The New Era of ACH Fraud: Are You Prepared for Next Month's New Nacha Rules?

Nanci McKenzie, MLS, JM, AAP, APRP, CAMS
Director, TM Product - Payments Expert

IOFM Spring
CONFERENCE & EXPO

Do you need NASBA CPE credits?

- Navigate to website: **iofm.cnf.io**

  or scan the QR code →

- Check-in and check-out of your sessions to track your attendance for NASBA CPEs

- Certified with IOFM? No need to check-in and out of sessions. Self-report CEUs on IOFM.com instead after the event!

IOFM Spring
CONFERENCE & EXPO

Disclaimer:

This session is for educational purposes only. This should not be taken as legal advice or views of Capital One or IOFM.

Q1 2026 ACH Network Highlights

Total ACH Volume

8.9 Billion

↑ 4.8% YoY

Total ACH Value

$24.1 Trillion

↑ 9.3% YoY

Same Day ACH Value

$1.1 Trillion

↑ 22.1% YoY

Growth by Payment Type (Q1 2026 vs. Q1 2025)

B2B Payments: 2.1 billion (up 9.4%)

Internet Payments: 2.9 billion (up 5.4%)

Healthcare Claims: 131.1 million (up 4.9%)

P2P Payments: 129.3 million (up 18.5%)

Same Day ACH Momentum: 403 million payments (up 23.6%). This marks the second consecutive quarter with value exceeding $1 trillion.

Resource: Nacha.org

Risk Management – Pieces of a puzzle

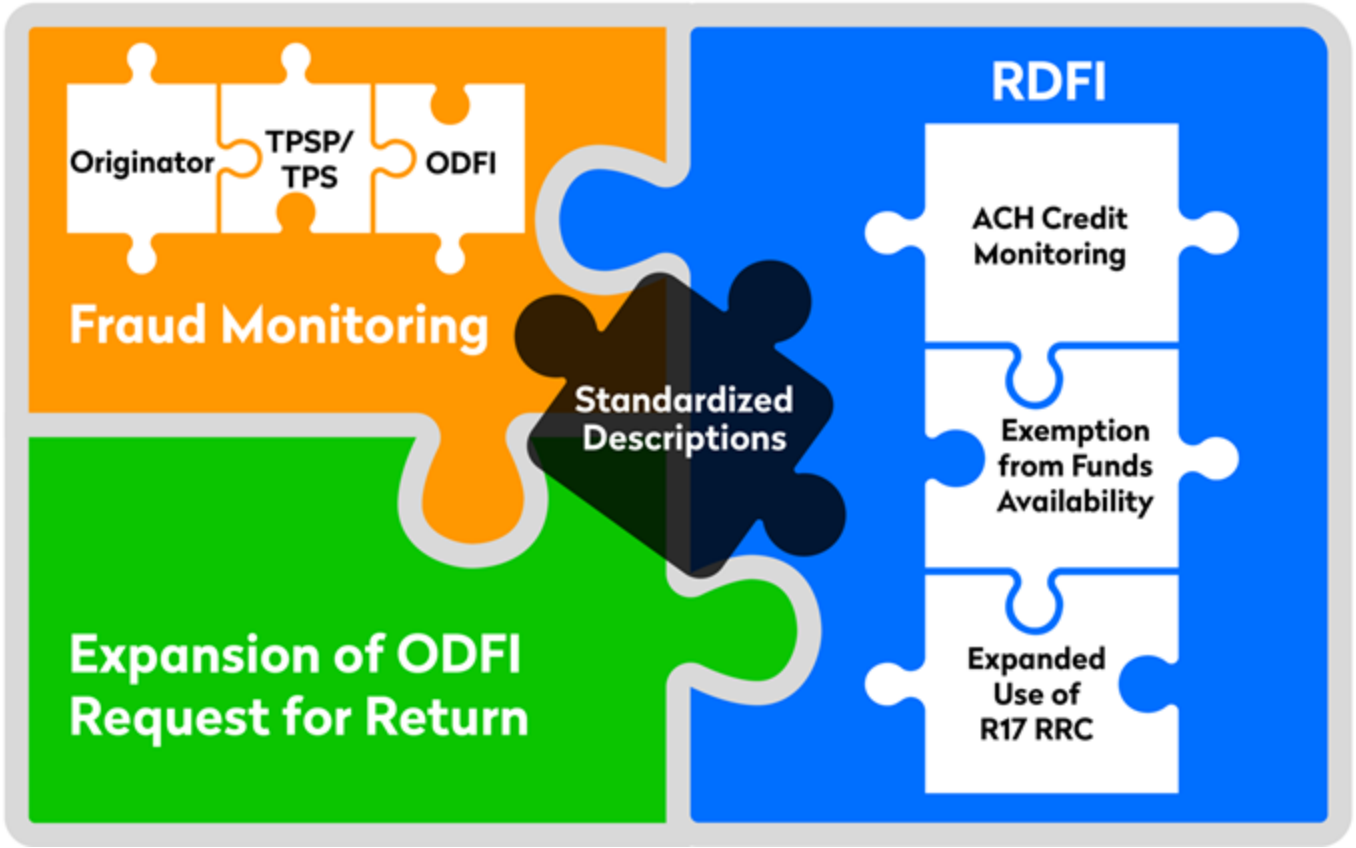


Image used with the permission from Nacha at Nacha.org

Effective Date	Rule Amendments
March 20, 2026	Fraud Monitoring (Phase 1) • All ODFIs • Non-consumer Originators, TPSPs, and TPSs with 2023 ACH origination volume of 6 million or greater ACH Credit Monitoring (Phase 1) • RDFIs with 2023 ACH receipt volume of 10 million or greater New Company Entry Descriptions – PAYROLL and PURCHASE
June 22, 2026	Fraud Monitoring (Phase 2) • All other non-consumer Originators, TPSP, and TPS ACH Credit Monitoring (Phase 2) • All other RDFIs
September 18, 2026	Definition of IAT Entries Funds Availability Requirements for Non-Same-Day Credit Entries
January 1, 2027	Registration of IAT Contacts in the ACH Contact Registry
March 19, 2027	Optional Date of Birth Field for IAT Entries Non-Bank Foreign Financial Agencies in IAT Entries
March 17, 2028	New Return Reason Code (R90) for Sanctions Compliance Obligations

Same Day ACH Per Payment Limit Increasing - $10 Million

- Effective Date - September 17, 2027
- All eligible SEC Codes *(Other dollar limits for ARC, BOC, POP, RCK and XCK entries would still apply. IATs would remain ineligible for SDA).*
- Credits and debits.
- Consumer and business payments.
- Using all three Same Day ACH settlement windows.

Considerations:

- Setting customized limits on LOB/individual Originators/all originated entries.
- Realizing and preparing for received debit entry settlement processes and reconciliation

Why Are There New ACH Risk Management Rules in 2026?

Recently, there have been significant fraud scenarios affecting consumers, businesses and other organizations that make use of ACH credits and other “push” payments.

- Business email compromise (BEC).
- Vendor impersonations.
- Payroll impersonations.
- Account takeovers.
- Other impersonations (e.g., real estate settlement).
- Fraudulent claims for benefits – unemployment, PPP loans, tax refunds.

These present key differences from prevention and remediation of unauthorized debits. The new Rules are intended to have all parties in the ACH Network to have a role in detecting and recovering from fraud.

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.

Fraud Monitoring vs. Fraud Detection

- **Fraud Monitoring** is the overarching, continuous risk management process and the established procedures to prevent and manage fraud. It involves a risk-based approach, annual reviews, and education. Under new rules, this includes establishing and implementing processes to identify entries suspected of being unauthorized or authorized under False Pretenses.
- **Fraud Detection** is the specific technique or action used within the monitoring process to identify a potential fraudulent event as quickly as possible. Your documents note that detection can rely on manual processes and static, rules-based logic, with an opportunity to shift to machine learning models for a more adaptive approach to identify complex patterns. Detection is the initial step that triggers the escalation and recovery process.

IMPORTANT POINTS – NEW REQUIREMENTS

Non-Consumer Originators (and vendors)

NEW

- Fraud monitoring on originated debits and credits
- Written processes and procedures covering risk based approach to fraud monitoring including what will be done with suspected fraud.

☆ **Note** – It is our responsibility as the ODFI to educate the non-consumer originators they must begin doing this.

☆ **Note** – This does not change the ODFI origination monitoring requirements but we can not do this for them.

PAYROLL and PURCHASE

NEW

- Originations must include in Company Entry Description field when known as a Payroll file or e-commerce Purchase file.

☆ **Note** – The purpose is to help with fraud investigations. (e.g. If Company Entry Description is Payroll, the likelihood of fraud is less.)

Receiving ACH Credit Monitoring

NEW

- Receiving Financial Institutions have never before been required to monitor any ACH entries. NOW, Receiving Financial Institutions are **REQUIRED** to monitor **ACH CREDITS** for potential fraudulent activity.

Extended Use of R17 - QUESTIONABLE

OFFICIAL

- Optional use of the R17-QUESTIONABLE return reason code to be used for suspicious ACH Credits received by the RDFI.

☆ **Note** – Return time frame within 2 Banking Days following the settlement date

☆ **Note** – No Hold Harmless Agreement necessary.

☆ **Note** – Recognizes a potential fraudulent situation between 2 financial institutions and information sharing is allowed.

Nacha's 2026 ACH Fraud Monitoring: Rules for Non-Consumer Originators

Understanding your role in fraud prevention and the new risk management requirements.

The New Rule

Each non-consumer Originator is required to establish and implement risk-based processes reasonably intended to identify ACH entries initiated due to fraud.

Why It Is Important

Establishing regular fraud detection monitoring can help create a baseline of typical activity, which makes atypical or suspicious activity much easier to identify.

The Goal

These rules are specifically designed to reduce the incidence of successful fraud attempts, such as account takeovers or transactions authorized under false pretenses.

Implementation

A risk-based approach to monitoring can consider factors such as transactional velocity, anomalies, and account characteristics.

Client Considerations for Fraud Monitoring

Essential compliance steps for implementing a risk-based fraud monitoring approach.

Written Processes and Practices

Originators must document their written processes and procedures covering their risk-based approach to fraud monitoring, explicitly including what to do when suspected fraud is identified.

Annual Review Requirement

Perform a review of your fraud monitoring processes and procedures at least annually, or whenever your fraud risks evolve.

Responding to Potentially Unusual Activity

When a suspicious transaction is identified, your process should dictate next steps. Recommended actions include:

- Receiver of ACH Entry validation
- Contacting ODFI to help determine validity.
- Contacting law enforcement if a fraudulent scheme is confirmed.

NEW Client/Originator Requirements

PAYROLL and PURCHASE

- **NEW (effective 3/20/26)**
  - Originations must include in Company Entry Description field when known as a **Payroll (PPD)** file or e-commerce **Purchase (debit WEB)** file.
  - Use of **PAYROLL** or **PURCHASE** descriptors in Company Entry Description field.

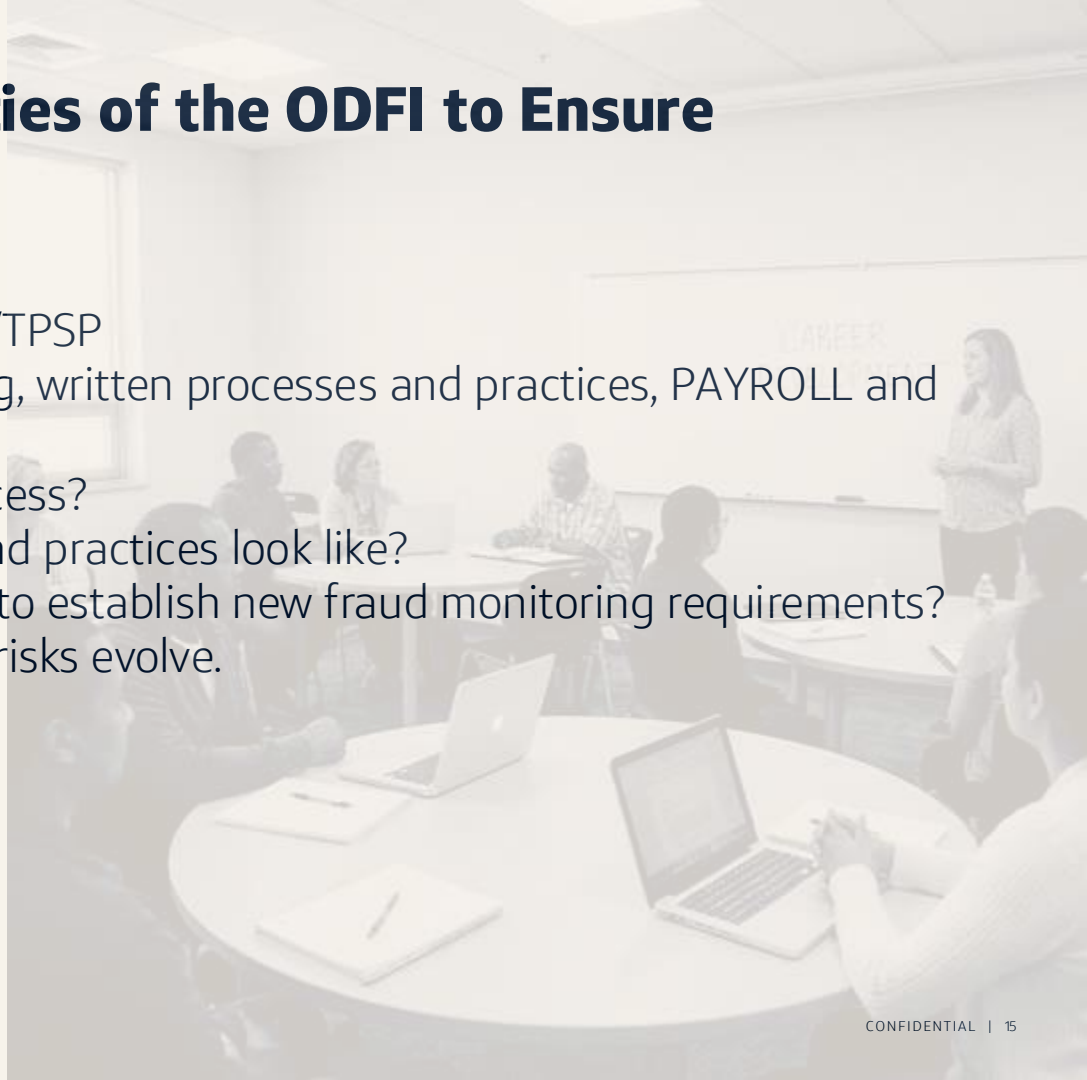
Non-Consumer Originators
(TPS and vendors)

- **NEW (effective 6/22/26)**
  - Originators must implement risk-based approach fraud monitoring on all originated debits and credits
  - Originators must maintain:
    - Written processes and procedures covering risk based approach to fraud monitoring including what will be done with suspected fraud entry(s).
    - Written processes and procedures reviewed at least annually or when new fraud risks identified.

What are the Responsibilities of the ODFI to Ensure Originator Compliance?

Communication

- To Non-Consumer Originators/TPS/TPSP
  - Rule updates - Fraud monitoring, written processes and practices, PAYROLL and PURCHASE
  - What is a fraud monitoring process?
  - What are the written process and practices look like?
  - What if your Originator refuses to establish new fraud monitoring requirements?
  - At least annual review or when risks evolve.
- **Internal Education**
  - Management
  - Fraud/Risk Management
  - Customer/Member facing
  - Operations
  - Sales/Treasury Management



What are the Responsibilities of the ODFI to Ensure Originator Compliance?

Reviews

- **ODFI Risk Management 2.2.3**
  - Periodic Reviews
  - Add to review - Questions
    - Have you reviewed and updated your processes and procedures for your fraud monitoring?
    - What do you do for fraud monitoring?
    - Can you provide a sample of what you have done for a suspicious transaction?
- **Remember the ODFI is responsible for everything their Originators do!**
  - TPS and TPSP must complete an ACH Compliance audit by December 31
  - Non-consumer Originators are not required to complete an audit
    - You must make sure they are in compliance with the fraud monitoring rules

Resources

Credit-Push Fraud Monitoring Resource Center

The Fraud Monitoring Rule Changes are effective in 2026. These Rules require fraud monitoring by Originators, Third-Party Service Providers, Third-Party Senders and ODFIs that is intended to identify ACH credit Entries initiated due to fraud. In addition, RDFIs are required to implement risk-based processes and procedures intended to identify credit Entries initiated due to fraud. The Rules are neutral regarding specific methods or technologies used to identify fraudulently

ADDITIONAL RESOURCES

2026 Fraud Monitoring Rule Changes

These Rule amendments related to monitoring for fraud become effective on March 20, 2026, and are part of a larger Risk Management package intended to reduce the incidence of successful fraud attempts and improve the recovery of funds after frauds have occurred. These amendments are related fraud monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs and ACH Credit monitoring by RDFIs.

RMAG Guidance on Risk-Based Controls

Nacha's Risk Management Advisory Group (RMAG) consists of risk management and compliance experts from financial institutions and payments associations. The group has published blogs and guidance to help FIs as they plan for implementation of the new fraud monitoring Rules.

Third-Party Service Vendors

Organizations may choose to contract with a company to provide fraud monitoring solutions. The below list provides some of the third-party vendors that offer fraud monitoring services.

Key: **PP** = Preferred Partner, **PIA** = Payments Innovation Alliance Member, **NC** = Nacha Certified

- Abrigo.
- ACI Worldwide. **PP PIA**
- Affirmative Technologies. **PIA**
- feedzai.
- Finovifi.
- LexAlign. **PIA**
- LSEG Risk Intelligence. **PP**
- Lyons. **PP**
- Nasdaq Verafin.
- PaymentWorks. **PP PIA**
- Plaid. **PP PIA**
- Q2. **PP PIA**
- Sardine. **PP**
- Socure.
- Splunk, a Cisco Company.
- The Federal Reserve Financial Services.
- Unit21.
- ValidiFi. **PP PIA**
- Vara Security.

Solution Providers: Please contact Nacha if you wish to be added or removed as a resource.

Thank you!

Questions?

nanci.mckenzie@capitalone.com

Please tell us what you think!

- Please scan this QR code using your mobile to access a short feedback survey →
- Also accessible via the mobile app