ORIGINATOR'S RESPONSIBILITIES
August 2, 2023

1. Required to comply with the Nacha Operating Rules and Guidelines and the warranties of the ODFI.
2. Required to justify ACH Return entries that exceed the established Return Rate levels:
    a. 0.5 percent unauthorized ACH Debit Return entries (Return Reason Codes R05, R07, R10, R11, R29 and R51)
    b. 3.0 percent administrative or account data errors ACH Debit Return entries (Return Reason Codes R02, R03 and R04)
    c. 15.0 percent all ACH Debit Return entries (excluding RCK entries)
3. No single ACH entry greater than $1 Million dollars ($1,000,000) or an entry with International ACH Transaction (IAT) Standard Entry Class Code is allowed to be a Same Day ACH transaction.
4. Any batch of ACH Credit and/or Debit entries submitted prior to 3:45 p.m. CT with an Effective Entry Date that is current day's date, invalid, or stale (in the past) will be processed at the next settlement opportunity which could result in same day processing of the entry.
5. Consumer Accounts – Notice by Originator to Receiver of Variable Debits
    a. Notice of Change in Amount – 10 calendar days prior to change
    b. Consumer may elect to receive notice only if amount falls within a specified range.
    c. Notice of Change in Date of Debit – 7 calendar days prior to change
6. Originators choosing to initiate Prenotifications must follow requirements of The Nacha Operating Rules and Guidelines. If a Prenotification is sent, live dollar entries may not be sent for three (3) banking days. Authorizations must be clear and readily understandable.
7. Originators must obtain the Receiver's authorization for entries and copies provided as required by the Nacha Operating Rules and Guidelines. Copies of authorizations are maintained for two years from the date the authorization is terminated and must be provided to the RDFI within ten banking days of the request. The Alternative to Proof of Authorization Rule allows an Originator to accept the return of a debit entry rather than expend the time and resources necessary to provide proof of authorization. If the RDFI requests proof of authorization it must be provided within ten days of the subsequent request.
    a. Corporate to Consumer (PPD) Credits – authorization required, oral or other non-written means accepted.
    b. Corporate to Consumer (PPD) Debits – written, signed, or similarly authenticated authorization required with copy provided to consumer.
    c. Consumer to Corporate (CIE) Credits – presumed agreement between consumer and company
    d. Destroyed Check entries (XCK) Debits – No authorization required (RDFI not required to accept these entries and should have the FI's policy on XCK entries documented in their internal procedures)
    e. Corporate Payment entries (CTX/CCD) Debits/Credits – agreement required for transfers between companies, written authorization implied.

    Note: Consumer Debit Authorizations must contain the minimum following information:
    1. Language clearly stating whether the authorization obtained from the Receiver is for a single entry, recurring entries, or one or more subsequent entries initiated under the terms of a standing authorization.
    2. The amount of the entry or entries, or a reference to the method of determining the amount of the entry(ies)
    3. The timing of the entries, including the start date, number of entries, and frequency of the entries
    4. The Receiver's name or identity
    5. The account to be debited (this should include whether the account is a demand deposit account or a savings account
    6. The date of the Receiver's authorization
    7. Language that instructs the Receiver how to revoke the authorization directly with the Originator. This must include the time and manner in which the Receiver must communicate the revocation to the Originator. For a single entry authorized in advance, the right of the Receiver to revoke authorization must provide the Originator a reasonable opportunity to act on the revocation instruction prior to initiating the entry

8. Entries that are returned as R01 or R09 may be reinitiated up to two additional times and within 180 days of the original Settlement Date. The word "RETRY PYMT" must be included in the Company Entry Description field to identify reinitiated entries to consumers on their periodic statements. The contents of the Company Name, Company Identification and amount fields of the Reinitiated Entry must be identical to the contents of the original entry. The contents of other fields should be modified only as necessary to correct an error or facilitate proper processing of the Reinitiated entry.
9. Originators receiving entries returned as "R07 Authorization Revoked by Customer", "R08 Payment Stopped", or "R10 Customer Advises Not Authorized" may not reinitiate these entries unless subsequent authorization of customer has been obtained. Originators should be aware that entries returned "R05 Unauthorized Debit to Consumer Account Using Corporate SEC Code" may not be reinitiated unless (a) subsequent authorization has been obtained, and (b) the Standard Entry Class Code has been corrected. Entries that are disputed by the customer as unauthorized, authorization revoked or unauthorized debit to consumer account using corporate SEC code may be returned through the ACH Network for up to 60 days from settlement date of the debit.
10. An Originator that has received a Return Entry Using Return Reason code R11 Customer Advises Entry Not in Accordance with the Terms of the Authorization") may correct, if possible, the error or defect in the original entry and transmit a new entry that conforms to the terms of the original authorization, without the need for re-authorization by the Receiver. The Originator must transmit the new entry within 60 days after the Settlement Date of the return entry. The following errors causing the return of the original entry as R11 cannot be corrected by the Originator, transmission of a new entry in these cases is prohibited: (1) if the Originator did not provide required notice for an ARC, BOC, or POP entry prior to accepting the check, or the notice did not conform to the requirement of the Rules; (2) if the source document for an ARC, BOC, or POP entry was ineligible for conversion
11. Originators receiving returns relating to Prenotifications which indicate that the RDFI cannot accept such entries will not initiate these entries.
12. Originators receiving Notification of Change entries are aware that requested changes should be made prior to the initiation of the next entry or within six banking days, whichever is later.
13. Originators ensure that reversing files and reversing entries are transmitted to the Receiving ACH Operator in such time to be transmitted or made available to the RDFI within five banking days following the Settlement Date of the duplicate or erroneous entry or file and within twenty-four (24) hours of the discovery of the error. The Originator must notify the Receiver before the reversing entry settles to the Receiver's account. The entry must be properly formatted with the term "REVERSAL" in the Company Entry Description field of the Company/Batch Header Record. The Company ID/Originator ID, SEC Code and Amount fields of the Reversing Entry must be identical to the original entry. The name of the Originator must reflect the same Originator identified in the Erroneous Entry to which the Reversal relates. (Minor variations to the Originator's name will be permissible for accounting or tracking purposes as long as the name remains readily recognizable to the Receiver). The contents of other fields may be modified only to the extent necessary to facilitate proper processing of the reversal. 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. A reversal can only be initiated for erroneous entries as defined in the Nacha Operating Rules and Guidelines. The initiation of Reversing Entries or Files for any reason other than those explicitly permissible under the Rules is prohibited. The RDFI is permitted to return an improper reversal.
14. Originators ensure that they clearly identify themselves in the Company Name field of an ACH entry through the use of a name that is known and readily recognized by the Receiver.
15. For all ACH transactions that involve the exchange or transmission of banking information (which includes, but not limited to, an entry, entry data, routing number, account number and a PIN or other identification symbol) via an Unsecured Electronic Network, Nacha Operating Rules require that such banking information be either:
    1. Encrypted communications using a commercially reasonable security technology that complies with current applicable regulatory guidelines, or
    2. transmitted via secure session using a commercially reasonable security technology that complies with current applicable regulatory guidelines.
    Transmissions or exchanges of banking information over an Unsecured Electronic Network by means of voice or keypad inputs from a wireline or wireless telephone to a live operator or voice response unit are not subject to this data security requirement.
16. The Originator is (1) in compliance with U.S. law, including, but not limited to, their obligations under programs administered by OFAC and FinCen to ask all employees paid via ACH if the entire net pay is being sent outside the territorial jurisdiction of the United States and if such net pay is being sent outside the territorial jurisdiction of the United States, the ACH entry is formatted as an IAT entry; (2) in compliance with the laws and payment system rules of the receiving country.

17. Originators are aware of their responsibilities in regard to the Data Passing Rule. This Rule prohibits sharing of certain customer information by Originators, Third-Party Service Providers and ODFIs for the purpose of initiating debit entries that are not covered by the original authorization.
18. The ACH Security Framework Rule requires Originators/Third Party Senders to implement and maintain security policies, procedures and systems related to the initiation, processing and storage of entries and resulting protected information. The policies, procedures and systems will protect the confidentiality and integrity of protected information until its destruction; protect against anticipated threats or hazards to the security or integrity of protected information until its destruction and will protect against the unauthorized use of protected information that could result in substantial harm to a natural person. Such policies, procedures, and systems will include controls on system access.
19. 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 two (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.
20. Originators/Third Party Senders are aware that upon receipt of a written request for a CCD, CTX or inbound IAT to a non-consumer account, an accurate record evidencing either the Receiver's authorization or the contact information for the Originator's name and phone number or email address has to be provided to the RDFI within ten banking days.
21. A Third-Party Sender must, upon the ODFI's request, provide the ODFI with any information the ODFI reasonably deems necessary to identify each Originator or other Third-Party Sender for which the Third-Party Sender transmits entries. A Third-Party Sender must also, upon the ODFI's request, provide the ODFI with the information necessary for the ODFI to complete Third Party Sender registration. The information must be provided to the ODFI within 2 Banking Days of receipt of the ODFI's request.
22. A Third-Party Sender must have an Origination Agreement with its Nested TPS(s).
23. A Third-Party Sender/Nested Third-Party Sender must conduct an annual audit of its compliance with the Nacha Operating Rules and must retain proof for a period of six years from the date of the audit.
24. A Third-Party Sender must conduct or have conducted, an assessment of the rules of its ACH activities, implement, or have implemented, a risk management program on the basis of such an assessment; and comply wit the requirements of its regulator(s) with respect to such assessment and risk management program.
25. Originators receiving return entries with Return Reason Code, R17 which includes the term "QUESTIONABLE" in the Addenda Information Field, will need to review returns more closely as this is indication the RDFI is returning an entry that does not have a valid account number and appears to be questionable, suspicious, or anomalous in some way.
26. Originators originating Return Fee entries should ensure the entry is authorized by notice in according with Nacha Operating Rules Section 2.14.2. The PPD SEC Code should be used for the entries. If the entry is authorized in a manner other than by notice, the SEC Code appropriate to the manner of authorization should be used. The Originator must submit Return Fee Entries as a separate batch that contains the words "RETURN FEE" in the Company Entry Description field of the Company/Batch Header Record. The Company Name field of the Return Fee Entry must be the same name of the Originator as identified in the Company Name field of the underlying Entry. The Return Fee amount should be the exact amount of the fee -not added to the original amount of the return entry. The Originator may impose only one Return Fee in relation to an underlying Entry or item that was returned, whether such Return Fee is collected via the ACH or otherwise. The Return Fee entry must have a Settlement Date within 45 days of the Settlement Date of the Return Entry of the underlying debit Entry or the return of the other underlying item.
27. The limitation on Warranty Claims for consumer accounts has two time periods: A limit for two years from the Settlement Date of the Entry and entries settling within ninety-five (95) calendar days from the Settlement Date of the first unauthorized debit to a consumer account. For non-consumer accounts, the warranty claim can be made for one year from the Settlement Date of the entry.
28. Standing Authorizations defined as an advance authorization by a consumer of future debits at various intervals can be obtained in writing or orally. Oral authorizations obtained via any channel will need to meet the requirements of an oral authorization. An Oral authorization obtained over the Internet that is not a telephone call will need to meet the risk and security requirements that currently apply to Internet-Initiated / Mobile (WEB) entries and will need to be originated with the WEB Standard Entry Class Code. Subsequent Entries (individual payments initiated based on a Standing Authorization) can be initiated in any manner identified in the Standing Authorization and can be initiated through voice commands, instructions, or affirmations. Flexibility is allowed in the use of consumer Standard Entry Class (SEC) Codes. The TEL or WEB SEC Code can be used for

Subsequent Entries when initiated by either a telephone call or via the Internet/wireless network, respectively, regardless of how the Standard Authorization is obtained. The authorization requirements of TEL or WEB will not need to be met; however, the requirements for risk management and security requirements associated with those SEC Codes will need to be met. Formatting for Payment Type Code field for TEL and WEB will be optional: (R) Recurring, (S) Single, (ST) Standing Authorization.

29. Originators obtaining electronic signatures for authorizations must ensure the electronic signatures comply with the terms of the Electronic Signatures in Global and National Commerce Act, including the provisions that reference state versions of the Uniform Electronic Transactions Act, including:
    - Being unique to the person using it
    - Verifiable, proof of authenticity
    - Under sole control of person using it
    - Process must guarantee the document signed cannot be altered.
    - Process must capture and preserve the signer's intent, consent, understanding, or responsibility related to a document that is being signed.
    - Consumer must be able to retain, store, print, or reproduce the information or else may be denied legal effect – Note: companies are not required to give customers an option to receive a paper contract.
    - Consumer must have given affirmative consent and must not have withdrawn consent.
    - Notice of right or option to have the record provided or made available on paper or in a non-electronic form, description of process to request, any fees.
    - Whether the consent applies only to the particular transaction that triggered the disclosure or to identified records that may be provided during the course of the party's relationship
    - Electronic signature must be attached to or located somewhere on the electronic document.

    Electronic signatures should evidence the identity of the person who signed and that person's assent to the terms of the record.
30. If your organization uses Micro-Entries (small value electronic (ACH) transactions used to validate an account that a customer is using to pay with or receive payments into) the total dollar amount of the Micro-Entry credit transactions must be equal to or greater than the value of the Micro-Entry debits. The result cannot be a net debit to the customer's account. Micro-Entries must be formatted with "ACCTVERIFY" in the Company Entry Description. The sender's name must be readily recognizable to the customer as the organization they are doing business with and be the same or similar to the name that will be used in future transactions.

    If an organization uses Micro-Entry debits to offset Micro-Entry credits (optional), it must send the debits and the corresponding credits at the same time and use the same Effective Entry Date. This ensures that all the transactions will reach the customer's account at approximately the same time, limiting the impact on the account balance. An organization that uses Micro-Entries may send future transactions to its customer's account as soon as the process for validating the Micro-Entries has been completed.

    Micro-Entries Rule, Phase 2, effective, March 17, 2023, requires an organization using Micro-Entries to use reasonable methods to recognize and prevent suspicious activity. At a minimum, volumes of sent and returned Micro Entry transactions must be monitored to recognize and address unusual activity. Another important mitigation is to recognize if the same or similar account number (ex. padded with zeros) is being used multiple times or for multiple customers.