

Take your ACH Payments to the Next Level

Brad Smith, AAP, Nacha

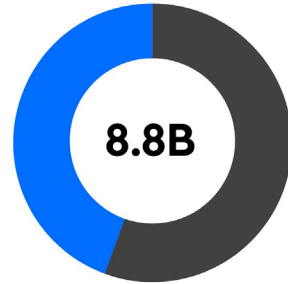
Debbie Barr, AAP, AFPP, CTP, Nacha



3Q 2025 ACH NETWORK

Volume Totals 8.8 Billion;
B2B Volume Rises 10% From a Year Earlier

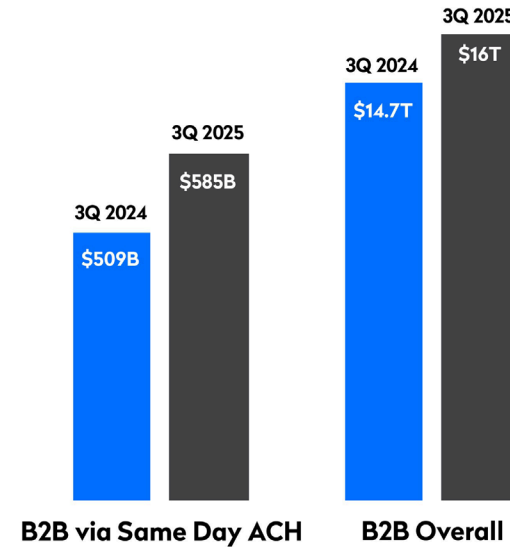
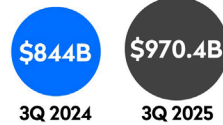
3Q 2025 Total ACH Network Volume



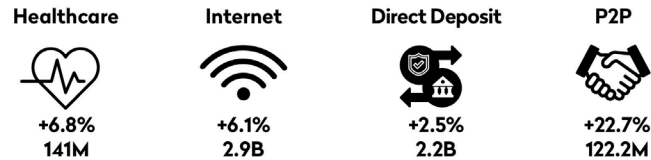
● 4.9 Billion Debits
● 3.9 Billion Credits

Overall value of B2B
increases 8.8%;
Value of B2B through
Same Day ACH climbs 15%

Same Day ACH value increases 15%



Volume across major transaction types compared to 3Q 2024



Learn more at nacha.org

© 2025 Nacha. All rights reserved.



What Is Pay by Bank?

- Generally, it refers to a payment or transfer from a bank account that is:
 - Initiated in an all-digital environment, and frequently mobile-first
 - Enabled by modern digital technologies – identity verification, account validation, open banking and APIs
 - Not reliant on consumers knowing and providing their routing and account numbers
- The underlying payment rail is typically ACH, but can refer to other methods.

What Is Pay by Bank?

- As a term, Pay by Bank is primarily used by industry – not by consumers.
 - The term Pay by Bank is an industry-driven term used to talk about emerging trends for payments but is not generally well known among consumers.
- As a product, Pay by Bank is primarily marketed by fintechs to businesses.
 - Products named Pay by Bank are typically marketed as payment tools for businesses, not direct B2C products.

Pay by Bank Use Cases

- Bill payments
 - Utilities; credit cards; loans; medical; insurance; dues, etc.
- Account transfers
 - Bank accounts; brokerage accounts; digital wallets
- Subscriptions
 - Streaming and digital services; gyms and fitness;
- Donations
 - Non-profits; schools (academics; scholarships; athletics; alumni); charities; houses of worship
- Services
 - Ride-share; home services; personal services
- Goods (digital and/or physical)
 - E-commerce purchases; in-store purchases

What Is Pay by Bank?

Nacha has formed a Pay by Bank project team within the Payments Innovation Alliance. The anticipated project deliverables are:

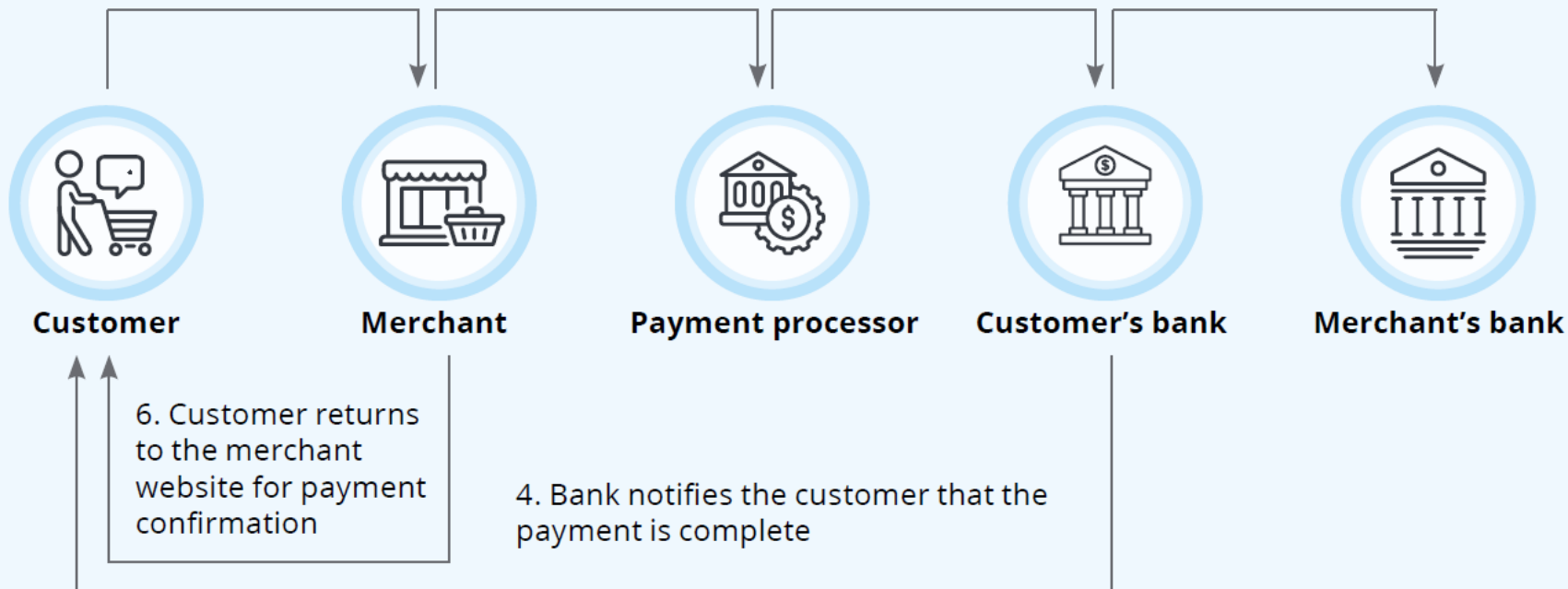
- Describe Pay by Bank use cases and articulate the benefits and risks for consumers, organizations and financial institutions.
- Assemble an inventory of publicly available or member-supplied Pay by Bank market research.
- Identify any operational or risk factors that could be addressed by industry guidance or Nacha Rule amendments.
- Identify consumer education needs and opportunities and develop educational resources.
- Publish and socialize all project deliverables.
- [Pay by Bank FAQs | Nacha](#)

1. Customer checks out and selects Pay by Bank as payment method.

2. Customer selects their bank and is redirected to bank portal

3. Customer enters account credentials and is validated

5. A transfer is made from customer's bank account to the merchant account over an existing payment rail like ACH, RTP, FedNow, etc.



Pay-by-bank transaction flow

Nacha Rules



© 2024 Nacha. All rights reserved. Nacha staff confidential. This document is confidential and contains information regarding Nacha staff matters. It should not be shared with other parties.

It's Important to Maintain Up-to-Date Routing Transit Numbers!

ACH payments use the RDFI's routing transit number.

Using updated routing information avoids failed payments, which not only upset customers but cause additional exceptions and expense, as well as reputational risk for organizations and financial institutions.

It's Important to Maintain Up-to-Date Routing Transit Numbers!

How Often Should You Check for Updates?

Users of certain software or services may have routing number verification provided to them. If so, consult with your software or service providers to ensure that timely updates are made.

When determining the frequency of routing number updates needed, consider that routing number changes may happen multiple times per week. Daily updates may be preferable for frequent or larger-volume participants.

Available solutions include:

[LexisNexis® Bankers Almanac® Routing Transit \(RTN\) File](#)

[Federal Reserve Banks' E-Payments Routing Directory](#)

Who Needs to Maintain Current Routing Information?

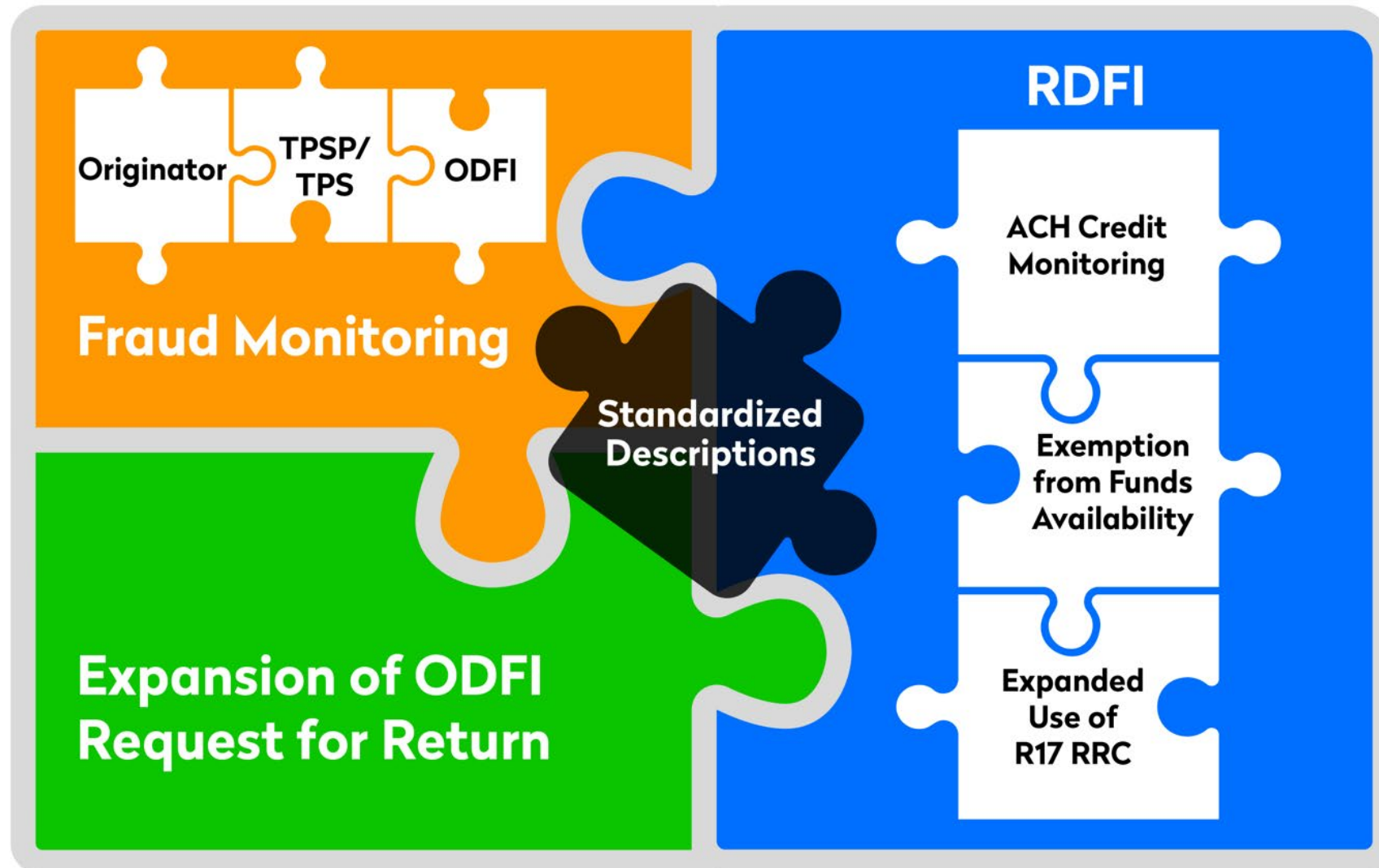
Originating parties, including:

- ✓ ODFIs.
- ✓ Originators (parties who initiate credit or debit ACH payments).
- ✓ Third-Party Service Providers (software/service vendors) including:
- ✓ Third-Party Senders (intermediary parties that transmit ACH payments).
- ✓ Vendors who host payment pages for Originators.
- ✓ Account validation vendors.

Dates	Effective Dates for Rule Amendments
March 20, 2026	☐ New Company Entry Descriptions – PAYROLL and PURCHASE ☐ Fraud Monitoring – Phase 1 • Non-consumer Originators (and vendors) with 2023 ACH origination volume of 6 million or greater ☐ ACH Credit Monitoring – Phase 1 • RDFIs with 2023 ACH receipt volume of greater than 10 million
June 22, 2026	☐ Fraud Monitoring – Phase 2 • All other non-consumer Originators (and vendors) ☐ ACH Credit Monitoring – Phase 2 • All other RDFIs

<https://www.nacha.org/newrules>

Risk Management – Pieces of a puzzle



False Pretenses

“the inducement of a payment by a Person misrepresenting (a) that Person’s identity, (b) that Person’s association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited.”

This definition covers common fraud scenarios such as Business Email Compromise (BEC), vendor impersonation, payroll impersonation, and other payee impersonations, and complements language on “unauthorized credits” (account takeover scenario). It does not cover scams involving fake, non-existent or poor-quality goods or services.

False Pretenses

Examples of credit Entries authorized under False Pretenses:

- Receiver of the credit Entry misrepresents the Receiver's identity or ownership of the receiving account.
 - Fraudster impersonates someone with the authority to order payment (e.g., a CEO/CFO via business email compromise) to induce someone with authority to originate a payment from the credit account to make a payment.
 - Fraudster claims to be a vendor with whom the accountholder has a relationship and requests payment to fraudster's account.
 - Fraudster claims to be a real estate settlement agent or attorney and requests funds transferred to fraudster's account.
 - Fraudster claims to be an employee of an organization and requests payment to fraudster's account; or, fraudster gains access to organization's payroll system and redirects payroll payments to fraudster's account.

False Pretenses

Examples of what is not considered an unauthorized credit Entry or a credit Entry authorized under False Pretenses:

- A dispute regarding the quality or condition of, or warranties or timing of delivery for, goods or services (provided there are not other circumstances that would give rise to a claim of False Pretenses or unauthorized payment). For example, a business payment to a vendor, for which the quantity or quality of goods delivered is later disputed.
- Payment is made to the right person/organization but induced on a basis other than False Pretenses (e.g., a contribution to a charitable organization because it says they are going to spend the funds on something particular and then spends it on something else).

Reminder - Example of credit Entry not authorized by the Originator:

- Account takeover - Fraudster gains access to the credentials necessary to initiate a transaction and initiates a credit entry from the accessed account. The accountholder (Originator) did not authorize the credit entry.

Standard Company Entry Descriptions

Transactions originated for these purposes must contain the required description.

PAYROLL

- Requirement applies to Originators of all types of employment compensation payments, regardless of the status of the employment relationship (i.e., employee, contract employee, other). Does not apply to benefits.
- Use of the term “PAYROLL” is intended for descriptive purposes only, to help identify compensation payments. Originators and ODFIs transmitting entries with this entry description make no representation or warranty regarding the Receiver’s employment status.

PURCHASE

- Requirement applies to Originators of online (including mobile/text) individual purchases. Includes, as an example, Buy Now Pay Later purchases that result in multiple payments.
- Does not include payment for ongoing services such as monthly recurring utility or rent payment set up online.
- Segments higher-risk online payments, the largest transaction type by volume.

Effective date: March 20, 2026 - This is a “no later than” date, companies and payroll providers may begin using the description as soon as practical.

Transaction Monitoring Rules

Upcoming Rules will require transaction monitoring by all parties in the ACH Network

“establish and implement risk-based processes and procedures...that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses”

For corporate ACH Originators, these processes and procedures could include internal controls to:

- Detect and prevent account takeover.
- Detect and prevent business email compromise (BEC) and similar attacks.
- Conduct out-of-band verification of payment instructions and changes.
- Identify other anomalies.

March 20, 2026 effective date

- Corporate ACH Originators (and vendors) with 2023 ACH origination volume of 6 million or greater.

June 22, 2026 effective date

- All other corporate ACH Originators (and vendors).

<https://www.nacha.org/newrules>

Fraud Monitoring by Originators, TPSPs, and ODFIs – Rule Requirement

Who: All non-consumer parties involved in the creation and sending of an ACH transaction

What:

- Must establish and implement processes and procedures that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses.
 - Risk-based
 - Relevant to the role it plays in the authorization or Transmission of Entries
- Make appropriate updates to address evolving risks.

When: These processes and procedures do not require the screening of every ACH transaction individually, and do not need to be performed prior to processing.

- Determination of timing should consider the ability to meet the spirit of the rule: prevention, recovery, and communication.

ACH Fraud Monitoring

- A risk-based approach cannot be used to conclude that no monitoring is necessary at all; *at a minimum, an entity should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.*
- Monitoring transactions prior to processing provides the greatest opportunity for detecting and preventing potential fraud but is not required.
- For transactions in which monitoring identifies a high potential for fraud, the Originator should consider some action based on the monitoring results. Actions may include, but are not limited to:
 - stopping further processing of a flagged transaction;
 - consulting with the Receiver, using previously verified communication methods, to determine the validity of the transaction;
 - consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and
 - using the results of account validation methods completed prior to ACH origination to determine if characteristics of the Receiver's account raise additional red flags.

ACH Fraud Monitoring

- Originators may be best placed to implement procedures to protect against account takeover or other vectors for initiating unauthorized transactions, such as change controls regarding payment information and instructions for vendor and payroll payments.
- Third-Party Senders and Third-Party Service Providers involved in the origination of ACH Entries may have processes and procedures to review the volume, velocity, dollar amounts and SEC Codes of their originated ACH Entries.
- The basis for relying on another originating entity should be reasonable and clear (e.g., allocated by contract and verified by appropriate oversight). Any processes and procedures implemented by RDFIs and other receiving side ACH participants do not affect the obligations of originating participants.

Fraud Monitoring by Originators – Implementation Considerations

All ACH payments – All SEC codes included in monitoring requirements

Risk assessment/identification as first step.

- Identify risks and size.

Consider expanding existing monitoring:

- Volume and value anomalies
- Velocity
 - Account number
 - Name on account
- Return monitoring/analysis
- Overpayments
- Account Validation
 - Always a Nacha best practice for many types of payments; usefulness in compliance determined by risk or even potentially ACH partner contracts.
 - If currently using for WEB, why not look to expand to all first use of account number as a potential step in RM rule compliance, as well?

Contract/ACH Origination Agreement review/update

- Dependencies/Roles should be defined, agreed upon and included in vendor/customer oversight.

Guidance

The 2025 Nacha Operating Guidelines have been updated for Originator Fraud Monitoring, providing guidance and considerations including:

- Understanding fraud threats.
- Internal controls specific to types of schemes.
- General controls for payment initiation.

Contact your FI or vendor or visit Nacha's website to obtain a copy.

Information is also found in Nacha's Risk Resource Center.

RISK MANAGEMENT RESOURCES

The safety of the ACH Network for all participants is key. Nacha has numerous risk management resources available including fraud prevention and Nacha Rules compliance. You can filter the information by both resource type and audience.

Risk Management Resources

• ALL RESOURCES • TOPIC ▾ • AUDIENCE ▾ • TYPE ▾ • DATE ▾



FRAUD PREVENTION



FRAUD PREVENTION



CONTACTS



FRAUD PREVENTION



Risk Management Resource Center

Access from Nacha.org home page, upper right corner <https://www.nacha.org/risk-resources>

Your go-to location for all risk content.

Filter by:

- Topics
- Audience
- Type
- Date

News

Consulting

Contact



Risk Resources



PAYMENTS ENABLEMENT ▾

LOGIN ▾

RISK MANAGEMENT RESOURCES

The safety of the ACH Network for all participants is key. Nacha has numerous risk management resources available including fraud prevention and Nacha Rules compliance. You can filter the information by both resource type and audience.

Risk Management Resources

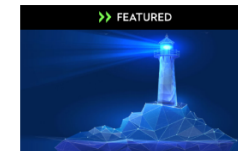
• ALL RESOURCES • TOPIC ▾ • AUDIENCE ▾ • TYPE ▾ • DATE ▾



FRAUD PREVENTION



FRAUD PREVENTION



CONTACTS



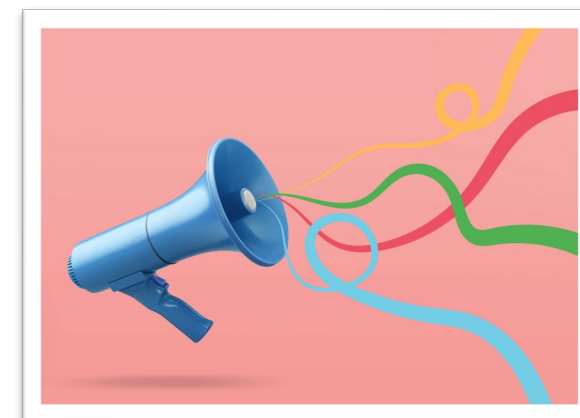
FRAUD PREVENTION

Be an Active Participant in the Rulemaking Process – Respond to Requests for Comment/Information

Nacha requests are open to all participants in the industry. Responses are kept confidential, and we review every response provided!

Available on the webpage – <https://www.nacha.org/rules/proposed> - often with a video to walk your team through the proposal, and special survey for end-users to provide input.

We want to hear from you!!



Hint: To be notified about proposals and receive helpful reminders of deadlines sign up for Rules News and Risk Management Tools: <https://www.nacha.org/RulesNews>

Resources to Help ACH End-Users with the Rules - *ACH Rules Resources for Corporates and Governmental Organizations*

An online resource created to help end users be aware of and understand changes to the Nacha Operating Rules

- Includes End User Briefings, links to new Rules information, links to open Requests For Comment, and other Resource Centers

Sign up for **Rules News & Risk Management Tools** – the free newsletter that provides hot-off-the-press news about all things ACH Rules related

To subscribe, Log in to nacha.org. Go to My Profile, then My Email Preferences. Or click here:

[Nacha Resources for Treasury, Finance and Payroll Professionals | Nacha](#)

Anyone can sign up and there's no marketing, just news and tools you can use!



Payments
Innovation Alliance®

[Alliance Project Teams | Nacha](#)

Alliance members join Project Teams to create deliverables that are available to all.

Deliverables from Alliance initiatives include creating resources and tools, developing best practices and testing proofs of concept – ultimately shaping the future of payments.

ACH for Developers Guide Project Team

Consumer Financial Exploitation Project Team

Cybersecurity & Payments AI Project Team

Faster Payments Playbook for Corporates Project Team

Faster Payments Professionals Certificate Project Team

Navigating Through Digital Payments Project Team

Pay by Bank Project Team

Quantum Payments

Former Project Teams and Resources

Additional Resources

[AFP Payments Guide to ACH: What Corporates Need to Know](#)

“This guide aims to highlight ways...to use ACH more efficiently, in ways that reduce operational cost and risk, and enhance your use of liquidity, given the constant threat of fraud.”

[2024 AFP Payments Fraud and Control Survey Report](#)

[Why is check fraud suddenly rampant?](#) By Michael Timoney, Federal Reserve Bank of Boston

Action Items

- Prepare for fraud monitoring in 2026
- Prepare for PURCHASE and PAYROLL entry descriptions in 2026
- Evaluate how and when you are updating your Routing Number tables for clean ACH entries
- Sign up for Rules News and Risk Management Tools

THANK YOU

Questions? Let's Connect:

Debbie Barr, AAP, CTP

Associate Managing Director,
ACH Network Rules, Process & Communications

dbarr@nacha.org

[LinkedIn.com/in/debbiebarraap](https://www.linkedin.com/in/debbiebarraap)

Brad Smith, AAP

Senior Director,
Industry Engagement and Advocacy

bsmith@nacha.org

[LinkedIn.com/in/bradsmith](https://www.linkedin.com/in/bradsmith)