ACH Origination
Annual Customer Information Training

Revisions to the NACHA Operating Rules (Your company will need to do these)

Annually, you will receive a letter from the bank explaining changes in the NACHA (National Automated Clearing House Association) rules. These changes are described in the Revisions to the NACHA Operating Rules section of the rule book. The changes will cover the time period of January 1 to December 31 of that year. If you have questions about the revisions, please contact us. Changes that will affect you are listed below.

1. Standard Company Entry Descriptions – Payroll and Purchase

Summary:
The Standard Company Entry Descriptions Rules will establish two new Company Entry Descriptions, PAYROLL and PURCHASE. The PAYROLL Company 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 similar types of compensation. The objective of adding PAYROLL as a Company 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.

The Rule will also establish the Company Entry Description PURCHASE, which must be used for e-commerce purchases. An e-commerce purchase will be defined as a debit entry authorized by a consumer Receiver for the online purchase of goods. The new Company Entry Description will enable identification of such e-commerce transactions. The Rule defines e-commerce purchases for the purpose of using the new Company Entry Description.

Impact to Participants:
Originators that handle payroll and e-commerce purchase transactions will need to update their systems to utilize the required Company Entry Description.

Effective Date:
The effective date for the Standard Company Entry Description rule is **March 20, 2026**. Originators may begin using the new descriptions as soon as practical, but must do so no later than **March 20, 2026**.

2. Fraud Monitoring by Originators.

Summary:
The Fraud Monitoring by Originators will require each non-consumer Originator to establish and implement risk-based processes and procedures reasonable intended to identify ACH entries initiated dure to fraud. Each of these parties will need to review at least annually their processes and procedures and make any appropriate updates to address evolving risks. The objective of the Rule is to reduce the incidence of successful fraud attempts through regular fraud detection monitoring.

Impact to Participants:
Originators, these entities may need to implement fraud detection processes and procedures if they are not doing so currently. There may be less of an impact for these Originators that have already implemented commercially reasonable fraud detection for WEB debits and/ or for Micro-Entries.

Effective Date:
The Rule will be implemented in two phases:
Phase 1 – does not apply.
Phase 2 – **June 19, 2026** – the Rule will apply to non-consumer Originators.

What is Same Day ACH (SDA)?

Same Day ACH gives the ability for an ACH file to be sent and received in the same day. What is needed to do a Same Day ACH?

- Each item within the file cannot exceed $1,000,000.00 (as of March 18, 2022)
- The total of the file, cannot exceed $1,000,000.00
- The SDA file has to be received at the bank by 11am (CT)
- You will need to contact the bank to tell them you want to send a SDA file
- There is an additional cost for SDA: $10.00 per file plus two times the per item fee

Same Day ACH will ONLY be available as a contingency basis. Same Day ACH will allow you to originate your credit/debit file on the same day as the effective date if needed. You will need to contract the Digital Banking area to have this feature turned on for a one time Same Day ACH submission. When you send a Same Day ACH file, the receiving institution has to have the funds posted to the receiver's account by 5:00pm (Receiving Institution's Local Time).

What are the Fraud Risks for ACH?

Origination fraud is not new to ACH. Origination fraud occurs when an originator or third party generates invalid transactions using the name of the true originator. Use of the Internet and web-based ACH origination systems has created this new vulnerability.

In one origination system hijacking scheme, perpetrators hack into the originator's (your company) computer system using compromised User IDs and passwords and originate ACH credits to "mule" accounts created for the express purpose of committing fraud. Those accounts are then emptied and abandoned. The true originator's account (your account) is debited for the invalid origination file. The credits are usually irretrievable by the time the fraud is discovered. The originator's credentials may have been compromised by an insider within the organization or stolen through key loggers or Trojan Horse programs on the compromised computer.

Due to the risk of this type of fraud, it is essential that all computer equipment used by your company to operate Citizens Bank's Digital Banking ACH Origination software is regularly updated and patched for security (including use of and updating of firewall, virus protection, malware protection, anti-spam protection). The appropriate steps should be taken within your company to ensure that all User ID's, Passwords, Authentication Methods and any other applicable security procedure issued to your employees are protected and kept confidential and that all staff understands the need for proper user security, password controls and separation of duties.

What types of controls are in place to help us combat ACH Origination fraud?

Citizens Bank's Digital Banking utilizes multi factor authentication. A device/profile database per user is created through Internet data profiling by looking at the IP addresses that the customer uses to log on, their ISP provider, their geographic locations and their connection type. After the device/profile has been created, when logging on from a PC at a location they have not signed on from before, the user's personal challenge questions may appear to verify their identity.

VeriSign VIP tokens provide hacker-resistant multi-factor authentication for online banking transactions by generating a one-time authentication code that changes every 30 seconds. The result is a unique, one-time-use pass code that positively authenticates the user and only permits access to Digital Banking if the code is validated. An email message is sent immediately after an ACH file is initiated to the bank. The email should be reviewed to validate the amount of the ACH file that was submitted. While all of these steps will hamper a hacker from gaining access outside of your company, the risk still exists for internal fraud by one of your employees or from a hacker who has gained access to your computer system through sophisticated key loggers or Trojan Horse programs.

Citizens Bank encourages companies to have separation of duties for ACH processing, in which one employee generates the ACH batch and the system requires a secondary employee to log in and approve the ACH batch known as Dual-control. Dual-control procedures such as this go a long way in preventing ACH origination fraud. It is also very important for your company to make it a practice of monitoring your accounts online daily. Checking your "Transaction History" screens daily within the Cash Management program will ensure that you are aware of all transactions, even when they have not yet posted to your account. The sooner ACH fraud is detected; the more successful the Bank will be in assisting to recover your company's potentially lost funds.

What is the ACH Network?

The Automated Clearing House (ACH) Network is an electronic payments network used by individuals, businesses, financial institutions and government organizations. The Network functions as an efficient, electronic alternative to paper checks. It allows funds to be electronically debited or credited to a checking account, savings account, financial institution general ledger account or credited to a loan account.

The ACH Network is a batch processing, store-and-forward system. Transactions are stored by financial institutions throughout the day and processed at specified times in a batch mode. This provides significant economies of scale and faster processing than check payments. All transaction information necessary to process a transaction accompanies the ACH entry.

Who Are the ACH Participants?

There are five key participants that contribute to the successful completion of an ACH transaction:

1. Your company is the **Originator** and has been authorized by the Receiver (consumer or company) to either credit or debit their account. When your company initiates a credit transaction to your employee's account for payroll or to a business customer's account for payment of goods and services, you are considered the Originator. Originators may also initiate debit transactions to a consumer or business account for payment of goods or services.
2. The **Receiver** can be either an individual or a company that has authorized the Originator (your company) to credit or debit their account. An employee is the Receiver if their company is initiating a payroll credit. A business partner is the Receiver if the Originator is sending a credit to pay for goods or services. The Originator can also be a Receiver, in situations where another party is initiating credits or debits to their account. The authorization is a key component of the ACH transaction, as it gives your company as the Originator the authority to send credit or debit transactions to the Receiver's account. Crediting a consumer requires only an oral agreement; however a consumer debit must always have a written agreement. For a company, whether a debit or credit transaction, a written agreement is required.

3. The **Originating Depository Financial Institution (ODFI)** is the financial institution that your company has a contractual relationship with for ACH services and is responsible for sending ACH entries into the ACH Network on your behalf.
4. The **ACH Operator** is the central clearing facility for ACH transactions. The ACH Operator is responsible for accepting files of ACH entries from ODFIs, which are then sorted and batched and forwarded to the Receiver's financial institution. The ACH Operator also performs some editing functions, insuring that mandatory information required in each ACH record is included.
5. The **Receiving Depository Financial Institution (RDFI)** is a financial institution with which the Receiver has an account relationship. Credit or debit entries sent to a Receiver's account will be received by the RDFI from the ACH Operator and then posted to the Receiver's account.

How Does the ACH Network Function?

As the Originator, your company must first obtain authorization to initiate a transaction to the Receiver's account or provide notice to the Receiver that a transaction will be initiated to their account. Your company (Originator) then creates a file of ACH transactions assigning a company name that is easily recognized by the Receiver. The file is then sent to your Originating Depository Financial Institution (ODFI), which may be a bank or credit union.

The ODFI collects ACH files from Originators with which it has contractual relationships, verifies the validity of these files and at specified times, transmits these files to the ACH Operator. The ACH Operator receives ACH files from the ODFI, edits the file to make sure they are formatted properly and distributes files of entries to the Receiving Depository Financial Institution (RDFI). The RDFI receives files of entries from the ACH Operator for its account holders. Entries are posted based upon the Settlement Date and account number. Periodic statements are provided to the Receiver with descriptive information about the ACH transaction, including the date of the transaction, dollar amount, payee (Originator) name, transaction description (Ie. payroll, water bill).

How Are ACH Funds Settled?

Settlement is the actual transfer of funds between financial institutions to complete the payment instructions of an ACH entry. The Federal Reserve Bank provides settlement services for ACH entries. The timing of settlement is based upon the Effective Entry Date indicated on the ACH file and the time of its delivery to the ACH Operator. Your company as the Originator will determine the Effective Entry Date of the file you send to your ODFI. This is the date your company intends the entries to post to the accounts of the Receivers (employees or customers). When the ACH Operator processes an ACH file, the Effective Entry Date is read and entries are settled based upon that date, known as the Settlement Date. The Effective Entry Date in most cases is the same as the Settlement Date, but it is possible that the Settlement Date could be after the Effective Entry Date. For example, if the ACH Operator cannot settle on the Effective Entry Date due to untimely file delivery, a stale date, weekend or holiday, the ACH Operator will apply a Settlement Date of the next business day.

What is a Pre-notification (Pre-note)?

Pre-notifications (pre-notes) are zero-dollar entries used by your company to verify that the account number, routing number and account type on an entry is valid at the RDFI. Pre-notes are optional and can be sent with any ACH application. Pre-notes are originated similarly to valued ACH entries, except that special transaction codes are used and a zero dollar amount is indicated. If your company chooses to send pre-notes, you should do so at least six banking days before sending the first live dollar entry. If there are any errors in a pre-note entry or it cannot be

processed, a Notification of Change (NOC) or Return will be sent back to your bank by the RDFI to notify your company of the necessary corrections to be made.

What is Pre-Funding?

In the case of ACH Credit Entries originated by Company, sufficient Available Funds must be in the Pre-Funding Account before Company transmits the ACH File to the Financial Institution, and, in all instances, a cut off time of 1pm (CT) and minimum of two (2) Business Days prior to Settlement Date, or Company's ACH Credit Entries may not be processed. Funds will be withdrawn at the time the ACH File is initiated. Financial Institution is under no obligation to hold the ACH File until Available Funds are in the Account and then process same ACH File, although Financial Institution may do so at its discretion. If the Financial Institution holds the ACH File until the account is funded, and the account is funded after the effective date of the original file transmission, the effective date will be changed by the Financial Institution to the earliest available Business Day and the ACH File will be processed. Financial Institution is under no obligation to contact Company in the event of insufficient Available Funds to process Company's requested Entry.

What is an ACH Return?

An ACH return is an ACH entry that the RDFI is unable to post for reasons defined by the various return codes (see common ones below). An RDFI may use the return process for pre-notifications as well as for valued ACH entries. The RDFI must transmit the return in time for your ODFI to receive it by opening of business on the second banking day following the Settlement Date of the original entry, also referred to as the "24-hour rule." Some return reasons allow extended deadlines. Your company as the Originator should receive prompt advice of ALL return entries from your ODFI with a code and/or description that describes the reason for the return.

Reason for Return	Action by Originator
R01 – Insufficient Funds	Originator may initiate a new ACH entry within 180 days of original Settlement date. (maximum of two attempts)
R02 – Account Closed	Originator must stop initiation of entries and obtain an authorization from the Receiver for another account.
R03 – No Account	Originator must stop initiation of entries and contact the Receiver for correct account information.
R04 – Invalid Account	Originator must stop initiation of entries until account number/structure is corrected.
R05 – Unauthorized Debit to Consumer Account Using Corporate SEC Code	Originator must stop initiation of entries.
R06 – ODFI Request for Return	Originator must accept requested return.
R07 – Authorization Revoked	Originator must stop initiation of entries until new consumer authorization is obtained.
R08 – Payment Stopped	Originator must contact Receiver to identify the reason for the Stop Payment and obtain authorization before reinitiating the entry.
R09 – Uncollected Funds	Originator may initiate a new ACH entry within 180 days of original Settlement date. (maximum of two attempts)
R10 – Customer Advises Not Authorized, Notice Not	Originator must stop initiation of entries.

Provided, Improper Source Document, or Amount of Entry Not Accurately Obtained from Source Document	
R12 – Account Sold to Another DFI	Originator must stop initiation of entries and obtain correct routing number information for initiation of subsequent entries.
R16 – Account Frozen	Originator must stop initiation of entries.
R17 – File Edit Record Criteria	Originator must identify and correct errors prior to initiation of further entries. This is more used for suspicious transactions and the RDFI should return with "QUESTIONABLE" in the note.
R20 – Non Transaction Account	Originator must stop initiation of entries.
R23 – Credit Entry Refused by Receiver	Originator must obtain Receiver authorization prior to reinitiating the entry.
R24 – Duplicate Entry	Originator should accept the return. If the entry has already been reversed, Originator should contact the RDFI to determine a solution. An Originator may reverse an erroneous or duplicate ACH entry/file up to 5 banking days after the Settlement Date of the entry/file. OR it may request the RDFI to send a return.
R29 – Corporate Customer Advises Not Authorized	Originator must stop initiation of entries until subsequent authorization has been obtained.
R31 – Permissible Return Entry	Originator must accept return as agreed upon with RDFI. If the Originator or ODFI has not given permission for the untimely return, the return may be dishonored. ACH return entries may be dishonored when they are untimely, when they contain incorrect information or have been misrouted.

- Disagreements regarding authorization should be handled OUTSIDE of the ACH Network
- Originators of Debit Entries must maintain a return rate below .5% for entries returned as unauthorized (R05, R07, R10, R29 and R51).

What is a Notification of Change (NOC)?

An NOC is a non-dollar entry transmitted by an RDFI to notify your ODFI that previously valid information contained in a posted entry has become outdated or is erroneous and should be changed. NOC's allow the RDFI to return information to your ODFI (and thus, your company) without returning the value of the entry. Many NOC's are the result of a merger or consolidation at the RDFI, which requires changes in Receiver account information. When the RDFI is able to recognize the intended account, NOC's provide a means for the RDFI to post the entry to the Receiver's account and to notify your company of necessary changes. Upon receipt of an NOC, your ODFI must report NOC information to you. 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.

What is an ACH Application (SEC) Code?

ACH applications are payment types used by Originators, such as your company, to identify ACH debit and/or credit entries transmitted to a corporate or consumer account at the RDFI. Each ACH application is identified and recognized by a specific Standard Entry Class (SEC) code,

which appears in the ACH record format. The SEC code also identifies the specific record layout that will be used to carry the payment and payment-related information.

Application (SEC) codes accepted by Cash Management within the Digital Banking platform are:

ACH Application (SEC) Code	Application Use
PPD	**Payment from or Deposit to a Consumer (person)**
CCD	**Payment from or Deposit to a Corporation (business)**
CTX	**Corporate Trade Exchange – Payment to a Corporation (business)**

Application (SEC) codes **NOT** accepted by Cash Management with in the Digital Banking platform are:

ACH Application (SEC) Code	Application Use
ARC	**Accounts Receivable entries (check conversion to ACH)**
BOC	**Back Office entries (check conversion to ACH)**
POP	**Point-of-Purchase (check conversion to ACH)**
TEL	**Telephone Initiated entries**
WEB	**Internet Initiated entries**
IAT	**Cross Border International entries (effective 9/18/09)**
RCK	**Re-Presented check collection (Only permitted with Bank exception)**

ACH & Wire Customer Security Best Practices?

- Perform all online banking activities on a stand-alone and completely locked down computer system not used for email or other web browsing.
- Be suspicious of emails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Citizens Bank will never contact you for this information.
- Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as DSL or cable.
- Create a strong password with at least 10 characters that includes a combination of mixed case letter, numbers, and special characters.
- Prohibit the use of “shared” usernames and passwords for online banking systems.
- Use a different password for each website that is accessed.
- Change the password a few times each year.

- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Install commercial anti-virus and desktop firewall software on all computer systems. Ensure virus protection and security software are updated regularly.
- Ensure security patches are applied regularly, particularly on operating systems and key applications.
- Consider installing spyware detection software.
- Verify use of a secure session (https, not http) in the browser for all online banking.
- Avoid using an automatic login feature that saves usernames and passwords for online banking.
- Never leave a computer unattended while using any online banking or investment service.
- Never access bank, brokerage, or other financial services information at Internet cafes, public libraries, etc.
- Familiarize yourself with your financial institution's account agreement.
- Stay in touch with other businesses to share information regarding suspected fraud activities.
- **Immediately escalate any suspicious transactions to your financial institution, particularly ACH and wire transfers.** There is a limited recovery window for these transactions, and immediate escalation may prevent further loss by the customer.