2026
Nacha Rule Changes

Bonus Content

2026 Standard Federal Reserve Bank Holidays

Understanding Returns and Return Codes

Understanding Your Role Regarding the Security of Non–Public Personal Information

Foreign Asset Control Requirements

Authorizations

Standard Entry Class Code

Identifying Fraud Scams

Nacha's role in ACH

Nacha®, the National Automated Clearing House Association, is a trade association that helps develop, implement and enforce rules governing the use of the Automated Clearing House network. Nacha creates rules and standards through consensus-led governance with collaboration and input from industry stakeholders. You can learn more about Nacha by visiting **their website**.

As an ACH Originator, understanding the Nacha Operating Rules is essential in ensuring your compliance with the rules. If you wish to purchase a copy of the Rules, you may purchase it at the **Nacha store**, or by contacting your ODFI to receive a copy at your expense.

Upcoming Rule changes

New Company Entry Description Rules take effect 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.

Originators are encouraged to begin using the new PAYROLL and PURCHASE descriptions as soon as possible, but no later than **March 20, 2026**. For more details on the new Company Entry Description requirements, visit **Nacha's website**.

New fraud monitoring requirements take effect March 20 and 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 go into effect **March 20, 2026**, for businesses with ACH origination volume greater than six million entries in 2023 and **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 require 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 can't have an effective date on a federal holiday because the Federal Reserve isn't 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.

2026 holidays

New Year's Day
Thursday, Jan. 1

Martin Luther King Jr. Day
Monday, Jan. 19

Washington's Birthday, Presidents Day
Monday, Feb. 16

Memorial Day
Monday, May 25

Juneteenth National Independence Day
Friday, June 19

Independence Day
Saturday, July 4

Labor Day
Monday, Sept. 7

Columbus Day
Monday, Oct.12

Veterans Day
Wednesday, Nov. 11

Thanksgiving Day
Thursday, Nov. 26

Christmas Day
Friday, Dec. 25

Understanding returns and return codes

Return codes are used when the receiving bank is unable to post an entry to the Receiver's account and returns the entry back to the originating bank. Return codes provide the reason for the return. The financial institution will notify you of a return and then credit or debit the amount to your account. Return notification is typically provided to you by regular mail, email or online notification. Originators should receive return information within two banking days from the settlement date.

Return codes explain why funds are being returned.

Common return codes are:

- R01 Insufficient funds
- R02 Account closed
- R03 No account or unable to locate account
- R04 Invalid account number
- R06 Returned per ODFI's request
- R08 Payment stopped or stop payment on item
- R09 Uncollected funds
- R16 Account frozen
- R23 Credit entry refused by receiver
- R29 Corporate customer/accountholder advises not authorized

Unauthorized Return Codes are red flags for potential fraud

Originators should promptly investigate any entries returned with an unauthorized return code because these are red flags for potential fraud. The Receiving financial institution has up to 60 calendar days to return unauthorized entries. Common unauthorized return codes are:

- R05 Unauthorized debit to a consumer account using a corporate SEC code
- R07 Authorization revoked by a consumer accountholder
- R10 Customer/accountholder advises not authorized
- R11 Customer/accountholder advises entry not in accordance with the terms of the authorization

Re-initiating a returned item – RETRY PYMT

The only transactions that can be re-presented for settlement are:

- Those returned for Insufficient Funds or Uncollected Funds. There is a limit of two re-presentments within 180 days of the original entry date.
- A transaction that was returned for Stop Payment. If re-presenting, it must be approved by the receiving party.

When re-initiating a returned item, RETRY PYMT in all capital letters is required in the Company Entry Description field. Identical content is required in the following fields: company, name, company ID and amount. Modifications to other fields are permitted, but only to those necessary to correct an administrative error made during processing.

Reversals

Reversals are defined as a credit or debit entry that reverses an erroneous entry. If an Originator creates erroneous ACH entries or files, corrections may be made by initiating reversing entries or files. An erroneous entry or file is defined as:

- A duplicate of an entry previously initiated by the originator or ODFI
- Orders payment to or from receiver not intended to be credited or debited
- Orders payment in a dollar amount different then was intended

Reversals are requests

Reversals aren't mandatory transactions for the receiving financial institution, and they don't guarantee you will recover any funds. Receiving financial institutions don't have to put themselves in a negative position, such as overdrawing the receiver's account, to process a reversal. Reversals may be returned by the receiving institution.

The following requirements must be met when submitting a reversal:

- REVERSAL must be in all capital letters in the description field of the company batch header record
- Originated within five banking days following settlement date of the erroneous entry
- Will need to build a new batch record
- Change the transaction codes to offset entries, for example debits reverse credits
- The effective date should be the same date as the original entry/file date for future dated files
- Notify the receiver of the reversal by the settlement date. In the case of an erroneous file, transmit a correcting file with the reversing file

We recommend that Originators use an authorization agreement with their Receivers that states they are authorized to debit/reverse any entries made in error. This is good business practice and will help with any disputes in the future.

Understanding your role regarding the security of non–public personal information

The Nacha Operating Rules require that each Originator and third–party sender must have policies and procedures in place regarding the initiation, processing and the storage of personal, non-public information, entries and files. Your security policies and procedures should accomplish the following requirements:

- Protect the confidentiality and integrity of the personal, non–public information, including financial information that you have on file, and the file information itself, until destruction. Other non–public information you may have on file includes EIN or tax ID numbers, dates of birth, social security numbers and addresses.
- Protect against anticipated threats and/or hazards that would threaten the security of the protected information until its destruction.
- Protect against the unauthorized use of that protected information which could cause harm to that individual and/or business.
- Security policies and procedures should be reviewed on an annual basis, or more frequently depending on your business needs. Check out **this guide** to help create your security incident response procedures.

Originators must comply with Office of Foreign Asset Control requirements

You're required to check payees/ACH recipients against OFAC compliance checklists. OFAC checklists contain lists of countries, groups and individuals with which U.S. companies aren't permitted to send or receive funds.

It's against the law to send debit or credit entries to OFAC-blocked entities. You can check the OFAC SDN list **here**.

Notification of change

If the information on a transaction you originated is incorrect, you may receive a non-dollar correction transaction called a notification of change. It specifies information such as:

- Correct account number
- Correct routing/transit number
- Correct account type, like checking and/or savings

For example, if a receiving bank, also called receiving depository financial institution, has been through a merger, it may send you a NOC to provide new information that should be included on future transactions you originate.

The financial institution will notify you of any NOCs received. Changes need to be made before originating any further transactions to the same account. This is important to avoid disruption of payments or fines for uncorrected information which your financial institution may pass on to you. Following the NOC process, the receiving bank ensures that the information provided on future ACH transactions will be correct. By complying with the NOC, your business can originate future transactions without having to obtain a new authorization.

Common NOC codes:

- C01 Incorrect bank account number
- C02 Incorrect routing/transit number
- C03 Incorrect routing/transit number and bank account number
- C05 Incorrect transaction code
- C06 Incorrect bank account number and transaction code
- C07 Incorrect routing/transit number, bank account number and transaction code

Authorizations

As an Originator, you're required to adhere to certain rules and agreements when initiating ACH transactions. An authorization is a document that is received by the Originator from the Receiver which authorizes the Originator to initiate a transaction on behalf of the Receiver.

- Consumer authorizations must be written and signed or similarly authenticated by the receiver.
- The receiver must also receive a copy of the written authorization.
- The terms of authorization must be clearly stated and understandable.
- Must contain instructions for termination.
- Originators are required to retain the authorization for two years from the termination or the revocation of the authorization.
- You must obtain authorization from a customer when making a one-time or recurring ACH debit and must indicate very clearly to the customer that they are authorizing a one-time or recurring ACH debit.
- You must take reasonable steps to ensure customers' routing numbers are valid.
- You must take steps to verify a customer's identity, without regard to whether a transaction is authorized online or by phone.
- You must be vigilant about possible fraud and do whatever is commercially reasonable to ensure the ACH transactions you initiate are not fraudulent.
- Ensure that you cancel a subscription promptly and stop making debits if a customer asks to cancel.

Standard Entry Class code

A Standard Entry Class code is a mandatory three-character code that's used in all batches to identify the types of entries within a batch.

Only one SEC code may be used for each batch of entries. If you have both consumer and business receivers, the entries will need to be split into separate batches, one for consumer Receivers, and one for corporate or business Receivers. If an incorrect SEC code is used for a batch, you will be subject to additional return risk exposure and the potential for monetary fines assessed by Nacha through the National System of Fines.

For example, if a batch of entries is sent to corporate or business receivers using the Pre-arranged Payment or Debit SEC code, debit entries may be returned for up to 60 days, and you must have an authorization.

Ensuring you're using the correct SEC code helps limit your liability for return entries and helps you avoid fines that may be assessed for using the improper SEC code. The most used SEC codes are:

PPD — Pre-arranged Payment or Debit

- For business-to-consumer use only
- Most used for direct deposit
- Written authorization from the Receiver must be on file if you're debiting their account

CCD — Cash Concentration or Disbursement

- For business-to-business use only
- Can be used for moving funds between a business's own accounts at different institutions
- Used for payments or debits to other businesses
- Agreements are handled by contract authorization between companies

You can't combine different recipient types like consumers and businesses within a single batch. Different SEC codes are required based on the recipient type.

For example, you can't generate an ACH batch that contains employees for weekly payroll and businesses you're paying for invoices or other payment needs. You would need to originate one PPD batch containing all the employee transactions, and one CCD batch containing all the B2B transactions.

Company name

To ensure clear identification of the source of an ACH transaction, the Rules contain specific requirements with respect to how an Originator must identify itself within an ACH record. The Rules require the Originator to populate the Company Name field with the name by which it is known and readily recognized by the Receiver. This name could be the Originator's doing business as name or trading as name.

The inclusion of a readily recognizable Originator name ensures that the Receiver can identify a transaction appearing on their periodic statement. The clear identification of the Originator of an ACH transaction improves overall network quality by reducing the number of unrecognized entries requiring investigation and possible returns.

Fraud corner

Spotting and avoiding phishing and quishing scams

The world is in a constant state of communication. Between emails, texts and phone calls we receive a countless number of messages each day. Most of these are legitimate, but others are cleverly disguised to trick people into giving up their personal or financial information. Here's how to spot and avoid quishing and phishing scams.

Phishing for information

Phishing is where criminals send emails to "fish" for sensitive information like passwords, bank account numbers or debit card details. These messages often mimic legitimate companies or people you know or work with to create a sense of urgency. The context of the email may claim you need to update payment information. It may say you need to confirm personal or financial information. The email may include an invoice you don't recognize with a link for a non-traditional way to pay. It might also contain malicious links or attachments that lead to fake websites. At first glance, these emails look real, but odds are they're not.

Here are some common signs an email could be a scam:

- Unusual email address
- Unexpected messages requesting money, log-in credentials or sensitive information
- Suspicious links
- Generic references or greetings
- Misspelled words or messages with poor grammar

The hidden threat of quishing

Quick response codes, more commonly known as QR codes, are 2-D black and white matrix codes that store data which can be scanned with a camera or code reader application. They're widely used to store data such as URLs, product details or contact information. However, they can also be used by malicious actors to trick people into giving them their personal and financial information.

Quishing or QR phishing is the use of a QR code to redirect a user to a malicious site or link to gain access to the user's device or personal information. Tactics may include overlaying legitimate QR codes with malicious ones to trick users or relying on traditional phishing tactics such as a too-good-to-be-true deal with murky or falsified details.

Once the user clicks on the malicious link, they may be prompted to download malware or other harmful software. This can compromise the device and expose sensitive data such as banking credentials, browser history or other mobile activity.

Protecting yourself from quishing and phishing scams

Whether through a QR code, an email or a text message, bad actors use a variety of communication methods to trick people into sharing their personal or financial information.

Here are some tips to protect yourself:

- Look out for typos and poor grammar
- Watch out for a false sense of urgency
- Avoid unusual requests or payment methods
- Don't click suspicious links
- Inspect QR codes before scanning to check for tampering or overlays

What are the fraud risks for ACH?

Fraud challenges all participants in the ACH Network. Originators must remain vigilant to prevent and defend against fraud risk. There are certain common fraud schemes which you should be aware of. In one fraud scheme, fraudsters hack into an Originator's computer system using compromised user IDs and passwords and originate ACH credits to mule accounts created for the express purpose of committing fraud. Those accounts are then emptied and abandoned. The true Originator's account, your account, is debited for the invalid origination file. The credits are usually irretrievable by the time the fraud is discovered. The originator's credentials may have been compromised by an insider within the organization or stolen through key loggers or Trojan Horse programs on the compromised computer.

Due to the risk this type of fraud presents, it's essential that all computer equipment your company uses to operate treasury management and ACH Origination applications is regularly updated and patched for security vulnerabilities, including use of and updates to firewall, virus protection, anti-malware protection and anti-spam protection.

What is website spoofing?

Website spoofing is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoofed websites are typically made to look exactly like a legitimate website published by a trusted organization.

To prevent fraud related to website spoofing:

- Pay attention to the web address of websites. A website may look legitimate, but the URL may have a variation in spelling or use a slightly different domain name.
- If you're suspicious of a website, close it and contact the company directly.
- Don't click links on social networking sites, pop-up windows or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.
- Only give sensitive information to websites using a secure connection. Verify the web address begins with https:// rather than just http://.
- Avoid using websites for which your browser displays certificate errors or warnings.

Federal Reserve FraudClassifier model

The Federal Reserve worked with the payments industry to create the FraudClassifier™ model to help organizations classify fraud consistently. Nacha participated in the development of the FraudClassifier model and encourages the model's use. The model supports a common fraud language across payment types and fraud methods that can help all parties work together to identify and fight fraud. Applying the model across organizations and the industry ensures greater consistency in fraud classification, more robust information and better fraud tracking.

For additional information on the FraudClassifer model, visit the Federal Reserve's **website**.

Common credit-push ACH fraud schemes

It's critical for Originators to understand the nature of evolving fraud schemes and adopt appropriate risk control measures to combat them. According to Nacha, the most common ACH fraud schemes are business email compromise, vendor impersonation fraud, payroll impersonation fraud and account takeover fraud.

Business email compromise schemes

Business email compromise schemes occur when the legitimate email account of a business officer is either compromised or impersonated and used to order or request the transfer of funds. The employee transfers funds to

the fraudster believing the order was from a reputable company email address owned by an officer with authority to make those orders. Business email compromise is classified as relationship and trust fraud by the Federal Reserve's FraudClassifier model because an authorized party was manipulated into initiating a payment.

Vendor impersonation fraud

Vendor impersonation fraud occurs when a business, public sector agency or organization receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The fraudster is paid by the business, agency or organization when the real contractor submits an invoice for work done or goods sold. Public sector organizations are frequently targeted because contract information is often in the public record. Vendor impersonation fraud is classified as relationship and trust fraud by the Federal Reserve's FraudClassifier model because an authorized party was manipulated into initiating a payment.

Payroll impersonation fraud

Payroll impersonation fraud targets employees and human resources departments. A fraudster will impersonate an employee and contact the HR department directly or through the employer's payroll portal using stolen credentials. The fraudster requests to change the account where the employee's regular payroll is deposited. Once updated, the employer pays the fraudster rather than the employee. Payroll impersonation fraud is classified as compromised credentials or impersonated authorized party depending on whether the fraudster uses stolen credentials to access the employer's HR portal or impersonates the employee when contacting the employer's HR department.

Account takeover fraud

Account takeover fraud occurs when a fraudster obtains the credentials of a consumer or a business bank account and pushes credits to their own accounts. The fraudster is active in the victim's online bank account, knows the account balances and can quickly deplete entire accounts. Account takeover fraud is classified as compromised credentials because an unauthorized party initiates payment using stolen credentials.

For additional information on cyber fraud, visit **Nacha's website**.