

ACH for P2P Transfers: Perils & Protections

Presented by:

Macha/PAR – Everything Payments - Everywhere

Jessica Lelii, AAP, APRP

Assistant Director of Education

www.macha.org

jlelii@macha.org



PROCEED WITH

CAUTION

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.
- © 2022 Macha/PAR All rights reserved

Regulation E

- Consumer Financial Protection Bureau

- <https://www.consumerfinance.gov/>

- CFPB implements and enforces Federal consumer financial law and ensures that markets for consumer financial products are fair, transparent, and competitive.

- <https://www.ecfr.gov/current/title-12/chapter-X/part-1005>

- **Purpose:** *“establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer and remittance transfer services and of financial institutions or other persons that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers and remittance transfers.”*



Regulation E

- There is no conflict between Regulation E's timeframe for reporting an error and the ACH Rules that relate to an RDFI's Right of Adjustment
- Regulation E does not state that an RDFI may return any ACH entry
- Neither Regulation E nor the ACH Rules provide rights related to the quality of goods or services related to the payment



Error

- Regulation E:
 - An unauthorized EFT
 - Incorrect
 - Omission of EFT from Statement
 - Computational or Bookkeeping error by the FI
 - Receipt of incorrect amount of money from electronic terminal
 - EFT not identified as required by the statement or telephone line
 - Request for information that allows consumer to determine if error exists



Error

- Nacha Rules:
 - Unauthorized ACH Entry
 - Incorrect Dollar Amount
 - Incorrect Debit Date
 - Revoked Authorization
 - For recurring entries only
 - Revocation with Originator prior to initiation of next entry

Risk vs. Reward



- Risk: All payment systems have inherent risk
- Reward: Ability to offer a variety of services to your account holders

What are we talking about today?

Electronic consumer transfers via ACH

Referred to as:

- P2P (person-to-person)
- A2A (account-to-account or me-to-me)
- External Transfers
- FI to FI transfer

What are we NOT talking about today?

Consumer Bill Pay

Loan Payments

Credit Card Payments

Venmo, PayPal, CashApp, Google Pay, Apple Pay, etc.

Nacha defines a “Person-to-Person Entry” or “P2P Entry” as:

- “a credit Entry initiated by or on behalf of a holder of a Consumer Account that is intended for a Consumer Account of a Receiver. A P2P Entry uses the Internet-Initiated/Mobile Entry (WEB) Standard Entry Class Code.” (Nacha Operating Rules & Guidelines, Section 8.75)
- “a credit WEB Entry is a credit Entry initiated by or on behalf of the holder of a Consumer Account that is intended for a Consumer Account of a Receiver, regardless of whether the authorization is communicated via the Internet or Wireless Network.” (Nacha Operating Rules & Guidelines, Section 2.5.17.1)

Do you know the difference?

- Person-to-Person (P2P)
 - Consumer Transaction Accounts are owned by different Consumers
 - Account-to-Account (A2A)
 - Both Consumer Transaction Accounts are owned by the same Consumer
- **Authorization is not required for credits between natural persons.**

The Rules allow:

Sending a **Credit** to myself or some else

- My financial institution will “debit” my account and send an ACH **Credit** to another financial institution.

Pulling a **Debit** from Myself

- My financial institution will “credit” my account and send an ACH **Debit** to another financial institution.

One consumer
cannot authorize
another consumer
to debit their
account.



Who, Me??

You are the ODFI of these entries, meaning **you** provide the warranty for these entries.



Risk-Pushing Credits

Incorrect Account but a valid account at the other financial institution

Online access

- Your account holder's credentials are compromised
- Imposter generates transactions
- Regulation E issue

Risk-Pulling Debits

- **Returns**
 - NSF, account closed, incorrect account number
 - Can you recover?
 - Debited valid account but “wrong” account
 - Automatic 60 day right of return in ACH
 - **ODFI has a warranty issue for much longer timeframe**
 - Your account holder’s credentials are compromised
 - Imposter generates transactions
 - If you offer both Credit push, debit pulls
 - They debit an account at another institution (not theirs)
 - They push that money to their account at another institution

You Decide!

- What services do you want to offer?
 - What types of entries?
 - Rules compliance based on type of entry
- Who is allowed to use the service?
- Internal Controls

What?

- Credit push and/or Debit pull
- Account-to-Account and/or Person-to-Person
 - Means of authorization
 - Security requirements

Recognize...



Entries you originated

The different types of entries you originate

Returned items

Supplementing Fraud Detection Standards for WEB Debits

March 19, 2021- The existing requirement that ACH Originators of WEB debits are required to use a “commercially reasonable fraudulent transaction detection system” to screen WEB debits for fraud was supplemented to make it explicit that “account validation” is part of a “commercially reasonable fraudulent transaction detection system.”

The new requirement applies to the first use of an account number, or changes to the account number that is to be debited.

Micro-Entries

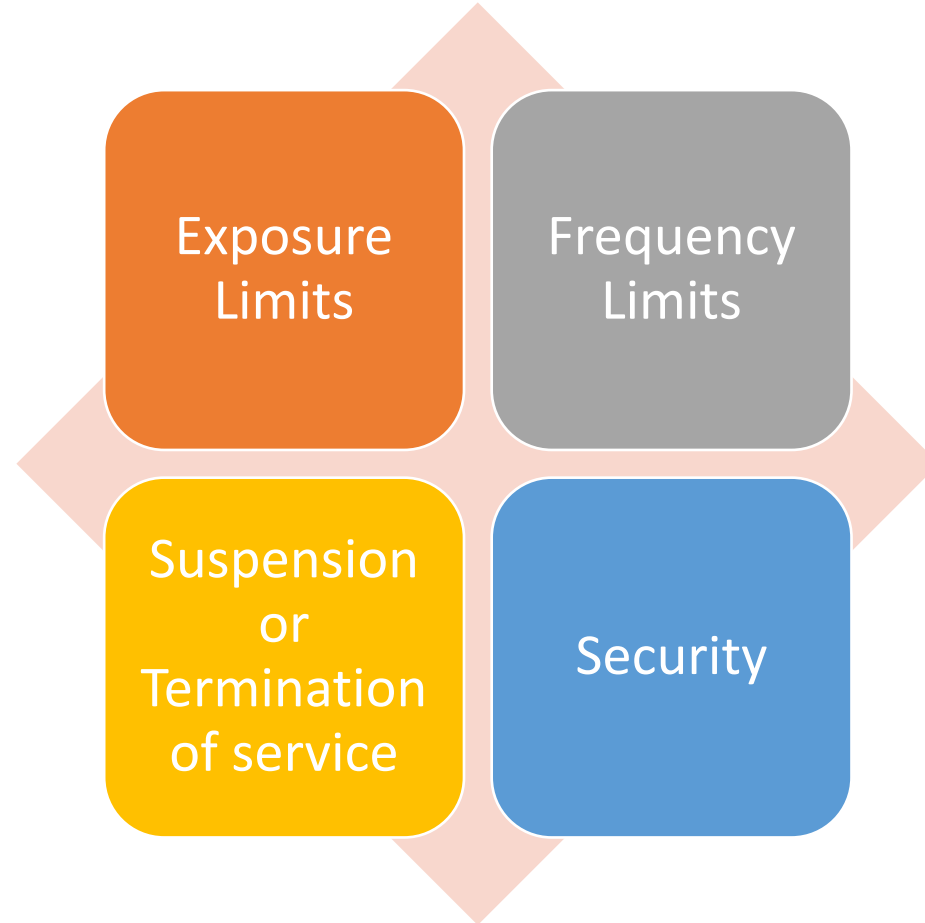
- New Rule
 - Phase 1 Effective: September 16, 2022
 - Phase 2 Effective: March 17, 2023
- Define “Micro-Entries” as ACH credits of less than \$1 and any offsetting ACH debits, used for the purpose of verifying a Receiver’s account
- Standardize the Company Entry Description and Company Name requirements for Micro-Entries
- Establish other Micro-Entry origination practices
- Apply risk management requirements to the origination of Micro-Entries

<https://www.nacha.org/rules/microentries>

Who?

- **Things you should consider:**
 - Account relationship
 - Tenure of relationship
 - New account holder??
 - **History of account activity**
 - Account balances
 - NSF's
 - Regulation E Claims
 - Recurring Deposits

Internal Controls



Educate!

- Be Proactive, Not Reactive!
 - Know current fraud trends and scams.
 - Provide education/information to your staff and account holders
 - Social Media
 - Flyers/Brochures
 - Videos
 - Emails
 - Newsletter



Moral of the story...

Be selective

Implement strong controls

Review, Revise, Repeat

Educate!

HOW DID ?
THIS HAPPEN ●

For Example:

- Credit Push – a credit was sent to another institution
- The account number is valid but it is not the “correct” account
- Does the RDFI have to return it to you?
 - **No** – not even if you ask nicely and the money is still in the account
 - There is no guarantee of recovery once that entry is sent!

For Example:

- Your account holder's access credentials are compromised by a "bad" actor
- Let's say you only push out credits...
 - Most likely you cannot recover those credits
 - Your account holder is claiming that the "debit" to their account for the credit you sent is unauthorized
 - This is a Regulation E claim
 - Unless you can prove otherwise – you are probably paying
 - Proving is the hard part
 - Your account holder's access was used – looks like them

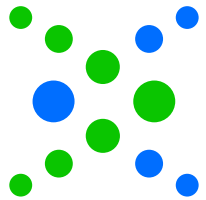
For Example:

- Your account holder's access credentials are compromised by a "bad" actor
- Let's say you offer **both** debits and credits
 - Bad actor sends debits to someone else's account, then sends the credits to their account
- The debits are returned (the credits are gone)
- Your account holder is claiming that their access was compromised – Regulation E claim
 - You end up losing out on the debits unless you can prove that your account holder did the transactions
 - **Remember – when the debits are returned by the RDFI you **cannot** refuse them if they are timely**

Questions



Continuing Education Credits



AAP[™]
Accredited
ACH Professional



APRP[™]
Accredited Payments
Risk Professional

ACH for P2P Transfers: Perils &
Protections

This session is worth 1.8 credits
(keep this slide for your records)