NOTICE OF AMENDMENT TO THE 2024 NACHA OPERATING RULES

April 12, 2024

SUPPLEMENT #1-2024

ACH Risk Management Topics

Effective Dates: *October 1, 2024*
March 20, 2026
June 19, 2026

Minor Rule Topics Rule Changes

Effective Date: *June 21, 2024*

Supplement #1-2024 to the Nacha Operating Rules

On March 15, 2024, the Nacha Voting Membership approved 15 amendments to the Nacha Operating Rules (the Rules) encompassing the following areas:

ACH Risk Management Topics:

- Codifying Expanded Use of Return Reason Code R17.
- Expanded Use of ODFI Request for Return - R06.
- Additional Funds Availability Exceptions.
- Timing of Written Statement of Unauthorized Debit.
- RDFI Must Promptly Return Unauthorized Debit.
- Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs.
- ACH Credit Monitoring by RDFIs.
- Standard Company Entry Descriptions - PAYROLL and PURCHASE.

Minor Topics Rules Changes

- General Rule/Definition of WEB Entries.
- Definition of Originator.
- Originator Action on Notification of Change.
- Data Security Requirements.
- Use of Prenotification Entries.
- Clarification of Terminology – Subsequent Entries.

The effective dates for these amendments range from June 21, 2024, through June 19, 2026. Please see each Rule change for its specific effective date.

This supplement provides ACH Network participants with a summary of the key components of the changes, along with details regarding the technical changes to Rules language. To ensure compliance with the most current rules, use this Supplement in conjunction with the 2024 edition of the Nacha Operating Rules.

ACH Risk Management Topics

The ACH Risk Management Topics comprise a set of amendments to the Nacha Operating Rules that, together, 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. Specifically, these new Rules:

- Codify use of Return Reason Code R17 for cases of suspected fraud.
- Expand use of the ODFI Request for Return (R06), allowing an ODFI to request a return for any reason.
- Permit an RDFI to delay funds availability when it suspects credits have been originated under False Pretenses.
- Make process enhancements to the Written Statement of Unauthorized Debit.
- Establish a time frame within which an RDFI must return an unauthorized debit after review of the consumer's Written Statement of Unauthorized Debit.
- Establish fraud monitoring requirements for Originators, Third-Party Service Providers/Third-Party Senders, and ODFIs.
- Establish credit monitoring requirements for RDFIs.
- Establish standard Company Entry Descriptions for payroll credits and e-commerce purchases.

Because these rules have been designed to work in tandem with each other, several of the changes noted above impact the same sections of the Nacha Operating Rules. For ease of use, and to avoid unnecessary repetition of language, this Supplement includes a consolidated summary of all changes (along with their impacts and individual effective dates), followed by a Combined Rule Changes section, in effective date order. The Combined Rule Changes portion of this supplement illustrates the impact of these changes on specific sections of the Nacha Operating Rules, with new language appearing in italics with gray highlighting immediately following the existing text that it replaces. For reference, Appendix A also includes a technical summary for each individual ACH Risk Management amendment.

CODIFYING USE OF RETURN REASON CODE R17

SUMMARY

RDFIs that may be able to identify an ACH entry as fraudulent may want to return the entry on this basis. However, the Rules currently do not have a defined Return Reason Code for this use. The Rules provide for using the return reason code that most closely approximates the reason for the return. In the past, Nacha has provided guidance that Return Reason Code R17 is likely the closest return code for incidents of potential fraud.

The Codify Use of Return Reason Code R17 Rule (the Rule) will explicitly allow an RDFI to use Return Reason Code R17 to return an entry that it believes is fraudulent. This use of Return Reason Code R17 is optional and at the discretion of the RDFI; it is not required under the Rules. The Rule retains the current requirement to include the descriptor "QUESTIONABLE" in the return addenda record for such use.

The Rule is expected to improve the recovery of funds originated due to fraud. By providing clarity on the use and meaning of the R17 Return Reason Code, RDFIs will have a return reason to use at their option. ODFIs, Originators, Third-Party Service Providers and Third-Party Senders will potentially receive funds back in questionable situations, while receiving a clear message related to the reason for the return.

IMPACT TO PARTICIPANTS

As the R17 Return Reason Code with the "QUESTIONABLE" descriptor is in use today, ODFIs, RDFIs and other parties should not need significant technical changes. However, participants may need to update their documentation regarding the use of R17. Participants will need to also provide education to staff to ensure proper usage.

RDFIs: RDFIs should be cognizant of the potential for false positives.

EFFECTIVE DATE

The Codifying Expanded Use of R17 Rule will be effective on October 1, 2024. As the use of the R17 Return Reason Code for returns believed to be fraudulent is optional by RDFIs, there is no implementation or compliance obligation by the effective date.

EXPANDED USE OF ODFI REQUEST FOR RETURN - R06

SUMMARY

Under the Rules, an ODFI may request that an RDFI return a defined Erroneous Entry or a credit entry that was originated without the authorization of the Originator using Return Reason Code R06. The RDFI may, but is not obligated to, comply with the ODFI's request. ODFIs that wish to request the return of a potentially fraudulent entry do not have a clear means to do so, because the Rules limit the use of R06 to specific situations.

The Expanded Use of ODFI Request for Return - R06 Rule (the Rule) will expand the permissible uses of the Request for Return to allow an ODFI to request a return from the RDFI for any reason. The ODFI will still indemnify the RDFI for compliance with the request and the RDFI's compliance remains optional at the RDFI's discretion. However, the Rule will require the RDFI to respond to the ODFI, regardless of whether the RDFI complies with the ODFI's request to return the entry. The RDFI must advise the ODFI of its decision or the status of the request within 10 banking days of receipt of the ODFI's request.

The objective of the Rule is to improve the recovery of funds when fraud has occurred. The Rule also provides more flexibility for ODFIs that want to indemnify and request the RDFI return a transaction for any reason. This change also aligns rules language for Return Reason Code R06 returns with anecdotally-understood business practices for some Originators and ODFIs.

IMPACT TO PARTICIPANTS

Originators, Third-Party Service Providers and Third-Party Senders: These participants may need education on the expanded use of Return Reason Code R06.

ODFIs and RDFIs: Financial institutions may need to update their procedures and training to manage the broader use of Return Reason Code R06.

EFFECTIVE DATE

The Expanded Use of ODFI Request for Return - R06 Rule will become effective on October 1, 2024.

ADDITIONAL FUNDS AVAILABILITY EXCEPTIONS

SUMMARY

The current Rules provide RDFIs with an exemption from funds availability requirements if the RDFI reasonably suspects the credit entry was unauthorized. This exemption encompasses cases of account takeovers, in which a party that is not the Originator is able to initiate an ACH credit from the Originator's account.

The Additional Funds Availability Exceptions Rule (the Rule) will provide RDFIs with an additional exemption from the funds availability requirements to include credit ACH entries that the RDFI suspects are originated under False Pretenses. RDFIs are still subject to requirements under Regulation CC for funds availability. An RDFI cannot delay funds availability because it has not monitored an ACH credit. However, an RDFI can delay funds availability if its fraud detection processes and procedures identify a flag. The Rule is not intended to otherwise alter an RDFI's obligation to promptly make funds available as required by the Rules.

The Rule will provide participants with an additional tool to manage potentially questionable or suspicious transactions that fall under the "authorized fraud" category. The Rule will provide RDFIs and ODFIs with additional time to communicate before funds availability is required. These two factors should improve the potential for recovery of funds when fraud has occurred.

IMPACT TO PARTICIPANTS

ODFIs: ODFIs should be aware that they may be contacted by RDFIs that are taking advantage of the funds availability exemption.

RDFIs: An RDFI may need to update their policies and procedures to take advantage of the additional exemption. RDFIs using the exemption must take reasonable steps to notify the ODFI to inform it of the exemption.

EFFECTIVE DATE

The Additional Funds Availability Exceptions Rule will be effective on October 1, 2024. As the use of the Rule is optional by RDFIs, there is no implementation or compliance obligation by the effective date.

TIMING OF WRITTEN STATEMENT OF UNAUTHORIZED DEBIT

SUMMARY

When a consumer Receiver notifies an RDFI of an unauthorized debit, the RDFI must obtain a Written Statement of Unauthorized Debit (WSUD). Under the current Rules, the WSUD must be dated on or after the Settlement Date of the unauthorized debit entry. However, through digital notifications and alerts, a consumer may be able to report an unauthorized debit prior to its posting to the account.

The Timing of Written Statement of Unauthorized Debit Rule (the Rule) will allow a consumer Receiver to sign and date a WSUD on or after the date on which the entry is presented to the Receiver, even if the debit has not yet posted to the account. Information about the incoming debit may be via posting to the Receiver's account or by a notice of a pending transaction. The Rule does not otherwise change the requirement for an RDFI to obtain a consumer's WSUD.

The Rule will improve the process and experience when debits are claimed to be unauthorized. Moving transaction data more quickly through earlier returns can help participants manage risk. Receivers may be less impacted by unauthorized and potentially fraudulent transactions, while ODFIs, Third-Party Senders, and Originators may receive returns faster.

IMPACT TO PARTICIPANTS

RDFIs: RDFIs may want to explore ways to use electronic notifications and alerts, and electronic WSUDs. RDFIs may want to provide training for their front-line and operational staff to properly use and gain the full benefit of this new Rule.

EFFECTIVE DATE

The Timing of Written Statement of Unauthorized Debit Rule will be effective on October 1, 2024. RDFIs should codify this practice as soon as possible. However, as the use of the Rule is optional by RDFIs, there is no implementation or compliance obligation by the effective date.

RDFI MUST PROMPTLY RETURN UNAUTHORIZED DEBIT

SUMMARY

The current Rules state that an RDFI must transmit an extended return entry for which it recredits a Receiver's account in such that time that the entry can be made available to the ODFI no later than the opening of business on the banking day following the sixtieth (60th) calendar day following the settlement date of the original entry. However, the Rules are silent as to the timeframe for the RDFI to return the entry after receiving a signed and dated Written Statement of Unauthorized Debit (WSUD).

The RDFI Must Promptly Return Unauthorized Debit Rule (the Rule) will require that an RDFI transmit the return of an unauthorized entry for which it has received a WSUD in such time that the entry can be made available to the ODFI no later than the opening of business on the sixth (6th) banking day following the completion of RDFI's review of the consumer's signed WSUD. In any case, the RDFI must transmit the return in such time that it is made available to the ODFI no later than the opening of business on the banking day following the sixtieth (60th) calendar day following the settlement date of the original entry. The Rule does not change the reasons or requirements for an RDFI to obtain a Receiver's WSUD.

The objective of the Rule is to improve the recovery of funds and reduce the incidence of future fraud. Accelerating some returns can help manage risk, as the prompt return of an unauthorized debit alerts the ODFI and Originator to a potential problem. RDFIs that currently delay returns will be made whole more quickly through the return settlement process.

IMPACT TO PARTICIPANTS

RDFIs: Some RDFIs may need to improve procedures for processing extended returns after receiving a customer's completed WSUD. RDFIs may need to educate operations staff and update procedures related to handling customer unauthorized debit claims.

EFFECTIVE DATE

The RDFI Must Promptly Return Unauthorized Debit Rule will implement on October 1, 2024.

FRAUD MONITORING BY ORIGINATORS, THIRD-PARTY SERVICE PROVIDERS/THIRD-PARTY SENDERS AND ODFIS

SUMMARY

The current Nacha Operating Rules (Rules) require Originators to use a commercially reasonable fraudulent transaction detection system to screen WEB debits and when using Micro-Entries. However, these requirements do not encompass any other transaction types, and do not currently apply to other types of debits or to any credits other than Micro-Entries.

The Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs Rule (the Rule) will require each non-consumer Originator, ODFI, Third-Party Service Provider, and Third-Party Sender to establish and implement risk-based processes and procedures reasonably intended to identify ACH entries initiated due to fraud. Each of these parties will need to review at least annually their processes and procedures and make any appropriate updates to address evolving risks.

The objective of the Rule is to reduce the incidence of successful fraud attempts through regular fraud detection monitoring. Such monitoring can establish baselines of typical activity, making atypical activity easier to identify. By expanding fraud detection responsibilities to more parties in the ACH Network, the Rule will provide additional opportunities to detect and prevent fraud, especially for frauds that make use of credit-push payments. Any reduction in the incidence of successful fraud will improve the quality of transactions in the ACH Network.

The Rule also includes a reference to a new defined term, False Pretenses. This new term covers common fraud scenarios such as Business Email Compromise, vendor impersonation; payroll impersonation and other payee impersonations. The definition complements existing language in the Rules related to unauthorized credits.

IMPACT TO PARTICIPANTS

Originators, Third-Party Service Providers, and Third-Party Senders: These entities may need to implement fraud detection processes and procedures if they are not doing so currently. There may be less of an impact for those that have already implemented commercially reasonable fraud detection for WEB debits and/or for Micro-Entries.

ODFIs: ODFIs may need to update their fraud detection processes and procedures to include credit entries, if these entries are not currently part of their review process.

EFFECTIVE DATES

The Rule will be implemented in two phases:

Phase 1 - March 20, 2026. On this date, the Rule will apply to all ODFIs and those non-consumer Originators, Third-Party Service Providers, and Third-Party Senders with an annual ACH origination volume that exceeds 6 million entries in 2023.

Phase 2 - June 19, 2026. The Rule will apply all other non-consumer Originators, Third-Party Service Providers, Third-Party Senders on this date.

RDFI ACH CREDIT MONITORING

SUMMARY

Currently, the Rules require ODFIs to perform debit transaction monitoring, but do not apply transaction monitoring requirements to RDFIs. However, existing regulatory obligations for financial institutions require monitoring for suspicious transactions.

The RDFI ACH Credit Monitoring Rule (the Rule) mirrors the Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs Rule in that it will require RDFIs to establish and implement risk-based processes and procedures reasonably intended to identify credit ACH entries initiated due to fraud. As with the other entities, RDFIs will need to review at least annually their processes and procedures and make any appropriate updates to address evolving risks.

The objective of the Rule is to reduce the incidence of successful fraud and better enable the recovery of funds when fraud has occurred. The Rule aligns with an institution's regulatory obligation to monitor for suspicious transactions. A risk-based approach to such monitoring can consider factors such as transactional velocity, anomalies and account characteristics, all of which are in keeping with anti-money laundering practices in place today. The Rule encourages necessary communication between compliance monitoring teams and operations, product management and relationship staff. Identifying fraud or potentially fraudulent transactions will better enable RDFIs to exercise heightened scrutiny of accounts that are receiving such transactions.

The Rule also includes a reference to a new defined term, False Pretenses. This new term covers common fraud scenarios such as Business Email Compromise, vendor impersonation; payroll impersonation and other payee impersonations. The definition complements existing language in the Rules related to unauthorized credits.

IMPACT TO PARTICIPANTS

RDFIs: RDFIs that have not done so will need to establish processes and procedures reasonably intended to identify credit entries that are suspected of being unauthorized or authorized under False Pretenses. For those RDFIs that already have such processes and procedures in place, they will need to ensure that their existing processes and procedures are satisfactory under the Rule, including updating such systems and their alert processes, if necessary. RDFIs may need to enable information sharing internally between teams that monitor transactions for suspicious activity and operations, product and relationship teams.

EFFECTIVE DATES

The Rule will be implemented in two phases:

Phase 1 - March 20, 2026. On this date, the Rule will apply to RDFIs with an annual ACH receipt volume exceeding 10 million entries in 2023.

Phase 2 - June 19, 2026. The Rule will apply all other RDFIs.

STANDARD COMPANY ENTRY DESCRIPTIONS - PAYROLL AND PURCHASE

SUMMARY

The Company Entry Description is a 10-character field that the Originator uses to describe the purpose of a payment. The Rules have required standards for specific Company Entry Descriptions such as ACCTVERIFY, REVERSAL, HCCLAIMPMT, and RETRY PYMT. Standardized uses of the Company Entry Description field can help parties in the ACH Network identify, monitor, and count the volume of payments for specific purposes.

The Standard Company Entry Descriptions Rule (the Rule) will establish two new Company Entry Descriptions, PAYROLL and PURCHASE. The PAYROLL Company Entry Description must be used for ACH credits bearing the PPD Standard Entry Class Code that are for the payment of wages, salaries and other similar types of compensation. The objective of adding PAYROLL as a Company Entry Description is to reduce the incidence of fraud involving payroll redirections. RDFIs that monitor inbound ACH credits will have better information regarding new or multiple payroll payments to an account.

The Rule will also establish the Company Entry Description PURCHASE, which must be used for e-commerce purchases. An e-commerce purchase will be defined as a debit entry authorized by a consumer Receiver for the online purchase of goods. The new Company Entry Description will enable identification of such e-commerce transactions. The Rule defines e-commerce purchases for the purpose of using the new Company Entry Description.

The Rule will allow improved, targeted risk mitigations and tools to be utilized as participants are better able to identify certain purposes of transactions. By standardizing the use of certain data, the Rules can help parties manage risk and improve ACH Network quality.

IMPACT TO PARTICIPANTS

Originators, Third-Party Service Providers, Third-Party Senders, and ODFIs: Originators, Third-Party Service Providers, Third-Party Senders and ODFIs that handle payroll and e-commerce purchase transactions will need to update their systems to utilize the required Company Entry Descriptions.

RDFIs: RDFIs may choose to take advantage of intelligence enabled by the new Company Entry Descriptions and may need to update their policies and procedures to do so. However, RDFIs will not be required to act as a result of the descriptors.

EFFECTIVE DATE

The effective date for the Standard Company Entry Descriptions rule is March 20, 2026. Originators may begin using the new descriptions as soon as practical, but must do so no later than March 20, 2026.

COMBINED RULE CHANGES RESULTING FROM ACH RISK MANAGEMENT TOPICS

This section shows consolidated text changes to the Rules and incorporates technical impacts for the ACH Risk Management Topics elements. New Rules language appears in italics with gray highlighting.

The following ACH Risk Management Topics changes are effective October 1, 2024.

ARTICLE TWO

Rights and Responsibilities of ODFIs, Their Originators, and Third-Party Senders

SECTION 2.10 Reversing Entries

SUBSECTION 2.10.1 General Rule for Reversing Entries

An Originator or ODFI may initiate a Reversing Entry to correct an Erroneous Entry previously initiated to a Receiver's account. The Reversing Entry must be Transmitted to the ACH Operator in such time as to be Transmitted or made available to the RDFI within five Banking Days following the Settlement Date of the Erroneous Entry.

A debit Reversing Entry must not contain an Effective Entry Date that is earlier than the Effective Entry Date of the credit Entry to which it relates.

For this Section 2.10 and Subsection 2.13.2 (ODFI Request for Return) only, an Erroneous Entry is defined as an Entry that:

For this Section 2.10 only, an Erroneous Entry is defined as an Entry that:

(a) is a duplicate of an Entry previously initiated by the Originator or ODFI;

(b) orders payment to or from a Receiver different than the Receiver intended to be credited or debited by the Originator;

(c) orders payment in a dollar amount different than was intended by the Originator;

(d) orders payment of a debit Entry on a date earlier than the Receiver was intended to be debited by the Originator; or payment of a credit Entry on a date later than the Receiver was intended to be credited by the Originator; or

(e) is a credit PPD Entry satisfying each of the following criteria:

(i) the credit PPD Entry is for funds related to a Receiver's employment;

(ii) the value of the credit PPD Entry is fully included in the amount of a Check delivered to the same Receiver at or prior to the Receiver's separation from employment; and

(iii) the credit PPD Entry was Transmitted by the Originator prior to the delivery of the Check to the Receiver.

The Originator must make a reasonable attempt to notify the Receiver of the Reversing Entry and the reason for the Reversing Entry no later than the Settlement Date of the Reversing Entry. For a credit PPD Entry satisfying the criteria of Subsection 2.10.1(e) above, the Originator must notify the Receiver of the Reversing Entry at the time the Check is delivered to the Receiver.

SECTION 2.13 Return Entries

SUBSECTION 2.13.2 ODFI Request for Return

An ODFI may, orally or in writing, request an RDFI to return an Erroneous Entry for any reason, or a credit Entry originated without the authorization of the Originator, that was initiated by the ODFI. The RDFI may, but is not obligated to, comply with this request. For purposes of this subsection, an Erroneous Entry has the same meaning as in Section 2.10 (Reversing Entries).

An ODFI may, orally or in writing, request an RDFI to return an Entry for any reason. The RDFI may, but is not obligated to, comply with this request.

SUBSECTION 2.13.3 Indemnification by ODFI for Requested Returns

An ODFI requesting that an RDFI return an Erroneous Entry, or a credit Entry originated without the authorization of the Originator, indemnifies the RDFI from and against any and all claims, demands, losses, liabilities and expenses, including attorneys' fees and costs, resulting directly or indirectly from compliance by the RDFI with such request.

An ODFI requesting that an RDFI return an Entry indemnifies the RDFI from and against any and all claims, demands, losses, liabilities and expenses, including attorneys' fees and costs, resulting directly or indirectly from compliance by the RDFI with such request.

SUBSECTION 2.13.6 Dishonor of Return Entries

SUBSECTION 2.13.6.1 Dishonor of Return by ODFI

An ODFI may dishonor a Return Entry, with the exception of an IAT Return Entry, if:

(a) the RDFI failed to return the Entry within the time limits established by these Rules;

(b) information in one or more of the following fields of the Return Entry is incorrect or missing;

(i) DFI Account Number;

(ii) Original Entry Trace Number;

(iii) Amount;

(iv) Individual Identification Number/Identification Number;

(v) Transaction Code;

(vi) Company Identification Number;

(vii) Effective Entry Date;

(c) the Return Entry was misrouted;

(d) the Return Entry was a duplicate;

(e) the Return Entry is coded as the Return of an Erroneous Entry at the request of the ODFI, as permitted by Subsection 2.13.2 (ODFI Request for Return), but the ODFI did not make such a request;

(e) the Return Entry is coded as the Return of an Entry at the request of the ODFI, but the ODFI did not make such a request;

(f) the Return Entry is coded as a permissable Return Entry, as permitted by Subsection 3.8.3.5 (Late Return Entries for CCD or CTX Entries with ODFI Agreement), but the ODFI did not agree to accept the Return Entry;

(g) the Return Entry would result in an unintended credit to the Receiver because (1) the Return Entry relates to a debit Erroneous Entry, (2) the ODFI has already originated a credit Reversing Entry to correct the Erroneous Entry, and (3) the ODFI has not received a Return of that credit Reversing Entry; or

(h) the Return Entry would result in an unintended credit to the Receiver because (1) the Return Entry relates to a debit Reversing Entry that was intended to correct a credit Erroneous Entry, and (2) the ODFI has not received a Return of that credit Erroneous Entry.

To dishonor a Return Entry, the ODFI must Transmit a dishonored Return Entry complying with Appendix Four (Return Entries) to its ACH Operator within five Banking Days after the Settlement Date of the Return Entry.

ARTICLE THREE

Rights and Responsibilities of RDFIs and Their Receivers

SECTION 3.3 Timing Requirements for RDFI to Make Credit and Debit Entries Available

SUBSECTION 3.3.1 General Rules for Availability of Credit Entries to Receivers

An RDFI's obligation to make funds available under this Subsection 3.3.1 is subject to its right to return the Entry under these Rules.

An RDFI that reasonably suspects that a credit Entry is unauthorized is exempt from the funds availability requirements of this Subsection 3.3.1. An RDFI invoking such an exemption must promptly notify the ODFI.

An RDFI that reasonably suspects that a credit Entry is unlawful, involves the proceeds of unlawful activity, or is otherwise suspicious, including a credit Entry the RDFI suspects to be unauthorized or authorized by the Originator under False Pretenses, is exempt from the funds availability requirements of this Subsection 3.3.1. An RDFI invoking any such an exemption must take reasonable steps to promptly notify the ODFI.

SECTION 3.8 RDFI's Right to Transmit Return Entries

SUBSECTION 3.8.6 Response to ODFI Request for Return (New Subsection)

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 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..

SECTION 3.12 Written Statement of Unauthorized Debit

SUBSECTION 3.12.4 Form of Written Statement of Unauthorized Debit

The Written Statement of Unauthorized Debit must be signed or similarly authenticated by the Receiver, submitted within the time frames provided by these Rules, and otherwise conform to the requirements of this Section 3.12.

The Written Statement of Unauthorized Debit must include the following minimum information for each Entry for which recredit is requested by the Receiver:

(a) Receiver's printed name and signature;

(a) Receiver's printed name;

(b) Receiver's account number;

(c) identity of the party (i.e., the payee) debiting the account, as provided to the Receiver, and, if different, the name of the intended third-party payee;

(d) date the Entry was posted to the account;

(d) date the Entry was posted to the Receiver's account or, if the Entry was not posted to the account, the Effective Entry Date of the debit Entry;

(e) dollar amount of Entry;

(f) reason for return;

(g) signature date;

(g) Receiver assertion that the Written Statement of Unauthorized Debit is true and correct;

(h) Receiver assertion that the Receiver is an authorized signer or has corporate authority to act on the account; and

(i) the Receiver's signature and signature date.

The Written Statement of Unauthorized Debit must be dated on or after the Settlement Date of the Entry(ies) for which recredit is requested.

The Written Statement of Unauthorized Debit must be signed and dated by the Receiver on or after the date on which the Entry is presented to the Receiver's account for payment, either by posting to the account or by notice of a pending transaction.

More than one unauthorized debit Entry from a single Originator may be documented on a Written Statement of Unauthorized Debit, provided that all of the information detailed above is provided for each debit Entry for which the Receiver is seeking recredit.

An RDFI may obtain a Written Statement of Unauthorized Debit as an Electronic Record, as permissible in Subsection 1.4.3 (Electronic Record Creation and Retention). An RDFI may accept a consumer's Electronic Signature, as permissible in Subsection 1.4.4 (Electronic Signatures), for a Written Statement of Unauthorized Debit regardless of its form or the method used to obtain it.

SECTION 3.13 RDFI Right to Transmit Extended Return Entries

SUBSECTION 3.13.1 RDFI May Transmit Extended Return Entries

An RDFI may Transmit an Extended Return Entry with respect to any debit Entry for which it recredits a Receiver's account in accordance with Section 3.11 (RDFI Obligation to Recredit Receiver), provided that:

(a) no error was made by the RDFI in the debiting of the original Entry to the Receiver's account, except with respect to a stop payment order; and

(b) the RDFI Transmits the Extended Return Entry to its ACH Operator by its deposit deadline for the Extended Return Entry to be made available to the ODFI no later than the opening of business on the Banking Day following the sixtieth calendar day following the Settlement Date of the original Entry.

(b) the RDFI Transmits the Extended Return Entry to its ACH Operator by its deposit deadline for the Extended Return Entry to be made available to the ODFI no later than the opening of business on the sixth Banking Day after the Banking Day on which the RDFI completes its review of the Receiver's signed Written Statement of Unauthorized Debit, but in no case later than the opening of business on the Banking Day following the sixtieth calendar day following the Settlement Date of the original Entry.

The Extended Return Entry must comply with the requirements of Appendix Four (Return Entries).

ARTICLE EIGHT

Definitions of Terms Used in These Rules

SECTION 8.42 "False Pretenses" (New Section)

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.

APPENDIX THREE

ACH Record Format Specifications

PART 3.2 Glossary of ACH Record Format Data Elements

SUBPART 3.2.2 Glossary of Data Elements

Addenda Information: 44 Positions – Addenda Record – Optional (Returns except IAT); 34 Positions – Addenda Record – Optional (IAT Returns); 21 Positions Addenda Record – Optional/Mandatory (dishonored Returns)

Addenda Information is associated with the immediately preceding Entry Detail Record.

The Addenda Information field of a Return Entry is used by the RDFI to relay explanatory information that is required with the use of Return Reason Code R17 (File Record Edit Criteria/Entry with Invalid Account Number Initiated Under Questionable Circumstances).

The Addenda Information field of a Return Entry is used by the RDFI to relay explanatory information that is required with the use of Return Reason Code R17 (File Record Edit Criteria/Entry Initiated Under Questionable Circumstances).

An RDFI using Return Reason Code R17 to return an Entry that contains an invalid DFI Account Number and is believed by the RDFI to have been initiated under questionable circumstances must insert "QUESTIONABLE" within the first twelve positions of this field. The RDFI may include additional explanatory information within the remaining positions of this field.

An RDFI using Return Reason Code R17 to return an Entry that is believed by the RDFI to have been initiated under questionable circumstances (which includes, but is not limited to, an Entry Transmitted without the Originator's authorization or an Entry that is authorized by the Originator under False Pretenses) must insert "QUESTIONABLE" within the first twelve positions of this field. The RDFI may include additional explanatory information within the remaining positions of this field.

The Addenda Information Field of a dishonored Return Entry is a mandatory field when the dishonored Return bears Return Reason Code R69 (Field Error(s)). When Using Return Reason Code R69, the ODFI must insert the appropriate code(s) from the list below, separated by an asterisk (*), within the Addenda Information Field of the Addenda Record Format for dishonored Returns to indicate the field(s) in which the errors occur:

01 Return Contains Incorrect DFI Account Number

02 Return Contains Incorrect Original Entry Trace Number

03 Return Contains Incorrect Dollar Amount

04 Return Contains Incorrect Individual Identification Number/Identification Number

05 Return Contains Incorrect Transaction Code

06 Return Contains Incorrect Company Identification Number

07 Return Contains an Invalid Effective Entry Date

*For example: 01*03*06*

PART 4.2 Table of Return Reason Codes

CODE	TITLE	DESCRIPTION	INITIATED BY	RETURN TYPE	ACCOUNT TYPE	TIME FRAME	WRITTEN STATEMENT REQUIRED	CROSS REFERENCE	NOTES
R03	**No Account/ Unable to Locate Account**	The account number structure is valid and it passes the check digit validation, but the account number does not correspond to the individual identified in the Entry, or the account number designated is not an existing account.	RDFI	Return	Consumer or Non-Consumer	* 2 Banking Days	No	Article Three, Section 3.8 - RDFI's Right to Transmit Return Entries.	This Return Reason Code may not be used to return ARC, BOC, or POP Entries or Return Fee Entries related to underlying ARC, BOC, or POP Entries solely because they do not contain the Receiver's name in the Individual Name/Receiving Company Name Field.
R04	**Invalid Account Number Structure**	The account number structure is not valid.	RDFI	Return	Consumer or Non-Consumer	* 2 Banking Days	No	Article Three, Section 3.8 - RDFI's Right to Transmit Return Entries.	The Entry may fail the check digit validation or may contain an incorrect number of digits.
R05	**Unauthorized Debit to Consumer Account Using Corporate SEC Code**	CCD or CTX debit Entry was Transmitted to a Consumer Account of the Receiver and was not authorized by the Receiver.	RDFI	Extended Return	Consumer	** 60 Calendar Days	Yes	Article Three, Section 3.13 - RDFI Right to Transmit Extended Return Entries. Article Three, Subsection 3.12.1 - Unauthorized Debit Entry. Article Three, Subsection 3.4.1.1 - Rule Exception for CCD and CTX Entries to Consumer Accounts.	
R06	**Returned per ODFI's Request**	The ODFI has requested that the RDFI return an Entry. Erroneous Entry, or a credit Entry originated without the authorization of the Originator. *The ODFI has requested that the RDFI return an Entry.*	RDFI	Return	Consumer or Non-Consumer	Not defined, determined by ODFI and RDFI.	No	Article Two, Subsection 2.13.2 - ODFI Request for Return.	If the RDFI agrees to return the Entry, the ODFI must indemnify the RDFI according to Article Two, Subsection 2.13.3 *If the RDFI agrees to return the Entry, the ODFI must indemnify the RDFI according to Article Two, Subsection 2.13.3 (Indemnification by ODFI for Requested Returns).*

* Each Return Entry must be received by the RDFI's ACH Operator by its deposit deadline for the Return Entry to be made available to the ODFI no later than the opening of business on the second Banking Day following the Settlement Date of the original Entry.

** Each Return Entry must be received by the RDFI's ACH Operator by its deposit deadline for the Return Entry to be made available to the ODFI no later than the opening of business on the Banking Day following the sixtieth calendar day following the Settlement Date of the original Entry.

PART 4.2 Table of Return Reason Codes (continued)

CODE	TITLE	DESCRIPTION	INITIATED BY	RETURN TYPE	ACCOUNT TYPE	TIME FRAME	WRITTEN STATEMENT REQUIRED	CROSS REFERENCE	NOTES
R17	**File Record Edit Criteria/Entry with Invalid Account Number Initiated Under Questionable Circumstances/ Return of Improperly-Intiated Reversal** ***File Record Edit Criteria/Entry Initiated Under Questionable Circumstances/ Return of Improperly-Intiated Reversal***	(1) Field(s) cannot be processed by RDFI; (2) the Entry contains an invalid DFI Account Number (account closed/no account/ unable to locate account/ invalid account number) and is believed by the RDFI to have been initiated under questionable circumstances; or (3) either the RDFI or Receiver has identified a Reversing Entry as one that was improperly initiated by the Originator or ODFI. *1) Field(s) cannot be processed by RDFI; (2) the RDFI has not posted the Entry to the Receiver's account because it believes the Entry to the Receiver's account was initiated under questionable circumstances (which includes, but is not limited to, an ACH Entry Transmitted without the Originator's authorization, or an ACH Entry authorized by the Originator under False Pretenses); or (3) either the RDFI or Receiver has identified a Reversing Entry as one that was improperly initiated by the Originator or ODFI.*	RDFI	Return	Consumer or Non-Consumer	* 2 Banking Days	No	Article Three, Section 3.8 - RDFI's Right to Transmit Return Entries. Appendix Three, Part 3.2 - Glossary of ACH Record Format Specifications	(1) Some fields that are not edited by the ACH Operator are edited by the RDFI. If the Entry cannot be processed by the RDFI, the field(s) causing the processing error must be identified in the Addenda Information field of the Return. (2) An RDFI may use Return Reason Code R17 to return an Entry that contains an invalid DFI Account Number and is believed by the RDFI to have been initiated under questionable circumstances. The RDFI must insert "QUESTIONABLE" within the first twelve positions of the Addenda Information field. The RDFI may include additional explanatory information within the remaining positions of this field. *(2) An RDFI has determined that an Entry should not be posted to the Receiver's account because the RDFI believes it to have been initiated under questionable circumstances (which includes, but is not limited to, an ACH Entry Transmitted without the Originator's authorization, or an ACH Entry that is authorized by the Originator under False Pretenses). The RDFI returning an Entry for this reason must insert "QUESTIONABLE" within the first twelve positions of the Addenda Information field. The RDFI may include additional explanatory information within the remaining positions of this field.* (3) An RDFI may use Return Reason Code R17 to return a Reversing Entry that was improperly initiated by the Originator or ODFI.

* Each Return Entry must be received by the RDFI's ACH Operator by its deposit deadline for the Return Entry to be made available to the ODFI no later than the opening of business on the second Banking Day following the Settlement Date of the original Entry.

** Each Return Entry must be received by the RDFI's ACH Operator by its deposit deadline for the Return Entry to be made available to the ODFI no later than the opening of business on the Banking Day following the sixtieth calendar day following the Settlement Date of the original Entry.

The following ACH Risk Management Topics change is effective March 20, 2026.

APPENDIX THREE

ACH Record Format Specifications

PART 3.2 Glossary of ACH Record Format Data Elements

SUBPART 3.2.2 Glossary of Data Elements

Company Entry Description: 10 Positions – Company/Batch Header Record – Mandatory (all batches)

The Originator establishes the value of this field to provide the Receiver with a description of the purpose of the Entry. For example, "Gas bill," "Reg. Salary," "ins. prem.," "Soc. Sec.," "DTC," "Trade Pay," "PURCHASE," etc.

The Originator establishes the value of this field to provide the Receiver with a description of the purpose of the Entry. For example: "Gas bill," "ins. prem.," "Soc. Sec.," "DTC," "Trade Pay," "PURCHASE," etc.

This field must contain the word "ACCTVERIFY" when the batch contains Micro-Entries.

This field must contain the word "NONSETTLED" when the batch contains Entries that could not settle.

This field must contain the word "PURCHASE" when the batch contains 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 SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL SEC Code. The ODFI has no obligation to verify the presence or accuracy of the word "PURCHASE" as a description of purpose.

This field must contain the word "RECLAIM" when the batch contains Reclamation Entries.

This field must contain the words "RETRY PYMT" when the batch contains Reinitiated Entries. For any Reinitiated Entry, the description "RETRY PYMT" must replace the original content of the Company Entry Description field transmitted in the original Entry, including content otherwise required by these Rules.

This field must contain the words "RETURN FEE" when the batch contains Return Fee Entries.

This field must contain the word "REVERSAL" when the batch contains Reversing Entries.

ADV: The Originator, i.e., the Originating ACH Operator, uses this field to describe to the institution receiving the ADV File the type of activity to which the accounting information relates.

CCD: This field must contain the word "HCCLAIMPMT" when the batch contains Health Care EFT Transactions.

ENR: This field must contain the word "AUTOENROLL" when the batch contains Automated Enrollment Entries.

PPD: This field must contain the word "PAYROLL" when the batch contains credits for the payment of wages, salaries, or similar types of compensation. The use of the term "PAYROLL" in this field is descriptive and 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. The ODFI has no obligation to verify the presence or accuracy of the word "PAYROLL" as a description of purpose or employment status.

RCK: This field must contain the word "REDEPCHECK".

TRX: This field contains the routing number of the keeper.

WEB: For a Person-to-Person Entry, this field must contain a description that the Receiver would readily recognize as descriptive of a Person-to-Person Entry.

XCK: This field must contain the words "NO CHECK".

The following ACH Risk Management Topics changes are effective March 20, 2026 and June 19, 2026.

ARTICLE TWO

Rights and Responsibilities of ODFIs, Their Originators, and Third-Party Senders

SECTION 2.2 Prerequisites to Origination

SUBSECTION 2.2.4 Identification of Unauthorized Entries or Entries Authorized Under False Pretenses (New Subsection)[1].

Each non-consumer Originator; each Third-Party Sender; each ODFI; and each Third-Party Service Provider that performs any functions of ACH processing on behalf of an Originator, Third-Party Sender, or ODFI must:

(a) establish and implement risk-based processes and procedures relevant to the role it 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; and

(b) at least annually review these processes and procedures and make appropriate updates to address evolving risks.

These processes and procedures do not require the screening of every ACH Entry individually and do not need to be performed prior to the processing of Entries. An ODFI's processes and procedures may take into account the processes and procedures implemented by other participants in the origination of Entries.

This Subsection 2.2.4 does not modify or create, and shall not be interpreted to modify or create, in any way, rights or obligations of any Person under Article 4A. An agreement to comply with the Rules or this Subsection 2.2.4 does not, and shall not be interpreted to, constitute agreement to a "security procedure" for purposes of Article 4A unless otherwise specifically designated as such in an agreement with the ODFI. The obligation to comply with this Subsection 2.2.4 is enforceable solely by the National Association in accordance with Appendix Nine (Rules Enforcement) of these Rules and does not create or imply any other duty to any other Person.

[1] *Phase 1 of this rule will become effective March 20, 2026, and will apply to all ODFIs, and to any non-consumer Originators, Third-Party Senders, and Third-Party Service Providers whose ACH Origination or Transmission volume exceeds 6 million Entries in 2023. Phase 2 will become effective June 19, 2026, and will eliminate the volume threshold applicable to Subsection 2.2.4. At that time, Subsection 2.2.4's coverage will be expanded to include all non-consumer Originators, Third-Party Senders, and Third-Party Service Providers, regardless of volume.*

ARTICLE THREE

Rights and Responsibilities of RDFIs and Their Receivers

SECTION 3.1 General Rights and Responsibilities of RDFIs

SUBSECTION 3.1.10 Identification of Unauthorized Credit Entries or Credit Entries Authorized Under False Pretenses (New Subsection)[2]

Each RDFI must:

(a) establish and implement risk-based processes and procedures relevant to the role the RDFI plays in connection with the receipt of credit Entries that are reasonably intended to identify credit Entries that are suspected of being unauthorized or authorized under False Pretenses, including processes and procedures for responding when credit Entries are identified as potentially unauthorized or authorized under False Pretenses; and

(b) at least annually review these processes and procedures and make appropriate updates to address evolving risks.

These processes and procedures do not require the screening of every ACH Entry individually and do not need to be performed prior to the processing of Entries.

This Subsection 3.1.10 does not modify or create, and shall not be interpreted to modify or create, in any way, rights or obligations of any Person under Article 4A. The obligation to comply with this Subsection 3.1.10 is enforceable solely by the National Association in accordance with Appendix Nine (Rules Enforcement) of these Rules and does not create or imply any other duty to any other Person.

[2] *Phase 1 of this rule will become effective March 20, 2026, and will apply to all RDFIs whose ACH receipt volume exceeds 10 million Entries in 2023. Under Phase 2 (effective June 19, 2026), the volume threshold will be eliminated and the requirements of Subsection 3.1.10 will apply to all RDFIs.*

APPENDIX A: ACH RISK MANAGEMENT TOPICS INDIVIDUAL TECHNICAL SUMMARIES

Codifying Expanded Use of Return Reason Code R17

Technical Summary

Below is a summary of the impact of the new rule Codifying the Expanded Use of Return Reason Code R17 on the Nacha Operating Rules.

- *Article Eight, Section 8.42 ("False Pretenses")* – New section to define False Pretenses.
- *Appendix Three, Subpart 3.2.2 (Glossary of Data Elements - Addenda Information)* – Updated to include additional language for unauthorized entries and entries authorized under False Pretenses.
- *Appendix Four, Part 4.2 (Table of Return Reason Codes)* – Updated to include modifications to the use of Return Reason Code R17.

Expanding the Use of ODFI Request for Return – R06

Technical Summary

Below is a summary of the impact of Expanding the Use of ODFI Request for Return – R06.

- *Article Two, Subsection 2.10.1 (General Rule for Reversing Entries)*. Updated to delete references to the ODFI request for return.
- *Article Two, Subsection 2.13.2 (ODFI Request for Return)*. Updated to allow an ODFI to request a return for any reason.
- *Article Two, Subsection 2.13.3 (Indemnification by ODFI for Requested Returns)* – Updated to remove restrictive language for entries qualified as reasons to request a return.
- *Article Two, Subsection 2.13.6.1 (Dishonor of Return by ODFI)* – Updated to remove reference to erroneous entry under list of qualified reasons to dishonor a return.
- *Article Three Subsection 3.8.6 (Response to ODFI Request for Return)* – New subsection adding the requirement for the RDFI to advise the ODFI of its decision or the status of the ODFI's request.
- *Appendix Four, Part 4.2 (Table of Return Reason Codes)* – Updated to include modifications to the use of Return Reason Code R06.

Additional Funds Availability Exceptions

Technical Summary

Below is a summary of the impact of the Additional Funds Availability Exceptions Rule.

- *Article Three, Subsection 3.3.1 (General Rules for Availability of Credit Entries to Receivers)*. Updated to add exemptions for credit entries the RDFI suspects are originated under false pretenses.
- *Article Eight, Section 8.42 (False Pretenses)*. New section to define False Pretenses.

Timing of Written Statement of Unauthorized Debit

Technical Summary

Below is a summary of the impact of the Timing of Written Statement of Unauthorized Debit Rule.

- *Article Three, Subsection 3.12.4 (Form of Written Statement of Unauthorized Debit)*. Updated to allow a WSUD to be signed and dated by the Receiver on or after the date on which the Entry is presented to the Receiver, even if the debit has not yet been posted to the account.

RDFI Must Promptly Return Unauthorized Debit

Technical Summary

Below is a summary of the impact of the RDFI Must Promptly Return Unauthorized Debit Rule.

- *Article Three, Subsection 3.13.1 (RDFI May Transmit Extended Return Entries)*. Updated to require an RDFI to transmit an Extended Return Entry so that it is made available to the ODFI no later than the opening of business on the sixth banking day following the RDFI's completion of its review of the consumer's signed WSUD.

Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs

Technical Summary

Below is a summary of the impact of the Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs Rule on the Nacha Operating Rules.

- *Article Two, Subsection 2.2.4 (Identification of Unauthorized Entries or Entries Authorized Under False Pretenses)* – New subsection to establish rules surrounding fraud monitoring.

- *Article Eight, Section 8.42 ("False Pretenses")*. New section to define False Pretenses. (This section will be effective October 1, 2024)

RDFI ACH Credit Monitoring

Technical Summary

Below is a summary of the impact of the RDFI ACH Credit Monitoring Rule on the Nacha Operating Rules. Sections of the Rules that are affected by this amendment are also included and reflect rule language as it will read upon implementation in highlighted, italicized text.

- *Article Three, Subsection 3.1.10 (Identification of Unauthorized Credit Entries or Credit Entries Authorized Under False Pretenses)* – New subsection requiring monitoring of incoming ACH credits by RDFIs.

- *Article Eight, Section 8.42 ("False Pretenses")* – New section to define False Pretenses. (This section will be effective October 1, 2024)

Standard Company Entry Descriptions PAYROLL and PURCHASE

Technical Summary

Below is a summary of the impact of the Standard Company Entry Descriptions PAYROLL and PURCHASE Rule.

- *Appendix Three, Subsection 3.2.2 (Glossary of Data Elements)*. Updated to add a new standard Company Entry Description for e-commerce purchases.

- *Appendix Three, Subsection 3.2.2 (Glossary of Data Elements)*. Updated to add a new standard Company Entry Description for PPD Credits for payment of wages, salaries and similar types of compensation.

Minor Topics Rule Changes

SUMMARY

The Minor Topics Rule Changes amend six specific areas of the Nacha Operating Rules (Rules) to address minor issues. Minor changes to the Rules have little to no impact on ACH participants and no significant processing or financial impact. These amendments address changes related to:

1. General Rule/Definition of WEB Entries.
2. Definition of Originator.
3. Originator Action on Notification of Change.
4. Data Security Requirements.
5. Use of Prenotification Entries.
6. Clarification of Terminology – Subsequent Entries.

KEY COMPONENTS OF RULE AMENDMENTS

General Rule/Definition of WEB Entries

The General Rule/Definition of WEB Entries amendment will re-word the WEB general rule in Article Two and definitions in Article Eight and Appendix Three to clarify that the WEB SEC Code must be used for all consumer–to–consumer credits, regardless of how the consumer communicates the payment instruction to the ODFI or the Person–to–Person service provider.

Scope of change: Clarification of the existing requirement on proper SEC Code use.

Definition of Originator

The Definition of Originator change will add a reference to the Originator's authority to credit or debit the Receiver's account, which is not currently addressed in the Rules. The change will include a notation to the definition that the Rules do not always require a Receiver's authorization, such as with Reversing, Reclamation and Person–to–Person Entries.

Scope of change: Clarification of intent - role of an ACH participant.

Originator Action on Notification of Change

The Rules currently allow the Originator discretion on whether it will act on Notifications of Change (NOCs) received for certain single entries bearing certain SEC Codes (ARC, BOC, POP, RCK, TEL, WEB, and XCK), but are silent on single entries bearing other SEC Codes. In practice, many Originators have been treating NOCs for all one-time entries similarly. This Originator Action on Notification of Change amendment will give Originators discretion on whether to make NOC changes for any single entry, regardless of SEC Code.

Scope of change: Clarification of intent and reflection of current business practice.

Data Security Requirements

The current Rules require each non-consumer Originator that is not a participating depository financial institution to protect DFI account numbers by rendering them unreadable when stored electronically. This requirement is threshold-

based and begins to apply to covered entities once those participants' annual ACH origination or transmission volume exceeds 2 million entries for the first time. The Rules include a grace period, which as currently worded, can be misinterpreted as giving relief to compliance for covered parties if their volume falls below the 2 million entry threshold in the future. The Data Security Requirements change will clarify that once a covered party meets the volume threshold for the first time, the requirement to render account numbers unreadable remains in effect, regardless of future volume.

Scope of change: Clarification of intent.

Use of Prenotification Entries

The Rules currently allow Originators to transmit prenotification entries for account validation prior to initiation of the first credit or debit entry to the Receiver's account. However, Originators have indicated a need to re-validate that certain accounts are open and can accept ACH entries, even after live entries previously have been transmitted. The recent rule on Micro-Entries does not limit validation to before first use. Furthermore, in practice, many Originators already use prenotes for re-validation. The Use of Prenotification Entries amendment will align the prenote rules with industry practice by removing language that limits prenote use to only prior to the first credit or debit entry.

Scope of change: Minor change to reflect current business practice.

Clarification of Terminology – Subsequent Entries

With the adoption of definitions and rules for Standing Authorization and Subsequent Entry, minor changes are needed to prenote and NOC language to remedy now-ambiguous references to the phrase "subsequent entry" when not referring to a defined Subsequent Entry. The Clarification of Terminology – Subsequent Entries amendment will replace references to "subsequent entry" in the Rules with synonymous terms (e.g., future, additional, another) to avoid any confusion with the new definition "Subsequent Entry."

Scope of change: Clarification of intent.

IMPACT TO PARTICIPANTS

All Participants: All ACH Network participants benefit from Rules language that is consistent and clear, and that takes established industry practices into consideration. Each of the Minor Topics Rule changes serves to improve overall ACH processing efficiency by enhancing and clarifying certain areas within the Rules that are troublesome or ambiguous to users. Nacha does not expect ACH Network participants to incur any substantial costs associated with the implementation of these changes.

EFFECTIVE DATE

Each of the Minor Topics Rule changes will become effective on June 21, 2024.

TECHNICAL SUMMARY

On the following pages is a summary of the impact of the Minor Topics Rule changes on the Nacha Operating Rules. Sections of the Rules that are affected by these amendments are included and reflect rule language as it will read upon implementation in highlighted, italicized text.

General Rule/Definition of WEB Entries

- *Article Two, Subsection 2.5.17.1 (General Rule for WEB Entries)* – clarifies that the WEB Standard Entry Class Code must be used for all WEB Entries, regardless of how the consumer Originator communicates the payment instruction to the ODFI/P2P service provider.

- *Article Eight, Section 8.55 ("Internet-Initiated/Mobile Entry")* – clarifies that the WEB Standard Entry Class Code must be used for all WEB Entries, regardless of how the consumer Originator communicates the payment instruction to the ODFI/P2P service provider

- *Appendix Three, Subpart 3.2.2 (Glossary of Data Elements)* – makes corresponding changes to the definition of WEB Entry under the description of the Standard Entry Class Code field.

ARTICLE TWO

Rights and Responsibilities of ODFIs, Their Originators, and Third-Party Senders

SUBSECTION 2.5.17 Specific Provisions for WEB Entries (Internet-Initiated/Mobile Entry)

SUBSECTION 2.5.17.1 General Rule for WEB Entries

A debit WEB Entry is a debit Entry to a Consumer Account originated based on (a) any form of authorization that is communicated from the Receiver to the Originator via the Internet or a Wireless Network, except for an Oral Authorization via a telephone call; or (b) any form of authorization if the Receiver's instruction for the initiation of the individual debit Entry is designed by the Originator to be communicated, other than orally via a telephone call, to the Originator via a Wireless Network.

A credit WEB Entry is a credit Entry initiated by or on behalf of the holder of a Consumer Account that is intended for a Consumer Account of a Receiver, regardless of whether the instruction is communicated via the Internet or Wireless Network.

A credit WEB Entry is a credit Entry initiated by or on behalf of the holder of a Consumer Account that is intended for a Consumer Account of a Receiver, regardless of the manner in which the consumer Originator communicates the payment instruction to the ODFI or Third-Party Service Provider.

ARTICLE EIGHT

Definitions of Terms Used in These Rules

SECTION 8.55 "Internet-Initiated/Mobile Entry" or "WEB Entry" or "WEB"

(a) a debit Entry initiated by an Originator to a Consumer Account of the Receiver based on (a) any form of authorization that is communicated from the Receiver to the Originator via the Internet or Wireless Network, except for an Oral Authorization via a telephone call; or (b) any form of authorization if the Receiver's instruction for the initiation of the individual debit Entry is designed by the Originator to be communicated, other than orally via a telephone call, to the Originator via a Wireless Network;

(b) at the discretion of the Originator, a debit Subsequent Entry for which the Receiver's affirmative action for the initiation of the Subsequent Entry is communicated by the Receiver to the Originator via the Internet, regardless of the manner in which the Standing Authorization was obtained; or

(c) a credit Entry initiated by or on behalf of the holder of a Consumer Account that is intended for the Consumer Account of a Receiver, regardless of whether the authorization of such Entry is communicated via the Internet or Wireless Network.

(c) a credit Entry initiated by or on behalf of the holder of a Consumer Account that is intended for the Consumer Account of a Receiver, regardless of the manner in which the consumer Originator communicates the payment instruction to the ODFI or Third-Party Service Provider.

APPENDIX THREE

ACH Record Format Specifications

PART 3.2 Glossary of ACH Record Format Data Elements

SUBPART 3.2.2 Glossary of Data Elements

Standard Entry Class Code: 3 Positions – Company/Batch Header – Mandatory (all batches)

This field contains a three-character code used to identify various types of Entries.

ACK: ACH Payment Acknowledgment – The code that identifies a Non-Monetary Entry initiated by an RDFI to provide an acknowledgment of receipt by the RDFI of a corporate credit payment originated using the CCD format.

ADV: Automated Accounting Advice – The code that identifies a Non-Monetary Entry that is used by an ACH Operator to provide accounting information regarding an Entry to Participating DFIs in machine-readable format. An Automated Accounting Advice is an optional service provided by ACH Operators and must be requested by a DFI desiring this service.

ARC: Accounts Receivable Entry – The code that identifies a Single Entry debit initiated by an Originator to the Receiver's account based on an Eligible Source Document provided to the Originator by the Receiver (1) via the U.S. mail or delivery service, (2) at a dropbox location, or (3) in person for payment of a bill at a manned location.

ATX: Financial EDI Acknowledgment – The code that identifies a Non-Monetary Entry initiated by an RDFI to provide an acknowledgment of receipt by the RDFI of a corporate credit payment originated using the CTX format.

BOC: Back Office Conversion Entry – The code that identifies a Single Entry debit initiated by an Originator to the Receiver's account based on an Eligible Source Document provided to the Originator by the Receiver at the point of purchase or at a manned bill payment location for subsequent conversion during back office processing.

CCD: Corporate Credit or Debit Entry – The code that identifies an Entry initiated by an Organization to transfer funds to or from an account of that Organization or another Organization.

CIE: Customer Initiated Entry – The code that identifies a credit Entry initiated by or on behalf of the holder of a Consumer Account to transfer funds to the account of the Receiver.

COR: Notification of Change or Refused Notification of Change – The code that identifies a Non-Monetary Entry Transmitted by (1) an RDFI for the purpose of identifying incorrect information contained within an Entry and providing correct data in the precise format to be used on future Entries, or (2) an ODFI to refuse a misrouted NOC or an NOC that contains incorrect information.

CTX: Corporate Trade Exchange – The code that identifies an Entry initiated by an Organization to transfer funds to or from the account of that Organization or another Organization that permits the inclusion of payment-related remittance information in ANSI or UN/EDIFACT syntax.

DNE: Death Notification Entry – The code that identifies a Non-Monetary Entry initiated by an agency of the Federal Government of the United States to notify an RDFI of the death of a Receiver.

ENR: Automated Enrollment Entry – The code that identifies a Non-Monetary Entry initiated by a Participating DFI to an agency of the Federal Government of the United States on behalf, and at the request, of an account holder at the Participating DFI to enroll in a service that will enable Entries to such Person's account at the Participating DFI.

IAT: International ACH Transaction – The code that identifies an Entry that is part of a payment transaction[3] involving a Financial Agency's office that is not located in the territorial jurisdiction of the United States. An office of a Financial Agency is involved in the payment transaction if it (1) holds an account that is credited or debited as part of the payment transaction, (2) receives payment directly from a Person or makes payment directly to a Person as part of the payment transaction, or (3) serves as an intermediary in the settlement of any part of the payment transaction.

MTE: Machine Transfer Entry – The code that identifies Entries initiated at an "Electronic terminal," as defined in Regulation E, to transfer funds to or from a Consumer Account maintained with an RDFI, i.e., an ATM cash deposit or withdrawal.

POP: Point-of-Purchase Entry – The code that identifies a Single Entry debit initiated by an Originator to the Receiver's account based on an Eligible Source Document provided to the Originator by the Receiver at the point of purchase or manned bill payment location to transfer funds from the Receiver's account.

POS: Point-of-Sale Entry – The code that identifies a debit Entry initiated at an "Electronic terminal," as defined in Regulation E, to transfer funds from a Consumer Account of the Receiver to pay an obligation incurred in a point-of-sale transaction, or to effect a point-of-sale terminal cash withdrawal. Also an adjusting or other credit Entry related to such debit Entry, transfer of funds, or obligation.

PPD: Prearranged Payment and Deposit Entry – The code that identifies an Entry initiated by an Organization based on a standing or a Single Entry authorization from a Receiver to transfer funds to or from a Consumer Account of the Receiver.

RCK: Re-presented Check Entry – The code that identifies a Single Entry debit constituting a presentment notice of an item eligible under Article Two, Subsection 2.5.13.3 (RCK Eligible Items). An RCK Entry is an item as defined by Revised Article 4 of the Uniform Commercial Code (1990 Official Text) only for the limited purposes of presentment as set forth in Article 4-110(c) and notice of dishonor as set forth in Article 4-301(a)(2).

SHR: Shared Network Transaction – The code that identifies a debit Entry initiated at an "Electronic terminal," as defined in Regulation E, to transfer funds from a Consumer Account of the Receiver to pay an obligation incurred in a point-of-sale transaction, or to effect a point-of-sale terminal cash withdrawal. Also an adjusting or other credit Entry related to such debit Entry, transfer of funds, or obligation. SHR Entries are initiated in a shared network where the ODFI and RDFI have an agreement in addition to these Rules to process such Entries.

TEL: Telephone-Initiated Entry – The code that identifies a debit initiated by an Originator pursuant to an oral authorization obtained over the telephone to transfer funds from a Consumer Account of the Receiver.

TRC: Check Truncation Entry – The code that identifies a debit Entry initiated pursuant to a Check Truncation Program that permits the Truncation of a single Check drawn on the paying bank.

TRX: Check Truncation Entries Exchange – The code that identifies a debit Entry initiated based on a Check Truncation Program that permits the Truncation of multiple Checks drawn on the same paying bank.

WEB: Internet-Initiated/Mobile Entry – The code that identifies (1) a debit Entry initiated by an Originator to a Consumer Account of the Receiver based on (a) an authorization that is communicated, other than by an oral communication, from the Receiver to the Originator via the Internet or a Wireless Network, or (b) any form of authorization if the Receiver's instruction for the initiation of the individual debit Entry is designed by the Originator to be communicated, other than by an oral communication, to the Originator via a Wireless Network; or (2) a credit Entry initiated by or on behalf of the holder of a Consumer Account that is intended for the Consumer Account of a Receiver, regardless of whether the authorization of such Entry is communicated via the Internet or Wireless Network.

[3] *See the Nacha Operating Guidelines chapter on International ACH Transactions for further guidance on payment transactions.*

WEB: Internet-Initiated/Mobile Entry – The code that identifies (1) a debit Entry initiated by an Originator to a Consumer Account of the Receiver based on (a) an authorization that is communicated, other than by an oral communication, from the Receiver to the Originator via the Internet or a Wireless Network, or (b) any form of authorization if the Receiver's instruction for the initiation of the individual debit Entry is designed by the Originator to be communicated, other than by an oral communication, to the Originator via a Wireless Network; or (2) a credit Entry initiated by or on behalf of the holder of a Consumer Account that is intended for the Consumer Account of a Receiver, regardless of the manner in which the consumer Originator communicates the payment instruction to the ODFI or Third-Party Service Provider.

XCK: Destroyed Check Entry – The code that identifies a debit Entry initiated with respect to an item eligible under Article Two, Subsection 2.5.18.2 (XCK Eligible Items).

Definition of Originator

- *Article Eight, Section 8.71 ("Originator")* – expands the definition of Originator to recognize the Originator's fundamental relationship with the Receiver.

ARTICLE EIGHT

Definitions of Terms Used in These Rules

SECTION 8.71 "Originator"

a person that has authorized an ODFI (directly or through a Third-Party Sender) to Transmit, for the account of that Person, a credit Entry, debit Entry, or Non-Monetary Entry to the Receiver's account at the RDFI.

a Person that (i) has been authorized by a Receiver to initiate a credit Entry, debit Entry, or Non-Monetary Entry to the Receiver's account at the RDFI (except where authorization is not required by these Rules); and (ii) has authorized an ODFI (directly or through a Third-Party Sender) to Transmit, for the account of that Person, a credit Entry, debit Entry, or Non-Monetary Entry to the Receiver's account at the RDFI.

Originator Action on Notification of Change

- *Article Two, Subsection 2.12.1 (ODFI and Originator Action on Notification of Change)* – modifies bullet (l) to clarify that the Originator has discretion to act on any single-entry NOC, regardless of SEC Code.

ARTICLE TWO

Rights and Responsibilities of ODFIs, Their Originators, and Third-Party Senders

SECTION 2.12 Notifications of Change

SUBSECTION 2.12.1 ODFI and Originator Action on Notification of Change (NOC)

An ODFI must accept a Notification of Change (also known as "NOC" and "COR Entry") or a corrected NOC that complies with the requirements of Appendix Five (Notification of Change) and is Transmitted by the RDFI within the time limits established by these Rules, unless otherwise provided for in this Section 2.12.

For each NOC or corrected NOC it receives, an ODFI must provide the Originator with the following minimum information within two Banking Days of the Settlement Date of the NOC or corrected NOC:

(a) Company Name;

(b) Company Identification;

(c) Company Entry Description;

(d) Effective Entry Date;

(e) DFI Account Number;

(f) Individual Name/Receiving Company Name;

(g) Individual Identification Number/Identification Number;

(h) Change Code;

(i) Original Entry Trace Number;

(j) Original RDFI Identification; and

(k) Corrected Data.

Except as noted below, the Originator must make the changes specified in the NOC or corrected NOC within six Banking Days of receipt of the NOC information or prior to initiating another Entry to the Receiver's account, whichever is later.

(l) The Originator may choose, at its discretion, to make the changes specified in any NOC or corrected NOC received with respect to any ARC, BOC, POP, RCK, Single-Entry TEL, Single-Entry WEB, and XCK Entry.

(l) The Originator may choose, at its discretion, to make the changes specified in any NOC or corrected NOC received with respect to any Single Entry.

(m) In the case of CIE and credit WEB Entries, the ODFI or the Third-Party Service Provider (rather than the consumer Originator) must make the changes specified in the NOC.

(n) For an NOC that is in response to a Prenotification Entry, the Originator must make the changes specified in the NOC prior to originating a subsequent Entry to the Receiver's account if the NOC is received by the ODFI by the opening of business on the second Banking Day following the Settlement Date of the Prenotification Entry.

Data Security Requirements

- *Article One, Section 1.6 (Security Requirements)* – clarifies that once a party is subject to the requirement to render data unreadable when stored electronically, it must continue to do so consistently thereafter, regardless of annual volume.

ARTICLE ONE
General Rules

SECTION 1.6 Security Requirements

Each non-consumer Originator, Participating DFI, Third-Party Service Provider, and Third-Party Sender must establish, implement, and update, as appropriate, policies, procedures, and systems with respect to the initiation, processing, and storage of Entries that are designed to:

(a) protect the confidentiality and integrity of Protected Information until its destruction;

(b) protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; and

(c) protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

Such policies, procedures, and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by such non-consumer Originator, Participating DFI, or Third-Party Service Provider to initiate, process, and store Entries.

Each non-consumer Originator that is not a Participating DFI, each Third-Party Service Provider, and each Third-Party Sender, whose ACH Origination or Transmission volume exceeds 2 million Entries annually must, by June 30 of the following year, protect DFI Account Numbers used in the initiation of Entries by rendering them unreadable when stored electronically.

Each non-consumer Originator that is not a Participating DFI, each Third-Party Service Provider, and each Third-Party Sender, whose ACH Origination or Transmission volume exceeds 2 million Entries annually must protect DFI Account Numbers used in the initiation of Entries by rendering them unreadable when stored electronically no later than June 30 of the year immediately following the year in which such volume first exceeds the 2 million Entry threshold, and consistently thereafter regardless of annual volume.

Use of Prenotification Entries

- *Article Two, Subsection 2.6.1 (General Rule for Prenotifications)* – removes the limitation that prenotifications may only be used prior to the first ACH credit or debit entry.

- *Article Eight, Section 8.81 ("Prenotification Entry" or "Prenotification" or "Prenote")* – removes the limitation that prenotifications may only be used prior to the first ACH credit or debit entry.

ARTICLE TWO
Rights and Responsibilities of ODFIs, Their Originators, and Third-Party Senders

SECTION 2.6 Prenotifications

SUBSECTION 2.6.1 General Rule for Prenotifications

Prior to the initiation of the first credit or debit Entry to a Receiver's account with an RDFI, an Originator may originate a Prenotification Entry to the RDFI.

Prior to the initiation of future credit or debit Entries to a Receiver's account with an RDFI, an Originator may originate a Prenotification Entry to the RDFI.

ARTICLE EIGHT

Definitions of Terms Used in These Rules

SECTION 8.81 "Prenotification Entry" or "Prenotification" or "Prenote"

A Non-Monetary Entry initiated by an Originator to an RDFI prior to the initiation of the first credit or debit Entry to a Receiver's account with the RDFI. A Prenotification notifies the RDFI that the Originator intends to initiate one or more credit or debit Entries to a Receiver's account with that RDFI in accordance with the Receiver's authorization.

A Non-Monetary Entry initiated by an Originator to an RDFI prior to the initiation of future credit or debit Entries to a Receiver's account with the RDFI. A Prenotification notifies the RDFI that the Originator intends to initiate one or more credit or debit Entries to a Receiver's account with that RDFI in accordance with the Receiver's authorization.

Clarification of Terminology – Subsequent Entries

- Article Two, Subsection 2.4.2 (Exceptions to ODFI Warranties for Entries Originated Using Corrected Data from Notification of Change) – replaces general references "subsequent entry" to avoid potential confusion with the defined term "Subsequent Entry."
- Article Two, Subsection 2.6.2 (Waiting Period Following Prenotification Entries) - replaces general references "subsequent entry" to avoid potential confusion with the defined term "Subsequent Entry."
- Article Two, Subsection 2.12.1 (ODFI and Originator Action on Notification of Change) - replaces general references "subsequent entry" to avoid potential confusion with the defined term "Subsequent Entry."

ARTICLE TWO

Rights and Responsibilities of ODFIs, Their Originators, and Third-Party Senders

SECTION 2.4 General Warranties and Liabilities of Originating Depository Financial Institutions

SUBSECTION 2.4.2 Exceptions to ODFI Warranties for Entries Originated Using Corrected Data from Notification of Change

An ODFI that relies on the information contained within the Corrected Data field of a Notification of Change Entry or Corrected Notification of Change Entry makes no warranty under Subsections 2.4.1.2 (The Entry Complies with the Rules) and 2.4.1.4 (The Entry Contains Required Information) with respect to the corrected information in subsequent entries.

An ODFI that relies on the information contained within the Corrected Data field of a Notification of Change Entry or Corrected Notification of Change Entry makes no warranty under Subsections 2.4.1.2 (The Entry Complies with the Rules) and 2.4.1.4 (The Entry Contains Required Information) with respect to the corrected information in future entries.

SECTION 2.6 Prenotifications

SUBSECTION 2.6.2 Waiting Period Following Prenotification Entries

An Originator that has originated a Prenotification Entry to a Receiver's account may initiate subsequent Entries to the Receiver's account as soon as the third Banking Day following the Settlement Date of the Prenotification Entry, provided the ODFI has not received a Return or a Notification of Change related to the Prenotification. If the ODFI receives a Return Entry or a Notification of Change in response to the Prenotification by opening of business on the second Banking Day following the Settlement Date of the Prenotification, the Originator must not transmit subsequent Entries to the Receiver's account until it has remedied the reason for the Return Entry or made the correction requested by the Notification of Change.

An Originator that has originated a Prenotification Entry to a Receiver's account may initiate additional Entries to the Receiver's account as soon as the third Banking Day following the Settlement Date of the Prenotification Entry, provided the ODFI has not received a Return or a Notification of Change related to the Prenotification. If the ODFI receives a Return Entry or a Notification of Change in response to the Prenotification by the opening of business on the second Banking Day following the Settlement Date of the Prenotification, the Originator must not transmit additional Entries to the Receiver's account until it has remedied the reason for the Return Entry or made the correction requested by the Notification of Change.

SECTION 2.12 Notifications of Change

SUBSECTION 2.12.1 ODFI and Originator Action on Notification of Change (NOC)

An ODFI must accept a Notification of Change (also known as "NOC" and "COR Entry") or a corrected NOC that complies with the requirements of Appendix Five (Notification of Change) and is Transmitted by the RDFI within the time limits established by these Rules, unless otherwise provided for in this Section 2.12.

For each NOC or corrected NOC it receives, an ODFI must provide the Originator with the following minimum information within two Banking Days of the Settlement Date of the NOC or corrected NOC:

(a) Company Name;

(b) Company Identification;

(c) Company Entry Description;

(d) Effective Entry Date;

(e) DFI Account Number;

(f) Individual Name/Receiving Company Name;

(g) Individual Identification Number/Identification Number;

(h) Change Code;

(i) Original Entry Trace Number;

(j) Original RDFI Identification; and

(k) Corrected Data.

Except as noted below, the Originator must make the changes specified in the NOC or corrected NOC within six Banking Days of receipt of the NOC information or prior to initiating another Entry to the Receiver's account, whichever is later.

(l) The Originator may choose, at its discretion, to make the changes specified in any NOC or corrected NOC received with respect to any ARC, BOC, POP, RCK, Single-Entry TEL, Single-Entry WEB, and XCK Entry.

(m) In the case of CIE and credit WEB Entries, the ODFI or the Third-Party Service Provider (rather than the consumer Originator) must make the changes specified in the NOC.

(n) For an NOC that is in response to a Prenotification Entry, the Originator must make the changes specified in the NOC prior to originating a subsequent Entry to the Receiver's account if the NOC is received by the ODFI by the opening of business on the second Banking Day following the Settlement Date of the Prenotification Entry.

(n) For an NOC that is in response to a Prenotification Entry, the Originator must make the changes specified in the NOC prior to originating another Entry to the Receiver's account if the NOC is received by the ODFI by the opening of business on the second Banking Day following the Settlement Date of the Prenotification Entry.

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.