

DEVELOPING AND MAINTAINING RISK-BASED PROCESSES AND PROCEDURES

This guide outlines key points to consider when developing and maintaining risk-based processes and procedures relevant to your role as an ACH Originator. These processes are designed to help identify ACH Entries that may be unauthorized or authorized under false pretenses.

FRAUD MONITORING AND PREVENTION POLICY

Define the scope, roles, and goals for detecting Entries suspected of being unauthorized or authorized under false pretenses. May include purpose, objectives, and responsibilities.

RISK ASSESSMENT AND FRAUD MONITORING METHODOLOGY

Show how fraud risks are identified, monitored, and evaluated based on ACH activity. May include risk factors, chosen controls, technology and tools to detect anomalies, thresholds, and rationale for exclusions.

PROCEDURES ACROSS THE ACH PAYMENTS LIFECYCLE

- **Onboarding**

Specify controls to verify payee legitimacy and prevent fraudulent setups during onboarding and payment initiation. May include bank account and ownership validation, callback verification at a previously known or confirmed number, optional prenotes, and secure data collection leveraging multi-factor authentication (MFA).

- **Approval and Release**

Detail steps to ensure ACH Entries and changes are properly authorized before release. May include dual approval, exception review triggers, and secure transmission practices.

- **Post-Release Monitoring**

Outline how released ACH Entries are monitored for suspected fraud and actions taken. May include daily reconciliation, anomaly detection, and escalation paths.

- **Change Management**

Describes controls to prevent fraud related to changes in bank account or payment details. May include MFA for account changes, out-of-band authentication, account validation, dual approval, and prenotes.

TRAINING AND AWARENESS

Cover education for staff on fraud risks, awareness, escalation procedures, and incident response. May include business email compromise (BEC), vendor impersonation, and payroll redirection scenarios.

ANNUAL REVIEW AND CONTINUOUS IMPROVEMENT

Record annual reviews of fraud monitoring processes and updates to address evolving risks. May include threshold tuning and changes to regulatory environment or business operations.

EVIDENCE RETENTION

Addresses documentation of alerts, investigations, and decisions to demonstrate compliance. May include logs, review records, and threshold changes.

AVAILABLE ACH ORIGINATOR RESOURCES

- **Nacha.org** – Official Nacha resources and updates
<https://www.nacha.org>
- **Nacha Operating New Rules** – provides the most recent listing of rules changes
<https://www.nacha.org/newrules>
- **Nacha Operating Rules and Guidelines** – Comprehensive rulebook
<https://www.nacha.org/rulesyourway>
(Available in print and digital formats; subscription options for updates)
- **Nacha Risk Management Portal** – Tools for risk assessment and fraud prevention
<https://www.nacha.org/risk-management>
- **Nacha Preferred Partner Program** – Nacha partners providing solutions for account validation, fraud detection, and risk monitoring
<https://www.nacha.org/preferred-partners>
- **Regional Payment Associations** – Nacha’s directory
<https://www.nacha.org/content/nacha-direct-member>
- **Wespay** – Education and compliance support for Western region
<https://www.wespay.org/>
- **Third Party Payment Processors Association (TPPPA)**
<https://www.tpppa.org>
- **Anti-Fraud and Cybersecurity Best Practices Checklist** – Available on your bank’s fraud-prevention webpage

The information provided in this guide is for general reference only and does not constitute legal advice or specific operational instruction. ACH Originators are solely responsible for understanding and complying with all applicable Nacha Rules. For guidance on interpretation or compliance, please consult your organization’s legal and compliance professionals. You are also responsible for adhering to the terms and conditions outlined in your account agreements and Treasury Management Service Agreements with the Bank.