2026

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, for companies originating 6M+ transactions in 2023

Phase 2 Effective Date: June 19, 2026, for all companies, regardless of annual origination activity

In 2026, fraud monitoring will be required for all ACH payments, regardless of the Standard Entry Class (SEC) code or payment type your company initiates. The intent of this requirement is to reduce the number of successful fraud attempts. Specifically, your company must establish and implement risk-based processes and procedures to identify payments that are suspected of being either unauthorized or authorized under false pretenses.

An **unauthorized** payment occurs when a fraudster gains access to your company's online banking credentials (e.g., through malware or by convincing an employee to share them) and initiates a payment without your knowledge.

A payment **authorized under false pretenses** occurs when a fraudster induces a person within your company to initiate a payment based on misrepresentation. These schemes rely on social engineering and include business email compromise, vendor impersonation, payroll impersonation and other payee impersonation tactics.

Risk-based processes and procedures do not require screening of individual ACH payments, nor do they need to be automated. A risk-based approach allows your company to apply resources where they are most effective. While the *ACH Rules* do not prescribe what these processes must include, having no procedures in place is not acceptable.

The requirement focuses on identifying payments suspected of being unauthorized or authorized under false pretenses. It does not obligate your company to prevent all fraudulent activity. In practical terms, your company is expected to make reasonable efforts to detect fraudulent transactions. Identifying and stopping suspicious payments before they are transmitted helps prevent financial losses. According to the FBI, the average loss for successful business email compromise (BEC) scams in 2023 ranged from $137,000 to over $140,000 per incident.

Your company may consider:

- Implementing procedures to protect against account takeovers and other fraud schemes.
- Educating staff on current fraud tactics delivered via email, text messaging, phone calls, faxes or mail.
- Training 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.
- Verifying changes verbally using a previously known phone number.
- Responding to emailed payment requests by using "forward" and selecting the correct address from a known contact list.
- Reminding staff to never share online banking credentials or account information with anyone, under any circumstances. No financial institution or legitimate organization will ever ask for this information.
- Verifying account information for first-time payments (e.g., ACH prenotes, micro-entries).
- Using security tools from your financial institution, such as dual controls.
- Reviewing accounts frequently (i.e., at least daily) for suspicious activity.

This list is not exhaustive, and there is no one-size-fits-all approach. Your company's risk-based processes and procedures should be tailored to your organization and its payments activities.

In addition to monitoring, your company should be prepared to take appropriate steps when fraud is detected—such as notifying designated personnel, your financial institution or law enforcement. Fraud monitoring processes and procedures should be reviewed annually and updated as needed to address evolving risks.

Preparations:

- Implement or update risk-based processes and procedures to detect fraudulent transactions.
- Schedule an annual review of your fraud monitoring practices.
- Contact your financial institution to understand their fraud-monitoring expectations and resources.
- Develop clear internal processes for reporting fraudulent activity.

Standard Company Entry Description

Effective Date: March 20, 2026

Your company uses the contents of the Company Entry Description field to describe the purpose of the ACH payment you are initiating. While you may enter any description you choose in this 10-character field, the *ACH Rules* specify required descriptions in certain situations (e.g., RETRY PYMT when reinitiating a payment returned for insufficient funds).

This amendment requires companies originating (1) Prearranged Payment and Deposit (PPD) credits related to a person's employment compensation to include the description PAYROLL and (2) WEB debits for e-commerce or online retail purchases to include the description PURCHASE.

Employment-related compensation includes wages, salary, sales commissions, bonuses and payments to independent contractors (such as 1099 workers). It does NOT include expense reimbursements, retirement payments or pension payments.

Examples of e-commerce or online retail purchases include physical products (clothing, home goods, electronics), digital goods (video game purchases, music or movie downloads) and event tickets. They do NOT include payment for items such as insurance premiums or mutual fund contributions.

Preparations:

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

Optional Inclusion of Date of Birth in International ACH Transactions (IATs)

Effective Date: March 19, 2027

An International ACH Transaction (IAT) is an electronic payment sent through the ACH Network that involves either sending money to (credit) or collecting money from (debit) an account held at a financial institution located outside of the United States.

The physical location of the company or individual you are paying does not determine whether an IAT is required. However, their location may provide clues about where their bank account is held. For example, a business operating outside the U.S. may maintain a foreign bank account, or they may still have a U.S.-based financial institution. Because of this, your company must determine whether any foreign financial institution is involved at any point in the payment process. If so, the transaction must be originated as an IAT.

IAT payments use a specific format that includes your company's name and full address, along with the recipient's name and full address. This information appears in the Addenda Records that accompany the payment. Currently, you cannot include an individual's date of birth in these records, even if your company has that information.

This amendment will allow your company to optionally include a person's date of birth (in YYYY-MM-DD format) in the Addenda Records of an IAT. This is not required, but providing the date of birth may support sanctions compliance efforts.

Preparations:

- Create or update policies and procedures related to the collection and inclusion of dates of birth, including how they will be securely stored and protected.
- Update systems or software to support the new IAT format.
- Train staff on your updated process.

New Return Reason Code (R90)

Effective Date: March 17, 2028

When your company sends an ACH payment, the receiving financial institution may return the Entry if it cannot process it. For example, if the recipient's account is closed, they may return the payment using the R02 (Account Closed) Return Reason Code. When your institution receives the return, it will notify you so you can address the issue, such as obtaining updated account information from the recipient.

Currently, receiving institutions may also return debit or credit Entries due to potential legal action on an account, such as an account restriction or an Office of Foreign Assets Control (OFAC) sanctions issue. Both situations use the same Return Reason Code R16 (Account Frozen/Entry Returned per OFAC Instruction). Although these situations are related, the actions your company must take differ depending on whether the account is restricted for internal/legal reasons or the return relates to an OFAC violation.

This *Rule* change eliminates that ambiguity by assigning separate Return Reason Codes.

- R16 will indicate the account is restricted due to action taken by the receiving institution for internal (e.g., the institution is preparing to close the account) or legal reasons.
- R90 is a new Return Reason Code that will indicate the individual or business is listed on OFAC's Specially Designated Nationals (SDN) and Blocked Persons List. This list includes individuals and entities tied to sanctioned countries, as well as groups such as drug traffickers or terrorist organizations.

By clearly distinguishing these two situations, your company can take the appropriate next steps when receiving an R16 or R90.

Preparations:

- Update processes and procedures to address the appropriate actions for R16 and R90 returns. For example, if an Entry is returned R16, you may contact the recipient to determine another way to make payment. And if an Entry is returned R90, you must not conduct business with the recipient.