2025

ACH Rules Update for Corporate Originators and Third-Party Senders

Nacha® Direct Member

EPCOR, as a Direct Member of Nacha, is specially recognized and licensed providers of ACH education, publications and advocacy.

Origination Fraud Monitoring

Phase 1 Effective Date: March 20, 2026 – Companies originating 6M+ transactions in 2023.

Phase 2 Effective Date: June 19, 2026 – All companies, regardless of annual origination activity.

Beginning in 2026, fraud monitoring will be required regardless of the Standard Entry Class (SEC) code or payment type your company initiates. This is intended to reduce the incidence of successful fraud attempts. Specifically, your company must establish and implement risk-based processes and procedures to identify payments suspected of being unauthorized or authorized under "false pretenses."

An **unauthorized** payment would result if a fraudster compromised your company's online banking login credentials (e.g., captured by malware, convinced you to share) and then initiated a payment unbeknownst to you.

An **authorized under false pretenses** payment refers to the inducement of a payment by a person misrepresenting themselves. Through social engineering, a fraudster convinces a person to initiate (authorize) a credit payment.

These fraud schemes include business email compromise, vendor impersonation, payroll impersonation and other payee impersonation.

Risk-based processes and procedures do not require screening of individual Automated Clearing House (ACH) payments, nor do they need to be automated processes. A risk-based approach allows your company to apply resources and take extra measures to identify and detect fraud. While the *ACH Rules* do not prescribe what your company's risk-based approach should be, having no monitoring is not acceptable.

The intent of this new requirement is for your company to identify payments suspected of being unauthorized or authorized under false pretenses. It does not impose an obligation on your company to prevent wrongful activity. In layperson terms, the expectation is to do your best to detect fraud.

Your company should consider taking the following actions:

- Implement procedures to protect against account takeover and other fraud schemes.
- Educate staff on current fraud schemes, including those originating via email, phone calls, faxes or letters in the mail.
- Train employees to recognize, question and independently authenticate changes in payment instructions, payment methods (e.g., ACH to wire) or pressure to act quickly or secretively.
- Verbally authenticate any changes via a telephone call to a previously known number.
- Respond to emails for payment requests using the "forward" option and type in the correct email address or select it from a known address book.
- Remind staff never to provide online banking login credentials or account information when contacted, even by your financial institution. Instead, hang up and call them via a known number.
- Verify account information associated with first-time payments (e.g., ACH prenotes, micro-entries).
- Initiate payments using dual controls.
- Review your accounts frequently (i.e., at least daily).

The above list of considerations is not all-inclusive, nor is it one size fits all. Your company's risk-based processes and procedures for detecting fraud should be unique to your company and its payment activities.

Beyond monitoring, your company should be prepared to take steps should you detect fraud (e.g., reporting to designated personnel, notifying your financial institution or law enforcement). You should also annually review your fraud monitoring processes and procedures and update them as needed to address evolving fraud risks.

Preparations:

- Implement or update risk-based processes and procedures to identify and detect fraudulent transactions.
- Set a reminder to review your fraud monitoring processes and procedures annually and update as needed to address evolving fraud risks.
- Contact your financial institution to better understand the new requirement and to learn about their risk-based processes and procedures related to fraud monitoring.
- Develop processes for reporting fraudulent activity.

Standard Company Entry Description

Effective Date: March 20, 2026

Your company establishes the contents of the Company Entry Description field to provide the recipient (e.g., employee, customer/member or vendor) with a description of the purpose of the payment. Their financial institution conveys this information to them giving them clarity and transparency of where their money is going or why money is coming to their account.

Currently, the *ACH Rules* dictate the contents of this field in certain circumstances (e.g., "RETRY PYMT" if you are reinitiating or trying to collect a payment returned for insufficient funds). This amendment requires companies initiating:

1.) Prearranged Payment and Deposit (PPD) credits related to wages/salaries to input a description of "PAYROLL" in the Company Entry Description, and

2.) E-commerce/online retail purchases (WEB debits) to use "PURCHASE".

Preparations:

- Update systems to utilize required Company Entry Descriptions.
- Update procedures for entering Company Entry Descriptions.
- Train staff on the new requirement.