ValidiFI

Nacha Fraud Rules for ACH Fraud Detection & Risk Management

Rule Changes and Definitions for FI's and Payment Partners

This Guide Covers:

- Why These Rules Exist
- What's Changing in 2026
- What Are "False Pretenses"?
- What "Risk-Based Monitoring" Means
- Checklist for Readiness

Fraud is no longer a back-office problem—it's a strategic threat impacting profitability, compliance, and customer trust. With Nacha's new Fraud Monitoring Rule taking effect on March 20, 2026, financial institutions and payment partners must shift from reactive fraud prevention to proactive, risk-based monitoring.

This eBook explains the rules, what's changing and definitions.

Motivation Behind the New Rules

Fraud rates continue to grow, impacting financial institutions and their customers

79% of organizations experienced payment fraud attempts in 2024

38% of organizations experienced ACH debit fraud, and 20% reported ACH credit fraud

$8.5B in reported losses from BEC fraud over last three years

$12.5B in consumer fraud losses reported in 2024, up 25% from 2023

Sources: 2025 AFP Payments Fraud and Control Survey, FTC, Mar 2025: "$12.5B lost to fraud in 2024, up 25% over 2023, IC3 2024 Annual Report

2021 vs. 2026 Nacha Rule: Quick Comparison

Aspect	2021 Rule	2026 Rule
Requirement Type	“Commercially reasonable” fraud detection	Mandated risk-based processes & procedures
Scope	Limited to certain ACH participants	All ACH participants (ODFIs, Originators, TPSPs)
Account Verification	Not always required	Now required for all ACH credits before payment
Monitoring	Informal/ad hoc policies common	Must formalize a documented process and regularly review
Compliance Evidence	Minimal documentation needed	Written procedures, logs, and audit trails
Timeline	Ongoing	Phase 1: Mar 20, 2026 (high-volume) Phase 2: Jun 19, 2026 (all others)

What to Know for Compliance

- *Risk-Based Approach* - Nacha now requires tailored fraud controls based on transaction volume and risk level—not just generic policies.
- *Account Ownership Verification* - Must verify account ownership before sending ACH credits; methods can vary.
- *Document Everything* - Written policies, process templates, and incident logs are essential. Nacha expects regular reviews and updates.
- *Focus on Scalable, Auditable Procedures* - Nacha does not prescribe specific tools.
- *Conduct Annual Reviews* - Ongoing training should be conducted.

Understanding “False Pretenses”

A payment is considered authorized under false pretenses when the sender believes they are paying a legitimate party or the receiver has misrepresented their identity or intent.

Examples:

- Business Email Compromise (BEC): Fraudster impersonates a company executive and instructs staff to send funds to a fraudulent account.
- Vendor Impersonation: Fake invoices or payment instructions from someone posing as a trusted vendor.
- Payee Impersonation: Fraudster claims to be a real estate settlement agent or attorney and requests closing funds.
- Payroll Diversion: Fraudster reroutes employee direct deposits by accessing payroll systems or impersonating employees.

What’s NOT Considered False Pretenses

- Disputes about goods or services quality.
- Payments made to the correct person or organization.

Why This Matters for RDFIs and ODFIs

- ODFIs: Must monitor origination risk and implement fraud detection processes.
- RDFIs: Must monitor incoming credits for suspicious patterns and act when fraud indicators appear.
- Both must document their approach and update annually to stay compliant.

What “Risk-Based Monitoring” Means

Non-Consumer Originators, ODFIs, and Third-Party Service Providers	RDFIs
Key principles: • Cannot conclude that no monitoring is necessary • Must differentiate higher-risk vs. lower-risk transactions. • Pre-processing monitoring offers best fraud prevention opportunity (though not required).	Key Principles: • Flag suspicious entries by analyzing patterns and account behavior (SEC code mismatch, Rapid fire credits, etc.)
Actions for high-risk transactions: • Stop processing flagged transactions. • Validate with originator. • Consult internal fraud teams. • Contact RDFI for account-level red flags or request fund freeze/return.	Actions for flagged transactions: • Use voluntary exemption from funds availability to allow more review time. • Leverage Nacha’s ACH Contact Registry to coordinate with ODFIs. • If confirmed suspicious, return the entry using Return Reason Code R17 (“Questionable”) within standard timeframes.

Ensure confidence, trust, and transparency in every transaction

ValidiFI can help you:

- Detect fraud early with ValidiFI's network before losses occur
- Future-proof your payments to stay ahead of compliance
- Scale securely with ValidiFI's solutions tailored for financial institutions and payment partners

✓ Download our guide: Fraud Monitoring Implementation Considerations

Still need help or have questions? Schedule a Fraud Strategy Consultation

Move beyond compliance for strategic advantage, learn more at www.validifi.com