Mechanics
COOPERATIVE BANK

NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION RULE CHANGES FOR NON-CONSUMER ORIGINATORS

The National Automated Clearing House Association (Nacha) has introduced new requirements focused on strengthening the security of the ACH Network. As your business is a "Non-Consumer Originator" of ACH transactions, you are now required to play a direct role in identifying and preventing fraudulent activity before it is transmitted for processing.

Our Commitment

Nacha's latest rule changes apply to all participants in the ACH Network, including banks, third-party vendors, and business customers.

Below, we have summarized the rule changes that directly impact your business as a "Non-Consumer Originator." To learn about the full set of changes, you can visit the Nacha website at www.nacha.org and click on Risk Resources.

What is Changing?

Beginning in 2026:

1. **Establish Risk-Based Procedures**
   Non-Consumer Originators must implement processes and procedures reasonably intended to identify potentially fraudulent transactions before they are sent. These procedures should align with the role your organization plays in the payment origination process and may take into account fraud monitoring performed by other parties involved. Monitoring is not required to occur before transaction processing.

2. **Standardized Entry Description for Payroll**
   When uploading a payroll file or creating a batch of payments through Digital Banking, Non-Consumer Originators must select the **"PAYROLL"** payment type. This ensures that your transactions are correctly identified with "Payroll" in the Company Entry Description field.

3. **Annual Reviews**
   Non-Consumer Originators should conduct and document an annual review of their ACH risk monitoring processes and procedures to ensure they remain effective against evolving fraud threats.

Continued on next page

Recommended Best Practices

To comply with these rules and protect your business from loss, we strongly recommend the following controls:

- **Anomaly Detection:** Establish a baseline of "normal" activity to help identify unusual transaction patterns, such as sudden changes in frequency, amounts, or receiver account numbers.
- **Verification of New/Changed Details:** Verify any requests to change payment instructions or account details using the contact information you already have on file. Never use information provided in a potentially compromised email.
- **Dual Control Processes:** Implement dual control requirements for approving and validating transactions to ensure payments are correct and authorized before being sent.
- **Annual Reviews:** Review your fraud prevention processes at least once a year to ensure they remain effective and aligned with your risk profile.

Next Steps: We recommend you begin assessing your current fraud monitoring capabilities and updating your internal documentation to reflect these mandatory security controls.

We're Here to Help

If you need assistance understanding these rule changes or implementing best practices for your business, we are here to help. Give us a call at 1-888-MECHANICS (632-4264).