Guide to Nacha 2026 Rule Changes

Protect Your Institution. Meet the New Standard.

Published August 2025

affirmative NEACH Payments Group

Introduction

Nacha's 2026 Fraud Monitoring Rule changes are the most significant ACH compliance shift in over a decade.

This guide includes:

- Nacha 2026 Overview
- Recent and upcoming rule changes tied to Nacha 2026
- Role-specific responsibilities
  - RDFIs
  - ODFIs
  - TPS
  - Originators
- FAQs
- A readiness evaluation checklist
- Technology and solution provider considerations

NACHA 2026 OVERVIEW

What Is the Nacha 2026 Rule Change?

The 2026 Rule Change represents the most significant update to ACH credit-side fraud controls in years. Finalized in 2025 and officially effective March 20, 2026, it introduces standardized Company Entry Descriptions for credits and a two-phase rollout of fraud monitoring obligations across the ACH Network.

Key Requirement:

- All ACH Network participants must implement risk-based procedures to monitor ACH credit entries.
- Monitoring must detect entries that are potentially unauthorized or initiated under false pretenses (e.g., BEC, account takeover, mule schemes).
- Applies to both receiving (RDFI) and originating (ODFI) institutions, as well as Originators, TPSPs, and TPSs.
- Monitoring procedures must be documented, periodically reviewed, and actionable.
- Aligns credit-side risk oversight with existing debit-side fraud controls.

Objectives:

- Reduce credit-push fraud across the ACH Network, including BEC, account takeovers, and money mule activity.
- Improve transparency and consistency with standardized Company Entry Descriptions (e.g., PAYROLL, PURCHASE).
- Require all participants to take an active role in detecting and managing risk related to ACH credits.
- Enable faster, more coordinated fraud responses between RDFIs and ODFIs.
- Support a more resilient ACH ecosystem through structured, risk-based fraud oversight.

NACHA 2026 OVERVIEW

Who Is Impacted?

Date	Rule / Rule Phase	Who Is Affected	Key Requirement
March 20, 2026	Standardized Company Entry Descriptions	Originators of payroll or e-commerce purchases.	Required use of PAYROLL and PURCHASE descriptions on PPD and WEB credits
March 20, 2026	Fraud Monitoring – Phase 1	RDFIs with ≥10M credit-entry ACH receipts in 2023; ODFIs + large non-consumer Originators, TPSPs, TPSs with ≥6M origination volume in 2023	Establish and implement documented, risk-based procedures to detect and respond to entries suspected of being unauthorized or originated under false pretenses.
June 19, 2026	Fraud Monitoring – Phase 2	All other RDFIs and Originators/TPSPs/TPSs that didn't meet volume thresholds in 2023	Establish and implement documented, risk-based procedures to detect and respond to entries suspected of being unauthorized or originated under false pretenses.

RELATED RULE CHANGES

Rule Changes that Support Fraud Monitoring

Within the past couple years, Nacha has set the stage for financial institutions to have the ability to effectively monitor fraud. For questions on the specifics of the changes, feel free to reach out to **NEACH Payments Group** or your Payment Association.

Expanded Use of Return Code R17

- **What:** Look for unusual patterns or anomalies (e.g., high-dollar credits inconsistent with past behavior).
- **Impact:** Allows RDFIs to alert ODFIs to potential fraud and can protect an Entry from going to an unintended recipient.

Expanded Use of Return Code R06

- **What:** Expands the permissible uses of the Request for Return to allow an ODFI to request a return from the RDFI for any reason.
  - The Rule requires the RDFI to respond to the ODFI, regardless of whether the RDFI complies with the ODFI's request to return the entry.
- **Impact:** Allows ODFIs to communicate with RDFIs on their request for return of an entry for any reason, which may include Entries initiated due to fraud.

RELATED RULE CHANGES

Rule Changes that Support Fraud Monitoring

Additional Funds Availability

- **What:** Provides RDFIs with an additional exemption from the funds availability requirements to include credit ACH entries that the RDFI suspects originated under False Pretenses.
  - RDFIs must still follow Reg CC requirements. (Next Day)
- **Impact:** Allows the RDFI to have additional time to review Entries before making an official decision.

Timing of Written Statement of Unauthorized Debit (WSUD)

- **What:** Allows RDFIs to accept WSUDs prior to the Settlement Date of an Entry.
- **Impact:** Facilitates faster Returns of unauthorized Entries, so that potential issues can be quickly identified and investigated.

Prompt Return of Unauthorized Debit

- **What:** Requires RDFIs to promptly Return an unauthorized Entry once the WSUD is completed.
- **Impact:** Facilitates faster Returns of unauthorized Entries, so that potential issues can be quickly identified and investigated.

RELATED RULE CHANGES

Rule Changes that Support Fraud Monitoring

Standardize Use of WEB Credit Entries

- **What:** Credit Entries utilizing the WEB SEC Code must only be Consumer Originated Entries intended for another Consumer. (P2P, A2A, etc.)
- **Impact:** Provides structure so that monitoring systems are better able to identify typical and atypical activity.

Standardize Use of Entry Descriptions

- **What:** Standardizes Entry Descriptions for specific types of Entries:
  - Entry Description for any Entry for the purpose of paying wages/payroll must be “PAYROLL”.
  - Entry Description for any WEB debit Entry for the purpose of an ecommerce purchase must be “PURCHASE”.
- **Impact:** Provides structure so that monitoring systems are better able to identify typical and atypical activity.

NACHA ‘26 RULE CHANGES – RDFIS

What RDFIs Need To Do?

Rule:
Mandated by Subsection 3.1.10 Identification of Unauthorized Credit Entries or Credit Entries Authorized Under False Pretenses of the Nacha Operating Rules & Guidelines.

- Establish and implement risk-based processes and procedures that are reasonably intended to identify credit Entries that are suspected of being unauthorized or authorized under False Pretenses.
- Establish and implement risk-based processes and procedures for responding when credit Entries are identified as potentially unauthorized or authorized under False Pretenses
- At a minimum, annually review these processes and procedures and make appropriate updates to address evolving risks.

The rule is risk-based, which means the exact approach is flexible. The Rule does not require the screening of every ACH Entry individually and does not need to be performed prior to the processing of Entries.

Necessary:
- Document processes and procedures to monitor incoming ACH credit Entries for unusual patterns or anomalies (e.g., high-dollar credits inconsistent with past behavior).
- Periodically (at least annually) review and update processes and procedures.

What RDFIs Need To Do?

Recommended:

- Use thresholds, velocity checks, or pattern recognition.
- Monitor by:
  - Receiver Name vs Name on the account
  - Entry Descriptions
  - SEC Codes (WEB credit Entries are always Consumer to Consumer)
  - Account Type (Consumer vs Corporate, Dormant or inactive accounts)
  - New account activity
- Ensure monitoring processes and procedures are communicated between various departments

Handling and Resolution:

- Document how suspicious credits will be reviewed and escalated.
- Define when to delay availability of funds or return entries.
- Document how and when to contact other network participants.
- Establish procedures to check for and process ODFI requests for Returns.

Recordkeeping:

  - Maintain evidence of monitoring and decisions made.

Important:

Nacha does not prescribe a specific technology or vendor. Institutions are responsible for defining their program.

What ODFIs Need To Do?

Rule:
Mandated by Subsection 2.2.4 Identification of Unauthorized Entries or Entries Authorized Under False Pretenses of the Nacha Operating Rules & Guidelines.

- 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.
- At a minimum, annually review these processes and procedures and make appropriate updates to address evolving risks.

The rule is **risk-based**, which means the exact approach is flexible. The Rule does not require the screening of every ACH Entry individually and does not need to be performed prior to the processing of Entries. An ODFI’s processes and procedures may consider the processes and procedures implemented by other participants in the origination of ACH Entries, providing ODFIs with flexibility in implementing required fraud monitoring.

Necessary:
- Document processes and procedures to monitor all ACH originations for unusual patterns or anomalies.
- Periodically (at least annually) review and update processes and procedures.

What ODFIs Need To Do?

Recommended:

- Look for unusual patterns or anomalies (e.g., high-dollar credits inconsistent with past behavior).
- Monitor ACH Entry Details such as SEC Codes & Entry Descriptions.
- Use thresholds, velocity checks, or pattern recognition.
- Ensure monitoring processes and procedures are communicated between various departments.

Agreements

- If the ODFI Relies on other participants for fraud monitoring, it must clearly be defined in applicable agreements.

Handling and Resolution:

- Document how suspicious Entries will be reviewed and escalated.
- Define when to stop further processing of a transaction.
- Define when the Originator should be contacted to determine validity of the transaction.
- Document how and when to contact other network participants.
- Establish procedures to check for and process RDFI requests for Returns.

Recordkeeping:

- Maintain evidence of monitoring and decisions made.

What Third Party Service Providers & Senders Need to Do?

Rule:
Mandated by Subsection 2.2.4 Identification of Unauthorized Entries or Entries Authorized Under False Pretenses of the Nacha Operating Rules & Guidelines.

- 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.
- At a minimum, annually review these processes and procedures and make appropriate updates to address evolving risks.

The rule is **risk-based**, which means the exact approach is flexible. The Rule does not require the screening of every ACH Entry individually and does not need to be performed prior to the processing of Entries.

Necessary:

- Document processes and procedures to monitor all ACH originations for unusual patterns or anomalies.
- Periodically (at least annually) review and update processes and procedures.

NACHA ‘26 RULE CHANGES – THIRD PARTIES

What Third Party Service Providers & Senders Need to Do?

Recommended:

- Look for unusual patterns or anomalies (e.g., high-dollar credits inconsistent with past behavior).
- Monitor ACH Entry Details such as SEC Codes & Entry Descriptions.
- Use thresholds, velocity checks, or pattern recognition.
- Ensure monitoring processes and procedures are communicated between various departments.

Handling and Resolution:

- Document how suspicious Entries will be reviewed and escalated.
- Define when to stop further processing of a transaction.
- Document how and when to contact other network participants.

Recordkeeping:

- Maintain evidence of monitoring and decisions made.

NACHA '26: ORIGINATORS

What Must Originators Do?

Rule:
Mandated by Subsection 2.2.4 Identification of Unauthorized Entries or Entries Authorized Under False Pretenses of the Nacha Operating Rules & Guidelines.

- 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.
- At a minimum, annually review these processes and procedures and make appropriate updates to address evolving risks.

The rule is **risk-based**, which means the exact approach is flexible. The Rule does not require the screening of every ACH Entry individually and does not need to be performed prior to the processing of Entries.

Necessary:
- Document processes and procedures to monitor all ACH originations for unusual patterns or anomalies.
- Periodically (at least annually) review and update processes and procedures.

NACHA '26: ORIGINATORS

What Must Originators Do?

Recommended:

- Look for unusual patterns or anomalies (e.g., high-dollar credits inconsistent with past behavior).
- Monitor ACH Entry Details such as SEC Codes & Entry Descriptions.
- Use thresholds, velocity checks, or pattern recognition.
- Ensure monitoring processes and procedures are communicated between various departments.

Handling and Resolution:

- Document how suspicious Entries will be reviewed and escalated.
- Define when to stop further processing of a transaction.
- Document how and when to contact other network participants.

Recordkeeping:

- Maintain evidence of monitoring and decisions made.

NACHA '26 FAQS

FAQ Nacha 2026 Rule Changes

This FAQ section is organized by the following sections:

- General Overview
- ODFIs, Originators, TPSs, TPSPs
- RDFIs
- Company Entry Descriptions

NACHA '26 FAQS: GENERAL

General Overview

Q1. What are the effective dates for the 2026 rule changes?

- **March 20, 2026** – Phase 1 begins (for high-volume originators/RDFIs).
- **June 19, 2026** – Phase 2 begins (for everyone else).

Q2. What's the purpose of these fraud monitoring updates?

To reduce credit-push fraud in the ACH Network by requiring all participants to detect unauthorized entries or entries authorized under false pretenses using risk-based procedures.

Q3. What does "authorized under false pretenses" mean?

It refers to cases where a Receiver technically authorized a payment, but did so based on deception—such as a business email compromise or vendor impersonation.

Q4. What is a "risk-based" monitoring approach?

A flexible framework where monitoring efforts are scaled based on transaction risk level. For example, higher scrutiny for large-dollar payrolls to new accounts.

Q5. Do these rules change liability or legal obligations?

No. Nacha includes disclaimers to ensure UCC Article 4A liability is unaffected. The rules create a duty only to Nacha for compliance purposes.

ODFIs, Originators, TPSs, TPSPs

Q6. Who is required to comply in Phase 1 vs. Phase 2?

- **Phase 1:** (March 20, 2026): All ODFIs and Originators/TPSs/TPSPs with >6M originated entries in 2023.
- **Phase 2:** (June 19, 2026): All others, regardless of volume.

Q7. What must ODFIs, Originators, TPSs, and TPSPs do under the new rules?

- Implement role-relevant, risk-based procedures to identify suspect entries.
- Review and update these at least annually.

Q8. Do the rules prescribe specific fraud detection processes?

No. They mandate a risk-based approach but allow each party to tailor procedures to their role. For example:

- Originators: Change controls on vendor/payroll data.
- TPSs: Velocity monitoring, SEC code reviews.
- ODFIs: May consider controls from upstream parties.

Q9. Are parties required to screen every ACH entry?

No. Monitoring is not required on an entry-by-entry basis.

Q10. Must entries be monitored before processing?

No. Pre-processing is encouraged but not mandatory.

ODFIs, Originators, TPSs, TPSPs

Q11. How often must risk procedures be reviewed?

At least annually, with updates based on evolving risks.

Q12. Can ODFIs rely on another party's controls?

Yes, if the allocation of responsibilities is documented and monitored, such as through contracts.

Q13. What actions should be taken when entries are flagged?

- Stop processing.
- Contact the Originator.
- Cross-check with internal systems.
- Reach out to the RDFI.
- Consider freezing or returning the funds.

Q14. Does this impact the allocation of liability?

No. Legal liabilities remain as outlined by UCC and current rule frameworks.

RDFIs

Q15. Which RDFIs are subject to the new credit monitoring rules?

- **Phase 1** (March 20, 2026): RDFIs with >10M entries received in 2023.
- **Phase 2** (June 19, 2026): All RDFIs, regardless of volume.

Q16. What is required of RDFIs under these rules?

Establish and maintain risk-based procedures to identify and handle credit entries suspected of being unauthorized or fraudulently authorized.

Q17. Do the rules require RDFIs to monitor every ACH entry?

No.

Q18. Are RDFIs required to monitor entries before posting?

No, but if they do, they may delay funds availability under existing exemptions.

Q19. How often must RDFIs review their fraud procedures?

At least annually, with updates for new threats.

Q20. Can RDFIs use third-party service providers?

Yes. RDFIs can delegate execution but not the responsibility for compliance.

RDFIs

Q21. What are examples of red flags RDFIs should watch for?

- High-dollar or unusual transaction types.
- Entries to dormant/new accounts.
- Business-to-consumer entry code mismatches (e.g., CCD to a consumer account).
- Multiple payroll/benefit entries in quick succession.

Q22. What actions can RDFIs take when fraud is suspected?

- Use R17 or R06 return codes.
- Delay availability (where allowed).
- Contact the ODFI using Nacha's Risk Portal.
- Investigate the receiving account characteristics.

Q23. Do these rules affect RDFI liability?

No. The rules focus on monitoring—not preventing—fraud and don't alter liability frameworks.

Company Entry Descriptions

Q24. What are the new entry descriptions and when are they required?

Originators must use standardized descriptors by March 20, 2026:

- **PAYROLL:** For PPD credits related to wages, salaries, or HSA deposits.
- **PURCHASE:** For WEB debits involving e-commerce transactions.

Q25. Who is required to use "PAYROLL" and "PURCHASE"?

All Originators of applicable PPD or WEB entries—and their supporting ODFIs—must comply.

Q26. Is use of "PAYROLL" required for contract (1099) employees?

Yes. This applies to all types of compensation, regardless of employment classification.

Q27. Do HSA contributions require the "PAYROLL" descriptor?

Yes. Since HSA contributions via payroll deduction are part of pre-tax compensation, they must carry the "PAYROLL" label.

Q28. Why is the PAYROLL descriptor required?

Standardizing this field:

- Helps RDFIs recognize patterns (e.g., multiple payrolls to one account).
- Improves early fraud detection (e.g., payroll redirection schemes).
- Supports risk-based availability and processing logic.

Company Entry Descriptions

Q29. Can I add more information after the descriptor?

Yes. Originators must use the first 7 characters for "PAYROLL" and can use the remaining 3 (up to 10 total) for additional descriptive info.

Examples:

- PAYROLL
- PAYROLL02
- PAYROLL424
- PAYROLLEMP

Q30. Where does the Company Entry Description field appear in the ACH record?

It's in positions 54–63 of the Company/Batch Header Record. For full detail, see Subpart 3.2.2 of Appendix Three in the Nacha Operating Rules.

Q31. Are ODFIs or RDFIs responsible for validating or acting on these fields?

- **ODFIs:** Not required to validate descriptor content.
- **RDFIs:** May use these descriptors to enhance fraud monitoring, but are not required to take action based solely on the presence of a descriptor.

NACHA '26 READINESS CHECKLIST

Checklist: Are You Ready?

1. Monitoring Procedures

- Have you documented your risk-based procedures for monitoring incoming ACH credit entries?
- Have you identified whether you fall under Phase 1 (March 20, 2026) or Phase 2 (June 22, 2026) of the rule rollout?
- Are your procedures designed to detect credits that may be unauthorized or initiated under false pretenses (e.g., BEC, account takeover, mule activity)?
- Do your policies clearly define what constitutes suspicious credit activity and how it should be flagged?
- Are your procedures scheduled for annual review and updates as required?

2. Detection & Tools

- Do you have tools or systems in place to detect unusual credit patterns, anomalies, or velocity changes?
- Have you reviewed vendor or internal solutions to support automation, exception monitoring, and alerting?
- Have you configured alerts or reports to flag specific risk indicators, such as large-dollar credits, micro-entries, or repeated returns?

3. Staff Training & Response

- Have relevant teams been trained on how to identify, escalate, and respond to suspicious credits?
- Do you have a defined escalation path and response plan for suspected fraud or anomalous activity?
- Are staff aware of their role in supporting compliance with both monitoring and entry description requirements?

NACHA '26 READINESS CHECKLIST

Checklist: Are You Ready?

4. Entry Descriptions

- If originating payroll credits, are you using "PAYROLL" in the Company Entry Description?
- If originating web based ecommerce debits, are you using "PURCHASE" in the Company Entry Description?
- Have you updated internal systems and Originator guidance to support this requirement?

5. Recordkeeping & Audit Readiness

- Are your recordkeeping and reporting processes updated to reflect new monitoring and detection activities?
- Are you capturing evidence of reviewed alerts, actions taken, and outcomes to support audit requests?
- Have you tested your procedures end-to-end to ensure they are working as intended and can be easily reviewed?

SOLUTIONS

How NEACH Payments Group Helps

Services

Our tailored services meet you where you are. Our industry experts provide insights and recommendations to overcome risks and pain points based on your unique environment.

- ACH Audits
- ACH Risk Assessments
- Fraud Monitoring Specific Risk Assessments
- BSA Audits
- BSA Risk Assessments
- Customized Consulting

Publications

Our interactive workbooks are an easy-to-use, customizable tool to guide your institution through every step.

- ACH Self-Audit Workbook
- ACH Self-Risk Assessment Workbook

Connect With Us

If you'd like to explore how NPG can support your Nacha 2026 readiness:

Visit
neachgroup.com

Email
info@neachgroup.com

Request a Proposal

SOLUTIONS

How affirmative Risk Manager Helps

Risk Manager is purpose-built for Risk Management, Compliance, and Risk-Based Fraud Monitoring, with a newly added reporting package designed to help ODFIs, RDFIs, and Third Parties prepare for and monitor the Nacha 2026 Rule changes. **Here's how:**

Originated Transaction Risk Scoring

We apply machine learning to identify the risk each transaction will be returned. Our models are trained on the industry's most comprehensive electronic payment database, which grows by over $1 trillion annually. The result is a highly accurate list of the suspicious transactions that ODFIs can investigate, verify, and or otherwise manage originator reserves to protect against unauthorized, NSF, and other return activity.

Received Transaction Fraud Pattern Detection

We also scan each incoming transaction to flag suspicious activity for timely, prioritized reviews.

Common fraud patterns include:

- Micro-entries: small dollar credit or debits - especially if not labeled as account verification entries - used to identify open, active accounts to use for fraud.
- Tax Payments: Identify accounts that receive an unusual number of credits from tax authorities.
- Dormant Originators: Identify accounts receiving credits or debits from originator accounts that have not been active in our system for at least 6 months.

SOLUTIONS

How affirmative Risk Manager Helps

Originator Risk Scoring

We leverage predictive analytics to identify originators with a high risk of unauthorized activity. Unauthorized debit returns are by far the most common form of ACH fraud. Typically, less than 2% of originators are responsible for over 80% of all unauthorized activity. Flagging high risk accounts BEFORE they have submitted unauthorized transactions enables effective fraud and credit risk management through limit management, reserve accounts, and risk-based service fees. This services also completely prioritizes and streamlines originator reviews.

Limit Utilization

Sudden changes in credit and debit utilization could indicate breakout fraud and/or account compromise. Quickly researching this activity and adjusting limits greatly minimizes exposure to both losses and NACHA violations.

Velocity

We provide alerts to flag unusual changes in both transaction counts and transaction amounts. This enables quick identification of account takeover fraud, identity fraud, and mule accounts.

Unauthorized Return Rates

Our system alerts when historical return rates exceed a preset threshold. High unauthorized return rates suggest an originator is initiating fraudulent debits. A pattern of high unauthorized returns could trigger NACHA thresholds (currently 0.5%) and require immediate review or even termination of origination rights.

SOLUTIONS

How affirmative Risk Manager Helps

R17 Returns

We monitor accounts for transaction activity flagged as questionable by the RDFI, enabling identification of fraudulent activity by originators before it becomes systemic.

Standard Entry Class (SEC) Codes

We monitor originator activity across SEC codes and provide alerts when that activity diverges from historical patterns. A sudden shift may indicate intentional misuse of entry types as well as an elevated fraud risk due to remote (ie. customer not present)origination activity.

Balanced v. Unbalanced Activity

Monitoring for changes in the ratio of credits to debits can identify compromised, manipulated, or misconfigured accounts. Our timely alerts to changes in this ratio enable quick action to confirm that account activity is legitimate.

Connect With Us

If you'd like to explore how Affirmative can support your Nacha 2026 readiness:

Visit

affirmativeusa.com/riskmanager

Email

info@affirmativeusa.com

Request a Proposal

Next Steps & Resources

- **Assess** your current fraud monitoring capabilities.
- **Evaluate** solutions like Risk Manager.
- **Train** your operations and compliance teams.
- **Stay Informed**:
  - Nacha.org Rule Details
  - Nacha Operations Bulletins
  - Industry webinars and FAQs.

Connect With Us

affirmative

Visit
affirmativeusa.com

Email
info@affirmativeusa.com

Schedule a demo

NEACH Payments Group

Visit
neachgroup.com

Email
info@neachgroup.com

Request a Proposal

Sources

- **Nacha Rule Book**
  - Note: many sections were used in this guide. A special call out to OG 36 -OG39.
- **Nacha's Summary of Upcoming Rule Changes**
  - https://www.nacha.org/content/summary-upcoming-rule-changes
- **Nacha's New Rules**
  - https://www.nacha.org/newrules
- **ACH Operations Bulletin #1-2024: Changes to Upcoming Rules Effective Dates**
  - https://www.nacha.org/news/ach-operations-bulletin-1-2024-changes-upcoming-rules-effective-dates
- **RISK MANAGEMENT TOPICS – (Fraud Monitoring Phase 1)**
  - https://www.nacha.org/rules/risk-management-topics-fraud-monitoring-phase-1
- **RISK MANAGEMENT TOPICS – (Fraud Monitoring Phase 2)**
  - https://www.nacha.org/rules/risk-management-topics-fraud-monitoring-phase-2
- **RISK MANAGEMENT TOPICS – Company Entry Descriptions**
  - https://www.nacha.org/rules/risk-management-topics-company-entry-descriptions