Unit21.ai

Guide

Addressing Nacha Changes: Building Fraud-Resilient ACH Operations in 2026

A comprehensive fraud compliance guide for ODFIs, RDFIs, TPSPs, and TPSs navigating Nacha's 2026 rule overhaul

Table of Contents

What's Inside

Introduction

> As the U.S. payments landscape continues to evolve, the Nacha 2026 rule changes mark a critical turning point for financial institutions, payment processors, and third-party providers.

Phase 1 of these rules took effect March 20, 2026. It applies to all ODFIs (regardless of volume), plus Originators, Third-Party Senders, and Third-Party Service Providers whose 2023 origination or transmission volume exceeded 6 million entries, and RDFIs whose 2023 ACH receipt volume exceeded 10 million entries.

Phase 2 takes effect June 19, 2026 (first applicable banking day: June 22), for all remaining non-consumer Originators, Third-Party Senders, Third-Party Service Providers, and RDFIs regardless of volume.

In the past, responsibilities for fraud detection were concentrated among originating financial institutions. However, these new rules place monitoring obligations squarely across the board, including Receiving Depository Financial Institutions (RDFIs), Originating Depository Financial Institutions (ODFIs), Third-Party Senders (TPSs), and Third-Party Service Providers (TPSPs).

With an emphasis on proactive fraud detection, behavioral monitoring, and risk-based logic, these changes demand that institutions adopt smarter, faster, and more collaborative approaches.

Before Nacha 2026 Rule Changes	New Expectations Under Nacha 2026
Fraud detection was primarily the responsibility of ODFIs. RDFIs had no mandate to monitor incoming transactions.	Fraud monitoring responsibilities are extended across all ACH participants: RDFIs, ODFIs, TPSs, and TPSPs.
RDFIs passively posted ACH credits without scrutiny.	RDFIs must now monitor inbound ACH credits for suspicious behavior (e.g., synthetic IDs, mule accounts) and take appropriate action, including returning funds where warranted under existing ACH return frameworks.
ODFIs focused on basic validation of originators without behavioral analysis.	ODFIs are expected to scrutinize originator behavior, flagging anomalies like high-risk new senders, irregular timing, unexpected amounts, and transactions authorized under false pretenses.
TPSPs had limited operational responsibility for fraud detection.	TPSPs must actively support client-specific fraud monitoring with risk-based controls tailored to each client's profile. Configurable rules and thresholds are one effective approach to meeting this obligation.
Compliance efforts were largely manual and static.	Institutions are expected to implement risk-based, adaptive monitoring — ideally automated and integrated with exception handling. Explainability and auditability, while not explicitly mandated, are strongly recommended for regulatory defensibility.
No standard requirement for real-time monitoring or exception handling documentation.	Nacha requires risk-based monitoring with documented processes, audit trails, and escalation frameworks for exceptions. Explainability — while strongly recommended as a best practice — is not explicitly mandated. Real-time monitoring is not required; the standard is proportionate, risk-calibrated controls.

This guide is designed to help your institution not only meet Nacha's expectations but also to use the rule change as a springboard for stronger fraud resilience and operational excellence.

Product Demo

Navigating Nacha's 2026 Operating Rules With Unit21

Keep Learning

Understanding the 2026 Rule Changes

The Nacha 2026 rules have reshaped the compliance landscape in several meaningful ways. First, RDFIs are now required to monitor inbound ACH credits, something previously outside their regulatory burden. For the first time, receiving institutions must analyze transaction behavior, detect patterns associated with synthetic identities or money mules, and take corrective action such as returning fraudulently obtained funds.

ODFIs are expected to deepen scrutiny of their outbound ACH activities, especially as they relate to originator behavior. This includes identifying anomalies such as unusually high transaction volumes from new originators, signs of business email compromise (BEC) schemes, and transactions authorized under false pretenses, cases where a customer was deceived into authorizing a payment through impersonation, spoofed invoices, or manipulated payment instructions. TPSPs and TPSs are also on the hook. As intermediaries, these entities must enforce fraud controls tailored to their client base and prove that monitoring practices are consistent, auditable, and scalable.

Importantly, Nacha has not issued a one-size-fits-all checklist. The rules emphasize a risk-based, outcome-driven approach, leaving implementation up to individual institutions. That means the burden, and opportunity, lies with you to build a program that meets your risk profile and operational realities.

Key Responsibilities by Role

RDFIs

- ✔ Must monitor inbound ACH credits.
- ✔ Must identify and return fraudulently obtained funds.
- ✔ New focus on:
  - ✔ Mule accounts
  - ✔ Synthetic IDs
  - ✔ Dormant-to-active patterns
  - ✔ Micro-deposit activity

ODFIs

- ✔ Continue monitoring outbound ACH debits/credits.
- ✔ Must assess originator behavior.
- ✔ Common risks include:
  - ✔ Payroll redirection
  - ✔ Business email compromise (BEC
  - ✔ Authorized-under-false-pretenses fraud
  - ✔ High-risk new originators

TPS

- ✔ Sends ACH entries on behalf of clients (originators) without direct relationship to ODFI.
- ✔ Must take full responsibility for fraud monitoring.

TPSP

- ✔ Supports ACH-related functions for ODFIs, TPSs, and originators.
- ✔ Expected to maintain monitoring controls, data formatting, and compliance workflows.

RDFIs: From Passive Posting to Active Monitoring

Historically, RDFIs functioned largely as passive participants in the ACH process. Their role was to post incoming transactions without the expectation of fraud analysis. Under the new rules, this changes dramatically. RDFIs must now monitor inbound credits for suspicious activity using entity-based logic that focuses on the receiver's behavior.

Effective monitoring strategies should include logic to detect synthetic ID use and mule activity. This can be achieved by analyzing account behavior such as sudden activation of dormant accounts receiving large deposits, patterns of multiple micro-deposits across accounts, and fuzzy-matched memos indicating payroll or refund schemes. The goal is not only to identify risk but to act upon it, RDFIs are now accountable for returning questionable funds promptly.

Scenario

RDFI Adapting to Inbound Fraud Monitoring

Institution
A mid-sized credit union

Before
ACH credits were auto-posted with no fraud screening.

Now
A dormant account suddenly receives a $9,800 deposit with a memo line: "payroll." The system flags this based on fuzzy matching and account behavior. Compliance reviews the flagged activity and, after investigation, initiates a return based on evidence of synthetic identity usage.

Keep learning about the impact Nacha rule changes will have on RFDIs in this blog and video.

ODFIs and TPSs: Deepening the Fraud Perimeter

For ODFIs, the challenge lies in elevating current monitoring practices. They must move beyond surface-level compliance to behavior-driven analysis of their originators. Fraud indicators might include new clients sending high-value transactions prematurely, unusual time-of-day activity, or risk signals stemming from Customer Risk Ratings (CRR). These patterns often precede events such as payroll redirection scams or invoice manipulation.

TPSs, often overlooked in fraud defenses, must now shoulder direct compliance responsibility. When initiating ACH entries on behalf of clients, they need to ensure fraud detection protocols are embedded in the process. This involves implementing sender-focused logic, monitoring entry volume spikes, and flagging out-of-pattern originator behavior.

Scenario

ODFI/TPS Elevating Originator Oversight

Institution
Regional commercial bank with fintech TPS clients

Before
Originators were vetted at onboarding but not continuously monitored.

Now
A new TPS originator begins submitting large debit batches to new vendors within 48 hours of approval. Unit21 flags the anomaly based on CRR score, early transaction behavior, and time-of-day analysis. An alert fires for investigation, preventing a $75,000 BEC fraud.

Keep learning about the impact Nacha rule changes will have on ODFIs & TPSs in this blog and video.

TPSPs: The ~~Compliance~~ Enablers

Third-Party Service Providers must facilitate fraud control across their client networks. While they may not own the transaction, TPSPs play a pivotal role in monitoring and alerting. Scalable detection rules, client-specific configurations, and no-code threshold tuning become critical assets in their compliance toolkit.

A TPSP must be capable of customizing monitoring rules across a diverse originator base. For instance, a payroll provider's clients may have predictable transaction windows and volumes. Any deviation from that pattern, such as weekend transactions or sudden volume surges, should trigger alerts for investigation.

Scenario

TPSP Scaling Monitoring Across Clients

Institution
A SaaS payroll platform supporting hundreds of small businesses

Before
No centralized fraud logic, each client managed their own alerting thresholds manually.

Now
The TPSP deploys a no-code rule engine to apply baseline transaction thresholds and velocity limits per client type. One retail client initiates high-volume ACH debits on a Sunday, triggering an alert. The system escalates based on client type, day-of-week behavior, and memo field anomalies. Investigation reveals compromised credentials and prevents mass payroll fraud.

Keep learning about the impact Nacha rule changes will have on TPSP in this blog and video.

Fraud Typologies: What the Rules Target

Several fraud typologies prompted Nacha's rule change, each representing significant risk to the ACH ecosystem.

Synthetic Identities

One prominent scheme involves synthetic identities used to receive payroll deposits or tax refunds. In these cases, newly opened or dormant accounts suddenly receive large deposits with payroll-related memos. Without adequate inbound monitoring, RDFIs may unknowingly facilitate large-scale fraud.

Business Email Compromise

Another common threat is business email compromise (BEC), where fraudsters manipulate payment instructions to reroute funds to accounts they control. These attacks frequently occur on the origination side, affecting ODFIs and their clients. TPSPs are particularly vulnerable when they process payments on behalf of multiple customers and fail to detect account substitution or pattern deviation.

Authorized Under False Pretenses

The Nacha 2026 rules explicitly expand the monitoring scope to include fraud authorized under false pretenses. This covers cases where a customer was deceived into authorizing a legitimate-looking transaction through vendor impersonation, spoofed invoices, fake payment portals, or social engineering. The transaction is technically "authorized," but the authorization itself was obtained fraudulently. ODFIs and TPSs cannot limit detection to unauthorized transaction signals alone; behavioral anomalies before authorization, destination changes, new payee patterns, and out-of-profile amounts are now part of the monitoring obligation.

Mule Networks

Mule networks often exploit micro-deposit verification. By using a small set of accounts to link numerous external accounts via micro-transfers, fraud rings can build extensive infrastructure without detection, unless institutions monitor for this behavior.

Payroll Entry Description

Nacha 2026 establishes the payroll entry description as a mandatory field for all applicable payroll ACH entries. This creates a specific detection opportunity: any ACH entry with the payroll description in which the receiving account or routing number changes within a short window around the payroll run date should trigger review. Fraud rings target payroll specifically because of predictable timing and high dollar volumes. The payroll field gives institutions a direct rule-building hook that didn't exist before.

3 Steps to Prepare for Nacha 2026 Rule Changes

Preparing for Nacha 2026 requires more than just upgrading your fraud platform. It demands a cross-functional, proactive strategy.

Start by conducting a comprehensive gap assessment. Map your current fraud detection capabilities against the new requirements based on your institution's role. Determine whether you can currently monitor both inbound and outbound transactions, whether your rule logic is adaptable, and whether you have sufficient coverage across transaction types.

Step 1

Build Your Compliance Roadmap

Start with structure. There are no official implementation templates, so you need a clear, cross-functional strategy:

- ✔ Create a detailed project plan with timelines and internal owners
- ✔ Define specific monitoring, alerting, and escalation requirements
- ✔ Lock in key milestones, and start now

Unit21 Tip: Get your fraud and compliance teams in the same room early. Nacha's rules will hit both.

Step 2

Know What You Can't Handle Alone

Manual monitoring is not scalable. Most institutions cannot feasibly review all originated and received ACH transactions without automation:

- ✔ Evaluate current vendors and fraud monitoring capabilities
- ✔ Consider tech partners with automated screening and alerting
- ✔ Assess team bandwidth, and avoid overloading analysts

Unit21 Tip: Transaction screening logic should be risk-based, explainable, and adaptive, not necessarily real-time. Nacha requires proportionate controls calibrated to your institution's risk profile.

Step 3

Operationalize the Exceptions

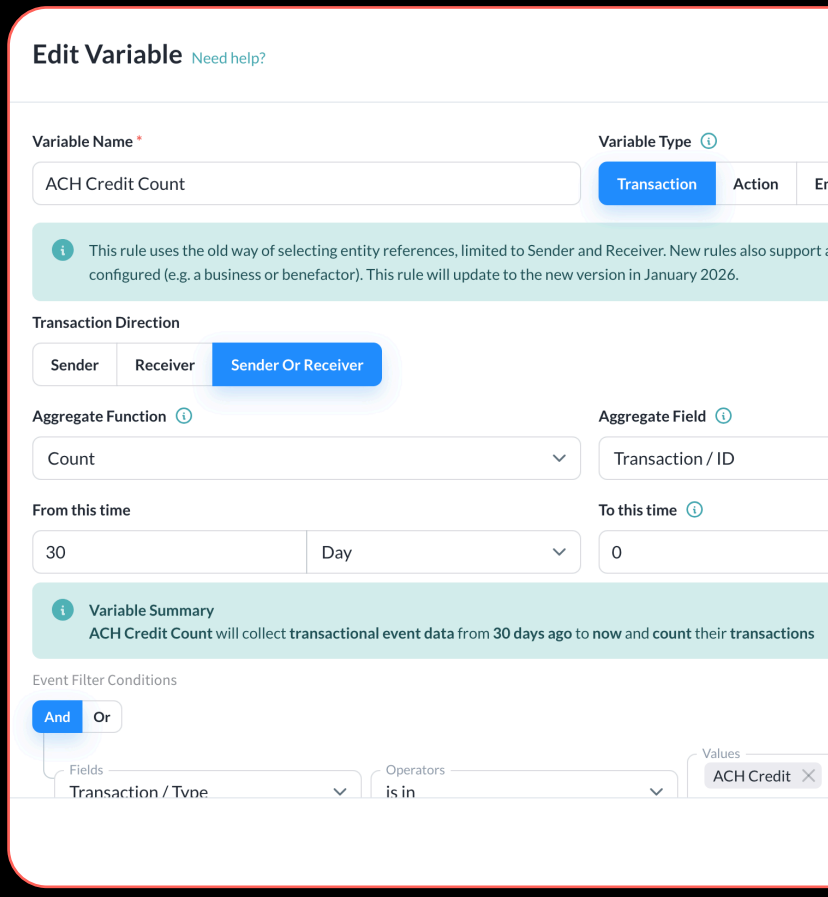
Compliance isn't just detection, it's control. Nacha expects you to manage the how and why of exception handling:

- ✔ Define risk thresholds and red flag triggers
- ✔ Pre-set exception handling rules (pause, escalate, auto-report)
- ✔ Ensure full audit trails for every flagged item

Unit21 Tip: Use dynamic AI Agents to auto-handle edge cases and reduce human error.

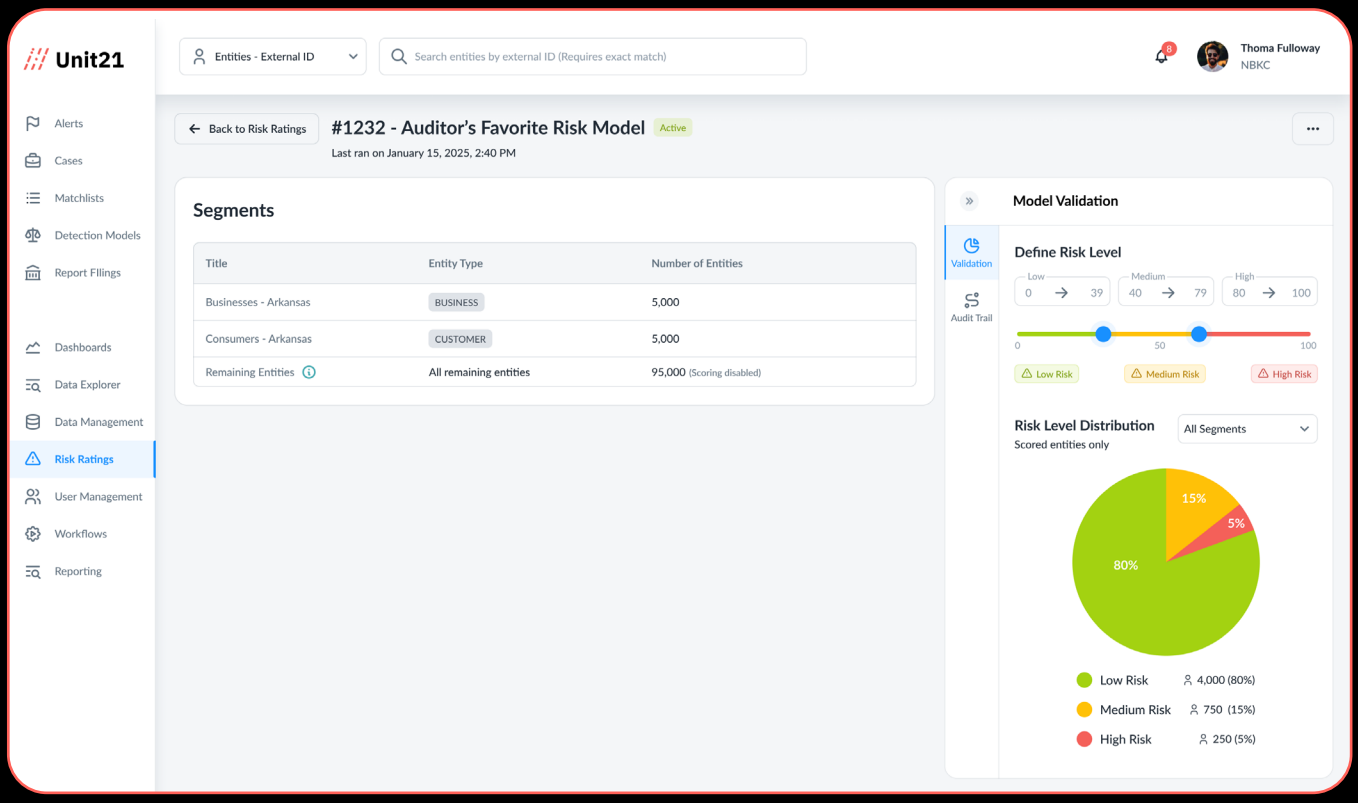
Unit21: Your Partner in Nacha 2026 Readiness (And Beyond)

Unit21 is uniquely positioned to help institutions adapt to the demands of the Nacha 2026 rule changes. Its no-code platform empowers compliance teams to build and adjust fraud rules independently, no engineering support required. Whether you're an RDFI needing to monitor inbound credits, an ODFI refining your oversight of originators, or a TPSP managing diverse client risk profiles, Unit21 offers solutions tailored to each role.



At the core of Unit21's platform is a flexible rule engine that allows users to define logic based on sender or receiver behavior, a critical capability under the new requirements. The platform supports entity-based analysis, enabling detection of synthetic identities, mule activity, and micro-deposit fraud schemes. Built-in features such as Customer Risk Ratings (CRR) let institutions apply risk-based logic dynamically, adjusting thresholds and workflows based on client profiles.

Unit21 also includes automated alerting, audit trail logging, and a modular AI Agent system that automates detection, investigation, alerts, and narratives. These capabilities not only streamline fraud detection but also reduce human error and support scalable compliance.



By implementing Unit21, institutions can meet Nacha's expectations with confidence, preparing for the regulatory deadline while strengthening their overall fraud resilience. To learn more schedule a demo or see our product demo on how Unit21 can help keep you compliant and proactively mitigate fraud risk.

Product Demo

Navigating Nacha's 2026 Operating Rules With Unit21

Keep Learning

Conclusion: Compliance as a Catalyst

> The 2026 Nacha rule changes offer a chance to transform compliance into a competitive advantage.

Institutions that embrace these requirements early, build intelligent fraud monitoring frameworks, and invest in the right technology will not only reduce risk but also inspire greater trust from customers and regulators alike.

Rather than viewing these changes as burdensome, forward-thinking institutions can use them as a catalyst for innovation, modernization, and improved operational integrity.

Phase 1 is live. For Phase 2 institutions, the June 22, 2026 deadline is the line in the sand. The fraud monitoring program built for Nacha 2026 is also the program that catches the next generation of ACH fraud schemes.

Everything You Need To Know, In One Place

Phase 1 is live. Phase 2 deadline: June 22, 2026. Are you ready?

Learn what's changed for RDFIs, ODFIs, TPSs, and TPSPs, and how Unit21 empowers you to build, investigate, and document your Nacha 2026 compliance program.

Keep Learning

Unit21.ai