Grand Bank Annual ACH Education 2026

*As an Originator of ACH entries at Grand Bank, it is important for you to stay up to date with the current ACH rules and fraud trends. Please review the information below in full and contact us with any questions. *This document is not all inclusive.*

2026 Rule Changes & Updates

Effective March 20, 2026

There is a new Standard Company Entry Description – "**PAYROLL"**. This description is required to be in all capital letters in the ACH Entry Description field of the batch header.

The **PAYROLL** 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 types of compensation.

- The objective of adding **PAYROLL** as an 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.

Reinitiation of Return Entries

An Originator may reinitiate an entry that was returned if:

- The entry was returned for insufficient or uncollected funds (the entry cannot be reinitiated more than twice within 180 days following the return of the original entry).
- The entry was returned for stopped payment and reinitiation has been authorized by the Receivers; or
- The Originator has taken corrective action to remedy the reason for the return.

All reinitiated entries must include the description "**RETRY PYMT**" in the ACH Entry Description field. Identical content to the original entry is required for the Company Name, Company ID, and Amount.

Reversals

In the event an erroneous or duplicate entry is originated, the ACH Rules allow the Originator to reverse the transaction. The following Rules must apply:

- The Reversal must be transmitted within 5 banking days from the Settlement Date of the erroneous or duplicate transaction.
- The word "**REVERSAL**" must appear in the ACH Entry Description field of the batch header.
- You are required to reach out to the payment recipient to inform them the reversal is in progress.

Note: Reversals are requests. They are not mandatory transactions for the receiving bank, and they do not guarantee you will recover any funds. Banks do not have to overdraw the receiver's account to process a reversal, and the reversal may be returned.

Notification of Change (NOC)

If the information on a transaction you originated is incorrect, you may receive a Notification of Change (NOC) from Grand Bank alerting you to correct the information.

- This information may include the routing number, account number, or account type (Checking vs Savings).
- Grand Bank will notify you via email of any NOCs received.
- The ACH Rules require your company to make the requested changes within 6 banking days of the receipt of the NOC or prior to the initiation of another ACH entry.
- By complying with the NOC, you can originate future transactions without having to obtain a new authorization.

Standard Entry Class (SEC) Codes

SEC Codes are used to identify how a payment was authorized by the recipient. You must use the correct SEC Code to identify your ACH batch. Grand Bank processes three SEC code options.

- **PPD -** Used for debit and credit transactions when the Receiver is a consumer (defined as a live person)
- **CCD -** Used for debit and credit transactions when the Receiver is a corporation or business/organization
- **CTX -** Corporate Trade Exchange – Payments to a Corporation (Business)

Note: You cannot combine different SEC types (consumer and business) within a single batch. Different SEC codes are required based on the recipient type.

Authorizations

As an Originator, you are required to obtain authorization from the Receiver which allows you to originate a transaction to or from their account. Authorizations must be retained for 2 years beyond the life of the payments.

- Consumer Credits (**PPD**)– Must have either oral or written authorization from the Receiver
- Consumer Debits (**PPD**) – Must have written authorization from the Receiver.
- Corporate Credits or Debits (**CCD, CTX**) – There is no rule dictating the form of the authorization. A written authorization is implied.

Note: We recommend that you use an authorization agreement that states you are authorized to debit/reverse any entries made in error. This will help avoid future disputes.

Security

As an ACH originator you are required to have policies and procedures in place regarding the initiation, processing, and the storage of personal, non-public information. The policies and procedures must accomplish the following.

- Protect the confidentiality and integrity of the personal, non-public information, including financial information that you have on file. Other non-public information you may have on file includes EIN or Tax ID numbers, dates of birth, social security numbers, and addresses.
- Protect against anticipated threats and/or hazards that would threaten the security of protected information until its destruction.
- Protect against the unauthorized use of that protected information which could cause harm to that individual and/or business.

Fraud Watch

Fraud schemes and scams are an ever-evolving threat that can impact anyone at any time. From phishing emails to AI generated videos, scams are becoming more sophisticated, targeted, and dangerous. As scams account for billions of dollars in losses each year, it is imperative that you are aware of the different types of fraud schemes and implement internal controls to combat them.

Business Email Compromise

According to the Federal Bureau of Investigation (FBI), Business email compromise is one of the most financially damaging online crimes. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request.

For example: A vendor you deal with regularly sends an invoice with updated ACH or wiring instructions. In good faith, you update the information and process the payment. Unfortunately, the vendor's email had been comprised, and the instructions came from a scammer. The funds are sent to the fraudster, and you may not be able to recover them.

To conduct this kind of fraud a scammer may:

- **Spoof an email account or website** - Slight variations of legitimate addresses fool victims into thinking fake accounts are authentic.
- **Send spearfishing emails** – Messages look like they are from a trusted source to trick victims into revealing confidential information.
- **Use Malware** – Malware can infiltrate company networks and gain access to their email accounts. It can also give criminals undetected access to passwords and financial account information.

To Protect yourself:

- Don't click on links or images in unsolicited emails or text messages.
- Carefully examine the email address, URL, and spelling used in any correspondence.
- Verify payment instructions in person or by calling a pre-determined phone number (not one included in the same email).

It is also essential that all computer equipment your company uses to process ACH is regularly updated and patched for security vulnerabilities (including use of and updates to firewall and virus protection).

Insider Threats

This kind of fraud occurs when an individual with legitimate access, such as an employee or contractor, maliciously or accidentally misuses their position to commit fraud for personal gain or to harm the company. Here are some examples:

- **Data Theft** – A disgruntled employee stealing sensitive data or intellectual property to sell to competitors. This can also occur by accident if an employee unknowingly leaks data to external threats.
- **Sabotage** - An insider with authorized access deliberately damaging or corrupting data to disrupt operations.
- **Fraud** – Manipulating financial records or diverting funds for personal use. ACH fraud is common among these cases.

Implementing security measures such as Dual Control and limiting employee access to systems and services can help prevent the risk of insider threats.

Account Takeover Fraud

This type of fraud occurs when a scammer obtains access to the credentials of a personal or business bank account and uses it to send funds to their own accounts. The scam artist can

quickly deplete entire accounts using this method. Criminals will use multiple methods to execute these attacks, including phishing, malware, and credential stuffing by using credentials leaked during data breaches and purchased on the dark web.

For example: You may receive a phone call or text that appears to be from your bank but is actually a scammer trying to gain access to your account. Scammers can easily 'spoof' phone numbers to make it look like they are calling from your bank and will try to create a sense of urgency to encourage you to give them information or access to your account.

To protect yourself:

- Be aware of the information you display online and on your social media accounts.
- Always keep two-factor authentication (2FA) codes private. Do not provide them via phone, text, or email to another party.
- Use strong unique passwords for all your accounts.
- Enable multi-factor authentication (MFA) whenever possible.
- Verify any unexpected communications or requests before proceeding. Do not click any links in unverified emails or texts.
- Monitor your accounts regularly for fraudulent activity.
- Set up alerts to warn you of activity that may not be legitimate.

Here are some tools Grand Bank has in place to protect your online account security:

- Account logins are protected by 2-Factor Authentication (2FA) when logging in from a new/unrecognized device or browser.
- High Risk Activities such as transferring funds or changing login information are also protected by 2-Factor Authentication (2FA).
- Automatic notifications are sent out to users when a new device is logged into.
- New devices for users with an existing device will be blocked from high-risk activities for 7 days. You can verify these devices using your regularly used device. Please contact us to unblock new devices if needed.

We take your account security very seriously. Contact us right away to verify any unusual messages, especially those asking for information or stating there is fraud on your account.

Additional Fraud Resource Links:

- Protecting Against Cyber Fraud
- Common Frauds and Scams
- Scams Mitigation Toolkit

2026 Federal Holiday Schedule

The Federal Reserve and Grand Bank are closed, and ACH will not process on these days.

- New Year's Day **(January 1)**
- Martin Luther King, Jr. Day **(January 19)**
- President's Day **(February 16)**
- Memorial Day **(May 25)**
- Juneteenth **(June 19)**
- Independence Day **(Observed July 6)**
- Labor Day **(September 7)**
- Columbus Day **(October 12)**
- Veterans Day **(November 11)**
- Thanksgiving Day **(November 26)**
- Christmas Day **(December 25)**

GRAND BANK™

Member FDIC