CORE BANK

Quarterly Newsletter

ISSUE #14 | Q1 2026

CONTENTS

RULES & REGULATIONS EDITION

Staying compliant with evolving payment system rules remains critical as fraud tactics, data standards, and settlement expectations continue to change. This Q1 2026 Rules and Regulations Edition builds on prior guidance and focuses on ACH, Third Party Senders, wire transfers, ISO 20022, and instant payments, with emphasis on regulatory and network rule updates now in effect or approaching key compliance deadlines.

NACHA (National Automated Clearing House Association) governs the ACH Network and sets the rules for ACH payments in the United States. For a deeper dive into the 2026 NACHA rule changes and what they mean for Originators and Third Party relationships, we encourage you to review our recent blog post: https://corebank.com/2026-nacha-rule-changes/

Additional technical guidance is also available through NACHA resources, or by contacting our Treasury Management team for a consultation.

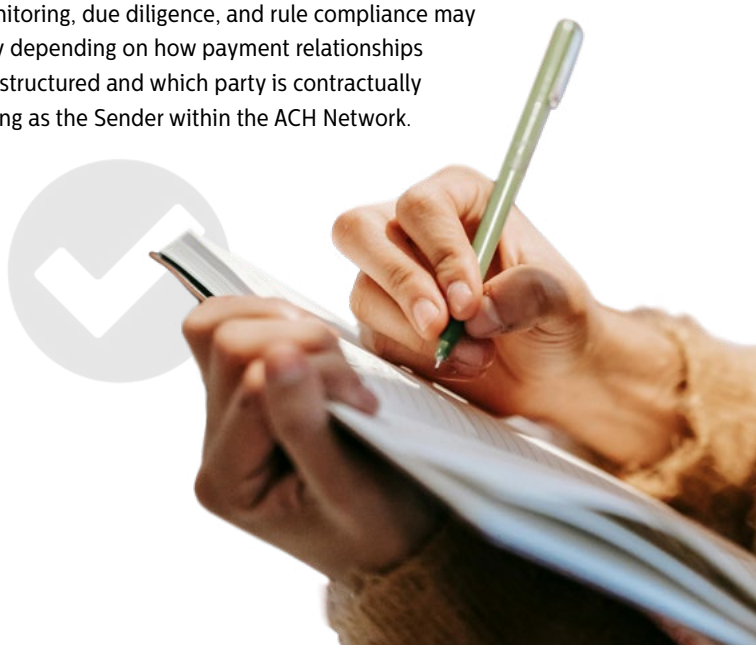
ACH NETWORK UPDATES

2026 NACHA RULE CHANGES:

NACHA has finalized several significant ACH Operating Rule updates that materially expand fraud detection, monitoring, and governance expectations across the ACH Network. These changes apply to several key participants within the ACH Network:

- Originators – businesses or entities that initiate ACH transactions to send or collect funds from another party.
- Third-Party Senders (TPS) – companies that act as intermediaries by submitting ACH entries to a financial institution on behalf of Originators.
- Third-Party Service Providers (TPSP) – vendors that provide ACH processing, software, or technical services related to ACH file creation or transmission but do not act as the submitting Sender.
- Originating Depository Financial Institutions (ODFIs) – financial institutions that enter ACH transactions into the ACH Network on behalf of their Originator customers and warrant compliance with ACH rules.
- Receiving Depository Financial Institutions (RDFIs) – financial institutions that receive ACH entries from the network and post them to the accounts of their customers.

Clarifying these roles is important, as responsibility for monitoring, due diligence, and rule compliance may vary depending on how payment relationships are structured and which party is contractually acting as the Sender within the ACH Network.



CORE BANK

Quarterly Newsletter

ISSUE #14 | Q1 2026

EXPANDED FRAUD MONITORING REQUIREMENTS

New NACHA rules in 2026 strengthen fraud detection expectations across the ACH Network.

Businesses, Third Party Senders, and financial institutions must maintain risk-based processes to identify and respond to potentially fraudulent ACH activity. These requirements apply broadly and are no longer limited to only certain ACH entry types.

Participants classified by Nacha as "larger" ACH participants are those that originate 6 million or more ACH entries annually. These organizations must comply beginning March 20th, 2026.

All remaining participants, those originating fewer than 6 million ACH entries annually, must comply by June 22nd 2026.

Annual reviews of fraud monitoring processes are required for all participants, regardless of volume.

While Nacha does not prescribe a one-size-fits-all framework, risk-based processes may include:

- Monitoring return rate trends (including unauthorized returns)
- Reviewing ACH activity for anomalies or velocity spikes
- Establishing documented escalation procedures
- Conducting periodic ACH risk assessments
- Performing enhanced due diligence for higher-risk Originators
- Board or senior management reporting, where appropriate

STANDARDIZED COMPANY ENTRY DESCRIPTIONS

Beginning March 20, 2026, NACHA requires standardized descriptions for certain ACH transactions to improve clarity and fraud detection.

KEY REQUIREMENTS

- The first 7 characters must contain PAYROLL or PURCHASE and be capitalized.
- The Company Entry Description field allows up to 10 characters.
- **PAYROLL** - Required for all PPD credit entries used for wages, salaries, or similar compensation.
  PURCHASE - Required for all e-commerce purchase transactions.

Businesses should confirm ACH templates and payment files are updated ahead of the effective date.

THIRD PARTY SENDER & THIRD PARTY SERVICE PROVIDER EXPECTATIONS

Third Party payment arrangements remain an area of heightened oversight. Businesses that rely on Third Party Senders or processors should expect stronger monitoring and governance requirements. This includes regular review of ACH activity, return trends, and unauthorized transactions, as well as confirmation that Originators are complying with NACHA standards.

NACHA has approved updates to International ACH Transaction rules to clarify when cross border ACH formatting applies. These changes take effect in September 18th 2026 and are intended to reduce confusion while maintaining sanctions and compliance controls.

WIRE TRANSFERS AND ISO 20022

FEDWIRE FUNDS SERVICE ISO 20022 MIGRATION

Wire transfers now use the ISO 20022 messaging standard following the Federal Reserve's July 2025 Fedwire migration.

ISO 20022 enables more detailed and structured payment information, improving accuracy, compliance screening, and reconciliation. Businesses should ensure wire templates and payment instructions include complete and accurate beneficiary information.

CORE BANK

Quarterly Newsletter

ISSUE #14 | Q1 2026

BEST PRACTICES

STRENGTHEN PAYMENT APPROVALS

Use dual approval for ACH, wire, and instant payment transactions whenever possible. Segregate duties so no single employee can create and release a payment.

TRAIN YOUR TEAM ON FRAUD PREVENTION

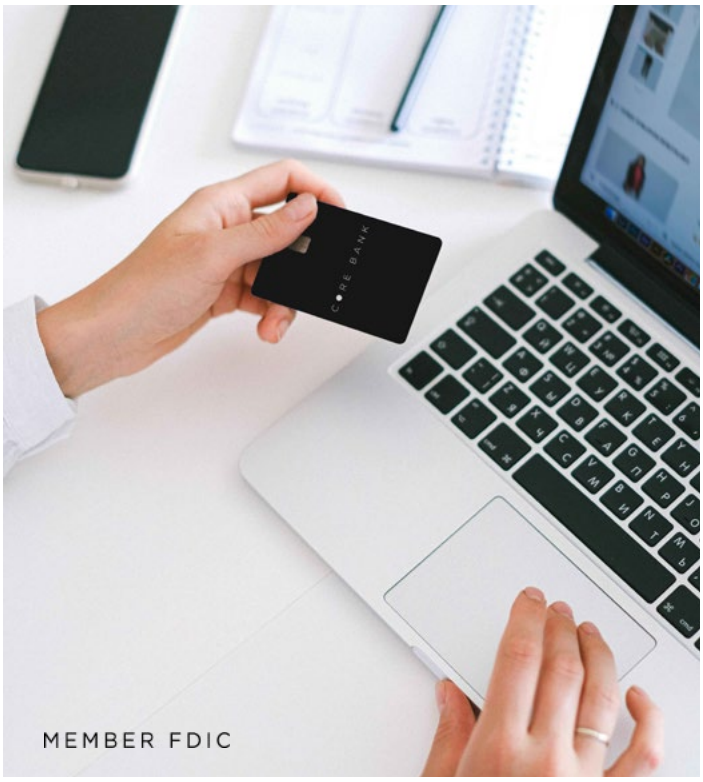
Educate employees on common fraud tactics such as phishing, business email compromise, and payment redirection schemes. Regular training helps teams recognize and stop suspicious activity before funds move.

VERIFY PAYMENT INSTRUCTIONS

Confirm new or changed payment instructions using a trusted, out of band contact method. Avoid relying solely on email for payment changes, especially for wires and instant payments.

SECURE YOUR PAYMENT PROCESS

Use dedicated and secure devices for banking activity. Monitor accounts daily and reconcile transactions promptly to quickly identify unauthorized or unexpected activity.



USE BANK SECURITY TOOLS

Take advantage of available tools such as ACH Positive Pay, transaction alerts, multi factor authentication, and soft tokens. These controls add critical layers of protection as payment speeds increase.

REVIEW THIRD PARTY PAYMENT ACTIVITY

If you use Third Party Senders or processors, regularly review ACH activity, returns, and unauthorized transactions. Understand how your partners monitor fraud and escalate issues.

These practices help reduce fraud risk and support compliance as payment rules and technologies continue to evolve.

STAYING AHEAD IN A RAPIDLY EVOLVING PAYMENTS ENVIRONMENT

With advancements in payments, and fraud prevention technology, early adopters gain a significant advantage. Secure systems and integrated payment options are now essential for meeting customer expectations. For more information, contact Core Bank's Treasury Services at TreasuryServices@CoreBank.com.

LOOKING FOR A PARTNER OR A ROBUST PAYMENTS SOLUTION?

Whether you are a fintech seeking a sponsor bank, a business exploring embedded finance, Core X is ready to help.

WE OFFER:

- Flexible APIs for payments, accounts, and verification
- Strong compliance and risk management support
- Dedicated relationship teams
- Modern sponsor and embedded banking infrastructure

Visit our Partner Banking website to explore how we can work together to build innovative and secure payment experiences.
Partner Banking | Core X

Core-X is a division of Core Bank.
For additional information on how Core Bank can help mitigate payment fraud please contact the Treasury Services team at treasuryservices@corebank.com.