Nacha Update

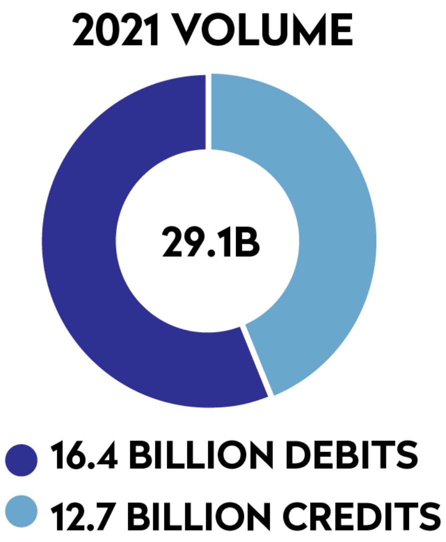
July 20, 2022

Jordan Bennett, AAP, APRP
Senior Director, Network Risk Management

Nacha®

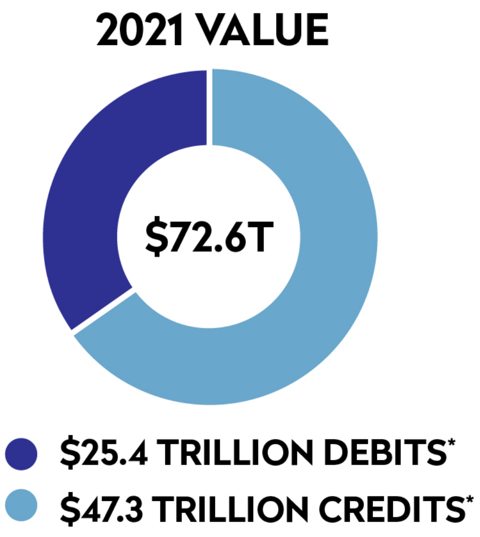
2021 ACH Network Volume and Value

29.1B TRANSACTIONS TOTALING $72.6T



● 16.4 BILLION DEBITS

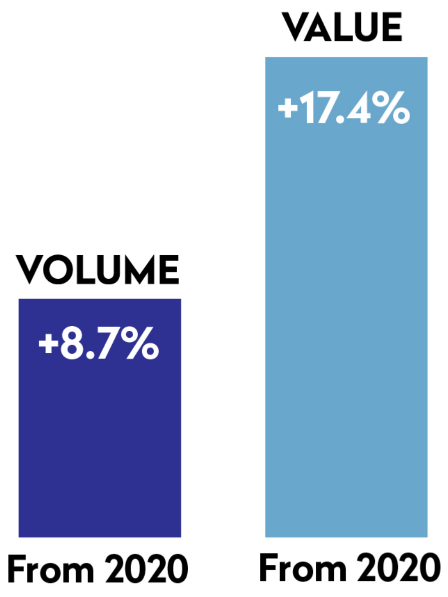
● 12.7 BILLION CREDITS



● $25.4 TRILLION DEBITS*

● $47.3 TRILLION CREDITS*

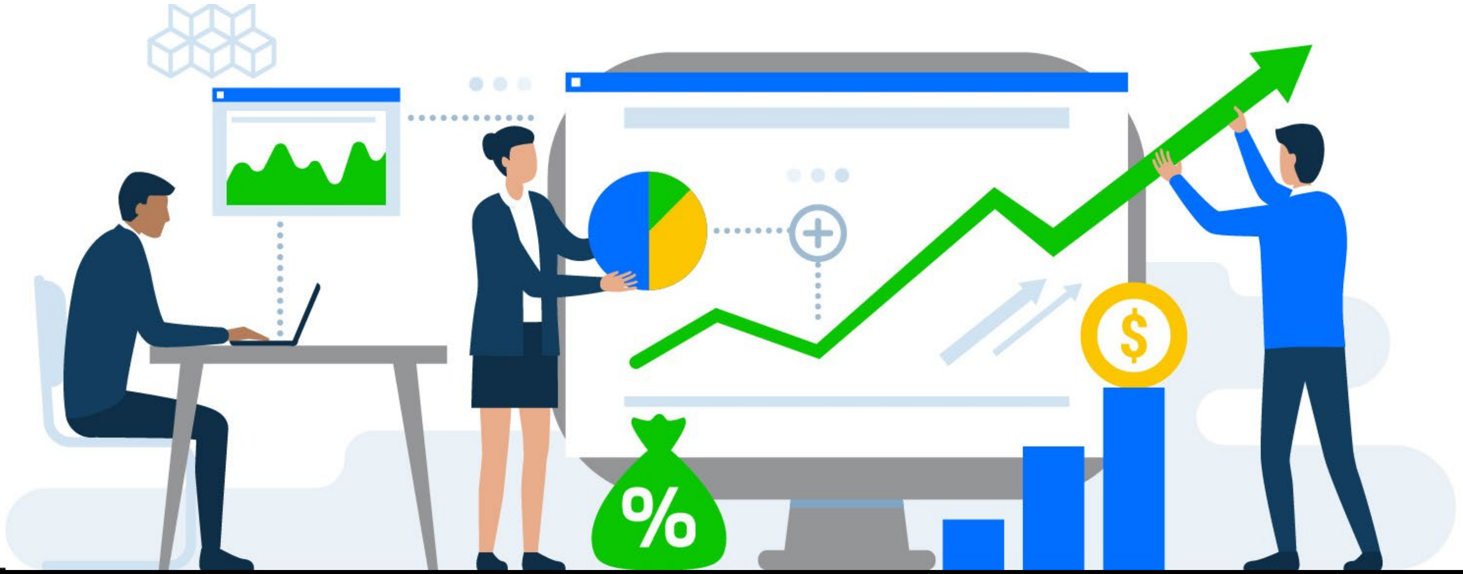
*Totals may not add due to rounding



2021 ACH Network Volume and Value

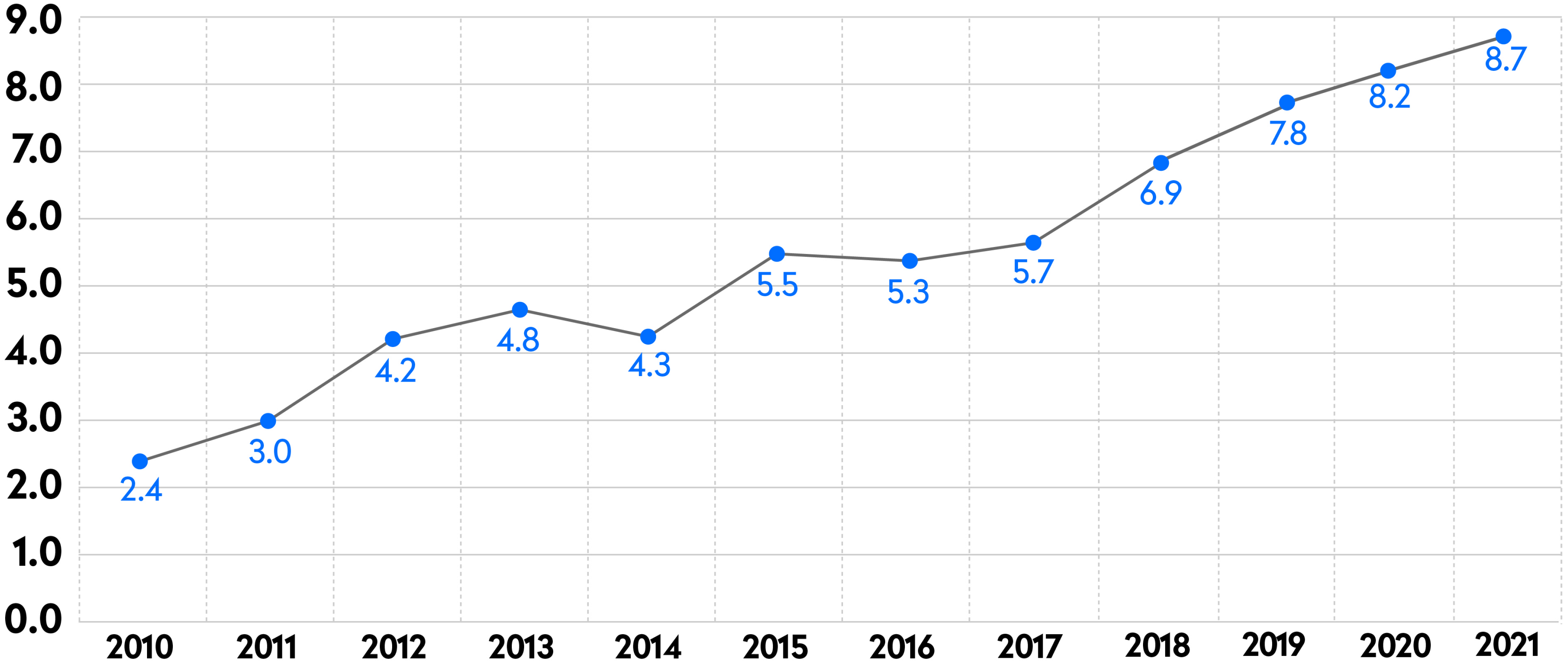
Volume has increased by **MORE THAN 1B** every year for the last 7 years

Value has increased by **MORE THAN $1T** every year for the last 9 years



The Annual Percentage Increase of ACH Network Transaction Volume Network

Transaction volume was up 8.7% in 2021

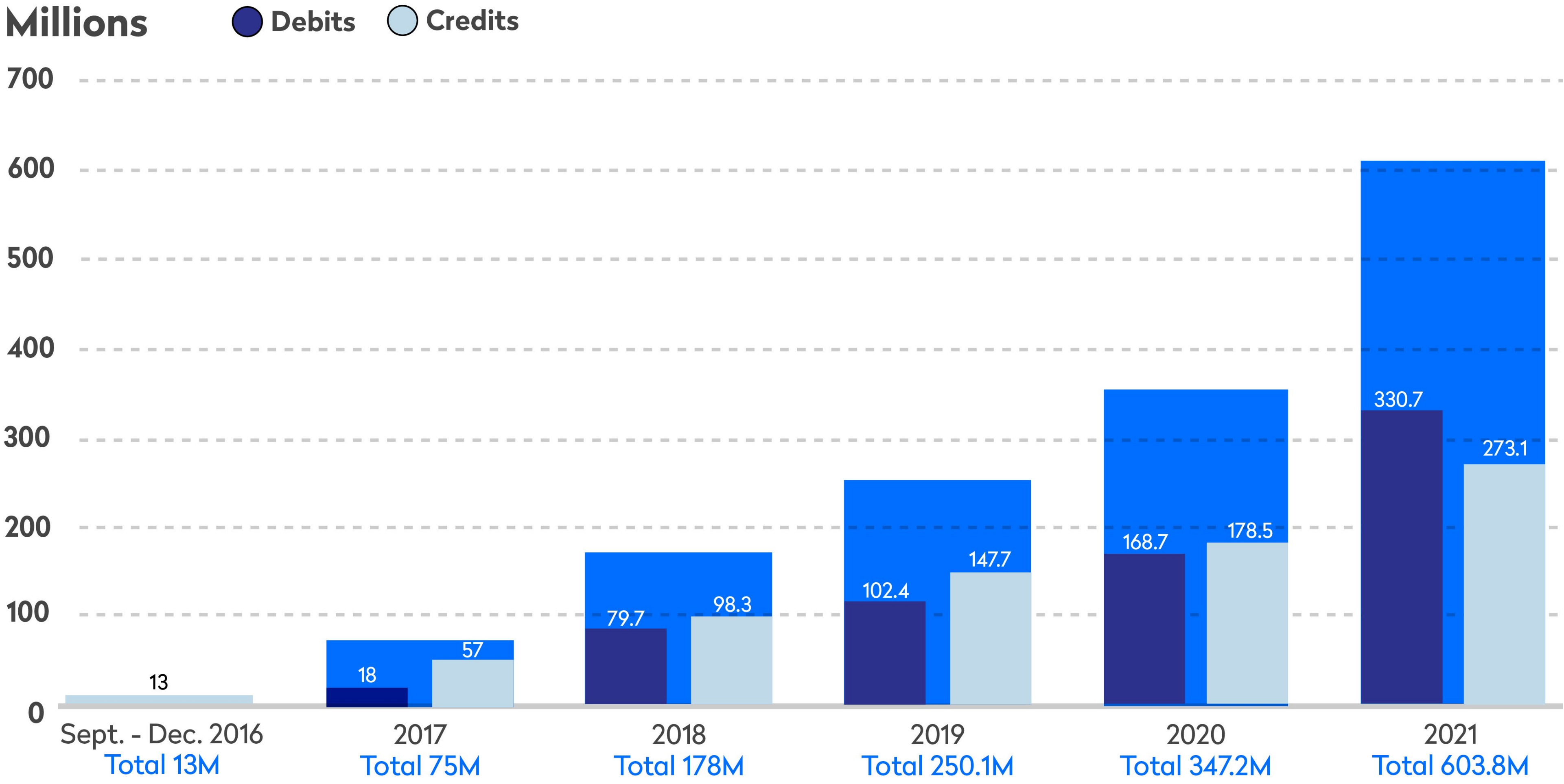


B2B is B-I-G…

5.3 billion B2B ACH payments in 2021, up 20.4% from 2020, transferring $49.8 trillion, up 19.4%

133.5 million B2B Same Day ACH payments in 2021, up 104.4% from 2020, transferring $387.4 billion, up 143.2%

Same Day ACH volume rose nearly 74% in 2021



2022 - 2023 Nacha Operating Rules Effective Dates

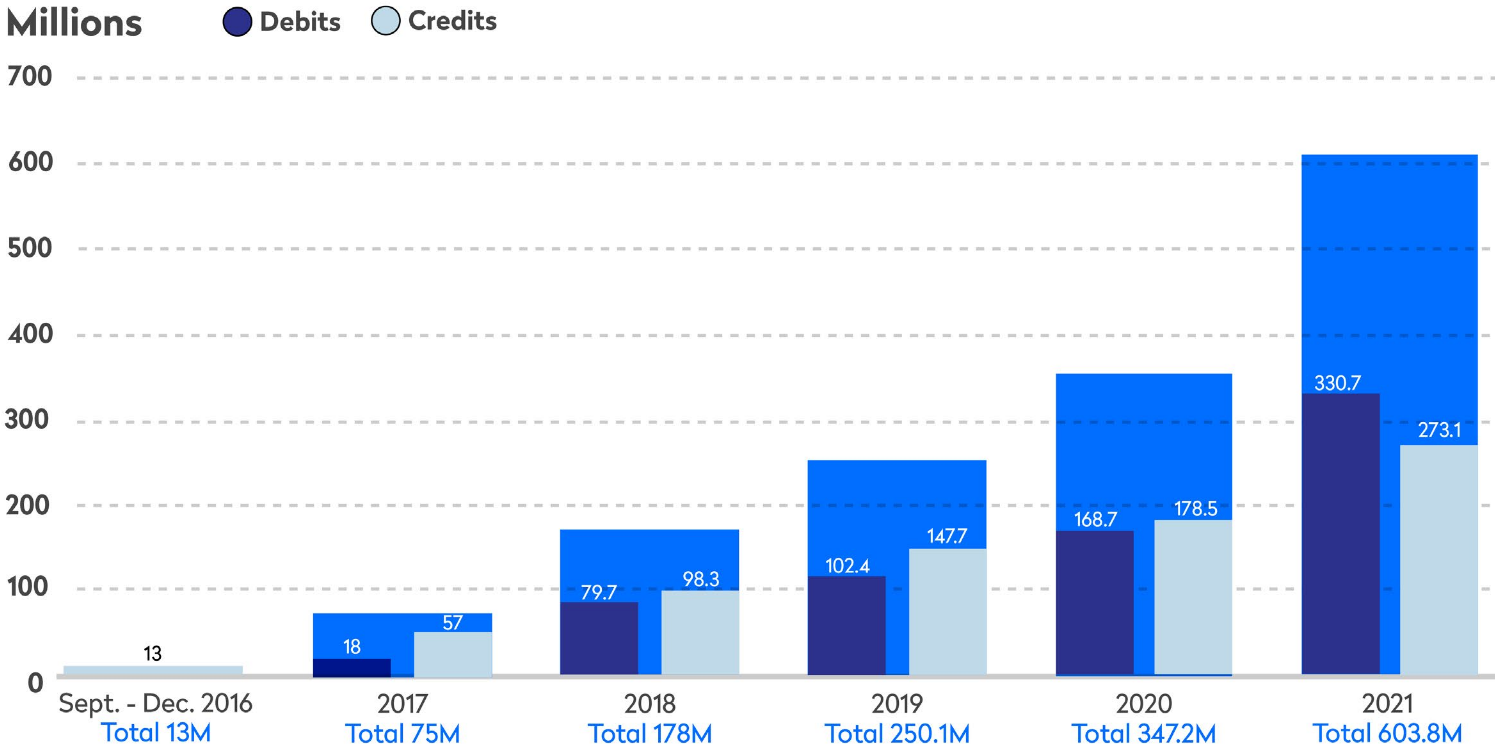
	Upcoming Rules
March 18, 2022	Same Day ACH dollar limit increase to $1M
June 30, 2022	Account Information Security Requirements (Phase 2)
Sept 16, 2022	Micro-Entries (Phase One)
Sept 30, 2022	Nested Third-Party Senders Third-Party Senders and Risk Assessments
March 17, 2023	Micro-Entries (Phase Two)

Effective **March 18, 2022**

Same Day ACH Transaction Limit Increase to $1M

7 phases of implementation so far:

1. Same Day Credits **Sept. 2016**
2. Same Day Debits **Sept. 2017**
3. Funds availability at 5 pm **Mar. 2018**
4. Better funds availability **Sept. 2019**
5. Dollar limit increase to $100K **Mar. 2020**
6. Third Same Day Window **Mar. 2021**
7. Dollar limit increase March 18, 2022



The Same Day ACH $1 Million Dollar Limit

On March 18, 2022, the per transaction dollar limit for Same Day ACH transactions increased from $100,000 to $1 million. Use cases include the following:

- B2B payments
- Payroll deposits and funding
- Insurance claims/Disaster assistance payments
- Tax payments
- Merchant funding for payment card transactions
- Account-to-account transfers
- Reversals
- Business Continuity

From Feb 2022 to March 2022, when the per payment limit went from $100k to $1M,the average value of a Same Day ACH payment grew by 26%.

Effective **March 19, 2021** Same Day ACH hours have been extended by 2 hours every banking day

ACH Schedules and Funds Availability

Processing window	ODFI deadline	RDFI receipt time	Settlement	Credit funds availability requirement
First Same Day ACH window	10:30 am ET	12 noon ET	1:00 pm ET	1:30 pm RDFI local time
Second Same Day ACH window	2:45 pm ET	4:00 pm ET	5:00 pm ET	5:00 pm RDFI local time
Third Same Day ACH window	4:45 pm ET	5:30 pm ET	6:00 pm ET	End of processing day
Next Day ACH	2:15 am ET	Throughout banking day according to ACH Operator schedule – last file 6:00 am ET	8:30 am ET	On Settlement Date
		If received prior to 5:00 pm RDFI local time		9:00 am RDFI local time

Effective **June 30, 2021/2022**

Account Information Security Requirements

The rule expands the existing ACH Security Framework rules to explicitly require large, non-FI Originators, Third-Party Service Providers (TPSPs) and Third-Party Senders (TPSs) to protect account numbers by rendering them unreadable when stored electronically.

- Aligns with existing language contained in PCI requirements
- Neutral as to methods/technology – encryption, truncation, tokenization, destruction, data stored/hosted/tokenized by ODFI, etc.

Phase I - ACH Originators/TPSPs/TPSs with ACH volume of 6 million transactions or greater annually (June 30, 2021)

Phase II - ACH Originators/TPSPs/TPSs with ACH volume of 2 million transactions or greater annually

- An Originator/Third-Party that originated 2 million or more ACH transactions in calendar year 2020 (June 30, 2022)

Nacha®

Commercially Reasonable Fraud Detection for WEB Debits

If your organization allows consumers to make purchases or payments via the internet or mobile devices and directly, electronically withdraws payments from their checking accounts, this rule applies to you:

The rule language is explicit that “account validation” is part of a “commercially reasonable fraudulent transaction detection system”

- 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.
  - This could be the first time a customer makes a payment, or when a consumer changes the account number being used for online payments.

First Use + WEB Debit = Account Validation

Update on Account Validation

The Supplementing Fraud Detection Standards for WEB Debits rule became effective:

March 19, 2021

- ➢ Aka “the Account Validation” rule

Nacha has seen decreasing number of industry participants asking about the new rule

Operations Bulletin #7-2020 (issued 10/19/2020) notified the industry that:

- ➢ March 2021 effective date would not be delayed
- ➢ Nacha would not enforce this rule for one year after the effective date to allow for additional time to implement solutions

Nacha’s Account Validation Resource Center **nacha.org/AVResources**

Nacha Micro-Entry Rule

WHAT:

A new Nacha Rule defining and standardizing Micro-Entry formatting and practices.

WHY:

To improve the effectiveness of Micro-Entries as a means of account validation; to better enable Financial Institutions and other parties to identify and monitor Micro-Entries; to improve ACH Network quality.

ACH Network

Nacha®

Nacha Micro-Entry Rule

WHEN:

Effective in two phases, though Nacha encourages all ACH Network participants to make use of the new provisions as soon as possible.

Phase 1 Effective Sept. 16, 2022:

- "Micro-Entries" will be defined as ACH credits of less than $1, and any offsetting debits, for account validation. Credit amounts must be equal to, or greater than, debit amounts, and must be transmitted to settle at the same time.
- Originators must use "ACCTVERIFY" in the company entry description field.
- Company name must be easily recognizable to Receivers and the same or similar to what will be used in subsequent entries.

Phase 2 Effective March 17, 2023:

- Originators must use commercially reasonable fraud detection. This includes monitoring forward and return Micro-Entry volumes.

ACH Network

Nacha®

Learn more at:
Nacha.org/MicroEntries

Micro-Entries - Examples

Examples of Micro-Entry credits and debits that would be **permitted** under this Rule:

- Example 1 - One credit Micro-Entry of $0.34 and one debit Micro-Entry of $0.19 (aggregate net credits are permitted)
- Example 2 - Two credit Micro-Entries of $0.18 and $0.49; no debit offsets (multiple credit Micro-Entries are permitted)
- Example 3 - Two credit Micro-Entries of $0.18 and $0.49; and 1 offsetting debit Micro-Entry of $0.67 (aggregate Micro-Entries net to zero)
- Example 4 - Two credit Micro-Entries of $0.37 and $0.84; and 1 offsetting debit Micro-Entry of $1.21 (debit Micro-Entries can be greater than $1 to offset multiple credit Micro-Entries)
- Example 5 - Two credit Micro-Entries of $0.52 and $0.63; and 2 offsetting debit Micro-Entries of $0.71 and $0.44 (multiple debit and credit Micro-Entries that net to zero)

Examples that would be improper under this Rule:

- Example 6 - One credit of $1.08 (a credit that is $1.00 or more)
- Example 7 - One credit of $0.19 and 1 debit for $0.34 (in aggregate, a net debit)
- Example 8 - One debit of $0.34 (a debit that is not an offset of a credit)

Meaningful Modernization Rules

Five specific Rules proposals, collectively referred to as “Meaningful Modernization”, were recently approved

The overarching purpose is to improve and simplify the ACH user-experience by

- Facilitating the adoption of new technologies and channels for the authorization and initiation of ACH payments
- Reducing barriers to use of the ACH
- Providing clarity and increasing consistency around certain ACH authorization processes; and
- Reducing certain administrative burdens related to ACH authorizations

Meaningful Modernization - Overview

The five Rules:

1. Explicitly define the use of standing authorizations for consumer ACH debits
2. Define and allow for oral authorization of consumer ACH debits beyond telephone calls
3. Clarify and provide greater consistency of ACH authorization standards across payment initiation channels
4. Reduce the administrative burden of providing proof of authorization
5. Better facilitate the use of electronic and oral Written Statements of Unauthorized Debit

Effective date for all of September 17, 2021

Standing Authorization - Purpose

The purpose of defining a Standing Authorization is to explicitly enable businesses and consumers to make payment arrangements for relationships that are ongoing in nature, especially those that make use of new technologies and channels for ongoing commerce

- The current authorization framework for consumer ACH debits encompasses recurring and single payments
  - Recurring payments occur at regular intervals and are for the same or similar amount – e.g., a monthly mortgage payment or utility bill
  - A single entry is a one-time payment, and can be between parties that have no previous relationship, such as in a purchase; or between parties that have a relationship but the payment is not "recurring" – e.g., a single payment on a credit card account
- Establishing a framework for standing authorizations in the Nacha Rules fills this gap between single and recurring payments, and help ACH Originators understand how to do it

Standing Authorization - Overview

This rule defines a “Standing Authorization”:

- An advance authorization by a consumer of future debits at various intervals
- Future debits can be initiated by the consumer through some further action,
  - Different from recurring entries which require no further action and occur at regular intervals

In addition to defining a Standing Authorization, other aspects of the rule include:

- A Standing Authorization can be obtained in writing or orally
- Individual payments initiated based on the Standing Authorization would be defined as Subsequent Entries
- Individual Subsequent Entries can be initiated in any manner identified in the Standing Authorization

Standing Authorization - Overview

This rule also allows Originators some flexibility in the use of SEC codes for individual Subsequent Entries

- Allows an Originator to use the TEL or WEB codes for Subsequent Entries when initiated by either a telephone call or via the Internet/wireless network, respectively, regardless of how the Standing Authorization was obtained
- In such cases, the Originator would not need to meet the authorization requirements of TEL or WEB, but would need to meet the risk management and security requirements associated with those codes

SEC Code Scenarios for Standing Authorizations and Subsequent Entries

Scenario 1

- ➢ An Originator that obtains a standing authorization on a paper form with a wet signature (current Rules result in PPD entries) would be allowed to use TEL or WEB for individual payments initiated by a telephone call or via the Internet/wireless network, respectively

Scenario 2

- ➢ An Originator that obtains an oral authorization on a telephone call (current Rules result in TEL entries) would be allowed to use WEB for individual payments initiated via the Internet/wireless network through an app or via text

Scenario 3

- ➢ An Originator that obtains authorization via the Internet/wireless network (current Rules result in WEB entries) would be allowed to use TEL for individual payments initiated via a telephone call

Standing Authorization – Additional Requirements

Retention Requirements for Standing Authorizations - Specifies that an Originator must retain a copy of each:

1. Standing Authorization for 2 years following termination/revocation of the Standing Authorization;
2. Proof that each entry was initiated by the Receiver for 2 years following the settlement date of the entry

Proof of authorization for Standing Authorizations must include:

1. A copy of the Standing Authorization, and
2. evidence of the Receiver's affirmative action to initiate a Subsequent Entry

Data security requirements for Subsequent Entries

- Where the Receiver's affirmative action for a Subsequent Entry may involve the communication or confirmation of any banking information via an unsecured electronic network, the Originator must comply with existing security requirements as defined within Section 1.7 (Secure Transmission of ACH Information Via Unsecured Electronic Networks)

Standing Authorization – Optional Formatting

An Originator may, at its discretion, identify an entry as having been originated under the terms of a Recurring Authorization, a Single-Entry Authorization, or a Standing Authorization

- Standard code values developed for this purpose
  - “R” - Recurring,
  - “S” - Single,
  - “ST” – Standing Authorization
- For PPD entries, these values may go within the optional Discretionary Data Field; for TEL and WEB, an Originator may choose to include these values within the Payment Type Code Field

To accommodate this option, this Rule:

- Removes the existing requirement that TEL and WEB entries must be identified as either Recurring or Single Entries
- Designates the field inclusion requirement for Payment Type Code as an “optional” field
- Permits Originators to use the Payment Type Code field to include any codes meaningful to the them, including, at the Originator’s discretion, use of the values “R,” “S,” or “ST,” as described above

Oral Authorizations

The purpose of allowing the use of Oral Authorizations more broadly is to better enable businesses to adopt ACH payments in transactional settings that make use of verbal interactions and voice-related technologies

Examples of how Oral Authorizations can be used include:

- Voice interactions with home digital assistants ("Alexa, pay my bill")
- Oral authorization of a bill payment via the Internet that is not a telephone call (Facetime, Skype, etc.)
- A consumer provides a Standing Authorization on a telephone call, and initiates subsequent payments online

Previously, the authorization rules did not provide for oral authorization of an ACH payment outside of telephone call

- ACH Originators wanting to make use of voice authorizations face ambiguous rules for their business scenarios with no clear guidance

Oral Authorizations

This rule defines and allows “Oral Authorization” as a valid authorization method for consumer debits distinct from a telephone call

- Currently, only the TEL transaction type has requirements and addresses risks specific to an oral authorization; but it is specific to a telephone call
- Many newer methods and channels make use of verbal interactions and voice-related technologies

Any oral authorization obtained regardless of the channel will need to meet the requirements of an Oral Authorization

An Oral Authorization obtained over the Internet that is not a telephone call also will need to meet the risk and security requirements that currently apply to WEB entries, and would use the WEB SEC Code

A Standing Authorization could be obtained orally

- Or, Subsequent Entries initiated under a Standing Authorization could be initiated through voice commands, instructions, or affirmations

Oral Authorizations – Additional Clarifications

Security requirements

- Clarifies that, where the Receiver’s Oral Authorization is communicated (other than a telephone call) over an Unsecured Electronic Network, the Originator must comply with existing security requirements as defined within Section 1.7 (Secure Transmission of ACH Information Via Unsecured Electronic Networks)

Retention/Proof of Authorization requirements

- Specifies that an Originator’s obligation for proof of authorization for an oral authorization is (1) the original or duplicate audio recording for a recurring entry; and (2) the original or duplicate audio recording or a copy of the written notice for single entry or subsequent entry

Other Authorization Proposals

Clarity

- Re-organizes the general authorization rules to better incorporate Standing Authorizations, Oral Authorizations, and other changes described below
- Defines “Recurring Entry” to complement the existing definition of Single Entry and the proposed new definition of Subsequent Entry, and align with terms in Regulation E

Flexibility

- Explicitly states that authorization of an ACH payment can be by any method allowed by law/regulation
- Only consumer debit authorizations require a writing that is signed or similarly authenticated

Consistency

- Applies the standards of “readily identifiable” and “clear and readily understandable terms” to all authorizations
- For all consumer debit authorizations, applies the minimum data element standards (i.e., what should be in a consumer authorization)

Effective **September 17, 2021**

Alternative to Proof of Authorization

Some ACH Originators report that a "pain point" occurs when they provide proofs of authorization at the request of their customer's financial institution, but then debits are still regularly returned as unauthorized

Some Originators would prefer to agree to accept the return of the debit rather than expend the time and resources necessary to provide proof of authorization

The rule alleviates the burden of providing proof of authorization in every instance in which it is requested

Alternative to Proof of Authorization

If permission to return is granted in lieu of the proof of authorization yet the copy is still needed, the requesting FI may submit a written subsequent request requiring the provision of proof of authorization.

- Specifies that an Originator's FI (ODFI) must provide the proof of authorization within 10 banking days of the RDFI's subsequent request to the ODFI
- Originators must provide copy in such a time to permit ODFI to comply
  - See ACH Origination agreement w/FI or Third Party Sender

Effective **September 17, 2021**

Written Statement of Unauthorized Debit via Electronic or Oral Methods

This Rule clarifies and makes explicit that a financial institution may obtain a consumer's Written Statement of Unauthorized Debit (WSUD) electronically or orally

- The same formats/methods permissible for obtaining a consumer debit authorization are permissible for obtaining a consumer's statement of unauthorized debit
- Although not prohibited, confusion existed in market
- An additional clarification that a consumer is permitted to sign a WSUD with an Electronic Signature

Originators that receive consumer unauthorized returns may request a copy of the signed written statement from the consumer's FI (RDFI) through their FI (ODFI) or third party provider.

- Copy to be provided by FI within ten banking days of the ODFI's request
- Requestors should be prepared that the statements may be in various formats

New Third-Party Sender Roles and Responsibilities Rules to Implement Sept 30, 2022

Nested Third-Party Senders

- Defines a Nested Third-Party Sender
- Updates the requirements of Origination Agreements for a Nested TPS relationship
- Establishes the “chain of agreements” and responsibilities in a Nested TPS arrangement
- Updates existing TPS registration to denote whether a TPS has Nested TPS relationships

Third-Party Senders and Risk Assessments

- Makes explicit that a Third-Party Sender, whether Nested or not, must complete a Risk Assessment of its ACH activities
- Clarifies that a Third-Party Sender cannot rely on a Rules Compliance Audit or a Risk Assessment completed by another TPS in a chain; it must conduct its own

Nested Third-Party Senders

This rule amendment defines a Nested Third-Party Sender, and provides for the “chain of agreements” and responsibilities in Nested TPS arrangements

- A “Nested Third-Party Sender” will be defined as a Third-Party Sender that has an agreement with another Third-Party Sender to act on behalf of an Originator, and does not have a direct agreement with the ODFI
- Nested TPSs must be addressed in ACH Origination Agreements
    - An ODFI Origination Agreement with a TPS must address whether the TPS can have Nested TPSs, and if so, “push down” the requirement for an Origination Agreement to exist between a TPS and a Nested TPS
    - An Origination Agreement must exist between a TPS and a Nested TPS
    - Changes to ACH Origination Agreements are applicable on a going-forward basis from the effective date of September 30, 2022
- Other TPS obligations and warranties have been updated to identify and cover Nested TPSs
- This rule amendment does not address or limit the number of levels in a Nested Third-Party Sender arrangement

Nacha®

Third-Party Senders and Risk Assessments

- Risk Assessments are already defined and required in the Nacha Rules for Financial Institutions and, by extension, for Third-Party Senders under their obligations to perform and warrant ODFI obligations
  - However, the Risk Assessment obligation for TPSs was not expressly stated
- The new rule expressly states that a Third-Party Sender, whether or not it is Nested, is required to conduct a Risk Assessment
  - As with other parties that conduct Risk Assessments, a Third-Party Sender must implement, or have implemented, a risk management program based on their Risk Assessment
  - The obligation to perform a Risk Assessment, as well as the required Rules Compliance audit, cannot be passed onto another party; i.e., each participant must conduct or have conducted its own

Third-Party Senders and Risk Assessments

- This rule amendment does not prescribe a specific methodology or list of topics for a TPS Risk Assessment
  - Risk Assessments for TPS should not be one-size-fits-all
  - Each TPS operates in a different space, with challenges, risks, and controls that may be different than the challenges, risk and controls faced by another TPS
- Attempting to prescribe the exact topics and methods for a TPS risk assessment would likely over-prescribe risk and controls for some TPSs, and fail to identify risk and controls for others
- Assistance in understanding and performing Risk Assessments is widely available in the marketplace, through Payment Associations, Nacha publications, and many other organizations

Third-Party Sender Roles and Responsibilities - Effective Date and Implementation Periods

- Both rule amendments would become effective on a single effective date: September 30, 2022

- Changes to ACH Origination Agreements are effective on a going-forward basis – i.e., applicable to agreements entered into on or after the effective date
    - ODFIs should notify TPSs of new Rules, even if not required to "re-paper" existing agreements, to ensure knowledge of and compliance with these Rules
- A six-month grace period, to March 31, 2023, has been provided for:
    - ODFIs to update TPS registrations to denote whether or not a TPS has Nested TPSs
    - TPSs that have not conducted a Risk Assessment to do so
        - A TPS need not wait for passage of this rule, or its effective date, to conduct a Risk Assessment

Tips to stay compliant

- Do business with Financial Institutions or Payment Processors that know and understand your business line.
- Work with your customers and Financial Institution or payment processor partners to correct issues rather than moving from one to another.
  - Proper Authorization and consumer understanding is essential.
  - Use the tools and options available in the market or from partners to verify and monitor customers.
  - Originators or Third-Party Senders may be placed on the TOD (Terminated Originator Database) when terminated. Other FIs and Third-Party Senders can see when and why an Originator was terminated and take that into account when onboarding.
- Stay current on new Nacha Rules.

Nacha Resources

jbennett@nacha.org

ACH Supports Businesses: https://www.nacha.org/business

ACH Quick Start Tool: https://www.nacha.org/quick-start-tool

Account Validation Resource Center
https://www.nacha.org/AVResources

New and upcoming ACH Rules and Requests for Comment (RFC) https://www.nacha.org/OperatingRules

Same Day ACH Resource Center
https://nacha.org/SameDayResources

Sign up for Rules News https://www.nacha.org/RulesNews

Purchase the Nacha Operating Rules and Guidelines
https://www.nacha.org/store