TEXAS PARTNERS BANK

Treasury Management

Important ACH Reminders and NACHA Rule Updates

This overview provides valuable information to be aware of as an originator of ACH transactions. ACH Originators must comply with the requirements associated with the type of ACH entry sent according to the NACHA Operating Rules & Guidelines. The following are reminders of compliance with NACHA ACH Operating Rules and highlights of the 2026 NACHA rule changes.

Upcoming Rule Changes — Effective Date

Standard Company Entry Descriptions – Payroll & Purchase .... March 20, 2026
Fraud Monitoring by Originators, TPSPs and ODFIs (Phase 2) .... June 22,2026

Standard Company Entry Descriptions – PAYROLL & PURCHASE

Standard Company Entry Description - PAYROLL

This rule establishes a new standard description for PPD Credits for payment of wages, salaries, and similar types of compensation. The Company Entry Description field must contain the description “**PAYROLL.”** All Originators will be required to use the new description “PAYROLL” for all PPD credits for the payment of wages, salaries, or other similar types of compensation no later than March 20, 2026. This is a “no later than’ effective date. Originators are encouraged to adopt this description for all types of compensation payments as soon as practical.

Standard Company Entry Description – PURCHASE

This amendment establishes a new standard description for e-commerce purchases; the Company Entry Description field must contain the description “**PURCHASE.”** 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 debit SEC Code, except as permitted by the rule on Standing Authorization to use the TEL SEC Code.

Fraud Monitoring by Originators, TPSPs and ODFIs (Phase 2)

This rule amendment requires all non-Consumer Originators, Third Party Service Providers, and Third-Party Senders to establish and implement risk-based processes and procedures reasonably intended to identify ACH Entries initiated due to fraud.

Each of these parties will be required to:

- Establish and implement risk-based processes and procedures, relevant to the role played in the authorization or transmission of entries, which are reasonably intended to identify entries suspected of being unauthorized or authorized under false pretenses.
- Review these processes and procedures at least annually and make appropriate updates to address evolving risks.

General Responsibilities for ACH Originators

ACH Originator Responsibilities

- Obtain proper authorization dependent on transaction type and retain authorizations for two years past revocation. Provide copy of authorization if requested by the financial institution within ten banking days of request.
- Give appropriate notice to receiver if changing the amount or date of a transaction.
- Protect your banking information and the systems used for origination.
- Make necessary changes to payee account information within six banking days when notified by the bank of a NOC (Notice of Change) to an ACH transaction originated.
- Cease subsequent entries if unauthorized/revoked ACH returns (R05, R07, R10, R29, R51) are received until you obtain a new authorization. For a complete list of return codes, refer to the NACHA Operating Rules.
- Check ACH payees against the OFAC compliance checklists.
- Ensure that information included in the NACHA ACH File is accurate and follows the technical specifications of NACHA ACH origination.
- Ensure that your computers are protected from corporate account attacks and takeovers.
- Educate your users about potential fraud schemes, including social engineering attempts.
- If your company originates ACH entries on behalf of another entity and you have not informed the Bank, please contact us immediately.

Direct Deposit Payroll Authorizations

- The Bank recommends you use direct deposit authorization forms to obtain authorization to debit employee accounts for adjustments. These forms may also be used to collect employee account information.
- The most common SEC code for direct deposit for consumers is PPD.
- Retain original authorization or a copy of each authorization for two years after termination or revocation of such authorization.

Consumer Debit Authorizations

- For consumers, an authorization to debit their account must be in writing or "similarly authenticated."
- The most common consumer SEC code is PPD (prearranged payments and deposits used for debits and credits).
- Retain original authorization or a copy of each authorization for two years after termination or revocation of such authorization as stated in the NACHA Operating Rules.

Corporate Authorizations

- For companies, there must be an agreement between the two parties. However, the rules do not define what business practices constitute an agreement.
- The most common corporate SEC codes are CCD (corporate credits and debits) and CTX (corporate trade exchange).

Changing Date or Amount of Debits

- ACH Rules require notification to your debtors of any changes in date or amount, complying with the following timelines:
  a.) Change in date for both consumer and corporate requires a notification of seven calendar days,
  b.) Change in amount for consumer only is ten calendar days.
- Sending the notice via U.S. Mail is acceptable, however, a best business practice is multiple communication channels to ensure your customer receives timely communication.

Pre-Notifications (Prenotes)

- The purpose of a prenote is to verify account information.
- Prenotes are zero-dollar entries that precede the first live ACH transaction and must precede the first live entry by at least three banking days.
- The Receiving Bank is not required to validate the name of the payee on the prenote, they are only required to validate the account number. This poses a risk for you as an Originator if the subsequent entry debits or credits the wrong account. This risk applies to all ACH originations, not just prenotes.

Notice of Change (NOC

- When ACH information is incorrect, a Notification of Change "NOC" is sent by the Receiving Bank requesting that future entries contain correct information. ACH Rules requires you to make the change within six banking days of receiving the information from the bank.
- The Receiving Bank warrants that the information they provide is correct.
- Prosperity Bank, as an originating bank, will notify you of any NOCs received. Any fines for non-compliance received from the National Automated Clearing House Association (NACHA) may be assessed to you.

Returns

- ACH returns must be processed by the Receiving Bank within 24 hours of settlement. Returns that are unauthorized beyond the 24 hours are the company's liability and any disputes may have to be settled outside the banking network. We recommend you view your account activity daily.
- An exception to the 24-hour rule is for consumer unauthorized returns, which may be returned within sixty calendar days of posting through the ACH network.
- The use of consumer (PPD) or corporate (CCD) entry codes determines applicable ACH return rules.
- If the Receiving Bank receives a dispute claiming a debit was unauthorized, the Receiving Bank must obtain a signed Written Statement of Unauthorized Debit from the account holder.
- As an Originating Depository Financial Institution (ODFI), we will notify you of any ACH returns received for your company.
- You may reinitiate a debit entry up to two times if you receive a return entry of "NSF" or "Uncollected Funds." It is a violation of ACH Rules to reinitiate the debit entry if a return is received for any other reason. All reinitiated entries must include the description "**RETRY PYMT**" in the Company Entry Description field to identify the entries.

ACH Reversals

- Reversals may only be sent for the following three conditions: 1) wrong dollar amount, 2) wrong account, or 3) duplicate transaction.
- The reversing entry must be for the full amount and must be sent within five banking days of original entry (effective entry date) and within 24 hours of discovering the error.
- For wrong amount or wrong account reversing entries, a correcting entry must also be sent.
- The Receiving Bank is under no obligation to post the reversing debit if it overdraws the payee's account or if the payee's account is closed.
- A payee must be notified if a reversing entry debits their account. However, a payee does not need to authorize the reversing debit.

Office of Foreign Asset Control (OFAC)

- An ACH Originator is required to check payees against the OFAC compliance checklists.
- The Office of Foreign Asset Control (OFAC) lists countries, groups, and individuals that U.S. companies are not allowed to send or receive funds from. It is against the law for company Originators to send debit or credit entries to OFAC-blocked entities.
- Originators may check the OFAC SDN list at ofac.treasury.gov.

Security

- It is your responsibility to protect your online banking access and utilize best business practices in protecting your account(s). Best business practices may include initiating ACH transaction with dual approval, monitoring accounts and transactions daily, and taking reasonable steps to maintain confidentiality and security of online banking access credentials. Ensure all confidential information is encrypted or sent when electronically submitting.
- Ensure that only users designated by your company Administrators have the authority to originate ACH transactions and that user limits and user access are monitored regularly. Notify the Bank immediately if the authority of any Lead Administrator(s) has changed or has been revoked.
- Maintain the physical, electronic, procedural, administrative, and technical security of data and systems to safeguard against unauthorized transactions.
- Limit access and securely store any ACH data used in the routing and settlement of ACH transactions.
- Implement internal guidelines to verify any requests for changes to payees and bank routing information. This is a common source of fraudulent activity. Verification with your payee prior to implementing the change is recommended.

Fraud Prevention

- Educate your representatives and employees as to the risks of fraud and contact us if you have identified a possible fraudulent situation. Each company should evaluate its risk of corporate account takeover, business email compromise and other fraud to implement measures to minimize this risk for your business.
- Monitor your accounts regularly, reviewing your account statements and activity to ensure all transactions posted are ones you have authorized.
- Be suspicious of any e-mail with urgent requests for financial information, personal information, or to change ACH information for a vendor or payee. Always confirm transaction changes by calling the number you have on file for your vendor or payee.
- Be cautious about opening any attachments or downloading any files, regardless of who sent them.
- Never give out your passwords or account credentials to anyone and do not share online credentials between company users. Never use the same password across your online accounts.
- Never throw away ATM receipts, credit cards, or bank statements in a usable form.
- Keep your anti-virus software up to date, use a firewall on your computer, and secure your wireless network.
- Encrypt devices and other media that contain sensitive information, including laptops, tablets, smartphones, removable drives, and cloud storage solutions.
- Keep all staff updated on fraud prevention and new risks and vulnerabilities.
- Consider enrolling in ACH payment blocks and filters to prevent unauthorized ACH items from posting to your account.
- Contact us to enroll in Prosperity's Check Positive Pay service, ACH Positive Pay or both. Payee match is recommended to be added to your Check Positive Pay service. Altered payee fraud continues to increase so adding this feature can help to minimize this type of fraud.

Please note this document does not represent the complete list of ACH requirements and is not intended to be legal advice. The NACHA Operating Rules & Guidelines govern the proper use of the ACH network and may be purchased online at www.nacha.org/store. More details on the rule changes can be found at www.nacha.org/rules/operating-rules.

If you have questions, contact Treasury Management Support at 800-814-4948 or treasurymgmt.service@texaspartners.bank.