Unit21.ai

Nacha 2026 Fraud Monitoring Rules

# Fraud Monitoring Checklist

A step-by-step checklist for ODFIs, RDFIs, Originators, TPSs, and TPSPs to verify their fraud monitoring programs meet Nacha's requirements. Built for audit readiness.

# How to use this checklist

Nacha's fraud monitoring rules are now in effect. Phase 1 (March 20, 2026) applied to high-volume originators and ODFIs. Phase 2 (June 22, 2026) eliminates volume thresholds entirely: every non-consumer Originator, ODFI, RDFI, TPS, and TPSP must comply, regardless of ACH volume.

This checklist helps all five participant types verify their fraud monitoring programs meet Nacha's requirements. Use it to prepare for audits, document your controls, and identify gaps before examiners do.

01 **Identify your role**
Start with Section 1 (shared), then go to your entity-specific section.

02 **Check each item**
Mark items your program already covers. Flag gaps for remediation.

03 **Document evidence**
For each checked item, note where the supporting documentation lives.

04 **Review annually**
Nacha requires at least annual review. Use this checklist as your framework.

05 **Prepare for examiners**
Section 7 maps directly to what auditors and examiners will request.

**Important Note**
Nacha requires "reasonably designed" risk-based controls, not real-time screening of every transaction. Your monitoring approach should be proportionate to your ACH volume, risk profile, and the types of entries you originate or receive. There is no one-size-fits-all requirement.

## Key Dates

| | |
|---|---|
| March 20 | **Phase 1 effective:** ODFIs/Originators/TPSs with 6M+ ACH originations |
| June 22 | **Phase 2 effective:** ALL remaining participants, no volume threshold |
| Ongoing | **Annual review** of fraud monitoring processes and procedures required |

Section 1

# Shared Requirements All ACH Participants

These apply to every Originator, ODFI, RDFI, TPS, and TPSP.

## Fraud Monitoring Program

- ☐ Established written, risk-based processes and procedures for identifying potentially fraudulent ACH entries
- ☐ Processes cover both unauthorized entries AND entries authorized under false pretenses (BEC, APP, payroll redirection)
- ☐ Monitoring scope includes ACH credit entries, not just debits
- ☐ Procedures define how suspected fraudulent entries are handled (hold, return, escalate, file SAR)
- ☐ Program is documented and can be produced for examiners on request

## Annual Review

- ☐ Processes and procedures are reviewed at least annually
- ☐ Annual review is documented with date, reviewer, findings, and changes made
- ☐ Review incorporates changes in fraud typologies, ACH volumes, and Nacha rule updates
- ☐ Review includes detection rule performance analysis (alert volumes, FP rates, dispositions)

## Audit & Examiner Readiness

- ☐ Written fraud monitoring procedures are current and accessible
- ☐ Evidence of monitoring activity exists (alert logs, case records, disposition history)
- ☐ SAR decision matrix or escalation criteria are documented
- ☐ Staff training records exist for fraud monitoring procedures
- ☐ Annual review documentation is retained for examiner review

Section 2

# Originator Non-consumer

> For non-consumer companies and entities that initiate ACH payments (e.g., employers running payroll, businesses paying vendors).

## Origination Controls

- ☐ Fraud monitoring covers all ACH entries you originate (credits and debits)
- ☐ Internal controls detect unauthorized changes to payment instructions (BEC, vendor impersonation)
- ☐ Dual-authorization or approval workflows exist for large or unusual ACH originations
- ☐ Process exists to verify new payee/ vendor bank account details before first ACH credit
- ☐ Monitoring flags deviations from normal origination patterns (volume, amount, frequency, new payees)

## WEB Debit Compliance

- ☐ WEB debit entries use a commercially reasonable fraud detection system to validate the first use of account info
- ☐ Subsequent WEB debits to the same account are similarly validated per Nacha rules

## Return Monitoring & Response

- ☐ Return codes are monitored for signs of fraud (R02, R03, R04, R07, R08, R10, R11, R29)
- ☐ Process exists to investigate elevated return rates and remediate root causes
- ☐ Fraud-related returns are escalated per your SAR decision matrix

Section 3

# ODFI (Originating Bank)

For Originating Depository Financial Institutions that submit entries into the ACH network.

## Origination Oversight

- ☐ Risk-based monitoring covers all non-consumer ACH originations submitted through the ODFI
- ☐ Account change velocity rules detect potential BEC (multiple payee changes in short windows)
- ☐ Rules flag anomalous origination patterns: unusual volumes, new payees, atypical amounts
- ☐ Monitoring distinguishes consumer vs. non-consumer originations (consumer excluded from scope)

## Return & Response Handling

- ☐ Return code monitoring is in place (R02, R03, R04, R05, R07, R08, R10, R11, R29)
- ☐ Elevated return rates trigger review and potential originator/TPS restrictions
- ☐ ACH Contact Registry is used to coordinate with RDFIs on suspected fraud
- ☐ Fund hold or delay procedures are documented for suspicious originations

## Third-Party Oversight

- ☐ Due diligence procedures exist for onboarding TPSs and TPSPs
- ☐ Agreements with TPSs and TPSPs require them to maintain their own fraud monitoring programs
- ☐ ODFI has visibility into TPS/TPSP origination activity for monitoring purposes
- ☐ Process exists to verify TPS and TPSP compliance with Nacha fraud monitoring rules
- ☐ ODFI can restrict or terminate TPS/TPSP relationships for non-compliance

Section 4

# RDFI (Receiving Bank)

For Receiving Depository Financial Institutions that post ACH credits to receiver accounts.

## Credit Entry Monitoring

- ☐ Risk-based processes identify inbound ACH credits initiated due to fraud
- ☐ Monitoring covers credits unauthorized OR authorized under false pretenses
- ☐ Procedures address handling of suspicious credits (hold funds, return, contact ODFI, file SAR)
- ☐ New account monitoring flags new accounts receiving large or unusual ACH credits

## Mule Account Detection

- ☐ Behavioral rules detect mule patterns: rapid inbound-outbound cycling, small credits followed by large withdrawals
- ☐ Velocity checks monitor frequency and volume of inbound credits to individual accounts
- ☐ Dormant account reactivation triggers review when followed by inbound ACH credits
- ☐ Fuzzy name matching or counterparty analysis detects mismatched sender/receiver relationships

## Response Procedures

- ☐ Process exists to return suspected fraudulent credits using appropriate return codes
- ☐ ACH Contact Registry is used to notify ODFIs of suspected fraud
- ☐ Fund delay/hold procedures are documented and compliant with Reg CC and UCC Article 4A
- ☐ SAR filing procedures cover ACH credit fraud scenarios with narrative guidance

Section 5

# Third-Party Sender (TPS)

For entities that submit ACH entries on behalf of Originators who don't have a direct ODFI relationship.

## TPS Fraud Monitoring

- ☐ TPS maintains its own fraud monitoring program independent of the ODFI
- ☐ Monitoring covers all ACH entries originated on behalf of Originators
- ☐ Processes detect unauthorized entries and entries authorized under false pretenses
- ☐ Monitoring distinguishes between Originator types and applies risk-appropriate controls

## Originator Oversight

- ☐ Due diligence is performed on Originators before onboarding
- ☐ Ongoing monitoring of Originator activity detects anomalous patterns
- ☐ Process exists to restrict or terminate Originators with elevated fraud risk
- ☐ Originator agreements reference Nacha fraud monitoring obligations

## ODFI Coordination

- ☐ TPS provides fraud monitoring reports or summaries to ODFI on request
- ☐ Escalation path exists for suspected fraud between TPS and ODFI
- ☐ TPS retains documentation of its monitoring program for ODFI and examiner review

Section 6

# Third-Party Service Provider (TPSP)

> For any organization performing ACH processing functions on behalf of an Originator, TPS, or ODFI. A TPS is a specific type of TPSP.

## TPSP Fraud Monitoring

- ☐ TPSP maintains its own fraud monitoring program for the ACH processing functions it performs
- ☐ Monitoring is appropriate to the TPSP's role (processing, formatting, transmitting, etc.)
- ☐ Processes detect unauthorized entries and entries authorized under false pretenses
- ☐ Program accounts for the specific fraud risks associated with the TPSP's processing functions

## Client & Upstream Coordination

- ☐ TPSP communicates its fraud monitoring capabilities to client ODFIs and Originators
- ☐ Escalation path exists for suspected fraud between TPSP and its client ODFI/TPS
- ☐ TPSP provides monitoring reports or summaries to clients on request
- ☐ Agreements with clients define fraud monitoring responsibilities and data-sharing obligations

## Documentation & Requirements

- ☐ TPSP retains documentation of its monitoring program for client and examiner review
- ☐ Program documentation clearly defines scope: which ACH processing functions are covered
- ☐ TPSP can demonstrate compliance with Nacha fraud monitoring rules to its ODFI

Section 7

# Program Governance & Documentation

What examiners will look for in your program documentation.

## Written Procedures

- ☐ Fraud monitoring policy is a standalone document (or clearly identified section within BSA/AML program)
- ☐ Policy names the owner (title/role) responsible for the fraud monitoring program
- ☐ Policy defines escalation paths: analyst > supervisor > BSA officer > SAR filing
- ☐ Triage standards are documented: what constitutes a TP, FP, and escalation criteria
- ☐ SAR decision matrix exists with clear thresholds and narrative guidance for ACH fraud

## Detection Rule Documentation

- ☐ Each active detection rule has documented rationale (why it exists, what fraud type it targets)
- ☐ Rule thresholds and parameters are documented with justification
- ☐ Rule change history is maintained (who changed what, when, and why)
- ☐ Rule performance metrics are tracked (alert volume, TP rate, FP rate)

## Evidence Retention

- ☐ Alert logs with timestamps and analyst dispositions are retained
- ☐ Case files with investigation notes, evidence, and outcomes are maintained
- ☐ SAR filings and 'no SAR' decisions are documented with reasoning
- ☐ Annual review reports are archived for at least 5 years
- ☐ Training records are maintained for all fraud monitoring staff

# Ready to automate your Nacha fraud monitoring?

Unit21 helps financial institutions and fintechs build fraud monitoring programs that satisfy Nacha's requirements, with self-service rules, automated alert triage, case management, and regulatory filing from a single platform.

Detection

## No-Code ACH Fraud Rules

Build and deploy Nacha-aligned detection rules in minutes, not sprints. Cover mule accounts, BEC, payroll fraud, and APP patterns with self-service configuration.

Investigation

## AI-Powered Alert Triage

AI Agents handle L1 triage, reviewing alerts, pulling context, and recommending dispositions. Your analysts focus on the cases that actually matter.

Filing

## SAR & Regulatory Reporting

File SARs directly from the case with AI-drafted narratives. Full audit trail from alert to filing. Document every decision for examiner review.

Unit21.ai

See it in action

Request a Demo →

Learn more on our hub

Keep Learning →