ValidiFI

NACHA Fraud Monitoring **Best Practices**

for ODFIs, non-consumer Originators, Third-Party Service Providers, and Senders

Risk Management Rule Amendments

ACH credit fraud, especially via Business Email Compromise (BEC) and vendor impersonation—is rising sharply, with average losses projected to exceed $300,000 per incident by 2026. Effective March 20, 2026, Nacha mandates that ODFIs, non-consumer Originators, Third-Party Service Providers, and Senders implement risk-based processes to detect ACH entries initiated due to fraud.

1. Review Account Activity

Assess accounts with vFraud from ValidiFI to spot payments that may be **unauthorized** or approved **under false pretenses** such as Business Email Compromise (BEC) fraud, Vendor or Payroll impersonation.

2. Analyze Existing Accounts

Perform robust account validation on current accounts, like vAccount, to detect high-risk indicators. This helps meet compliance requirements and proactively prevent unauthorized payments.

3. Validate New Accounts

For accounts with no prior history, perform one-time validation using a service like vAccount that can confirm account status and layer in authentication of account ownership. While not required, this step offers the highest fraud prevention and protection.

4. Ongoing Monitoring

For high-risk accounts, implement step-up authentication tools like vAuth or vConnect. Establish a cadence for monitoring—weekly, monthly, or bi-annually—based on risk exposure.

Don't Just Comply, ValidiFI It

Manual processes are no longer sufficient. Fraudsters exploit gaps in consumer and vendor onboarding and account change workflows. Strengthen your entire payment and onboarding process. Turn Nacha's requirement into a strategic advantage.

Nacha Preferred Partner

From compliance to custom workflows tailored to your use case, we've got you covered.
Contact your account representative or visit validifi.com to learn more.