LexisNexis®
RISK SOLUTIONS

Preparing for Nacha's 2026 ACH Rule Changes: What Non-Bank Companies Need to Know

The upcoming Nacha rule changes, effective in 2026, will significantly impact non-bank companies that originate ACH credit transactions. These updates are designed to strengthen fraud prevention and improve payment transparency, particularly in response to rising threats like vendor impersonation and business email compromise (BEC) scams.

Key Changes and Requirements

1. Enhanced Fraud Detection

Companies must implement and annually review risk-based processes to detect fraudulent ACH credit transactions. This includes monitoring for payments made under false pretences, expanding beyond traditional unauthorized access prevention.

2. Account Ownership Verification

Before initiating payment, companies are expected to establish risk-based processes and procedures reasonably intended to identify ACH entries initiated due to fraud, as encouraged by Nacha guidelines. This step is critical to prevent vendor impersonation fraud.

3. Standardized Company Entry Descriptions

Certain transaction types require specific descriptions:

- "Payroll" must be used for all payroll deposits.
- "Purchase" is required for e-commerce transactions.

4. Phased Implementation Timeline

- Phase 1 (March 20, 2026): Applies to originators and third-party senders with 6 million+ ACH entries in 2023.
- Phase 2 (June 19/22, 2026): Applies to all other non-consumer ACH originators.

Impact on Non-Bank Companies

Operational Burden
Organizations must assess current fraud prevention capabilities and may need to invest in new systems or services. This includes auditing workflows and automating compliance processes.

Cross-Functional Adaptation
Departments including finance, procurement, vendor management, and compliance will need to revise their internal processes. As a best practice, LexisNexis® Risk Solutions strongly recommends adding bank account validation to vendor onboarding.

Increased Costs
Budgeting for account verification tools and fraud detection software will be necessary to meet compliance standards.

Compliance Risks
Non-compliance could result in audits, remediation requirements, reputational damage, and legal exposure in the event of fraud.

How LexisNexis® Risk Solutions Can Help

As a Nacha preferred partner, LexisNexis® Risk Solutions offers best-in-class tools to support compliance. This dual-layered approach ensures robust compliance and enhanced fraud protection:

- **Identification Solutions**: Turnkey tools for fraud monitoring and identity verification.
- **Safe Payment Verification (SPV)**: A solution that validates the match between an ACH originator and a bank account holder either for the sending or receiving account, depending on how the customer uses the service.

How can you Prepare?

Assess
Conduct ACH risk assessments to identify vulnerabilities

Implement
Deploy behavioral analytics and payment monitoring tools

Consult
Engage your LexisNexis® Risk Solutions Account Team to explore compliance solutions

Review
Update fraud monitoring processes annually

Summary of Rule Impacts

- Real-time fraud monitoring is required for outgoing ACH entries
- Specific company entry descriptions (e.g., “Payroll”, “Purchase”) are mandated.
- Account validation is mandatory for first-time consumer bank account use and new accounts.
- Non-compliance may result in fines, audits, payment disputes, and loss of customer trust.

LexisNexis® RISK SOLUTIONS

risk.lexisnexis.com/financial-services/payments-efficiency