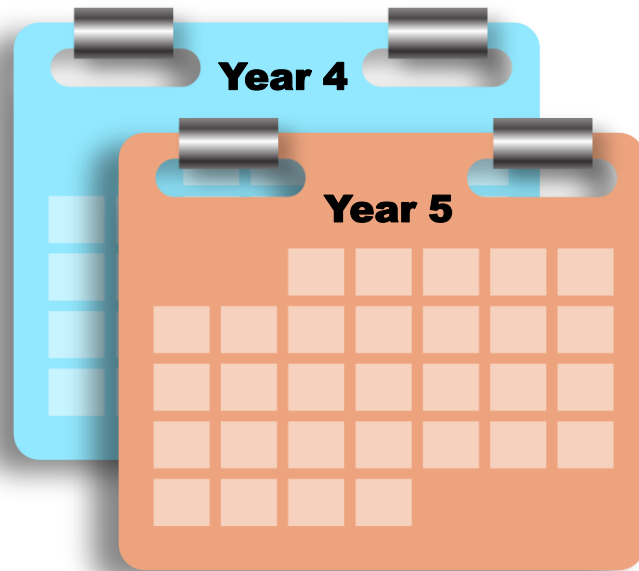


Consumer notifies its RDFI of unauthorized debits, which have been taken out monthly for the past 5 years

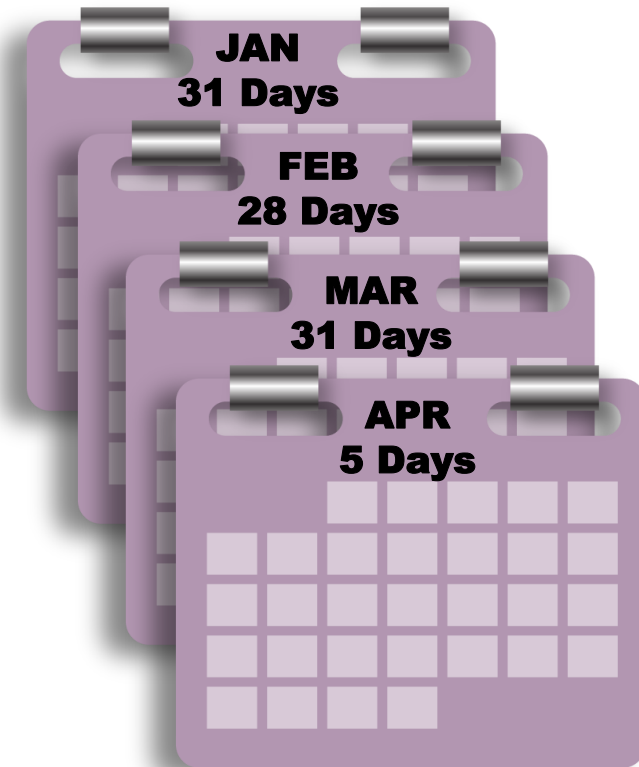
What is the limitation on the warranty claim?

Limitations on Warranty Claims

Consumer Dispute Beyond 2 Years



Last 2 years



95 calendar days
of Year 1

WEB Debit Fraud Detection Standards

WEB Debit Originators must use Commercially Reasonable Fraud Detection Standards to screen WEB Debits for fraud. Specifically, that Account Validation, for first use of account numbers, will be required as part of Commercially Reasonable Fraud Detection.

Operational Impacts

Updates to ACH Originators' fraud detection systems

- Or implementation of a system for Originators who currently do not perform any fraud detection for WEB debits
- These impacts could increase the cost of originating WEB debits for some parties

RDFIs could receive a greater volume of ACH prenotifications, micro-transactions, or other account validation requests

- Some could be in lieu of receiving live-dollar transactions initially

Supplementing Data Security Requirements

- For Originators and Third-Parties with ACH volume greater than 2 million entries

ACH Security Framework including its data protection requirements during initiation, processing, and storage.

Recent rules are supplemented to explicitly require large, non-FI Originators, Third-Party Service Providers (TPSPs) and Third-Party Senders (TPSs) to protect deposit account information by rendering it unreadable when it is stored electronically.

Supplementing Data Security Requirements

Data at rest must be protected, unreadable

- Article One, Section 1.6 (Security Requirements) to require each Non-Consumer Originator that is not a Participating DFI, each Third-Party Service Provider, and each Third-Party Sender, whose ACH Origination or Transmission volume exceeds 2 million Entries annually to protect DFI Account Numbers used in the initiation of Entries by rendering them unreadable when stored electronically.

QUESTIONS

For Your Records

Continuing Education Credits

ODFI Roles and Responsibilities

This session is worth 6 credits

(keep this slide for your records)

