ECSI

How NACHA Rules Affect your Payment Processing

Introductions

Lori Carbonara

ECSI

Sr. Director, Product and Program Management

Julia Norwood

ECSI

Product Manager, Payments and Refunds

NACHA Background

NACHA, National Automated Clearing House Association established in 1974

- ❖ NACHA manages and administers the rules for the ACH payment networks:
  - √ Facilitates private-sector Operating Rules for ACH payments
  - √ Define Roles and Responsibilities of ACH Network participants
  - √ Defines and Enforces the Rules for ACH payments
  - √ Provides Education and Certification

- ❖ ACH Network provides businesses and consumers with a secure and efficient method to send and receive electronic payments:
  - √ Connects all 12,000 US financial institutions
  - √ Moves Money and Information directly from one Bank Account to another Bank Account
  - √ ACH Transactions include Direct Deposit and Direct Payment
  - √ ACH Transactions include One-Time and Recurring Payments

New NACHA Rules:
Fraud Detection & Data Security

- Supplementing Fraud Detection Standards for WEB Debits
  - **effective March 19, 2021**

- Supplementing Data Security Requirements:
  - Phase 1 – **effective June 30, 2021** for Originators and Third-Parties with ACH **volume greater than 6 million in 2019**
  - Phase 2 – **effective June 30, 2022** for Originators and Third-Parties with ACH **volume greater than 2 million in 2020**

COVID Relief NACHA Operating Rules

Due to the impact of the coronavirus pandemic, NACHA announced relief from a variety of requirements of the NACHA Operating Rules.

- ACH Operations Bulletin #7-2020, October 19, 2020
  - Supplementing Fraud Detection Standards for WEB Debits
    - effective date March 19, 2021
    - Rule will not be enforced for an additional period of one year from effective date
  - Supplementing Data Security Requirements:
    - Phase 1 – effective date June 30, 2021
    - Rule will not be enforced for an additional period of one year from effective date
    - Phase 2 – effective date June 30, 2022
    - Rule will not be enforced for an additional period of one year from effective date

Need for Fraud Detection & Data Security

Invalid Routing Number, Incorrect or Closed Account Number Risks

❖ Costs – Resources, Money & Relationships

- ➢ Payroll Delays
- ➢ ACH Reversals and ACH Recalls
- ➢ Vendor Payment Delays
- ➢ Accounts Receivable Delays
- ➢ NSFs, Returns

Account Information Exposure Risks

❖ Costs – Resources, Fines & Reputation

- ➢ Unauthorized Use of Account Data
- ➢ Potential Data Breach

2020 YoY Growth

8.2% - Transaction Volume
10.2% - Dollar Value

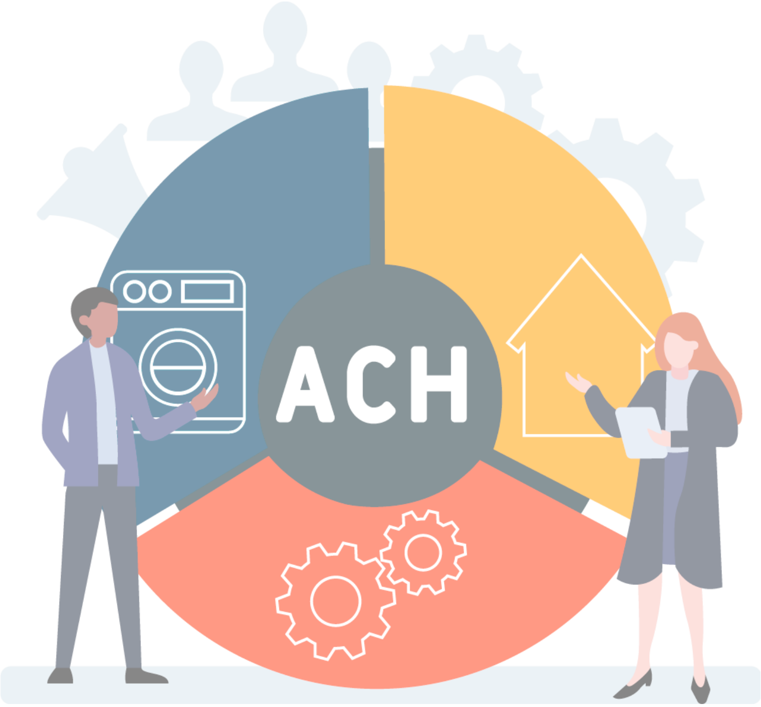
2020

26.8 Billion ACH Transactions = **$61.9 Trillion**

- 15.2B ACH Debit
- 11.6B ACH Credit

Network Volume

Increased by more than **1 BILLION EVERY YEAR** for the last 6 years



Network Value

increased by more than **1 TRILLION EVERY YEAR** for the last 8 years

2019

24.7 Billion ACH Transactions = **$55.8 Trillion**

SUPPLEMENTING FRAUD DETECTION STANDARDS FOR WEB DEBIT ENTRIES

Supplementing Fraud Detection Standards for WEB Debits

Currently, **ACH Originators** of **WEB debit entries** are required to use a **“commercially reasonable fraudulent transaction detection system”** to screen WEB debits for fraud.

- This existing screening requirement will be supplemented to make it explicit that **“account validation”** is part of a “commercially reasonable fraudulent transaction detection system.”
- The supplemental requirement applies to the **first use of an account number**, or **changes to the account number**.

❖ Account Validation is required with

- √ WEB Debit entries (ACH), internet or mobile devices
- √ first use of an account number
- √ any changes to the account number

Account Validation FAQs & Clarifications

Does the new rule require an Originator to verify account numbers for all existing WEB Debit customers?

No. This **rule applies on a “going-forward” basis** and **applies to new account numbers obtained** for initiating WEB debits.

This **rule does not apply retroactively** to account numbers that have already been used for WEB debits.

❖ Account Validation Rule

- √ applies to new account numbers obtained “going-forward”
- √ is not retroactive

Account Validation FAQs & Clarifications

If a WEB debit customer authorizes use of an account number that has been previously used successfully for non-WEB debits, must an Originator do additional validation of that account number?

No. Use of an **account number with a proven history of prior successful payments is a sufficient means for validation** for use of the account with a new WEB authorization.

- Accounts with a proven history of prior successful payments do not require re-validation.

Account Validation FAQs & Clarifications

If an Originator of WEB debits receives a Notification of Change from an RDFI requesting an update to the RDFD customer's account number, must the Originator validate the new account number before its use?

No. The accuracy of an **account number change requested by the RDFI via the NOC process** is warranted by the RDFI, which serves as validation. The **Originator need not re-validate the change**, provided it has correctly applied the change requested by the RDFI.

❖ NOC, Notice of Change does not require re-validation.

Account Validation FAQs & Clarifications

What does the term “validate” mean?

At a minimum, the Originator must use a **commercially reasonable means** to determine that the **account number** to be used for the **WEB debit** is for a **valid account** – that is, that the account to be used is a **legitimate, open account** to which **ACH entries may be posted** at the RDFI.

❖ Account must be a Valid Account
  - ✓ legitimate, open account
  - ✓ accept ACH entries

Account Validation FAQs & Clarifications

Does the new rule on account validation mean that an Originator must also validate the ownership of the account?

No. The **minimum standard** imposed by the Nacha Operating Rules **requires Originators to validate that an account is open and accepts ACH entries**.

However, because the determination of whether a business practice is considered **commercially reasonable depends on a particular Originator’s business model and risk profile**, and how it compares to similarly situated Originators, each Originator will need to determine for itself, in consultation with its own advisors, such as legal counsel and risk department, whether verifying simply that an account is open is sufficient. **For some Originators**, a more rigorous assessment that **also verifies account ownership may be appropriate** to meet a commercially reasonable standard.

- ❖ Minimum standard does not require verifying Account Ownership
    - ➢ determine if the business practice is considered commercially reasonable based on the business model and risk profile
    - ➢ consult with advisors, legal counsel and risk department

Account Validation FAQs & Clarifications

Does an account validation method or service have to cover 100% of potential account to be considered commercially reasonable?

No. An **account validation service or method might be commercially reasonable** for a specific set of facts and circumstances, **even if it does not cover 100% of potential accounts or account validation attempts**.

- ❖ Account Validation method does not have to include 100% Account Coverage
  - ➢ determine if the business practice is considered commercially reasonable based on the business model and risk profile
  - ➢ consult with advisors, legal counsel and risk department
  - ➢ consider using a secondary account validation method if deemed necessary

Account Validation FAQs & Clarifications

If an attempted account validation results in a “no hit” (i.e., neither a positive or a negative outcome), can an Originator initiate a WEB debit entry to that account number and still be compliant with the Rule?

Yes. A **commercially reasonable account validation method**, assessed based on the factors described in the Rule and these FAQs, **may include instances where a WEB debit entry is initiated even if the attempted account validation resulted in a “no hit.”**

❖ “No Hit” results do not require an account to be re-validated

Account Validation FAQs & Clarifications

Do the NACHA Operating Rules require a specific method for validating the account information?

No. The NACHA Operating Rules are **neutral with regard to specific methods or technologies** to validate account information.

❖ NACHA is neutral regarding a specific Account Validation method or technology

Account Validation FAQs & Clarifications

Are there methods of account validation that NACHA recognizes as sufficient?

Examples of methods to validate an account **may include, but are not limited to**, the use of a **Pre-notification Entry**, **ACH micro-transaction verification**, use of a **commercially available validation service provided by either an ODFI or a third-party**, and use of **account validation capabilities or services enabled by APIs**.

❖ Account Validation method examples may include, but are not limited to:

- ✓ Pre-notification Entry,
- ✓ ACH Micro-Transaction Verification,
- ✓ commercially available Validation Service provided by either an ODFI or a Third-Party,
- ✓ and Account Validation capabilities or services enabled by APIs.

Account Validation Methods

PRENOTIFICATION ENTRY

- Prenote sent to bank account, Zero-Dollar ACH Transaction
- Connects to all 12,000 US Financial Institutions

Challenges

- Response time is typically 3 or more days
- Account Ownership cannot be verified

ACH MICRO-TRANSACTION VERIFICATION

- Micro-Deposit(s) sent to a bank account, small Credit/Debit ACH Transactions
- Customer verifies amounts
- Verifies Receiver has Account Access
- Connects to all 12,000 US Financial Institutions

Challenges

- Requires response from customer, less likely to complete
- Response time may take several days
- Account Ownership cannot be verified

ACCOUNT VALIDATION SERVICE

- Real-time verification (WEB or API), bank sourced data
- Verifies Account Ownership (optional)
- Connects to bank consortium of participating US Financial Institutions

Challenges

- Not all Financial Institutions participate
- Rural/smaller banks' data can be limited

Account Validation Considerations

- Are you the ACH Originator or do you use a Third-Party Service?

- Identify and review areas of ACH Origination.

- What is your fraud risk? Do you need to validate account ownership?

- How quickly do you need a response?

ACH Origination Areas

Accounts Receivable

Student Direct Payments

Student Loan Payments

Student Online Payments

Student/Employee Physical Point of Sale

Accounts Payable

Student Refund Payments

Student/Employee Direct Deposit Payments

Vendor Payments

Account Validation Required

ACH WEB Debit Entries

Internet & Mobile Devices

Account Validation Optional

ACH WEB Credit Entries

Internet & Mobile Devices

Account Validation Questions

Do you need to Validate All ACH Transactions?

- ACH WEB Debit Entries (required)
- ACH WEB Credit Entries (optional)

Do you need to Validate Only New Bank Accounts Obtained?

- One-Time ACH Transactions, Same-Day or Future-Dated (required)
- Recurring ACH Transactions
  - New Setup Only (required)
  - Each Scheduled Transaction (optional)

Do you need to Validate Notice of Changes (optional)?

Which Account Validation Method option meets your need?

- Pre-notification
- Micro-Deposit
- Account Validation Service

SUPPLEMENTING DATA SECURITY REQUIREMENTS

Supplementing Data Security Requirements

The existing **ACH Security Framework** including its **data protection requirements** will be 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**.

- Implementation begins with the largest Originators and TPSPs (including TPSs) and initially applies to those with **ACH volume of 6 million transactions or greater annually**.
- A second phase applies to those with **ACH volume of 2 million transactions or greater annually**.

Data Security FAQs & Clarifications

When an Originator initiates entries through multiple accounts at one ODFI, or uses multiple ODFIs, how do the thresholds apply?

A **Non-Consumer ACH Originator** that originates ACH entries through **multiple settlement accounts at one ODFI**, or originates ACH entries through **multiple ODFIs**, should **consider its total, combined origination volume** when determining whether it meets the 6-million/2-million-entry thresholds.

- ❖ For ACH Originators, thresholds are based on the total, combined ACH origination volume
  - ➢ across multiple settlement accounts
  - ➢ across multiple ODFIs

- ❖ For Third-Party Servicers Providers or Third-Party Senders, thresholds are based on the total, combined ACH origination volume
  - ➢ across all Clients

Data Security FAQs & Clarifications

How does this rule impact non-financial-institution Originators and Third-Parties with volumes below the threshold?

Non-financial-institution Originators, **Third-Party Senders**, and **Third-Party Service Providers** that **do not meet these thresholds** are currently **not mandated by the *Rules*** to render ACH account information stored electronically unreadable while at rest.

Nevertheless, **NACHA strongly encourages voluntary adoption** of this **data security standards** as a **sound business practice**.

- Currently, the Rules do not apply to ACH volumes below the 2 million threshold
  - NACHA strongly encourages voluntary adoption of the rule

Data Security FAQs & Clarifications

Does the new rule to render account information unreadable apply to consumer accounts only, non-consumer accounts only, or both?

Both. If an **account number** is used for **ANY ACH payment** (**consumer or corporate**), it must be **rendered unreadable** while **stored electronically**.

- Requirement applies to any ACH payment, consumer or corporate

Data Security FAQs & Clarifications

Does the account requirement to render ACH account numbers unreadable apply only to systems where transactions can be created, or does it extend to other systems within the organization?

Any place where **account numbers** related to **ACH entries** are **stored** is in scope. This includes **systems** on which **authorizations are obtained** or **stored electronically**, as well as **databases** or **systems platforms** that **support ACH entries**.

As an example, for a **Third-Party Service Provider** whose **client is a financial institution**, these can include **platforms** that **service ACH transaction warehousing** and **posting**, and client information **reporting systems**.

For **Originators** and their **Third-Party Service Providers**, **accounts payables** and **accounts receivables systems** will be impacted, as may be other systems (for example, claims management systems for insurance companies).

- ❖ Any place where ACH Account Numbers are stored electronically
  - ✓ Platforms where ACH authorizations are obtained or stored
  - ✓ Databases where ACH entries are stored
  - ✓ Files or reports that contain ACH records, entries, returns, NOCs, etc.

Data Security FAQs & Clarifications

We have scanned our paper authorizations and ACH records into our database for easier storage. Does the new rule apply to the scanned documents even though the same documents in paper form would not be covered?

Yes. Although the new rule does not apply to the storage of ACH account information in physical, paper form, the **requirement to render the account information unreadable DOES apply** if these paper authorizations or other **documents containing ACH account numbers** are **scanned** for **electronic record retention** and **storage purposes**.

❖ Requirement applies to scanned images containing ACH Account Numbers stored electronically

Data Security FAQs & Clarifications

Do the NACHA Operating Rules prescribe the specific manner in which data at rest must be rendered unreadable?

No. The **Rules are neutral** as to the **methods/technologies** that may be used to **render data unreadable while stored at rest electronically**. Encryption, truncation, tokenization, destruction, or having the financial institution store, host, or tokenize the account numbers, are among options for Originators and Third-Parties to consider, but each **Originator** or **TPSP** will need to **make its own business decision in consultation with its legal counsel and technology providers**.

- ❖ NACHA is neutral regarding a specific method or technology to be used, but requires that a commercially reasonable method be used
  - ➢ determine if the business practice is considered commercially reasonable based on the business model and risk profile
  - ➢ consult with advisors, legal counsel and risk department

Data Security FAQs & Clarifications

Our electronic documents are stored on platforms that are not encrypted, but access is restricted by access controls- e.g., passwords, etc. Data is not accessible except to those with proper credentials. Does this comply with the new rule requirement?

No. Although access controls such as passwords help to secure ACH-related data at rest, these do not meet the new standard. Even with the use of **various physical security controls** and **restricted access**, the **electronic data at rest** still must be **rendered unreadable**.

- ❖ ACH account information at rest must be rendered unreadable

Data Security FAQs & Clarifications

What if I need access to my customer's full DFI account number in order to conduct customer service or other job-related functions? How does the new rule apply?

When access to and the **ability to view a customer's full DFI account number** is **necessary to perform a customer service function** or **to conduct authorized business**, the **data is considered "active" and not in an at-rest state**, and the requirement that the **account number be unreadable does not apply**.

Nevertheless, even in an "active" state, the **account information must be protected** from **unauthorized use or unauthorized access** through the use of **appropriate risk controls** (such as passwords and other access controls) that **limit access to "active" data only to authorized personnel**. Once access to the account number is no longer needed to conduct a particular business function and is returned to a passive state, it must be returned to an unreadable state for storage purposes.

- ❖ Data is considered "active" if it is being used to perform a customer service function or to conduct authorized business
- ❖ Access to the data must be limited to authorized individuals with a business need for the time frame that the business need exists and further protect the data from unauthorized access using additional access controls such as passwords.

Data Security Requirements

ACH Originators must protect deposit account information by rendering it unreadable when stored electronically

- any place where account numbers related to ACH entries are stored electronically
- data at rest must be unreadable

Applies to ACH Entries

- ✓ Credit and Debits
- ✓ Consumer and Corporate

Does not include

- Payment Methods other than ACH
- Routing Numbers, Account Type, Account Holder Name

Requirement applies to non-consumer Originators

- ✓ non-FI Originators
- ✓ Third-Party Service Providers (TPSPs) & Third-Party Senders (TPSs)

Data Security Considerations

- Are you the ACH Originator or do you use a Third-Party Service?
- Determine your total ACH Volume? Which threshold applies?
- Identify areas where ACH Entries are obtained or stored electronically.
- Consult with your IT staff and partners, contact your Bank, payments and technology Vendors.

SUMMARY & RESOURCES

Supplement Fraud Detection Summary

❖ Supplementing Fraud Detection Standards for WEB Debit

The first time a **consumer checking account** is used for an **electronic (ACH) payment**, if the payment is taken or initiated over an **online channel**, the **account number must be validated first**.

- **Effective Date**, **March 19, 2021**

NACHA will not enforce this rule for an additional period of one year from the rule’s effective date with respect to covered entities that are working in good faith toward compliance, but that require additional time to implement solutions.

Supplement Data Security Summary

❖ Supplementing Data Security Requirements

The rule expands the existing ACH Security Framework rules to explicitly require large senders of payments to **protect account numbers by rendering them unreadable when stored electronically**

- **Tier 1 – Effective Date, June 30, 2021** for Originators and Third-Parties with ACH **volume greater than 6 million in 2019**
- **Tier 2 – Effective Date, June 30, 2022** for Originators and Third-Parties with ACH **volume greater than 2 million in 2020**

NACHA will not enforce this rule for an additional period of one year from the rule’s effective date with respect to covered entities that are working in good faith toward compliance, but that require additional time to implement solutions.

NACHA Resources

- ACH Rules Resources for Corporates is free to use and provides access to:
  - Sign Up for Rules News, End-User Briefings, Upcoming Rule Changes, Resources & more
  - https://www.nacha.org/content/ach-rules-resources-corporates
- Supplementing Data Security Requirements
  - https://www.nacha.org/rules/supplementing-data-security-requirements
- Supplementing Fraud Detection Standards for WEB Debit
  - https://www.nacha.org/rules/supplementing-fraud-detection-standards-web-debits
- ACH Operations Bulletin #7-2020, dated October 19th, 2020
  - https://www.nacha.org/sites/default/files/2020-10/ACH_Operations_Bulletin_7-2020_Nacha_Provides_COVID_Relief_Update_October_19_2020.pdf
- Account Validation Resource Center
  - https://www.nacha.org/content/account-validation-resource-center
- Account Validation Webinar Series, February 16th to 19th, 2021
  - Complimentary, hosted by NACHA's Preferred Partners
  - visit: https://www.nacha.org/events/account-validation-webinar-series-0

THANK YOU!

Questions?