ORIGINATOR'S RESPONSIBILITIES
March 20, 2026

Every year, the National Automated Clearinghouse Association (NACHA) publishes new rules that expand upon ACH services and/or requirements related to ACH entries. Campus Federal is committed to supporting your compliance with NACHA's Operating Rules and Originator Responsibilities for the transactions you originate through the Automated Clearing House (ACH) network.

Updated NACHA rules, processing deadlines, and retention periods are available on NACHA's website at www.nacha.org, including links to detailed information relevant to your needs. Free access was provided to you upon your initial set up for ACH services. Complete guides to NACHA Operating Rules and Guidelines are also available for purchase from NACHA's website. Below you will find rule changes since the last Originators Responsibilities update you received dated May 9, 2025.

1. COMPANY ENTRY DESCRIPTION – PAYROLL
    - Establishes a new standard description of "PAYROLL" for PPD Credits related to wages, salaries, and other similar types of compensation.
    - New language clarifies that the use of the term "PAYROLL" is descriptive and does not represent or warrant the Receiver's employment status by the Originator, ODFI, or any Third-Party Service Provider.
2. COMPANY ENTRY DESCRIPTION – PURCHASE
    - Establishes a new description of "PURCHASE" for e-commerce purchases.
    - New language defines e-commerce purchases as debit entries authorized by a consumer receiver for online purchases of goods, including recurring purchases first authorized online.
    - E-commerce purchases use the WEB debit SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL debit SEC Code.
3. FRAUD MONORTORING BY ORIGINATORS, TPSPS, AND ODFIS
    - Requires non-consumer Originators, ODFIs, Third-Party Senders (TPSPs), and Third-Party Service Providers (TPS) to establish and implement risk-based processes and procedures reasonably designed to identify ACH Entries and initialed due to fraud.
    - These processes must be reviewed at least annually and updated as needed.
4. DATA SECURITY & INFORMATION PROTECTION
    - Originators must protect banking and customer data by implementing appropriate security measures and strict data-handling controls.
    - As an ACH originator, your company plays a critical role in safeguarding Protected information. In the context of payment originators, Protected Information refers to non-public personal and financial data of a natural person used to create or contain within an ACH entry and it's related addenda. Protection this information is increasingly important due to rising threats like: corporate account takeovers, viruses, network intrusions, employee/email fraud and hacking.
    - To address these risks, your company is required to establish, implement and regularly update policies, procedures and systems designed to protect the confidentiality and integrity of Protected Information until its destruction, guard against anticipated threats or hazards to the security or integrity of Protected Information until its destruction and prevent unauthorized use of Protected Information that could cause substantial hard to a natural person.
    - For any banking information transmitted over an unsecured network, Originators must use either encryption or secure session technology (note: voice or keypad transmissions to an operator or IVR are excluded from this requirement).
    - ACH originators must not share customer information for initiating debits beyond what is covered by the original authorization.

- Non-consumer Originators with more than 2 Million annual entries must render stored DFI account numbers unreadable by June 30 of the following year and maintain this protection consistently thereafter.
- When responding to an ACH Receiver request to change account information, you must verify the request with a phone call or a trusted number on file – not one provided in an email request.
- Campus Federal encourages all ACH Originators to use dual authorization for the creation of ACH batches. Opting out of dual control increases the level of risk and originator liability.

5. WARRANTY CLAIM LIMITATIONS
    - Consumer Accounts: Warranty claims may be filed up to 2 years from the settlement date, and must include entries that settle within 95 calendar days of the Settlement Date of the first unauthorized Entry.
    - Non-Consumer Accounts: Warranty claims must be filed within 1 year of the settlement date.
6. ELECTRONIC SIGNATURES
    - Electronic signatures must comply with the E-Sign Act, including uniqueness, verification, consent, and retention.
7. SAME DAY ACH RESTRICTIONS
    - No single ACH entry over $1,000,000 may be Same Day ACH. IAT (International ACH Transaction) entries may not be Same Day ACH. Any batch submitted before 3:45 p.m. CT with an Effective Entry Date that is current, invalid, or stale will be processed at the next settlement, which may result in same-day posting.
8. AUTHORIZATION REQUIREMENTS
    - Originators must obtain clear, understandable authorization from the Receiver. Copies must be retained for 2 years after termination and provided within 10 banking days upon request.
    - Authorization types include:
        - PPD Credits: Oral or non-written authorization accepted
        - PPD Debits: Written, signed, or similarly authenticated authorization required Consumer debit authorizations must include, at a minimum:
            - Must state if authorization is for a one-time entry, a recurring entry, or future entries made under a standing authorization.
            - The Receiver's name or identity
            - The amount of the debit or the method for determining the amount
            - The timing of the debit(s), including start date and frequency
            - The account to be debited
            - The method for revoking authorization, including how and when the Receiver must notify the Originator
            - The date the authorization was obtained
        - CIE Credits: Presumed agreement
        - XCK Debits: No authorization required (RDFI may refuse)
        - CTX/CCD: Agreement required; written authorization implied
            - Upon request, Originators must provide authorization records or contact info within 10 banking days.
            - The Alternative to Proof of Authorization Rule allows the Originator to accept the return of a debit entry instead of providing proof of authorization.
9. VARIABLE DEBIT NOTICES FOR CONSUMER ACCOUNTS
    - Originators must notify consumers before variable debit changes:
        - Change in Amount: 10 calendar days prior
        - Change in Date: 7 calendar days prior

- Consumers may choose to be notified only when amounts fall within a specified range.

10. STANDING AUTHORIZATIONS
    - Standing authorizations may be written or oral. Subsequent entries may be initiated by voice or online instructions.
    - TEL or WEB SEC codes may be used for subsequent entries if security requirements are met.
11. PRENOTIFICATIONS
    - If Originators choose to send prenotes, they must follow Nacha rules. No live dollar entries may be sent for 3 banking days after a prenote is sent.
12. MICRO-ENTRIES
    - The total amount of Micro-Entry credits must be equal to or greater than Micro-Entry debits, so the customer's account is never left with a net debit. All Micro-Entries must include "ACCTVERIFY" in the Company Entry Description. Activity must be monitored for suspicious behavior or unusual patterns.
13. CLEAR IDENTIFICATION
    - Originators must use a Company Name that is recognizable to the Receiver.
14. ACH RETURN RATE REQUIREMENTS
    - Originators must justify ACH Debit return entries that exceed established return rate levels:
    - 0.5% unauthorized returns (R05, R07, R10, R11, R29, R51)
    - 3.0% administrative/account data errors (R02, R03, R04)
    - 15% of all returns (excluding RCK entries)
15. REINITIATING RETURNED ENTRIES
    - R01 (NSF) or R09 (Uncollected Funds) returns may be reinitiated up to two times within 180 days of the original settlement. "RETRY PYMT" must be in the Company Entry Description and the Company Name, ID, and Amount must match the original entry.
16. RESTRICTED REINITIATIONS
    - Entries returned as R07 (Authorization Revoked), R08 (Payment Stopped), and R10 (Customer Advises Not Authorized) may not be reinitiated without new authorization. Entries returned as R05 (Unauthorized Debit Consumer Account Using Corporate SEC Code) may only be reinitiated if authorization is obtained and SEC Code corrected. Unauthorized disputes may be returned up to 60 days from settlement.
17. CORRECTING R11 RETURNS
    - Entries returned as R11 (Customer advises not within Authorization Terms) may be corrected and re-submitted within 60 days without new authorization, unless the error is due to ARC/BOC/POP notice or eligibility issues.
18. ODFI-REQUESTED R06 RETURNS
    - ODFIs may request RDFIs to return an entry using R06 (ODFI Requested Return) for any reason. RDFI compliance is optional, but response is required within 10 banking days.
19. R17 RETURNS (QUESTIONABLE ACTIVITY)
    - R17 (File Record Edit Criteria / Entry Initiated Under Questionable Circumstances/ Return of Improperly-Initiated Reversal) returns containing "QUESTIONABLE" in addenda must be reviewed closely and within 24 hours of discovery, as they indicate potential fraud.
20. RETURN FEE ENTRIES
    - Return fee entries must be authorized and submitted in a separate batch clearly labeled "RETURN FEE." Only one fee may be submitted per returned item, and all submissions must be made within 45 days.
21. PRENOTIFICATION RETURNS
    - If a prenote is returned indicating the RDFI cannot accept the entry, the Originator must not initiate the entry.

22. NOTIFICATION OF CHANGE (NOC) HANDLING
    - Originators must update requested changes before the next entry or within 6 banking days, whichever is later.
23. REVERSALS (DUPLICATE OR ERRONEOUS ENTRIES)
    - Reversals must be sent within 5 banking days of settlement or 24 hours of discovery.
    - Must include "REVERSAL" in Company Entry Description and the Receiver must be notified before the reversal settles. Debit reversals cannot be dated earlier than the original credit.

FRAUD SCENARIOS

BUSINESS EMAIL COMPROMISE SCHEMES

Business email compromise schemes occur when the legitimate email account of a business officer is either compromised or impersonated and used to order or request the transfer of funds. An employee transfers funds to the fraudster believing the order was from a reputable company email address owned by an officer with authority to execute those orders.

VENDOR IMPERSONATION FRUAD

Vendor impersonation fraud occurs when a business, public sector agency or organization receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The fraudster is paid by the business, agency, or organization when the real contractor submits an invoice for the work done or good sold. Public sector organizations are frequently targeted because contact information is often in public record.

PAYROLL IMPERSONATION FRAUD

Payroll impersonation fraud targets employees and human resources departments. A fraudster will impersonate an employee and contact the HR department directly or through the employer's payroll portal using stolen credentials. The fraudster requests to change the account where the employee's regular payroll is deposited. Once updated, the employer pays the fraudster rather than the employee.