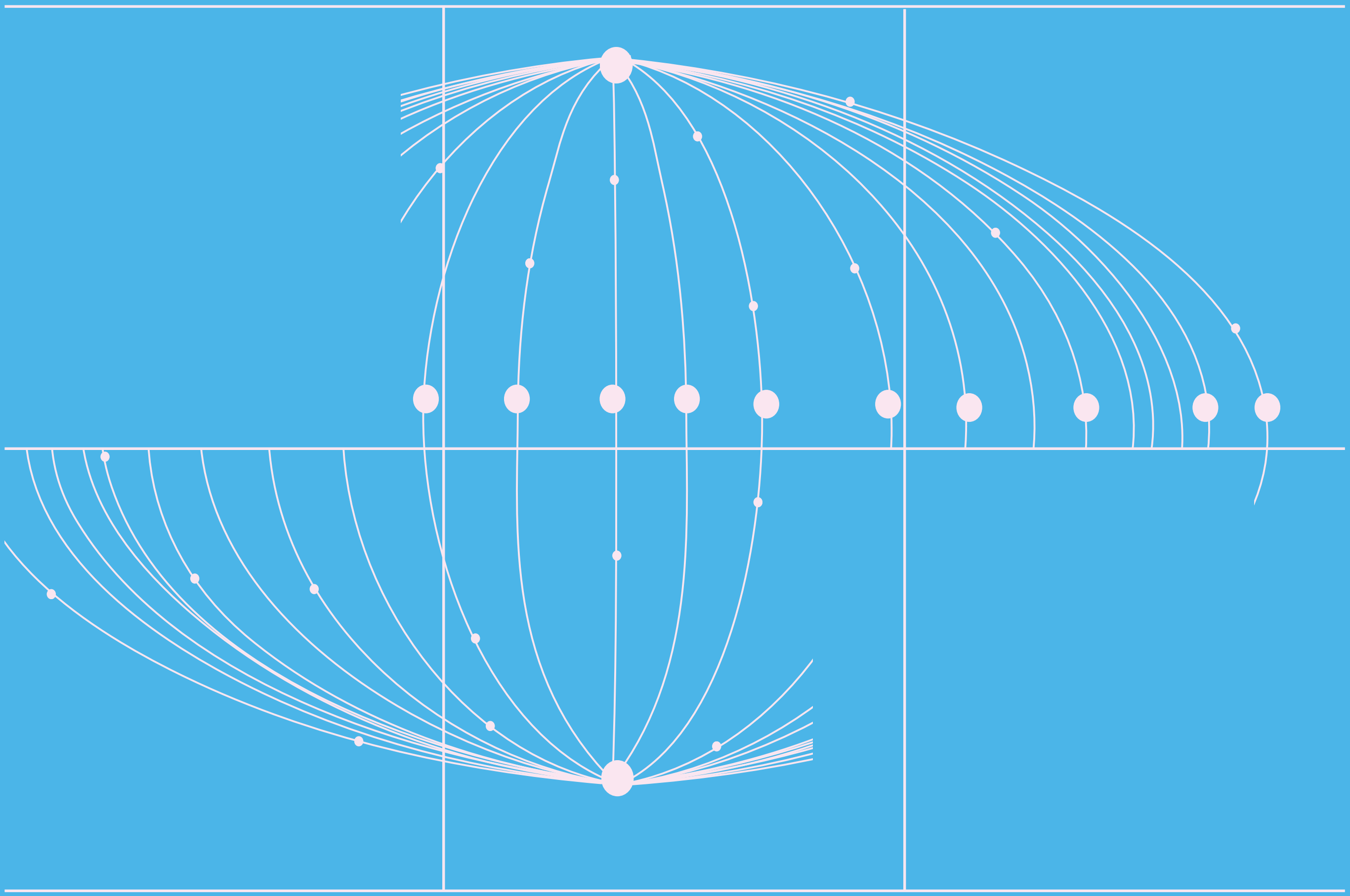
GUIDE

The Nacha 2026 mandate: Understanding false pretenses and shared accountability

A guide to what's changing and how to prepare



Sardine

Table of contents

For years, fraud decisions often hinged on a straightforward question: Did the customer authorize the payment? If the credentials matched and the two factor authentication passed, that was typically the end of the inquiry. Nacha's 2026 rule changes officially end that era. By expanding monitoring to include "False Pretenses," the burden has shifted from verifying the user to verifying the intent.

This pivot is the cornerstone of a multi-year strategy that began with the 2022 Risk Management Framework. We are moving toward a total visibility model where both ODFIs and RDFIs share the weight of identifying scams like BEC and payroll diversion, even when transactions are technically authorized. This 2026 mandate is part of a larger roadmap that includes new Payroll and Purchase descriptors, major international ACH transactions (IAT) updates in 2027, and new R90 sanction codes in 2028.

These updates reflect a shift in how ACH fraud is understood. Modern scams exploit trust and routine workflows to produce perfectly legitimate looking payments but are induced through deception. This guide covers what the new Nacha rules require, how expectations differ by institution size, and practical ways to prepare without slowing payments or overwhelming teams.

The shift from authentication to intent

The ACH network has become a victim of its own success. With businesses having moved away from paper checks in the past few years, credit-push volume has surged, reaching $93 trillion in 2025 alone. This efficiency has created a massive, high-speed target for fraudsters.

Nacha is closing three specific gaps that have allowed these scams to become a path of least resistance:

- **The authorization gap**
  Rules have historically focused solely on unauthorized access. If a CEO is tricked into approving a fake vendor invoice, such as the infamous 2019 UK energy firm incident, the transaction is technically authorized. By codifying False Pretenses, Nacha is forcing banks to look past the login and evaluate the legitimacy of the request itself.

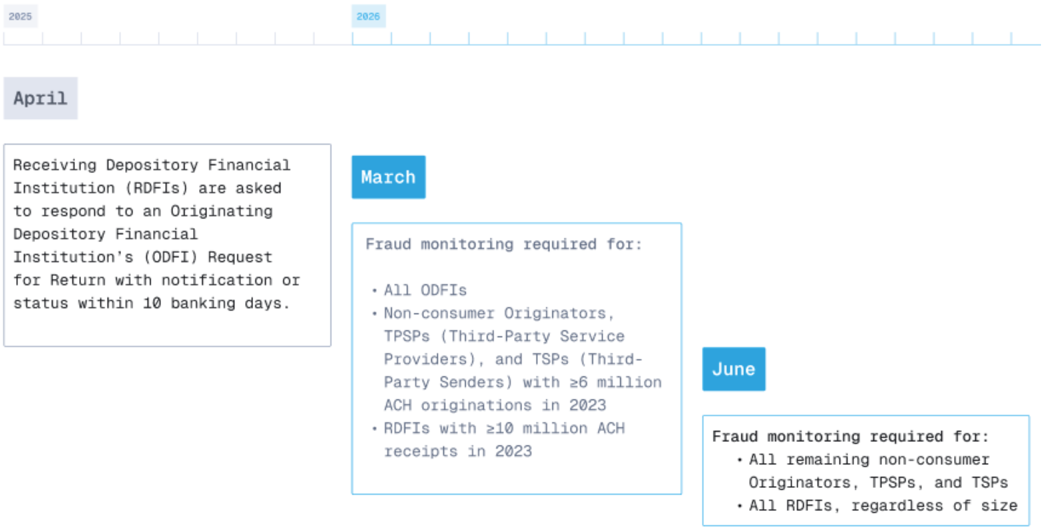
- **The vague standard problem.**
  For too long, “commercially responsible” was the benchmark. This led to a patchwork of defenses. Scammers simply targeted the banks with the thinnest controls. Replacing this ambiguity with documented, risk-based procedures creates a universal floor for the entire network.

> “The scammers have taken advantage of the characteristic of the ACH network by using it as a mechanism to push out funds that may not be able to be recouped.”
> **Mark Dixon Senior Consultant, Nacha**

The 2026 rules replace the old hands-off approach with a model of shared accountability. The network is finally acknowledging that knowing a customer’s intent is just as important as knowing the customer themself.

What's changing in 2026

Nacha is implementing the new requirements in phases, prioritizing the highest-volume entry points of the network. The goal is to establish a defensive floor at the largest institutions before expanding the mandate to the entire ecosystem.



April

Receiving Depository Financial Institution (RDFIs) are asked to respond to an Originating Depository Financial Institution's (ODFI) Request for Return with notification or status within 10 banking days.

March

Fraud monitoring required for:

- All ODFIs
- Non-consumer Originators, TPSPs (Third-Party Service Providers), and TSPs (Third-Party Senders) with ≥6 million ACH originations in 2023
- RDFIs with ≥10 million ACH receipts in 2023

June

Fraud monitoring required for:

- All remaining non-consumer Originators, TPSPs, and TSPs
- All RDFIs, regardless of size

> **Key distinction:** Nacha isn't looking for perfection on these dates. They are looking for a documented standard of care. If you don't have a written policy that explicitly addresses "False Pretenses" by your deadline, you are out of compliance, even if you haven't lost a cent to fraud.

Understanding False Pretenses:

The core of the 2026 mandate is the formal inclusion of False Pretense, defined as inducing a payment by misrepresenting identity, authority, or account ownership. This creates an operational "line in the sand" for fraud and compliance teams.

> **Operationally, this distinction matters.** Institutions are not expected to investigate every customer dispute or adjudicate intent. The focus is on payments that appear valid on the surface but violate established behavioral, contextual, or trust patterns.

This targets the impersonation typologies like business email compromise, vendor impersonation, payroll diversion, and certain account-takeover-driven scams. It does not cover "Quality of Goods" disputes. If a customer pays for a service that isn't performed to their liking, that is a private dispute. Nacha is strictly concerned with identity deception and induced payments.

The risk-based mandate that goes beyond AML

A common pitfall is assuming existing Anti-Money Laundering controls satisfy these rules. AML traces the movement of "dirty" money; Nacha 2026 targets the "theft" of clean money. Because these transactions are technically authorized, "risk-based" procedures must be role-specific:

- **ODFIs and Originators:** These are the verification gates. They must verify the identity and authority of the person hitting send, particularly when instructions change.
- **TPSPs and Fintechs:** These are the pattern gates. They must monitor aggregate volume and velocity across all clients to spot unusual spikes that individual originators miss.
- **RDFIs:** These are the destination gates. They must monitor for new or dormant accounts that suddenly receive high-velocity "PAYROLL" credits, a key indicator of mules.

> "Many of these entries look authorized on the surface. What matters is whether the payment fits established behavior, context, and trust patterns, not just whether the customer clicked 'send.'"
> **Hailey Windham Community Lead for Banking, Sardine**

Expanded monitoring: The new expectations

The 2026 rules broaden the scope of responsibility across the entire ACH lifecycle.

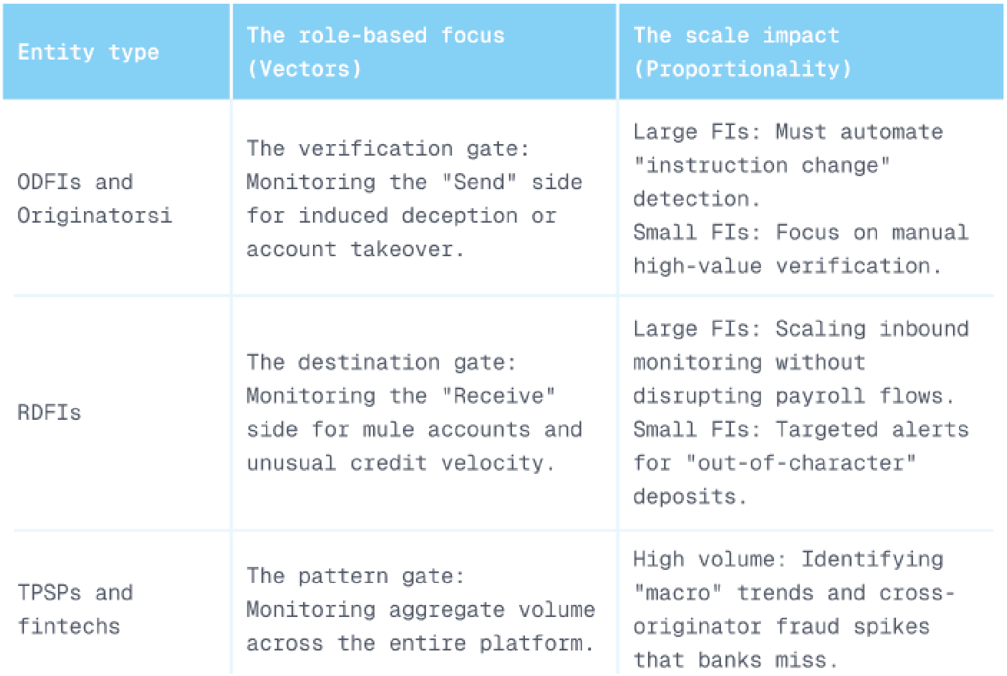
- **For ODFIs and Originators:** There must be established risk-based procedures to detect both unauthorized entries and those induced under False Pretenses. While AML focuses on the source of funds, these rules require consistent monitoring of the theft of funds.
- **For RDFIs:** The receiving-end blind spot is officially closing. It is now required to monitor for suspicious ACH credits and specifically looking for mule activity where inbound payments don't match the account's historical profile.

What this is NOT:

Nacha does not require transaction-by-transaction manual review or real-time blocking of every entry. It requires a Documented Standard of Care. Examiners aren't looking for zero fraud; they're looking for evidence that controls are reviewed annually and applied consistently.

The responsibility matrix: Role vs. scale

Nacha's focus is on shared responsibility. The risk-based mandate means requirements scale based on both size (volume) and role (where the organization sits in the transaction flow).



Entity type	The role-based focus (Vectors)	The scale impact (Proportionality)
ODFIs and Originatorsi	The verification gate: Monitoring the "Send" side for induced deception or account takeover.	Large FIs: Must automate "instruction change" detection. Small FIs: Focus on manual high-value verification.
RDFIs	The destination gate: Monitoring the "Receive" side for mule accounts and unusual credit velocity.	Large FIs: Scaling inbound monitoring without disrupting payroll flows. Small FIs: Targeted alerts for "out-of-character" deposits.
TPSPs and fintechs	The pattern gate: Monitoring aggregate volume across the entire platform.	High volume: Identifying "macro" trends and cross-originator fraud spikes that banks miss.

Why proportionality matters

Although the rules apply network-wide, the practical impact shifts based on operational complexity.

> "We tried to take a holistic view... we needed to look at it from the standpoint of all the participants and how they're interacting with these different payment scenarios."
> **Mark Dixon - Senior Consultant, Nacha**

- **For large institutions:** The challenge isn't the will to monitor, but the ability to do so consistently and explainably at scale. The goal is to catch high-velocity fraud without flagging thousands of legitimate corporate payments.

- **For credit unions and community banks:** The focus is avoiding the weak link status. For these leaner teams, "good" compliance means documented, risk-based controls that are manageable but consistently applied, not necessarily expensive.

Best practices: Executing the mandate

Meeting the new Nacha requirements requires aligning fraud controls with how ACH scams actually unfold, often well before funds move.

1. **Monitor across the customer lifecycle:**
   Transaction-only monitoring is insufficient. Many scams reveal warning signs earlier through changes to payment instructions, deviations from onboarding info, or sudden shifts in account behavior.

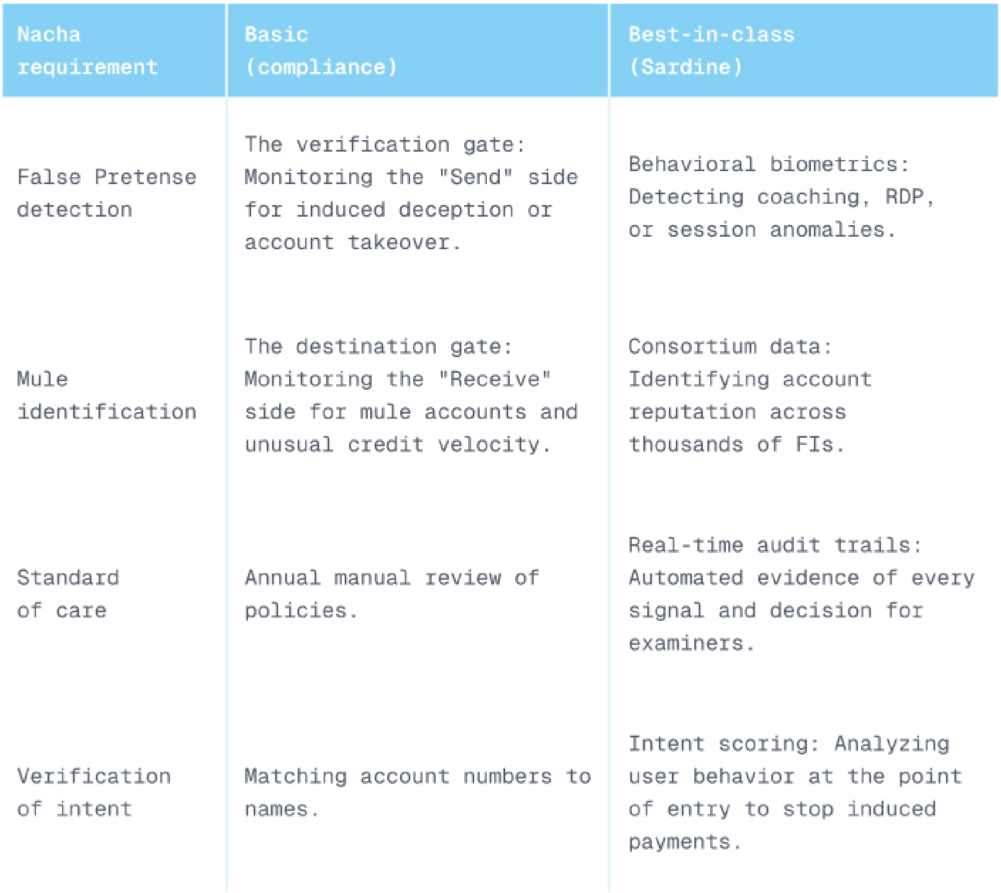
2. **Use behavioral and device signals:**
   Behavioral intelligence is a leading indicator. Signals such as typing cadence, device changes, VPN use, or remote desktop tools often appear well before suspicious ACH activity.

3. **Apply role-specific controls:**
   As outlined in the matrix, controls must reflect your position. ODFIs must flag outbound volume shifts, while RDFIs correlate inbound credits with KYC and account history. Use Nacha network tools strategically: When risk is identified, use the Contact Registry and R17 ("QUESTIONABLE") to coordinate with counterparties rather than waiting for an immediate customer dispute.

4. **Break down silos between fraud and payment ops:**
   Fraud detection spans front-line signals and back-office action. Compliance now expects documented workflows defining who investigates alerts and who approves returns or holds.

How Sardine bridges the gap

To meet the best-in-class standard, you need to look at signals that exist outside of the ACH file itself.



Nacha requirement	Basic (compliance)	Best-in-class (Sardine)
False Pretense detection	The verification gate: Monitoring the "Send" side for induced deception or account takeover.	Behavioral biometrics: Detecting coaching, RDP, or session anomalies.
Mule identification	The destination gate: Monitoring the "Receive" side for mule accounts and unusual credit velocity.	Consortium data: Identifying account reputation across thousands of FIs.
Standard of care	Annual manual review of policies.	Real-time audit trails: Automated evidence of every signal and decision for examiners.
Verification of intent	Matching account numbers to names.	Intent scoring: Analyzing user behavior at the point of entry to stop induced payments.

The compliance toolkit: Nacha's built-in controls:

Strong compliance is about more than new software; it's about using the network's updated mechanics to resolve False Pretense scenarios.

- **The Nacha contact registry:** Communication is now a requirement. You must keep your ACH Operations and Fraud contacts updated in the Nacha portal. This is the primary channel for coordinating "Requests for Return" when a scam is identified.

- **Return code R17 (The questionable signal):** As of late 2024, Nacha codified the use of R17 for suspicious activity. If an entry looks anomalous but lacks a formal "unauthorized" claim, RDFIs can return it using R17 with the descriptor "QUESTIONABLE" in the addenda record. This provides a formal audit trail for examiners.

- **The voluntary exemption** (The pause button): One of the most powerful tools in the 2026 framework is the expanded exemption from funds availability. If a PAYROLL or PURCHASE entry triggers a fraud flag, you have the right to delay funds availability while you investigate, effectively stopping the money from being cashed out by a mule.

Your 2026 readiness roadmap

From an examiner perspective, preparation is demonstrated through documentation, repeatable processes, and evidence that monitoring is actually used, not just written.

To prepare for the 2026 rules, institutions should begin now by:

- **Auditing the registry:** Ensure your fraud and operations teams are reachable in the Nacha Contact Registry today.
- **Updating R17 workflows:** Define the specific internal triggers that authorize your team to use the "Questionable" return code.
- **Codifying the "hold" policy:** Document exactly how your institution will apply the voluntary funds availability exemption to buy time for investigation.

Early preparation reduces operational risk and gives teams time to remediate gaps without disrupting payments.

More resources to help you prepare for Nacha's 2026 ACH fraud monitoring requirements:

ON-DEMAND
Sardine
FIS
Meeting Nacha's Upcoming Fraud Monitoring Requirements
HAILEY WINDHAM
Community Lead, Banking
Sardine
STACEY GROSS
Head of ACH and Instant Payments
FIS
SATHYA GOPALAKRISHNAN
Enterprise Sales Engineer
Sardine

On-demand webinar :

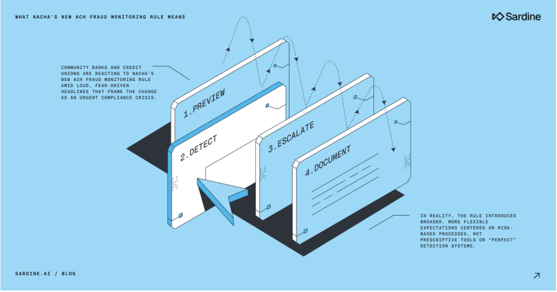
New Nacha Risk Management Rules: A Playbook for Institutions

On-demand webinar :

Meeting Nacha's 2026 Fraud Monitoring Requirements

Podcast:

Small FIs & the New Nacha Fraud Monitoring Rules (Phase 1)


WHAT NACHA'S NEW ACH FRAUD MONITORING RULE MEANS
Sardine
COMMUNITY BANKS AND CREDIT UNIONS ARE REACTING TO NACHA'S NEW ACH FRAUD MONITORING RULE AMID LOUD, FEAR-DRIVEN HEADLINES THAT FRAME THE CHANGE AS AN URGENT COMPLIANCE CRISIS.
1.PREVIEW
2.DETECT
3.ESCALATE
4.DOCUMENT
IN REALITY, THE RULE INTRODUCES BROADER, MORE FLEXIBLE EXPECTATIONS CENTERED ON RISK-BASED PROCESSES, NOT PRESCRIPTIVE TOOLS OR "PERFECT" DETECTION SYSTEMS.
SARDINE.AI / BLOG

Blog:

What Nacha's new ACH fraud monitoring rule actually means for community banks and credit unions