Nacha Fraud Prevention Controls – Quick Reference Guide

Overview

ACH Originators are now required under Nacha Rules to implement fraud monitoring and detection. Controls must be risk-based, scalable, and may be developed internally, or sourced from third-party providers. Layered security is strongly recommended.

Key Controls

Dual Controls

- Requires two individuals to complete payment initiation and release.
- Prevents fraud by adding an extra verification step.
- Often offered and required by financial institutions.

Account Validation

- Confirm new accounts and/or changes to existing accounts with known sources.
- Basic: Verify account is open at Receiving Depository Financial Institution.
- Advanced: Includes KYC data (name, address, balance, IP).
- Commonly provided by third-party services.

Multi-Factor Authentication (MFA)

- Adds a second factor beyond passwords (e.g., token, biometric).
- Stronger than password-only authentication.
- Out-of-Band Authentication and/or Biometric Authentication are preferred additional layers of security outside of MFA security questions.

Payment Instruction Update Verification

- Verify payment requests or changes using a different channel than the original request.
- Example: Confirm vendor changes via internal contact info, not the same call/email.

Routine & Red Flag Reporting

- Daily account reviews and reconciliations.
- Flag and verify: Transactions to new relationships, existing customers sending to new accounts, abnormal activity.

Review User Rights

- Regularly review online banking access.
- Promptly remove access for terminated or transferred employees.

Secure Systems & Applications

- Maintain firewalls and up-to-date antivirus software.
- Apply latest vendor security patches to all systems and applications.