2024 Revisions to the Nacha Operating Rules

This Revisions section includes a technical summary of changes to the Rules that were implemented in 2023. The text changes were officially communicated via Supplements, but they are summarized here for reference. Please note that since these changes are already effective, they are not marked within the text of the Rules.

Technical Summary of 2023 Changes to the Rules

The following is a technical summary of changes to the Nacha Operating Rules implemented during 2023. The text changes were officially communicated via Supplements to the Rules, but they are summarized here for reference. Please note that since these changes are already effective, they are not marked within the text of the 2024 Rules.

MARCH 17, 2023 EFFECTIVE DATE

Micro-Entries, Phase 2

Approved January 31, 2022

The first phase of the Micro-Entry Rule defined "Micro-Entries" as a term and type of payment within the Rules. Since its implementation, Originators of Micro-Entries are required to use "ACCTVERIFY" as a standard Company Entry Description and populate the Company Entry Name field with the same or similar name to be used in future entries. Originators using debit entry offsets must send the debit and corresponding credit Micro-Entries simultaneously for settlement at the same time. The rule also requires that the total amount of the credit Micro-Entry(ies) must be equal or greater than the value of the debit Micro-Entry(ies) and that the aggregate total of debits and credits cannot result in a net debit to the Receiver. The use of Micro-Entries requires the Receiver to complete a verification process with the Originator prior to the transmission of future entries. Phase 1 became effective on September 16, 2022.

Phase 2 of the Micro-Entries rule built upon its initial implementation by requiring Originators of Micro-Entries to use commercially reasonable fraud detection practices, including the monitoring of forward and return Micro-Entry volumes.

• Article Two, Subsection 2.7.5 (Commercially Reasonable Fraud Detection for Micro-Entries) – New subsection to require Originators to conduct commercially reasonable fraud detection when using Micro-Entries.

ACH Operations Bulletin #1-2024

Changes to Upcoming Rules Effective Dates

July 1, 2024

Summary

The effective date of the recently adopted rules language requiring an RDFI to notify the ODFI of the status of a request for return within 10 banking days has been extended by 6 months to April 1, 2025.

In addition, two upcoming rules have effective dates of Friday, June 19, 2026. As this is a federal holiday, the practical effective date for these two rules will be the next banking day – Monday, June 22, 2026.

Discussion

Expanding the ODFI Request for Return

On March 15, 2024, Nacha members approved[1] a rule that expands the reasons for which an ODFI may request the return of an entry and establishes a new requirement for the RDFI to respond to the ODFI when it receives such a request. Specifically, upon implementation, an ODFI will be permitted to request the return of an entry for any reason, and the RDFI will have an obligation to advise the ODFI of its decision or the status of the request within ten (10) banking days of receipt of the ODFI's request. These changes were approved with an effective date of October 1, 2024.

Nacha has received a number of comments about the ability of RDFIs to be able to comply with the new requirement by the October 1 effective date. Nacha's Rules and Operations Committee recommended extending the effective date for the specific portion of the new rule that requires RDFIs to respond to the ODFI, and the Nacha Board of Directors approved such an extension to April 1, 2025.

This extension applies only to new Rules Subsection 3.8.6, which is the portion of the rule requiring a response by RDFIs.

> ***SUBSECTION 3.8.6 Response to ODFI Request for Return (New Subsection – Effective April 1, 2025)***
> An RDFI may, but is not obligated to, comply with an ODFI's request for the return of an Entry, as provided under Subsection 2.13.2 (ODFI Request for Return). Regardless of whether the RDFI complies with the ODFI's request to return the Entry, the RDFI must

[1] See Supplement #1-2024 to the Nacha Operating Rules.

advise the ODFI of its decision or the status of the ODFI's request within ten (10) Banking days of receipt of the ODFI's request.

Changes enabling ODFIs to request the return of an entry for any reason recognize current industry use of the ODFI Request for Return process and will still become effective on October 1, 2024. RDFIs should recognize that they may receive such requests from ODFIs "for any reason" prior to the extended response deadline of April 1, 2025.

Nacha strongly encourages RDFIs to work toward compliance as soon as possible. In addition, a new feature will go live in the Risk Management Portal prior to the April 1, 2025, effective date that will enable an RDFI to provide such a notification to the ODFI through the portal.

June 19, 2026, Rules Effective Date

Two risk management rules were recently approved with Friday, June 19, 2026, as the effective date[2]:

- Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFI (Phase Two), and
- ACH credit monitoring by RDFIs (Phase Two).

As June 19 is a federal holiday, the practical effective date for these two rules will be the next banking day – Monday, June 22, 2026. All affected parties are encouraged to become compliant with these rules as soon as possible, but no later than June 22, 2026.

###

[2] See Supplement #1-2024 to the Nacha Operating Rules.

NOTICE OF AMENDMENTS TO THE 2024 NACHA OPERATING RULES & GUIDELINES

September 26, 2024

SUPPLEMENT #2-2024

1. Nacha Operating Guidelines: Updates to ACH Risk Management Requirements for Fraud Monitoring

Effective Dates: March 20, 2026
June 19, 2026

2. Nacha Operating Rules: Network Administration Fees

Effective Date: January 1, 2025

Supplement #2-2024 to the Nacha Operating Rules & Guidelines

On March 15, 2024, the Nacha Voting Membership approved a set of nine specific changes comprising the ACH Risk Management Topics amendments (as previously issued via Supplement #1-2024 on April 12, 2024). Together, these nine changes are intended to strengthen the ability of the ACH Network to detect and reduce the incidence of successful fraud attempts and improve the recovery of funds if fraud has occurred. These various changes become effective beginning on October 1, 2024, through June 19, 2026.

The material within the Guidelines portion of this supplement focuses primarily on the new requirements for ACH participants (Originators, ODFIs, Third-Party Service Providers, Third-Party Senders, and RDFIs) to establish and implement risk-based processes and procedures that are reasonably intended to identify entries suspected of being unauthorized or authorized under False Pretenses. The guidance and sound business practices included within this document are provided to assist ACH participants in establishing their own practices and procedures to comply with the new fraud monitoring rules.

This supplement includes excerpts from the 2024 Nacha Operating Guidelines that have been updated to reflect key aspects of the new fraud monitoring rules. In some cases, where broader revisions were necessary, new chapters have been added to the Guidelines. Users should note that this supplement is not intended provide replacement text for every change corresponding to the new risk rules set. The 2025 edition of the Nacha Operating Guidelines will incorporate additional updates, where appropriate, to reflect more minor clarifications related to the risk amendments as well as the most recent set of Minor Topics rule changes.

For a detailed description of all Rules changes resulting from the ACH Risk Management Topics amendments, please refer to Supplement #1-2024 to the Nacha Operating Rules.

Supplement #2-2024 also contains the 2025 ACH Network Administration Fees as approved by the Nacha Board of Directors. The new fee schedule is effective January 1, 2025.

To ensure compliance with the most current rules, this Supplement #2-2024 should be used in conjunction with the 2024 edition of the Nacha Operating Rules & Guidelines.

Nacha Operating Guidelines

A new discussion on "Fraud Monitoring" will be added to Chapter 7 (ODFI Risk Management) following the section entitled "Know Your Customer."

CHAPTER 7

ODFI Risk Management

FRAUD MONITORING

Beginning in 2026, the Nacha Operating Rules will require each ODFI, each non-consumer Originator, each Third-Party Sender, and each Third-Party Service Provider that performs functions of ACH processing on behalf of an ODFI, Originator, or another Third-Party Sender to establish and implement risk-based processes and procedures, relevant to the role each party plays in the authorization or transmission of entries, that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses. At least annually, the parties subject to this requirement must review their processes and procedures and must make appropriate updates to address evolving risks.

These new requirements will be implemented in two phases:

1. No later than March 20, 2026, all ODFIs, and any non-consumer Originators, Third-Party Senders, and Third-Party Service Providers whose annual ACH origination or transmission volume exceeded 6 million entries in calendar year 2023 must be compliant with the requirements for fraud monitoring; and

2. No later than June 19, 2026, all other non-consumer Originators, Third-Party Senders, and Third-Party Service Providers, regardless of origination or transmission volume, must be compliant with the requirements for fraud monitoring.

False Pretenses, Unauthorized Entries, and Other Disputes

The term "False Pretenses" refers to the inducement of a payment by a person misrepresenting (a) that person's identity, (b) that Person's association with or authority to act on behalf of another person, or (c) the ownership of an account to be credited. For example, False Pretenses covers the following fraud scenarios, which are described in detail in Chapter 15 (Originator Risk Management):

- Business Email Compromise (BEC).

- Vendor impersonation.

- Payroll impersonation.

- Other payee impersonations.

"False Pretenses" does not cover scams involving fake, non-existent, or poor-quality goods or services. A payment made to the right person but induced on a fraudulent basis is not considered to have been made under False Pretenses. The term "False Pretenses" complements language on "unauthorized credits" (i.e., account takeover scenario), but entries made under False Pretenses are not "unauthorized."

Examples of credit entries authorized by the Originator under False Pretenses:

- The Receiver of the credit Entry misrepresents the Receiver's identity or ownership of the receiving account.
- A fraudster impersonates someone with the authority to order payment (e.g., a CEO/CFO via business email compromise) to induce someone with authority to originate a payment from the credit account to make a payment.
- A fraudster claims to be a vendor with whom the account holder has a relationship and requests payment to fraudster's account.
- A fraudster claims to be a real estate settlement agent or attorney and requests funds transferred to fraudster's account.
- A fraudster claims to be an employee of an organization and requests payment to fraudster's account; or, fraudster gains access to the employee-facing component of an organization's payroll system and redirects payroll payments to fraudster's account.
- A fraudster claims to be a governmental agency (e.g., IRS) claiming a person is delinquent in a payment (e.g., taxes) with consequences if not paid.
- A fraudster claims to be the account holding ODFI and tells the Originator that his/her account has been cmpromised and to avoid losses they need to move their funds to another account that has been opened for them.

An unauthorized credit entry is an entry for which the account holder (Originator) did not authorize the credit entry. An unauthorized credit entry is different from an entry authorized under False Pretenses.

Example of unauthorized credit entry:

- Account takeover - Fraudster gains access to the credentials necessary to initiate a transaction and initiates a credit entry from the accessed account.

Some disputes do not involve either unauthorized credit entries or credit entries authorized under False Pretenses and therefore do not qualify to be handled through the ACH Network but should be resolved directly between the merchant and customer.

Examples:

- A dispute regarding the quality or condition of, or warranties or timing of delivery for, goods or services (provided there are not other circumstances that would give rise to a claim of False Pretenses or unauthorized payment). For example, a business payment to a vendor, for which the quantity or quality of goods delivered is later disputed.
- Payment is made to the right person/organization but induced on a basis other than False Pretenses (e.g., a contribution to a charitable organization because it says they are going to spend the funds on something particular and then spends it on something else).

Risk-Based Fraud Monitoring

Risk-based processes and procedures do not require the screening of every ACH Entry individually. A risk-based approach to fraud monitoring enables financial institutions, ACH Originators, and other parties to apply resources and take extra measures to detect fraud in transactions in which the party has determined risks to be elevated and take only basic precautions where it has determined that risks are lower. However, a risk-based approach cannot be used to conclude that no monitoring is necessary at all.

Monitoring transactions prior to processing provides the greatest opportunity for detecting potential fraud. However, monitoring does not need to be performed prior to the processing of Entries. As an example, with respect to debits, a robust return rate monitoring program in conformance with existing Rules may be sufficient as a minimum standard to assist ODFIs and Originators in identifying instances where customers have provided account information that is invalid or does not belong to them, prompting Originators to adopt better methods of account validation for future entries. However, this type of monitoring is reactive, rather than proactive, and does not prevent the origination of fraudulent entries in the first place. The adoption of proactive measures prior to the origination of entries (including, but not limited to, ensuring that routing numbers are not used as account numbers, and not accepting or permitting the origination of entries for amounts in excess of an amount owed) can help stop the origination of some fraudulent debits.

For transactions in which monitoring identifies a high potential for fraud, the ODFI should consider actions based on the monitoring results. Actions may include, but are not limited to:

- stopping further processing of a flagged transaction.
- consulting with the Originator to determine the validity of the transaction.
- consulting with other internal monitoring teams or systems to determine if the transaction raises other flags.
- contacting the RDFI to determine if characteristics of the Receiver's account raise additional red flags or requesting the freeze or the return of funds.

Appropriate processes and procedures to identify unauthorized entries and entries authorized under False Pretenses will vary, depending on the role of the participant and the nature of the transaction. For example, Originators may be best placed to implement procedures to protect against account takeover or other vectors for initiating unauthorized transactions. Third-Party Senders and Third-Party Service Providers involved in origination of ACH Entries may have processes and procedures to review the volume, velocity, dollar amounts and SEC Codes of their originated ACH Entries.

An ODFI's processes and procedures may consider the processes and procedures implemented by other participants in the origination of ACH Entries, providing ODFIs with flexibility in implementing required fraud monitoring. The extent to which the ODFI chooses to take into account fraud monitoring established by the Originator (as permitted by the Nacha Operating Rules), and the ODFI's basis for relying on the Originator's fraud monitoring processes/procedures, should be clearly addressed within the origination agreement between ODFI and Originator. The processes and procedures implemented by RDFIs and other receiving side ACH participants do not affect the obligations of originating participants.

Express disclaimers of modification of Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, will allow Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

The following new chapter will be added to Section II - Originating Depository Financial Institutions to address Originator obligations for risk management and fraud monitoring.

CHAPTER 15

Originator Risk Management

FRAUD MONITORING

Beginning in 2026, the Nacha Operating Rules will require each ODFI, each non-consumer Originator, each Third-Party Sender, and each Third-Party Service Provider that performs functions of ACH processing on behalf of an ODFI, Originator, or another Third-Party Sender to establish and implement risk-based processes and procedures, relevant to the role each party plays in the authorization or transmission of entries, that are reasonably intended to identify entries that are suspected of being unauthorized or authorized under False Pretenses. At least annually, the parties subject to this requirement must review their processes and procedures and must make appropriate updates to address evolving risks.

These new requirements will be implemented in two phases:

1. No later than March 20, 2026, all ODFIs, and any non-consumer Originators, Third-Party Senders, and Third-Party Service Providers whose annual ACH origination or transmission volume exceeded 6 million entries in calendar year 2023 must be compliant with the requirements for fraud monitoring; and

2. No later than June 19, 2026, all other non-consumer Originators, Third-Party Senders, and Third-Party Service Providers, regardless of origination or transmission volume, must be compliant with the requirements for fraud monitoring.

False Pretenses, Unauthorized Credit Entries, and Other Disputes

The term "False Pretenses" refers to the inducement of a payment by a person misrepresenting (a) that person's identity, (b) that person's association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited. For example, False Pretenses covers many of the following fraud scenarios, which are described in more detail under the "Understanding Fraud Threats" section of this chapter:

- Business Email Compromise (BEC).
- Vendor impersonation.
- Payroll impersonation.
- Other payee impersonations.

"False Pretenses" does not cover scams involving fake, non-existent, or poor-quality goods or services. A payment made to the right person but induced on a fraudulent basis is not considered to have been made under False Pretenses. The term "False Pretenses" complements language on "unauthorized credits" (i.e., account takeover scenario), but entries made under False Pretenses are not "unauthorized."

Examples of credit entries authorized by the Originator under False Pretenses:

- Receiver of the credit Entry misrepresents the Receiver's identity or ownership of the receiving account.

- Fraudster impersonates someone with the authority to order payment (e.g., a CEO/CFO via business email compromise) to induce someone with authority to originate a payment from the credit account to make a payment.

- Fraudster claims to be a vendor with whom the accountholder has a relationship and requests payment to fraudster's account.

- Fraudster claims to be a real estate settlement agent or attorney and requests funds transferred to fraudster's account.

- Fraudster claims to be an employee of an organization and requests payment to fraudster's account; or, fraudster gains access to the employee-facing component of an organization's payroll system and redirects payroll payments to fraudster's account.

- Fraudster claims to be a governmental agency (e.g., IRS) claiming a Person is delinquent in a payment (e.g., taxes) with consequences if not paid.

- Fraudster claims to be the account holding ODFI and tells the Originator that his/her account has been compromised and to avoid losses they need to move their funds to another account that has been opened for them.

An unauthorized credit entry is an entry for which the account holder (Originator) did not authorize the credit entry. An unauthorized credit entry is different from an entry authorized under False Pretenses.

Example of an unauthorized credit entry:

- Account takeover - Fraudster gains access to the credentials necessary to initiate a transaction and initiates a credit entry from the accessed account.

Some disputes do not involve either unauthorized credit entries or credit entries authorized under False Pretenses and therefore do not qualify to be handled through the ACH Network but should be resolved directly between the merchant and customer.

Examples of other disputes:

- A dispute regarding the quality or condition of, or warranties or timing of delivery for, goods or services (provided there are not other circumstances that would give rise to a claim of False Pretenses or unauthorized payment). For example, a business payment to a vendor, for which the quantity or quality of goods delivered is later disputed.

- Payment is made to the right person/organization but induced on a basis other than False Pretenses (e.g., a contribution to a charitable organization because it says they are going to spend the funds on something particular and then spends it on something else).

Risk-Based Fraud Monitoring

Risk-based processes and procedures do not require the screening of every ACH Entry individually. A risk-based approach to fraud monitoring enables ACH Originators, financial institutions, and other parties to apply resources and take extra measures to detect fraud in transactions in which the party has determined risks to be elevated, take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk. However, a risk-based approach cannot be used to conclude that no monitoring is necessary at all.

Monitoring transactions prior to processing provides Originators with the greatest opportunity for detecting potential fraud. However, monitoring does not need to be performed prior to the processing of Entries. As an example, with respect to debits, a robust return rate monitoring program in conformance with existing Rules may be sufficient as a minimum standard to assist Originators and their ODFIs in identifying instances where customers have provided

account information that is invalid or does not belong to them, prompting Originators to adopt better methods of account validation for future entries. However, this type of monitoring is reactive, rather than proactive, and does not prevent the origination of fraudulent entries in the first place.

For transactions in which monitoring identifies a high potential for fraud, the Originator should consider some action based on the monitoring results. Actions may include, but are not limited to:

- stopping further processing of a flagged transaction;
- consulting with the Receiver, using previously verified communication methods, to determine the validity of the transaction;
- consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and
- using the results of account validation methods completed prior to ACH origination to determine if characteristics of the Receiver's account raise additional red flags.

Appropriate processes and procedures to identify unauthorized Entries and Entries authorized under False Pretenses will vary, depending on the role of the participant and the nature of the transaction. For example, Originators may be best placed to implement procedures to protect against account takeover or other vectors for initiating unauthorized transactions. Third-Party Senders and Third-Party Service Providers involved in origination of ACH Entries may have processes and procedures to review the volume, velocity, dollar amounts and SEC Codes of their originated ACH Entries.

The requirement to establish processes intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses should not be interpreted to impose an obligation on originating ACH participants to prevent wrongful activity. Express disclaimers of modification of Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, allows Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

Issues to Consider:

- Because fraud monitoring applies to all types of ACH payments and Standard Entry Class Codes, Originators may find it appropriate to conduct a risk assessment as a first step, taking into account the nature, types, and scope of the risks those payments present.
- As a starting point to develop risk monitoring practices and procedures, Originators can consider a review of their current practices and procedures to identify risk and fraud controls they may already have in place and to formalize those practices and procedures, as needed.
- Originators are encouraged to consider whether existing monitoring could be expanded to adopt or improve:
  - the identification of anomalies in the volume and value of ACH payments originated, including the frequency and velocity of payments to the same account number or the same Receiver name on accounts.
  - return data monitoring and analysis to identify anomalies in origination.
  - account validation prior to first use of an account number for any ACH payment, regardless of SEC Code and whether the Entry is a credit or debit.
- When originating debit entries, Originators need to be aware of the potential for abuse of or fraud schemes involving payments authorized in excess of the amount owed to the Originator by the Receiver. Originators are encouraged to implement processes and procedures to limit or prohibit the acceptance/authorization of overpayments.

UNDERSTANDING FRAUD THREATS

As fraud schemes continue to grow, evolve, and target legitimate businesses, non-profits, governments, and other public sector organizations, it is critical that Originators understand the nature of those fraud schemes and adopt appropriate risk control measures to combat them.

Following are key terms commonly used in the discussion of various fraud schemes:

- **Malware**: Malicious software including viruses, ransomware, and spyware, typically consisting of code designed to cause extensive damage to data and systems or to gain unauthorized access.
- **Money Mule**: Someone who transfers or moves illegally acquired money on behalf of a fraudster. Fraudsters recruit money mules to help launder proceeds derived from many of the fraud schemes discussed below.
- **Social Engineering**: The use of deception to manipulate individuals into providing confidential or personal information.
- **Spear-phishing**: Sending emails supposedly from a known or trusted sender to induce the recipient to reveal confidential information.
- **Spoofing**: Disguising an email from an unknown source as being from a known, trusted source.

The following discussion summarizes six of the most common types of cyberfraud schemes and includes suggested internal controls that Originators can adopt to help protect themselves against these schemes.

Business Email Compromise

With Business Email Compromise, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business' officers and monitor his or her account for patterns, contacts and information. Using information gained from social media or "out of office" messages, the fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions. The fraudster monitors the officer's accounts for patterns, contacts and information. After identifying the target, ploys are conducted such as spear-phishing, social engineering, identity theft, email spoofing, and the use of malware to either gain access to or convincingly impersonate the email account. The fraudster uses the compromised or impersonated account to send payment instructions. Payment instructions direct the funds to an account controlled by the fraudster or a money mule. (Refer to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/Home/BEC for more information on Business Email Compromise.)

Internal Controls

- Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume it's a cybersecurity problem.
- Educate and 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.
- Review accounts frequently.
- Initiate payments using dual controls.
- Never provide password, username, authentication credentials, or account information when contacted.

- Do not provide or post nonpublic business information on social media.
- Avoid free web-based email accounts for business purposes. A company domain should always be used in business emails.
- To make impersonation harder, consider registering domains that closely resemble the company's actual domain.
- Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book

Vendor Impersonation Fraud

Vendor Impersonation Fraud can occur when a business, public sector agency, or organization (example: a municipal government agency, a school district, etc.) receives an unsolicited request, purportedly from a legitimate vendor or contractor, to update or change payment information or change payment method. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payment along with routing and account information. This type of request could come from fraudsters and not the vendor or contractor. Although any business entity could be the target of this type of social engineering attack, public sector entities may be specifically targeted because their contracting information is often a matter of public record.

Internal Controls

- Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume this is a cybersecurity issue.
- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, pressure to act quickly, and any change of payment method (e.g., ACH to wire).
- Verbally authenticate any payment changes via a telephone call to a previously known number.
- Review accounts frequently.
- Initiate payments using dual controls.
- Do not provide or post non-public business information on social media.
- Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book.
- Make vendor payment forms available only via secure means or to known entities.
- Require changes to payment account information be made or confirmed only by site administrators and use methods like the transmission of verification codes to existing contacts.
- Do not ignore calls from a financial institution questioning the legitimacy of a payment.

Payroll Impersonation Fraud

Payroll Impersonation Fraud occurs when a fraudster targets an employee by sending a phishing email that impersonates the employee's human resources or payroll department and/or the company's payroll platform. The email directs the employee to log in to confirm or update payroll information, including bank account information. The employee clicks the link or opens the attachment within the email and confirms or updates the payroll information. The fraudster then uses the stolen login credentials to change payment information to an account controlled by the fraudster or a money mule.

Internal Controls

- Alert employees to watch for phishing attacks and suspicious malware links.
- Direct employees to check the actual sender email address, rather than just looking at the subject line, to verify that the email came from their employer or payroll service provider.
- Educate employees not to reply or respond to any suspicious email; instead, have them forward the email to a company security contact.
- Instruct employees to not enter their login credentials when clicking on a link or opening an attachment in an email.
- Employer self-service platforms should authenticate requests to change payment information using the employee's previously known contact information. For example, require users to enter a second password that is emailed to an existing email address, or to use a hard token code.
- Employer self-service platforms should re-authenticate users accessing the system from unrecognized devices, using the employee's previously known contact information.
- Set up alerts on self-service platforms for administrators so that unusual activity may be caught before money is lost. Alerts may include when banking information is changed, and multiple changes that use the same new routing number or identical account numbers.
- Consider validating employees' new Direct Deposit information by using ACH prenotification entries, Micro-Entries, or other account validation service.

GENERAL CONTROLS FOR PAYMENT ORIGINATION

An Originator's adoption of proactive measures, such as those listed below, that are employed prior to the initiation of entries can help Originators minimize the potential for transmitting erroneous, unauthorized, or potentially fraudulent entries:

1. Authenticate the requester.
2. Confirm the validity of the authorization.
3. Verify the account number of the Receiver.
4. Verify the routing number of the Receiver.
5. Confirm the effective date of the transaction.
6. Confirm any payment-related information.
7. Confirm there are sufficient funds in funding account.
8. Obtain required internal approval for the transaction.
9. Initiate the transaction.
10. Require a second person to confirm and release the transaction.

The last two steps are particularly important and constitute a traditional fraud mitigation activity called "dual control." Originally designed to thwart internal fraud, dual control has a renewed relevance in an age of identity theft, imposter fraud, and business email compromise.

When any of these steps goes wrong, the error decreases the efficiency of the payment process and it can cause a transaction to be misrouted, possibly without opportunity for recovery. Steps such as these can be adopted by Originators to improve the quality of transactions it originates. This list provides Originators with a starting point for use in developing and customizing their own internal controls to help to mitigate error and fraud. Consistent application of the resulting controls to all payments can help Originators ensure each transaction complies with rules, is free of errors, and reaches the intended recipient.

In the specific context of payroll fraud, the adoption of similar steps can help mitigate the risk of fraud schemes that attempt to redirect payroll transactions to accounts controlled by fraudsters. The first two steps in the checklist below are critically important since a great deal of payroll fraud is predicated on a change of account information to redirect a payment. For this reason, Originators should consider treating any request to change account information as an attempt to commit fraud. Authenticating a requester and confirming a request through a separate channel, using known contact information, can greatly reduce the likelihood of successful fraud.

1. Authenticate the requester when adding or updating a Receiver (i.e., a payee).
2. Confirm any change request through a separate channel, using known contact information.
3. Verify the account number of the Receiver prior to the first payment.
4. Verify the routing number of the Receiver prior to the first payment.
5. Confirm the effective date of the transaction.
6. Confirm any payment-related information.
7. Confirm there are sufficient funds in the payroll funding account.
8. Obtain required internal approval for the transaction.
9. Initiate the transaction.
10. Require a second person to confirm and release the transaction.

ACH DATA SECURITY

The Nacha Operating Rules require ACH participants, including ODFIs and non-consumer Originators, to protect the security and integrity of certain ACH data throughout its lifecycle. All non-consumer Originators, Participating DFIs, Third-Party Service Providers, and Third-Party Senders must establish, implement and, as appropriate, update security policies, procedures, and systems related to the initiation, processing and storage of entries and resulting Protected Information.

The Rules also impose specific data security requirements for all ACH transactions that involve the exchange or transmission of banking information (which includes, but is not limited to, an entry, entry data, a routing number, an account number, and a PIN or other identification symbol) via an Unsecured Electronic Network. Originators must abide by these requirements.

ACH data security requirements are discussed in detail in Chapter 4 of these Guidelines.

A new section on "Third-Party Sender Risk Management" will be added to Chapter 21 (Relationship with Originators and ODFIs) following the section entitled "Know Your Customer."

CHAPTER 21

Relationship with Originators and ODFIs

THIRD-PARTY SENDER RISK MANAGEMENT

Beginning in 2026, the Nacha Operating Rules will require each ODFI, each non-consumer Originator, each Third-Party Sender, and each Third-Party Service Provider that performs functions of ACH processing on behalf of an ODFI, Originator, or another Third-Party Sender to establish and implement risk-based processes and procedures, relevant to the role each party plays in the authorization or transmission of entries, that are reasonably intended to identify entries that are suspected of being unauthorized or authorized under False Pretenses. At least annually, the parties subject to this requirement must review their processes and procedures and must make appropriate updates to address evolving risks.

These new requirements will be implemented in two phases:

1. No later than March 20, 2026, all ODFIs, and any non-consumer Originators, Third-Party Senders, and Third-Party Service Providers whose annual ACH origination or transmission volume exceeded 6 million entries in calendar year 2023 must be compliant with the requirements for fraud monitoring; and

2. No later than June 19, 2026, all other non-consumer Originators, Third-Party Senders, and Third-Party Service Providers, regardless of origination or transmission volume, must be compliant with the requirements for fraud monitoring.

Please see Chapter 50 of these Guidelines for more information on Risk Management requirements for Third-Party Service Providers.

The following new chapter will be added to Section III - Receiving Depository Financial Institutions to address RDFI obligations for risk management and fraud monitoring.

CHAPTER 23

RDFI Risk Management

FRAUD MONITORING

Beginning in 2026, the Nacha Operating Rules will require each RDFI to establish and implement risk-based processes and procedures, relevant to the role it plays in connection with the receipt of credit entries, that are reasonably intended to (1) identify credit entries suspected of being unauthorized or authorized under false pretenses, and (2) address the handling of such credit entries identified as potentially unauthorized or authorized under false pretenses. Each RDFI must review such processes and procedures at least annually and make appropriate updates to address evolving risks.

These new requirements will be implemented in two phases:

1. No later than March 20, 2026, all RDFIs whose annual ACH receipt volume exceeded 10 million entries in calendar year 2023 must be compliant with the requirements for credit fraud monitoring; and

2. No later than June 19, 2026, all RDFIs, regardless of annual ACH receipt volume, must be compliant with the requirements for credit fraud monitoring.

False Pretenses, Unauthorized credit Entries, and Other Disputes

The term "False Pretenses" refers to the inducement of a payment by a person misrepresenting (a) that person's identity, (b) that person's association with or authority to act on behalf of another person, or (c) the ownership of an account to be credited. Examples of False Pretenses include the following fraud scenarios, which are described in detail in Chapter 15 (Originator Risk Management):

- Business Email Compromise (BEC).

- Vendor impersonation.

- Payroll impersonation.

- Other payee impersonations.

"False Pretenses" does not cover scams involving fake, non-existent, or poor-quality goods or services. A payment made to the right person but induced on a fraudulent basis is not considered to have been made under False Pretenses. The term "False Pretenses" complements language on "unauthorized credits" (i.e., account takeover scenario), but entries made under False Pretenses are not "unauthorized."

Examples of credit entries authorized by the Originator under False Pretenses:

- Receiver of the credit Entry misrepresents the Receiver's identity or ownership of the receiving account.

- Fraudster impersonates someone with the authority to order payment (e.g., a CEO/CFO via business email compromise) to induce someone with authority to originate a payment from the credit account to make a payment.

- Fraudster claims to be a vendor with whom the account holder has a relationship and requests payment to fraudster's account.

- Fraudster claims to be a real estate settlement agent or attorney and requests funds transferred to fraudster's account.

- Fraudster claims to be an employee of an organization and requests payment to fraudster's account; or, fraudster gains access to the employee-facing component of an organization's payroll system and redirects payroll payments to fraudster's account.

- Fraudster claims to be a governmental agency (e.g., IRS) claiming a person is delinquent in a payment (e.g., taxes) with consequences if not paid.

- Fraudster claims to be the account holding ODFI and tells the Originator that his/her account has been compromised and to avoid losses they need to move their funds to another account that has been opened for them.

An unauthorized credit entry is an entry for which the account holder (Originator) did not authorize the credit entry. An unauthorized credit entry is different from an entry authorized under False Pretenses.

Example of unauthorized credit entry:

- Account takeover - Fraudster gains access to the credentials necessary to initiate a transaction and initiates a credit entry from the accessed account.

Some disputes do not involve either unauthorized credit entries or credit entries authorized under False Pretenses and therefore do not qualify to be handled through the ACH Network but should be resolved directly between the merchant and customer.

Examples of other disputes:

- A dispute regarding the quality or condition of, or warranties or timing of delivery for, goods or services (provided there are not other circumstances that would give rise to a claim of False Pretenses or unauthorized payment). For example, a business payment to a vendor, for which the quantity or quality of goods delivered is later disputed.

- Payment is made to the right person/organization but induced on a basis other than False Pretenses (e.g., a contribution to a charitable organization because it says they are going to spend the funds on something particular and then spends it on something else).

Risk-Based Fraud Monitoring

Risk-based processes and procedures do not require the screening of every ACH credit entry individually. A risk-based approach to fraud monitoring enables an RDFI to apply resources and take extra measures to detect fraud in transactions in which it has determined risks to be elevated and take only basic precautions where it has determined that risks are lower. However, a risk-based approach cannot be used to conclude that no monitoring is necessary at all. At a minimum, an RDFI applying a risk-based approach to fraud monitoring should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.

Although monitoring transactions prior to processing provides the greatest opportunity for detecting potential fraud, RDFIs are not required to perform such monitoring prior to the processing of Entries. To the extent that an RDFI's processes and procedures incorporate pre-posting monitoring of credits, an RDFI may delay funds availability for the Entry, as permitted by the rules governing exemptions to the funds availability requirements, to investigate the appropriateness of the Entry.

RDFIs must review their credit fraud monitoring processes and procedures at least annually and make appropriate updates to address evolving risks. RDFIs may determine that more frequent review is appropriate, based on their specific circumstances.

The requirement for an RDFI to establish processes reasonably intended to identify entries suspected of being unauthorized or authorized under False Pretenses does not impose any obligation on the RDFI to prevent wrongful activity or change the allocation of liability between parties. Express disclaimers of modification of Uniform Commercial Code (UCC) Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, will allow Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

When establishing processes and procedures reasonably intended to identify credit entries suspected of being unauthorized or authorized under False Pretenses, the RDFI should consider a number of issues. An RDFI will not likely know the circumstances under which a credit entry was originated. However, entries that are unauthorized or authorized under False Pretenses potentially may be identified based on characteristics of the entry and the receiving account, such as:

- a Standard Entry Class Code that does not align with the type of receiving account, such as a corporate CCD entry to a consumer account.

- a high-dollar transaction that is atypical for the receiving account.

- a series of similar credit entries received within a short period of time, such as multiple payroll or benefit payments.

  (Note: No later than March 20, 2026, Originators of payroll and other types of compensation payments will be required to include the description "PAYROLL" in the Company/Entry Description field. This standardized description can be used by RDFIs, at their discretion, to assist with various risk monitoring and mitigation efforts. For example, a standard identifier for payroll entries provides additional information to RDFIs that may choose to implement logic to provide or suppress early funds availability. The standardized description can also be used, at the discretion of the RDFI, to facilitate the identification of new or multiple payroll credits to a particular account.)

- any of the above to a new account, a dormant account, or to an account acting as a mule.

  In situations where an RDFI reasonably suspects that a credit entry is unlawful, involves the proceeds of unlawful activity, or is otherwise suspicious (which includes an entry the RDFI suspects to be unauthorized or authorized under False Pretenses), it may take advantage of the voluntary exemption from the funds availability requirements defined by the Nacha Operating Rules, thus providing more time to examine a particular transaction and receiving account. An RDFI that delays making funds available under this Nacha Operating Rule exemption must take reasonable steps to promptly notify the ODFI of the delay in funds availability. (RDFIs should note that this exemption applies only to the Nacha Operating Rule provisions on funds availability, allowing an RDFI to delay making funds available to the Receiver up to the Regulation CC funds availability deadline of 9:00 a.m. the day following the settlement date of the entry.)

The RDFI can utilize Nacha's Risk Management Portal and ACH Contact Registry for contact information for the ODFI to help in its determination. If the RDFI believes an entry to be unauthorized or authorized under False Pretenses, and it concludes that the best course of action is to return the funds, it may return the entry using Return Reason Code R17 "QUESTIONABLE" or, at the ODFI's request, using Return Reason Code R06.

ADDITIONAL FRAUD MONITORING GUIDANCE FOR RDFIS

The following additional guidance is provided to assist RDFIs in establishing reasonable practices and procedures to identify credit-push fraud and help with the potential recovery of funds for the victims of these schemes. RDFIs

are not required to adopt any of the practices listed below, and the manner in which RDFIs comply with the fraud monitoring rule should be guided by the RDFI's own risk assessment. Nevertheless, these are suggested as sound business practices that RDFIs can consider when developing their own risk-based approach to identify potentially unauthorized or fraudulent credit entries .

Monitoring Incoming Transactions

Anomaly detection and velocity checks come in many forms. These controls can identify suspicious activity but should not be used alone to determine the validity of an incoming credit transaction. Some financial institutions can build and monitor these controls, while others will use third-party solutions. Once a monitoring control is in place, additional research is often required to confirm whether a flagged item is likely fraud or should be posted as received.

- *Account Type and SEC Code*

  The correct SEC code is determined by the intended receiver of the item. Consumer SEC codes should be used in entries to consumer accounts, while business SEC codes should go to commercial accounts at the RDFI. A mismatch between a commercial SEC Code and a consumer account can indicate a fraudster attempting to receive illicit funds from a business email compromise, account takeover, or vendor impersonation scheme. While it can be more common for a commercial account to receive a consumer SEC code, a new or a large-dollar commercial SEC to a consumer account could receive additional scrutiny.

- *Behavioral Tolerances and Pattern Recognition*

  Financial institutions can set behavioral expectations and track previous transactions for their business and consumer account holders. Established relationships with recurring transactions and values are at a much lower risk for undetected fraud. Accounts receiving a higher volume of credit transactions than normal or with a dollar value not expected from the account history, especially from new originators with no previous relationship to the receiver, could receive increased scrutiny.

- *Name Matching*

  The Nacha Operating Rules do not require an RDFI to examine the name on any entry to determine whether it matches the name on the account to which the entry posts. The volume of transactions processed in a batch ACH environment makes name matching impractical. In addition, names with complex spellings, nicknames for the account holder, or customers using their middle names would all create instances of false positives at an unmanageable scale. However, comparison of the name on a transaction with the name on an account can be useful when an ACH payment has been flagged and escalated for review. Name comparison can be used selectively, in combination with other flags, in determining the validity of an item or group of items. Credit transactions with a gross mismatch between the name on the transaction and the name on the account, or accounts suddenly receiving multiple credits under multiple names, may indicate an account is being used to receive illicit funds in a credit push fraud scheme.

- *Dollar Tolerances*

  Each financial institution could set dollar tolerances for their controls commensurate with their risk appetite. An RDFI may be willing to perform fewer controls and accept the risk on incoming transactions with a value in the low hundreds of dollars but may apply additional controls to incoming credits with higher value. Restrictions on early funds availability might be appropriate for higher-dollar credits.

Communication

Communication is key to investigating flags identified by the financial institution's controls. Knowing how to quickly communicate with either the customer and/or peer financial institution helps the financial institution gain access to information about the transaction faster and make better decisions.

- Notify the account relationship owner at your financial institution. The relationship owner should assist in determining whether the customer is an unwitting mule, an active mule, or the victim of an account takeover

scheme. Account takeover schemes at the RDFI are used to receive illicit funds and transfer them to another account. If an account takeover scheme is determined, work with the customer to identify and remediate any weaknesses in security controls.

- Nacha's Risk Management Portal houses the ACH Contact Registry. This registry contains contact information for all financial institutions on the ACH Network. Make sure your financial institution's contact information is up-to-date and your employees know how to access the ACH Contact Registry or to contact a teammate who has access. Timing and communication are important when your financial institution identifies a suspicious transaction. Knowing who to contact at the other financial institution and contacting them quickly can help resolve the issue and prevent delays that benefit the fraudster.

Controls on Early Funds Availability

Early funds availability should be offered commensurate with an RDFI's risk appetite. In addition to the controls above, an RDFI should consider when to offer early funds availability to its customers and place controls on early funds to ensure this service is not abused by fraudsters.

- **Account Type** – Early funds availability is commonly offered only to consumers. Consider limiting early availability to consumer accounts only.

- **Seasoned Accounts** – New accounts may be more likely to be used by mules or fraudsters to gain access to funds from credit-push fraud schemes. Consider offering early funds availability only to seasoned accounts.

- **Limited Activity** – Fraudsters might know that accounts must be seasoned before early funds availability is offered. They may open an account and wait for 30, 60, 90 days or more prior to using the account to receive funds. Consider offering early funds availability only after an account history has been established or on the second or third receipt of a regular recurring transaction.

- **Types of Credits that are Accepted** –RDFIs may choose to limit the types of transactions that are eligible for early funds availability. Payroll and Social Security transactions are easily identified and are the largest transactions most consumers receive on a regular basis. Consider limiting early funds availability to specific transaction types and uses.

- **Dollar Tolerances** –RDFIs should consider limiting early funds availability to a specific dollar amount per entry (e.g., the first $500) or to a limit over a period of time, similar to ATM and remote deposit limits. This could reduce the risk from large-dollar or multiple transactions.

For additional guidance on fraud detection, prevention, and recovery, including the latest information on current fraud threats or concerns, refer to the Risk Management tab on Nacha's website at https://www.nacha.org/RiskFramework.

ACH DATA SECURITY

The Nacha Operating Rules require ACH participants, including RDFIs, to protect the security and integrity of certain ACH data throughout its lifecycle. All non-consumer Originators, Participating DFIs, Third-Party Service Providers, and Third-Party Senders must establish, implement and, as appropriate, update security policies, procedures, and systems related to the initiation, processing and storage of entries and resulting Protected Information.

The Rules also impose specific data security requirements for all ACH transactions that involve the exchange or transmission of banking information (which includes, but is not limited to, an entry, entry data, a routing number, an account number, and a PIN or other identification symbol) via an Unsecured Electronic Network.

ACH data security requirements are discussed in detail in Chapter 4 of these Guidelines.

New language on "Third-Party Service Provider/Third-Party Sender Risk Management" will be added to Chapter 50 (Third-Party Service Providers) following the section on the "Role of the Third-Party Service Provider."

CHAPTER 50

Third-Party Service Providers

THIRD-PARTY SERVICE PROVIDER/THIRD-PARTY SENDER RISK MANAGEMENT

Beginning in 2026, the Nacha Operating Rules will require each ODFI, each non-consumer Originator, each Third-Party Sender, and each Third-Party Service Provider that performs functions of ACH processing on behalf of an ODFI, Originator, or another Third-Party Sender to establish and implement risk-based processes and procedures, relevant to the role each party plays in the authorization or transmission of entries, that are reasonably intended to identify entries that are suspected of being unauthorized or authorized under False Pretenses. At least annually, the parties subject to this requirement must review their processes and procedures and must make appropriate updates to address evolving risks.

These new requirements will be implemented in two phases:

1. No later than March 20, 2026, all ODFIs, and any non-consumer Originators, Third-Party Senders, and Third-Party Service Providers whose annual ACH origination or transmission volume exceeded 6 million entries in calendar year 2023 must be compliant with the requirements for fraud monitoring; and

2. No later than June 19, 2026, all other non-consumer Originators, Third-Party Senders, and Third-Party Service Providers, regardless of origination or transmission volume, must be compliant with the requirements for fraud monitoring.

False Pretenses, Unauthorized credit Entries, and Other Disputes

The term "False Pretenses" refers to the inducement of a payment by a Person misrepresenting (a) that Person's identity, (b) that Person's association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited. Examples of False Pretenses include common fraud scenarios such as:

- Business Email Compromise (BEC);
- vendor impersonation;
- payroll impersonation; and
- other payee impersonations.

"False Pretenses" does not cover scams involving fake, non-existent, or poor-quality goods or services. A payment made to the right person but induced on a fraudulent basis is not considered to have been made under False Pretenses. The term "False Pretenses" complements language on "unauthorized credits" (i.e., account takeover scenario), but entries made under False Pretenses are not "unauthorized."

Examples of credit entries authorized by the Originator under False Pretenses:

- Receiver of the credit Entry misrepresents the Receiver's identity or ownership of the receiving account.

- Fraudster impersonates someone with the authority to order payment (e.g., a CEO/CFO via business email compromise) to induce someone with authority to originate a payment from the credit account to make a payment.

- Fraudster claims to be a vendor with whom the account holder has a relationship and requests payment to fraudster's account.

- Fraudster claims to be a real estate settlement agent or attorney and requests funds transferred to fraudster's account.

- Fraudster claims to be an employee of an organization and requests payment to fraudster's account; or, fraudster gains access to organization's payroll system and redirects payroll payments to fraudster's account.

- Fraudster claims to be a governmental agency (e.g., IRS) claiming a Person is delinquent in a payment (e.g., taxes) with consequences if not paid.

- Fraudster claims to be the account holding ODFI and tells the Originator that his/her account has been compromised and to avoid losses they need to move their funds to another account that has been opened for them.

An unauthorized credit entry is an entry for which the account holder (Originator) did not authorize the credit entry. An unauthorized credit entry is different from an entry authorized under False Pretenses.

Example of unauthorized credit entry:

- Account takeover - Fraudster gains access to the credentials necessary to initiate a transaction and initiates a credit entry from the accessed account.

Some disputes do not involve either unauthorized credit entries or credit entries authorized under False Pretenses and therefore do not qualify to be handled through the ACH Network but should be resolved directly between the merchant and customer.

Examples of other disputes:

- A dispute regarding the quality or condition of, or warranties or timing of delivery for, goods or services (provided there are not other circumstances that would give rise to a claim of False Pretenses or unauthorized payment). For example, a business payment to a vendor, for which the quantity or quality of goods delivered is later disputed.

- Payment is made to the right person/organization but induced on a basis other than False Pretenses (e.g., a contribution to a charitable organization because it says they are going to spend the funds on something particular and then spends it on something else).

Risk-Based Fraud Monitoring

Risk-based processes and procedures do not require the screening of every ACH Entry individually. A risk-based approach to fraud monitoring enables financial institutions, ACH Originators, and other parties to apply resources and take extra measures to detect fraud in transactions in which the party has determined risks to be elevated and take only basic precautions where it has determined that risks are lower. However, a risk-based approach cannot be used to conclude that no monitoring is necessary at all.

Monitoring transactions prior to processing provides the greatest opportunity for detecting potential fraud. However, monitoring does not need to be performed prior to the processing of Entries. As an example, with respect to debits, a robust return rate monitoring program in conformance with existing Rules may be sufficient as a minimum standard to assist ODFIs and Originators in identifying instances where customers have provided account information that is invalid or does not belong to them, prompting Originators to adopt better methods of account validation for future entries. However, this type of monitoring is reactive, rather than proactive, and does not prevent the origination of

fraudulent entries in the first place. The adoption of proactive measures prior to the origination of entries (including, but not limited to, ensuring that routing numbers are not used as account numbers, and not accepting or permitting the origination of entries for amounts in excess of an amount owed) can help stop the origination of some fraudulent debits.

For transactions in which monitoring identifies a high potential for fraud, Third Party Service Providers and Third-Party Senders should consider some action based on the monitoring results. Actions may include, but are not limited to:

- stopping further processing of a flagged transaction.
- consulting with the Originator to determine the validity of the transaction.
- consulting with other internal monitoring teams or systems to determine if the transaction raises other flags.

Appropriate processes and procedures to identify unauthorized Entries and Entries authorized under False Pretenses will vary, depending on the role of the participant and the nature of the transaction. For example, Originators may be best placed to implement procedures to protect against account takeover or other vectors for initiating unauthorized transactions. Third-Party Senders and Third-Party Service Providers involved in origination of ACH Entries may have processes and procedures to review the volume, velocity, dollar amounts and SEC Codes of their originated ACH Entries.

The requirement to establish processes intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses should not be interpreted to impose an obligation on originating ACH participants to prevent wrongful activity.

Express disclaimers of modification of Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, will allow Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

Nacha Operating Rules

Network Administration Fees

The Nacha Operating Rules require each Participating Depository Financial Institution that transmits or receives ACH entries (commercial and Federal Government) to pay an annual fee and a per-entry fee to cover costs associated with the administration of the ACH Network. These Network Administration Fees apply to all entries subject to the requirements of the Nacha Operating Rules, whether such entries are transmitted via an ACH Operator, sent directly from one Participating DFI to another, or sent through another entity. The Network Administration Fees have been established by the Nacha Board of Directors and are reviewed and modified, as appropriate, on an annual basis.

NETWORK ADMINISTRATION FEES AND DATA REPORTING REQUIREMENTS

The accompanying chart provides information on the amount of the annual and per-entry fees for the 2025 calendar year. The ACH Operators collect the annual fees and per-entry fees on behalf of Nacha for entries sent from one Participating DFI to another Participating DFI through the ACH Operators.

Financial institutions are required to report and Nacha collects directly the per-entry fees for ACH entries not sent through the ACH Operators, but that are sent as part of direct send or "on-we" arrangements. A direct send or "on-we" arrangement is one in which a Participating DFI sends a payment file that uses the Nacha formats and/or is covered by the Nacha Operating Rules, where that file is not processed by an ACH Operator, but instead is exchanged with another non-affiliated Participating DFI, either directly or through another entity. This definition applies regardless of how interbank settlement is accomplished.

Participating DFIs with direct send or "on-we" volume exceeding 5 million entries annually are obligated to file the requisite reporting with Nacha quarterly. Participating DFIs with direct send volume below this threshold are obligated to file with Nacha annually. These financial institutions are required to submit transaction volume data and any associated fees directly to Nacha using Form N-7 (2025). Any Participating DFI whose direct send or "on we" volume of entries originated or received exceeds 5 million for any quarter ending March 31, June 30, September 30, or December 31, 2025 must submit the above data and fees on a quarterly basis thereafter. The submission deadlines for quarterly filers are April 30, July 31, and October 31, 2025, and January 31, 2026. Participating DFIs that exceed the threshold during the calendar year must aggregate all prior quarters' fees in their current quarter's Form N-7 (2025) payment. Participating DFIs whose direct send volume is below this threshold must submit the above data and fees for calendar year 2025 by January 31, 2026.

Nacha
2025 Schedule of Fees

ACH Network Administration Fees

This Schedule of Fees has been established by the Nacha Board of Directors for calendar year 2025 in accordance with the requirements of the Nacha Operating Rules, Article One (General Rules), Section 1.13 (Network Administration Fees).

- Per-Entry Fee (January 1–December 31) . . . . . $ .000185
- Annual Fee . . . . . $ 366.00

NETWORK ADMINISTRATION FEES — FILING REQUIREMENTS FOR PARTICIPATING DEPOSITORY FINANCIAL INSTITUTIONS

Form N-7 (2025) is provided for the purposes of reporting and submitting payment of Network Administration Fees, as required by the Nacha Operating Rules, on ACH entries that are transmitted or received under a direct send or "on-we" arrangement. These reporting requirements are not applicable to Participating DFIs whose entries are processed exclusively through an ACH Operator, where all applicable transaction volume will be reported to and fees collected by the ACH Operators on behalf of Nacha.

Who Must File

Any Participating DFI that transmits or receives entries that use the Nacha formats and/or are covered by the Nacha Operating Rules, where those entries are not processed by an ACH Operator, but instead are exchanged with another non-affiliated Participating DFI, either directly or through another entity, during the 2025 calendar year.

Who Does Not Have to File

Any Participating DFI that transmits and receives 100% of its ACH entries during 2025 through an ACH Operator or with affiliated Participating DFIs does not need to file Form N-7 (2025). All applicable Network Administration Fees are billed and collected on Nacha's behalf by the ACH Operator, and appear on your customer statement as "Nacha Admin Network Fee/Entry" and "Nacha Admin Network Fee/Month."

When and Where to File

Any Participating DFI whose direct send or "on-we" volume of entries originated and received exceeds 5 million for any quarter ending March 31, June 30, September 30, or December 31, 2025 must file on a quarterly basis thereafter. The submission deadlines for quarterly filers are April 30, July 31, and October 31, 2025, and January 31, 2026. Participating DFIs that exceed this threshold during the calendar year must aggregate all prior quarters' fees in the current quarter's payment. Participating DFIs whose direct send or "on-we" volume is below the threshold must submit their calendar year 2025 data and fees by January 31, 2026.

Completed forms and payment must be received by Nacha no later than the above deadlines. Submit forms electronically to N7Form@nacha.org.

Payment via ACH credit is preferred. The ACH credit must be initiated by the organization filing Form N-7. UPIC Routing & Transit # 021052053, Acct # 59058945. Use CCD format for single filing. Complete in Batch Header (1) Company Name (2) Company Entry Description (specify Form N-7 (2025)).

If paying by check, please make the check payable to Nacha and mail to: Nacha, Attn: Finance Department, 11951 Freedom Drive, Suite 1001, Reston, VA 20190.

Form Instructions

Line 1. Enter legal name of Participating DFI.

Line 2. Enter mailing address of Participating DFI.

Line 3a. List the number of ACH entries transmitted and received by the Participating DFI that were not processed by an ACH Operator but were exchanged with another non-affiliated Participating DFI, either directly or through another entity, for the applicable period. Entries should be sorted by routing number of the non-affiliated DFI and include debits, credits and entries of non-value. If there are more routing numbers than spaces available, attach another sheet. Total columns and add together to calculate the grand total.

Line 3b. Enter the grand total from line 3a.

Line 4. Represents the 2025 per entry fee of $.000185

Line 5. Multiply line 3b by line 4 [example: (line 3b) 100,000 x (line 4) $.000185 = (line 5) $18.50]

Line 6. Payment due is equal to the amount on line 5. Indicate payment method. If amount on line 5 is less than one dollar, submit the completed form only; no payment is due.

Still Need Additional Information?

Downloadable Forms and Instructions are available at https://www.nacha.org/content/network-administration-fees or contact Nacha, 800-487-9180 or 703-561-1100 or email: N7Form@nacha.org.

FORM N-7 (2025)

Select Filing Period and Deadline (check all that apply):

	Period	*Filing Deadline*
For annual filers:	☐ December 31, 2025	January 31, 2026
For quarterly filers:	☐ March 31, 2025	April 30, 2025
	☐ June 30, 2025	July 31, 2025
	☐ September 30, 2025	October 31, 2025
	☐ December 31, 2025	January 31, 2026

1. Financial Institution Name _____

2. Business Address _____

_____

_____

3. Direct Send Information

a. 2025 direct send ACH entries by routing number of non-affiliated Participating DFI (see instructions)

DIRECT SEND DETAIL

ROUTING NUMBER	ENTRIES RECEIVED	ENTRIES ORIGINATED
TOTALS		
GRAND TOTAL (TOTAL RECEIVED + TOTAL ORIGINATED)		

FORM N-7 (2025)
(continued)

b. 2025 total direct send ACH entries (see instructions) _____

4. 2025 per entry fee x $.000185

5. Uncollected 2025 Network Administrative Fees (line 3b x line 4) $ _____

6. Payment Due: (Amount on line 5) Date of ACH credit _____ or Check_____

(If less than $1.00, no payment due, submit form only)

I declare that I have examined this form and to the best of my knowledge and belief, it is true, correct and complete.

Signature _____ Date _____

Printed Name _____

Title _____

Financial Institution Name _____

Email Address _____ Phone Number _____

Submit completed form to: N7Form@nacha.org

Submit payment. Payment via ACH credit preferred:

The ACH credit must be initiated by the organization filing Form N-7. UPIC Routing & Transit # 021052053, Acct # 59058945. Use CCD format for single filing. Complete in Batch Header (1) Company Name (2) Company Entry Description (specify Form N-7 (2025)).

If sending a check, please make the check payable to Nacha and mail to: Nacha, Attn: Finance Department, 11951 Freedom Drive, Suite 1001, Reston, VA 20190.

ACH Operations Bulletin #3-2024:

Open Banking and ACH Payments: The Impact of the CFPB's Personal Financial Data Rights Final Rule

October 31, 2024

Executive Summary

On October 22, 2024 the Consumer Financial Protection Bureau ("CFPB") released its final rule implementing section 1033 of the Consumer Financial Protection Act (the "Personal Financial Data Rights Final Rule" or "Final Rule").[1] This ACH Operations Bulletin provides an overview of the Final Rule and an initial assessment of its applicability and impact on ACH Network participants and ACH payments. ACH Network participants should take note, in particular, that:

1. A consumer's authorization to share data as provided for in the Final Rule, including the "information to initiate payment to or from a Regulation E account," is separate and distinct from a consumer's authorization to initiate an ACH payment to credit or debit their account;

2. Receiving Depository Financial Institutions ("RDFIs") must comply with the Final Rule's requirement to make routing and account numbers available through consumer and developer interfaces at no cost; [2] and,

3. The Nacha Operating Rules ("Nacha Rules") apply, and will continue to apply, to all ACH payments, including those for which the routing and account numbers are obtained through open banking methods, just as if the Receiver had provided that information directly to the payment Originator.

The CFPB's Personal Financial Data Rights Rule

On October 22, 2024 the CFPB released the Personal Financial Data Rights Final Rule implementing section 1033 of the Consumer Financial Protection Act and requiring the establishment of an open banking framework. Under the Personal Financial Data Rights Final Rule, data providers, including depository institutions, must make covered data available, at no cost, to consumers and their authorized third parties in a usable electronic form. Data providers

---

[1] *See* CFPB Personal Financial Data Rights Final Rule, https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/. As of this writing, the Final Rule has been challenged in court, so its ultimate implementation remains uncertain.

[2] The court challenge asserts that the CFPB overstepped its statutory authority with respect to including payment information as part of the Final Rule's covered data.

must provide such covered data to consumers and authorized third parties through established consumer and developer interfaces.

In order to receive covered data, authorized third parties must obtain the consumer's express, informed consent through a signed authorization disclosure that is clear and conspicuous and segregated from other materials. Authorized third parties are also subject to a number of obligations related to their data access, including restrictions on data collection, use and retention, satisfaction of information security requirements and the provision of a reasonable method for consumers to revoke the third party's authorization to access their covered data. Compliance dates for the Final Rule are staggered for depository institutions based on asset size, with the largest depository institutions, those holding at least $250 billion in total assets, having until April 1, 2026 (the earliest applicable date) to comply.[3]

Impact of the Personal Financial Data Rights Final Rule on ACH Network Participants and ACH Payments

Nacha understands that some ACH Network participants have questions about the implications of the Final Rule for ACH transactions. First and most importantly, the Final Rule relates to required information sharing by data providers. It does not change any applicable requirements regarding the authorization, origination or processing of ACH transactions. Second, the Nacha Rules continue to provide important guardrails if covered data is used in connection with ACH transactions. Accordingly, this Bulletin is intended to highlight the continued applicability of the Nacha Rules to ACH payments that involve data obtained through the open banking framework.

Applicability of the Personal Financial Data Rights Final Rule to ACH Network Participants

The CFPB's Final Rule solely governs the sharing of consumer data between data providers and authorized third parties and consumers; it does not impose any requirements related to the authorization or processing of consumer ACH transactions. However, ACH Network participants are impacted by the Final Rule due to their status as data providers. Specifically, RDFIs are covered under the Final Rule as data providers of the information needed to initiate a payment to or from a consumer's Regulation E account, i.e. routing and account numbers. As covered data providers, RDFIs must comply with the Final Rule's data sharing and interface establishment requirements. Additionally, the Final Rule requires third parties to obtain a consumer's consent to access data through a clear and conspicuous, segregated authorization. ACH Network participants should keep in mind that "authorized data access, in and of itself, is not payment authorization" and that "product or service providers that access information and initiate payments [must] obtain separate and distinct consumer authorizations for these separate activities."[4]

---

[3] Data providers with assets equal to or less than the Small Business Administration (SBA) size standard are exempt from the Final Rule. The current SBA size standard for commercial banking is $850 million in assets.

[4] *See* CFPB, Consumer Protection Principles: Consumer-Authorized Data Sharing and Aggregation, 4 (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

Applicability of Existing Nacha Rules to Payments Using Information Obtained Through Open Banking

While the ability of authorized third parties to obtain information necessary to initiate ACH transactions pursuant to the Final Rule potentially raises risks for financial institutions involved in such transactions, the Nacha Rules continue to govern the actual authorization, processing and movement of ACH payments. Moreover, the existing Nacha Rules already incorporate various established protections for banks and consumers that will continue to apply under the open banking regime, including with respect to transaction authorization procedures, consumer protection from unauthorized ACH transactions, record retention, data security, sharing of certain ACH data, and risk management.

Authorization Procedures

- With respect to ACH Entries that utilize data obtained via open banking (e.g., routing and account numbers),[5] the Nacha Rules' existing transaction authorization requirements continue to apply. Mere authorization to share data does not constitute authorization to initiate transactions based on that data. The Nacha Rules already require that authorizations for consumer debit Entries be in writing signed or similarly authenticated by the Receiver[6] and be clear and readily understandable.[7] Moreover, the Nacha Rules specifically require that authorizations be obtained by (and revoked with) the payment Originator.[8] The Final Rule is consistent with this requirement by mandating that open banking data authorization disclosures be "clear, conspicuous, and segregated from other material," e.g., a transaction authorization.[9]

Consumer Protection from Unauthorized ACH Transactions

- The Nacha Rules provisions regarding allocation of responsibility for unauthorized ACH Entries apply and will continue to apply to Entries that rely on open banking data. The existing Nacha Rules requirements already provide robust allocation of responsibility to the ODFI, and by extension to the Originator, for unauthorized ACH Entries.[10] Under the

[5] The Final Rule permits RDFIs to tokenize account numbers that are provided through the open banking regime. *See* 12 C.F.R. § 1033.211(c)(1). Although the Nacha Rules also permit tokenization of account numbers, tokenization involves a variety of complexities, including the ability to relate transactions involving tokens to underlying accounts for customer service purposes.

[6] Under the Nacha Rules, a Receiver is a Person that has authorized an Originator to initiate a credit Entry, debit Entry, or Non-Monetary Entry to the Receiver's account at the RDFI. With respect to debit Entries, the term "Receiver" means all Persons whose signatures are required to withdraw funds from an account for purposes of the warranty provisions of Subsection 2.4.1 (General ODFI Warranties). *See* Nacha Rules: Section 8.84. For example, a consumer who authorizes the sharing of his/her account number pursuant to the Final Rule, is the "Receiver" of any debit Entry based on that account information and would need to separately authorize the ACH debit to his/her account.

[7] *See* Nacha Rules: Section 2.3.1 (Originator Must Obtain Authorization from Receiver); Section 2.3.2.2 (Debit Entries to Consumer); and Section 2.3.2.5 (Standing Authorization for Debit Entries to Consumer Accounts).

[8] *See* Nacha Rules: Section 2.3.2.2 (Debit Entries to Consumer).

[9] Proposed 12 C.F.R. § 1033.411(a).

[10] *See* Nacha Rules: Section 2.13.2 (ODFI Request for Return); Section 3.7.1 (RDFI Obligation to Stop Payment of Entries to Consumer Accounts); Section 3.12 (Written Statement of Unauthorized Debit (WSUD)); Section 3.12.1 (Unauthorized Debit Entry/Authorization for Debit Has Been Revoked); Section 3.12.4 (Form of Written Statement of Unauthorized Debit); and Section 3.12.5 (Retention of Written Statement of Unauthorized Debit).

Nacha Rules, an RDFI must recredit a consumer for an unauthorized ACH debit if the consumer provides timely notice. The Nacha Rules further allow the RDFI to return such an unauthorized ACH debit to the ODFI within specified timeframes. ODFIs will want to ensure that their Originators that use open banking data are obtaining separate ACH transaction authorizations that meet the standards of the Nacha Rules.

Record Retention

- Although the Final Rule has certain record retention requirements for authorized third parties that obtain covered data, the Nacha Rules' existing record retention requirements related to the authorization and processing of ACH Entries[11] apply and will continue to apply to Entries that rely on open banking data.

Data Security

- Although the Final Rule imposes data security requirements on authorized third parties that obtain consumer data under the open banking framework, the Nacha Rules' existing data security requirements apply and will continue to apply to routing and account numbers used in ACH Entries, regardless of whether this information is obtained through open banking methods. These Nacha Rule provisions already require the secure handling and protection of origination information.[12] It is generally expected that compliance with the Gramm-Leach-Bliley Act "safeguards" requirements referenced in the Final Rule will also satisfy the Nacha Rules' requirements.

Data Sharing by Authorized Third Parties

- The Final Rule limits the purposes for which "authorized third parties" can reshare data gathered via open banking. Consistent with federal law limiting "data passes" to post-transaction third party sellers in internet transactions, and with the goal of protecting consumers against unintended charges against their accounts, the Nacha Rules further already prohibit an ODFI or Originator from disclosing a Receiver's account number or routing number to a third party to originate a separate debit entry.[13] This provision of the Nacha Rules applies to the same extent to information obtained through open banking as it does to information directly entered by a consumer themselves.

Risk Management

- The Nacha Rules already impose general risk management standards on ODFIs that include, among other things, an obligation to assess the nature of an Originator's ACH activities and the risks those activities present.[14] As open banking is implemented, ODFIs

---

[11] *See* Nacha Rules: Section 1.4.1 (Retention Requirement for Records of Entries); Section 1.4.2 (Provision Requirement for Records of Entries); Section 1.4.3 (Electronic Record Creation and Retention); Section 2.3.2.7 (Retention and Provision of the Record of Authorization); and Section 3.1.4 (RDFI May Request Copy of Receiver's Authorization of Entry from ODFI).

[12] *See* Nacha Rules: Section 1.6 (Security Requirements); and Section 1.7 (Secure Transmission of ACH Information via Unsecured Electronic Networks).

[13] *See* Nacha Rules: Section 2.3.4 (Restrictions on Data Passing).

[14] *See* Nacha Rules: Section 2.2.3 (ODFI Risk Management).

should assess the impact that reliance on open banking data has on their respective Originators.

Nacha staff is continuing to work with industry representatives to assess the implications of the Final Rule and whether any enhancements to the Nacha Rules or applicable guidance are warranted to minimize any potential adverse impacts from the implementation of the Final Rule.

###