2024

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.

2345 Grand Blvd., Suite 1700, Kansas City, Missouri 64108 • www.epcor.org

Several upcoming amendments to the *ACH Rules* may impact how your company processes ACH payments. Listed below are four changes that take effect in 2024 and two that become effective in 2026.

Action on Notification of Change

Effective Date: June 21, 2024

If the account information your company obtains from a payee (e.g., employee, customer, vendor) is valid, your payment will automatically be processed to the payee's account. However, if the account information provided is erroneous or has become outdated, the payee's financial institution may manually process the payment to the payee's account and send a Notification of Change (NOC). An NOC contains the information in error along with the corrected information and will be provided to you by your financial institution.

If your company sends recurring payments to a payee's account (e.g., daily, bi-weekly, monthly), then you are required to update the information in error either before sending the next payment or within six banking days of receiving the NOC information.

If your company initiates a single or one-time payment to a payee's account, then you may, at your discretion, make the changes noted in the NOC. This amendment clarifies this is applicable regardless of the type of one-time payment originated (i.e., credit or debit transaction).

Preparations:

- Your organization may need to update policies and procedures related to handling Notifications of Change (NOCs).

Use of Prenotification Entries

Effective Date: June 21, 2024

A prenotification, or prenote, is a non-monetary entry used to verify that the account number provided by the payee is a valid account number at the receiving institution. Prenotes do not verify if the payee is an owner of the account. Typically, prenotes are only sent prior to transmitting the first credit or debit payment to the payee's account. This Rule change removes language limiting prenotes to this use. Therefore, your company may send prenotification entries at its discretion or as required by your financial institution.

Preparations:

- Your organization may need to update policies and procedures related to processing prenotification entries.

Return Reason Code R17 (Entry Initiated Under Questionable Circumstances)

Effective Date: October 1, 2024

If a payee's financial institution is unable to process an ACH payment, they will return it using a Return Reason Code to convey why it is being returned (e.g., R02 means the payee's account is closed). Return information is provided to you by your financial institution.

Currently, Return Reason Code R17 with QUESTIONABLE in the Addenda Information field indicates the payee's institution believes the payment is suspicious or questionable. While R17 could mean fraud, the *ACH Rules* currently do not explicitly state that. This update allows a payee's institution to use R17 in situations where they believe the transaction was initiated under "false pretenses" (i.e., the result of an account takeover, business email compromise, vendor impersonation fraud, payroll impersonation scam or other payee impersonation scheme).

Preparations:

- Educate your staff receiving return information on the meaning of Return Reason Code R17.
- Your organization may require procedure changes to include the handling of fraudulent transactions.

Return Reason Code R06 (Return per ODFI's Request)

Effective Date: October 1, 2024

Currently, the *ACH Rules* allow your financial institution to request a payee's financial institution return an erroneous entry using Return Reason Code R06. An erroneous entry is a payment that has been duplicated in error, sent for the wrong amount or transmitted to the wrong payee. While your institution may make the request, the payee's institution is not obligated to comply. Therefore, the request is just an attempt to recover from an error and not a guarantee.

With the increase in fraud, your organization could benefit from allowing R06 requests to be used to recover fraudulent payments. This update explicitly allows R06 requests for this purpose but does not change the obligations of the payee's institution (i.e., they are not required to return the funds).

Preparations:

- Your organization may require procedural changes related to the recovery of fraudulent entries, including notifying your financial institution immediately upon learning of fraud.

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 payment initiated. Currently, the *ACH Rules* dictate what goes in this field in certain circumstances (e.g., RETRY PYMT if you are reinitiating a payment returned for insufficient funds).

This amendment requires companies initiating (1) 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.

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

Currently, the *ACH Rules* require companies initiating WEB debit transactions and micro-entries to use commercially reasonable means to identify and detect potential fraud. Nacha's Board of Directors has issued a policy statement "urging all participants to implement adequate controls and/or systems to detect and prevent fraud." However, a policy statement is not an enforceable rule. Instead, it is a strongly recommended practice that ACH participants should follow.

With this amendment, your company is required to establish and implement risk-based processes and procedures to identify entries suspected of being unauthorized or authorized under "false pretenses" (e.g., business email compromise, vendor impersonation, payroll impersonation, account takeover). Fraud monitoring is required regardless of the Standard Entry Class (SEC) code, or payment type, initiated and is intended to reduce the incidence of successful fraud attempts.

Preparations:

- Your organization may require implementation of, or updates to, risk-based processes and procedures to identify and detect fraudulent transactions.