RED RIVER BANK

ACH Rules and Updates for
Business Originators

ANNUAL NOTICE TO ACH
ORIGINATION CUSTOMERS

Every year, the National Automated Clearinghouse Association (Nacha) publishes new rules that expand upon ACH services and/or requirements related to ACH entries. Red River Bank 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. Complete guides to Nacha Operating Rules and Guidelines are also available for purchase from Nacha's website.

UPCOMING RULE CHANGES

The following rule changes take effect March 20, 2026, but may be adopted earlier:

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 standard 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 MONITORING 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 initiated due to fraud.

FRAUD MITIGATION:
PREVENTING FRAUDULENT ACH TRANSACTIONS

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 contained within an ACH entry and its related addenda. Protecting this information is increasingly important due to rising threats like:

- Corporate account takeovers
- Viruses
- Network intrusions
- Employee/email fraud
- 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.
- Prevent unauthorized use of Protected Information that could cause substantial harm to a natural person.

Additionally, when responding to an ACH Receiver requests to change account information, you must verify the request with a phone call to a trusted number on file – not one provided in the email request.

Red River Bank 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 customer liability. Please contact Treasury Support at (318) 561-5864 with any questions regarding dual authorization or to opt in to this service if you have previously opted out.

CREDIT PUSH 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 FRAUD

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

RED RIVER BANK

STANDARD ENTRY CLASS CODE

A Standard Entry Class Code (SEC) is a mandatory three-character code that is used in all batches to identify the various types of entries within a batch.

Using the correct SEC code helps you limit your liability for return entries, and helps you avoid potential fines that may be assessed for using the improper SEC codes:

PPD – PRE-ARRANGED PAYMENT OF DEBIT

- Most commonly used for direct deposit
- For business to consumer use only
- Written authorizations must be on file with recipient if you are debiting their account

CCD – CASH CONCENTRATION OR DISBURSEMENT

- For business to business use only
- Can be used for moving funds between a business's own accounts at different institutions
- Used for payments or debits to other businesses

If you have any questions about ACH or any of our Treasury Management products, please contact us at (318) 561-5864.