Nacha 2026 Compliance Brief

How ScamZero Supports ACH Fraud Prevention Requirements

Version: 1.0 **Date:** February 2026

⚠ Compliance Deadlines Approaching

Phase 1: March 20, 2026 - High-volume originators and RDFIs

Phase 2: June 19, 2026 - *All* RDFIs regardless of volume

📅

June 2026

All RDFIs must comply with new fraud monitoring rules

🎯

"False Pretenses"

New rules specifically target social engineering and BEC fraud

✓

ScamZero Helps

Member education demonstrates "reasonable procedures"

What's Changing in 2026

Nacha's 2026 Risk Management amendments represent the **most significant ACH rule changes in two decades**. The new rules expand fraud monitoring requirements beyond transaction screening to include protection against **"false pretenses" fraud**.

New "False Pretenses" Definition

Nacha now explicitly defines "false pretenses" fraud to include:

- **Business Email Compromise (BEC)** - Fraudulent emails impersonating executives or vendors
- **Vendor Impersonation** - Fake invoices or payment redirection requests
- **Payroll Diversion** - Scammers redirecting employee direct deposits
- **Identity Misrepresentation** - Impersonating someone's authority to act

> ℹ️ Key Insight
>
> These fraud types succeed through **social engineering** - manipulating people rather than hacking systems. Technical controls alone cannot prevent them. **Member education is essential.**

New Requirements for RDFIs

Requirement	What It Means
Risk-based fraud monitoring	Processes "reasonably intended to identify" ACH entries initiated due to fraud
Documented procedures	Written policies and processes for fraud prevention
Annual review	Review of fraud monitoring procedures at least annually
Staff training	Education on fraud scenarios including "false pretenses"

⚠️ Important

Nacha specifies that **concluding "no monitoring is necessary" is not acceptable**. All RDFIs must have active fraud prevention measures in place.

How ScamZero Supports Compliance

ScamZero directly addresses the **social engineering component** of Nacha's "false pretenses" fraud by educating members to recognize manipulation tactics *before* they authorize fraudulent payments.

Alignment with Nacha Requirements

Nacha Requirement	How ScamZero Helps
Risk-based fraud monitoring	Enables members to verify suspicious communications *before* acting on them
"False pretenses" fraud prevention	AI specifically trained to identify BEC, impersonation, and social engineering tactics
Documented procedures	Provides documented member education channel that can be included in compliance documentation
Staff training	Staff can use ScamZero to verify suspicious communications and learn scam patterns
Annual review	Portal analytics provide data for annual compliance reviews

What ScamZero Detects

ScamZero's AI is specifically designed to identify the manipulation tactics used in "false pretenses" fraud:

- ✓ Urgency and pressure tactics
- ✓ Authority impersonation
- ✓ Payment redirection requests
- ✓ Spoofed email domains
- ✓ Invoice manipulation
- ✓ Wire transfer scams

- ✓ Unusual sender behavior
- ✓ Account verification phishing

Demonstrating "Reasonable Procedures"

Nacha's standard requires institutions to have procedures **"reasonably intended to identify"** fraud. ScamZero helps demonstrate compliance by providing:

24/7	Real-time	Documented
Member Access	Scam Analysis	Education Channel

Evidence of Compliance

When examiners or auditors ask what you're doing to prevent "false pretenses" fraud, ScamZero provides:

- ✓ **A dedicated member education portal** - Demonstrates proactive fraud prevention
- ✓ **Scam verification tool** - Members can check suspicious messages before acting
- ✓ **Educational content** - Current information about active scam threats
- ✓ **Recovery guidance** - Support for members who've been victimized
- ✓ **Usage analytics** - Data showing member engagement with fraud prevention resources

> ✓ Examiner-Ready
>
> ScamZero gives you a clear answer when asked: *"What are you doing to educate members about social engineering and BEC fraud?"*

Easy Implementation

Unlike transaction monitoring systems that require integration with your core, ScamZero deploys in days with **zero technical integration**.

Deployment Timeline

Step	Timeline	Effort
Portal setup (branding, domain)	Same day	30 minutes
Staff training	1-2 days	Self-service
Member communication	As scheduled	Templates provided
Go live	When ready	Flip a switch

No Integration Required

- ✕ No core banking integration
- ✕ No API connections
- ✕ No data feeds
- ✕ No IT project

ScamZero is a standalone portal. Members visit it like any website. Your IT team's only involvement is approving the subdomain (yourcu.scamzero.com).

The Cost of Inaction

Social engineering fraud is the **fastest-growing fraud category** affecting credit unions. A single successful BEC attack can result in losses of $50,000 to $500,000+.

Prevention vs. Recovery

Scenario	Cost
ScamZero annual subscription	$2,999 - $14,999/year
Average BEC fraud loss	$125,000+
Nacha compliance fine (potential)	Up to $500,000
Reputational damage	Incalculable

ℹ️ ROI Perspective

Preventing **a single fraud incident** pays for years of ScamZero service. And unlike reactive measures, member education prevents fraud before it happens.

Summary

Nacha's 2026 rules specifically target the **social engineering fraud** that technical controls alone cannot prevent. Credit unions need documented member education programs to demonstrate compliance.

ScamZero provides:

- ✓ A branded, member-facing scam verification portal
- ✓ AI trained to detect BEC, impersonation, and social engineering
- ✓ Documented evidence of fraud prevention procedures
- ✓ Zero integration - deploy in days, not months
- ✓ Affordable pricing for credit unions of all sizes

Ready to discuss how ScamZero can support your Nacha 2026 compliance?

Contact us at or visit

References

- Nacha Operating Rules - Risk Management Topics (Fraud Monitoring Phase 2)
- Nacha News: "New Fraud Compliance Responsibilities for All Organizations Sending ACH Payments"
- NCUA Examiner's Guide - Third-Party Risk Management