First Carolina Bank

NACHA's 2026 ACH Updates

Annually, we look forward to sending our ACH origination customers an update explaining changes in the National Automated Clearing House Association (NACHA) rules. We hope this will help you maximize your efficiency, save you money, and allow you to participate effectively in the area of faster payments.

This year's changes introduce strengthened fraud prevention requirements and new standards designed to enhance security and transparency across the ACH network, including financial institutions, originators, and third-party service providers. The updates are taking place in two phases, with the first having gone into effect on March 20, 2026, and the second coming up on June 19, 2026.

Expanded Fraud Monitoring Requirements

As of March 20, 2026, NACHA is requiring ACH participants — including originators, originating depository financial institutions (ODFIs) and third-party providers — to implement risk-based processes and procedures to detect entries initiated due to fraud. This expands fraud monitoring responsibilities beyond WEB debits and micro-entries to include a broader range of ACH transaction types. The rules aim to reduce fraud, improve recovery of funds, and establish baseline activity patterns to help identify anomalies.

This rollout is occurring in two phases:

- **Phase 1 (March 20, 2026):** Applies to high-volume non-consumer originators and third parties.
- **Phase 2 (June 19, 2026):** Expands to all remaining originators and third-party providers.

Standardized ACH Company Entry Descriptions

Also, as of March 20, 2026, specific ACH transactions must use standardized Company Entry Descriptions:

- **PAYROLL** for all PPD credits related to wages or salary payments
- **PURCHASE** for all online consumer debit entries related to e-commerce transactions

These changes aim to improve clarity, consistency and transparency across ACH files and assist financial institutions in more easily identifying transaction types.

Focus on Preventing False Pretenses Fraud

The updated rules incorporate a more explicit definition of false pretenses, covering fraud schemes such as Business Email Compromise (BEC), vendor impersonation, and payroll diversion. NACHA now emphasizes the need for proactive fraud monitoring, shifting from simple account validation to verifying identity and detecting suspicious behavior before transactions are initiated.

Impact on Businesses and Financial Institutions

These updates will require businesses to evaluate and, in some cases, overhaul their internal fraud-prevention practices. Businesses may need to work with their financial institutions to ensure monitoring systems are in place and undergo annual reviews to stay compliant. For treasury teams, the changes underscore the importance of establishing strong internal controls and leveraging fraud-prevention tools.

Additional Reminders and Fraud Best Practices

Never accept changes to banking information for ACH payees strictly based on emails or a single call from an unknown employee of the vendor. It only takes a moment to place a call back to a phone number you already have on file and speak to someone you know or request information that allows you to properly verify it is your vendor making the request. Below, we have listed other actions to take to make it more difficult for criminals to commit fraud.

- Implement dual control, out-of-band authentication on all online payment transactions and be proactive in monitoring return activity.
- Implement ACH Debit Filter services on all accounts so you can control which ACH transactions should post to your account.
- Implement debit blocks to block all ACH debits from posting to specific accounts.
- Notify your banker to return unauthorized ACH debits to your account within 24 hours.
- Tightly limit access on who can manage recipient information to prevent changes to key fields, like beneficiary account information. Monitor changes to these fields, paying close attention in payroll files.
- Run background checks and credit checks on all new employees who have access to your finances and continue to reinforce not sharing online credentials (via training).
- Get all changes to vendor payment account number in writing and verify with a phone call to the number you have on file.
- Keep account authorizations up-to-date and notify the bank when an authorized signer or online banking user leaves your company.

If you have questions about any of this information, please contact your banker or local branch. We are happy to assist!