EAST WISCONSIN SAVINGS BANK

Member FDIC

ACH Originator Education

NACHA Rules:

The National Automated Clearing House Association (NACHA) administers the NACHA Rules and oversees the ACH networks. These rules are the foundation for every ACH payment. By defining the roles and responsibilities of the Depository Financial Institutions (DFI) and establishing clear guidelines for each ACH network participant, the NACHA rules ensure that millions of payments occur smoothly and easily each day.

NACHA rules are also meant to safeguard your customers' sensitive financial and non-financial data and ensure that all ACH transactions are handled securely. Sensitive information includes things like bank account numbers and routing numbers, social security numbers, driver's license numbers, and more. If you collect and store non-public sensitive information like this, you need to comply with NACHA requirements.

The NACHA rules are updated and published annually. As an ACH Originator you are required to comply with the NACHA rules pursuant to your ACH Origination Agreement. Annually, you will receive notification from the bank explaining changes in the NACHA rules. These changes are described in the Revisions to the NACHA Operating Rules section of the rule book or for more information on NACHA rules visit https://www.nacha.org/.

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 of company) to either credit or debit their account. When your company initiates a credit transaction on 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 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 initiating credits or debits to their account. The authorization is a key component of the ACH transactions, 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 to 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 ODFI's, which are then sorted, batched and forwarded to the Receiver's financial institution. The ACH Operator also performs some editing functions, ensuring 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 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 on an entry is for a valid account at an 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 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.

Return Reason	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 Provided, Improper Source Document, or Amount of Entry Not Accurately Obtained from Source Document	Originator must stop initiation of entries.
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.
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 are ACH reversals?

Reversals are credit or debit entries that reverse an erroneous entry. Reversals may only be made under certain conditions, including wrong dollar amount, wrong account, or duplicate transactions.

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. NOCs allow the RDFI to return information to your ODFI (and thus, your company) without returning the value of the entry. Many NOCs 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, NOCs 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 the bank via the Cash Management ACH Origination System are:

(SEC) Code	Application Use
PPD	Payment from or Deposit to a Consumer (person)
CCD	Payment from or Deposit to a Corporation (business)

*Application (SEC) codes **NOT** accepted by the bank via the Cash Management ACH Origination System are:*

(SEC) Code	Application Use
ARC	Accounts Receivable entries (check conversion to ACH)
BOC	Back Office entries (check conversion to ACH)
CTX	Corporate Trade Exchange – Payment to a Corporation (business)
POP	Point-of-Purchase (check conversion to ACH)
RCK	Re-Presented check collection
TEL	Telephone Initiated entries
WEB	Internet Initiated entries
IAT	Cross Border International entries (effective 9/18/09)

Do Originators have to comply with OFAC requirements?

Yes, you are required to check payees/ACH recipients against Office of Foreign Asset Control (OFAC)

compliance checklists. You may check the OFAC SDN list at https://sanctionssearch.ofac.treas.gov/.

What are some sound practices to promote information security?

Sound practices to promote information security is the responsibility of the Originator. Sound practices to promote information security include, but are not limited to, the following:

- Use a dedicated computer for all business online banking transactions, as casual internet browsing can expose your computer to malware.
- Use and regularly update antivirus and anti-spyware software to monitor for spyware and/or malware.
- Remove the administrative rights on company computers to protect them against certain activities, including uploads, downloads and installation.
- Use strong passwords; passwords confine system access to authorized users and may extend the amount of time it takes a hacker to access a password through an attack. The more complex the password is, the more difficult they are to break. Requiring employees to change passwords on a regular basis is also recommended.

What are the Fraud Risks for 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 vulnerability. Fraud challenges all participants in the ACH network. Originators must remain vigilant to prevent and defend against fraud risk.

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 the bank's ACH Origination Digital Banking system 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.

As ACH Origination is a higher risk commercial banking function, we suggest that your company perform its own internal risk assessment and controls evaluation periodically to ensure you are considering all available security options.

East Wisconsin Savings Bank encourages companies to make it a practice of monitoring your accounts online daily. Checking your "Transaction History" screens daily within the Online Banking system 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.