



## 2026 Nacha Rule Changes: What Originators Need to Know

### *New Company Entry Description Rules (Effective March 20, 2026)*

#### **Company Entry Description – PAYROLL**

The Company Entry Description field must contain PAYROLL, all capitalized, for PPD Credits paying wages, salaries and other similar types of compensation. New language indicates that the use of the term PAYROLL in this field is descriptive. By use of the word, neither the Originator, nor the ODFI or any third-party service provider acting on behalf of an Originator or ODFI, makes any representation or warranty to the RDFI or the Receiver regarding the Receiver's employment status.

#### **Company Entry Description – PURCHASE**

The Company Entry Description field must contain PURCHASE, all capitalized, for e-commerce purchases. For this purpose, an e-commerce purchase is a debit entry authorized by a consumer receiver for the online purchase of goods, including recurring purchases first authorized online. An e-commerce purchase uses the WEB debit SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL debit SEC Code.

Since March 20, 2026, originators are encouraged to begin using the new PAYROLL and PURCHASE descriptions. For more details on the new Company Entry Description requirements, visit [Nacha's website](#).

### *New Fraud Monitoring Requirements (Effective March 20, 2026 & June 19, 2026)*

Starting in 2026, business Originators will be required to establish and implement risk-based fraud monitoring processes and procedures reasonably intended to identify ACH Entries initiated due to fraud. The Originator's processes and procedures must be designed to reasonably identify entries suspected of being unauthorized or made under false pretenses, and they must be reviewed and updated at least annually to address evolving risks. These rule changes are part of Nacha's new risk management rules and fraud prevention requirements.

The new fraud monitoring requirements went into effect on **March 20, 2026** for businesses with ACH origination volume greater than six million entries in 2023. The requirements go into effect on **June 19, 2026**, for businesses that originate less than six million entries annually.

A common question we hear is: What practical steps should Originators, large or small, take to comply?

To keep it simple, most ACH transactions are sent to the same Receivers whether payroll, utility payments, vendor invoices or accounts payable. So, it makes sense to focus on transactions that are unusual or non-recurring. Originators should consider focusing their processes and procedures on brand-new Receivers and existing Receivers who suddenly change account information.

#### **New Receivers**

A new relationship needs to be established before sending an ACH credit. First, Originators should perform best practice due diligence reviews to ensure the individual or business is legitimate through verifying identification,



performing background checks and ensuring that the proper signers and authorized personnel represent a real entity. Then, Originators should securely store the account information in an encrypted fashion and maintain a valid contact number on file for any future verification.

### **Existing Receivers who suddenly change account information**

If a long-time Receiver unexpectedly sends new account details, especially via email, text or fax, treat it as a red flag. The Originator should use the contact information on file, not the information in the change request message, to verify account changes. Apply “know your customer” practices to confirm the request is legitimate before proceeding. Your company is responsible for following up on any request to change a Receiver’s account information with a phone call to the number on file in your records, without relying on the contact information included in the request.

For more details regarding the new fraud monitoring requirements, visit [Nacha's website](#). Chapter 15 in the 2026 Nacha Rule book, specifically pages OG74-OG80, provides additional guidance to help Originators implement the new requirements. You can also read [Nacha's blog](#) for additional tips that’ll help Originators comply with the upcoming risk management rules.

### **Compliance with existing Nacha Rules helps Originators mitigate fraud risk**

#### **Secure transmission of ACH information**

According to Article one section 1.7 of the 2026 Nacha Rules, sensitive account information such as the routing transit numbers, account numbers or the entries themselves, must be securely transmitted via encryption or a secure session. Thus, any Originator who’s transmitting account information via clear-text or unencrypted email is in violation of this Rule and is being exposed to fraud. Since Originators have direct relationships with Receivers, they’re in the best position to spot red flags, like new account setups or unexpected changes, and should have escalation processes in place to investigate before transmitting any unusual or suspicious entries.

#### **Originator must obtain authorization from the receiver**

Article two, section 2.3 of the Nacha Rules requires Originators to obtain authorization from the Receiver to originate one or more entries to the Receiver’s account. This authorization must comply with applicable legal requirements, meaning it must clearly link the Receiver to the consent provided. Common, easily spoofed methods like email don’t meet this standard. Instead, secure and traceable authorization methods, such as HR portals, written authorizations, or voided checks, could be used to protect both parties and ensure compliance.

#### **ACH data security**

Nacha Rules require all ACH participants to protect the security and integrity of certain ACH data throughout its lifecycle. Your company plays a vital role in maintaining proper security over protected information obtained as an ACH payment Originator. In the context of payment originations, protected information may be referred to as non-public personal which includes the financial information of a natural person used to create an entry, or contained within an entry, and any related addenda record. Originators must be vigilant in their effort to protect the security of protected information due to the increased focus on privacy of data, threats from data breaches and other unscrupulous activity, such as corporate account takeovers, viruses, network intrusions, employee/email fraud and hacking.

Your company is required to establish, implement and update policies, procedures and systems including controls with respect to the initiation, processing and storage of protected information that are designed to:

- Protect the confidentiality and integrity of the protected information until its destruction.



- Protect against anticipated threats or hazards to the security or integrity of protected information until its destruction.
- Protect against unauthorized use of protected information that could result in substantial harm to a natural person.

Chapter four of the 2026 Nacha Rule book, pages OG24-OG28, provides guidance to help Originators comply with the ACH Data Security rules, which also helps mitigate fraud risk.

#### 2026 standard Federal Reserve Bank holidays

The FedACH holiday schedule is published and available on the Federal Reserve [website](#). Keep in mind that a payment cannot have an effective date on a federal holiday because the Federal Reserve is not open for processing. Therefore, it's important that you take note of the holiday schedule to make sure the transactions you initiate process on time.

**For additional information about ACH and step by step instructions on how to use our services, we encourage you to visit [www.ODNB.Bank](http://www.ODNB.Bank) or notify our Treasury team at [Treasury@odnb.bank](mailto:Treasury@odnb.bank).**

**We're here to help! If you need any assistance or have questions, give us a call at 703-657-2971.**