West Bank
westbankstrong.com • Member FDIC

West Bank Annual ACH Education

As an Originator of ACH entries, it is important to stay up-to-date with the current ACH rules and fraud trends. An Originator is any entity that creates electronic payments and deposits.

Understanding Returns and Return Codes

Return codes are used when the receiving bank is unable to post an entry to the receiver's account and may return the entry back to the originating bank.

The financial institution will notify you of a return and then credit or debit the amount to your account to reflect the nature of the return. Return notification is typically provided to you by regular mail, email or online notification. Originators should receive return information within two banking days from the settlement date.

The codes detail why the funds are being returned. The most common return codes used:

R01 Insufficient funds
R02 Account closed
R03 No account or unable to locate account
R04 Invalid account number
R06 Returned per ODFI's request
R07 Authorization revoked by customer
R08 Payment stopped or stop payment on item
R09 Uncollected funds
R10 Customer advises not authorized
R11 Customer advises entry not in accordance with the terms of the authorization
R16 Account frozen
R23 Credit entry refused by receiver
R29 Corporate customer advises not authorized

RETRY PYMT Re-initiating a Returned Item

- The only transactions that can be re-presented for settlement are (1) those returned for Insufficient Funds or Uncollected Funds (there is a limit of two re-presentments within 180 days of the original entry date), or (2) a transaction that was returned for Stop Payment (if re-presenting it was approved by the receiving party).
- When re-initiating a returned item, the words "RETRY PYMT" in all capitalized letters are required in the Company Entry Description field. Identical content is required in the following fields: Company Name, Company ID, and Amount. Modifications to other fields are permitted but only to those necessary to correct an administrative error made during processing.

Reversals

Defined as a credit or debit Entry that reverses an Erroneous Entry. If an Originator creates erroneous ACH entries or files, corrections may be made by initiating reversing entries or files. An erroneous entry or file is defined as:

- A duplicate of an entry previously initiated by the originator or ODFI
- Orders payment to or from receiver not intended to be credited or debited
- Orders payment in a dollar amount different then was intended

Reversals are Requests

They are not mandatory transactions for the receiving financial institution, and they do not guarantee you will recover any funds. Receiving financial institutions do not have to put themselves in a negative position (i.e. overdraw the receiver's account) to process a reversal. Reversals may be returned by the receiving institution.

1. **REVERSAL** (must be in all capitalized letters) in the description field of the Company Batch Header Record.
2. Originated within five banking days following settlement date of the erroneous entry.
3. The effective date should be the same date as the original entry/file date for future dated files.
4. Notify the receiver of the reversal by the settlement date. In the case of an erroneous file, transmit a correcting file with the reversing file.

Note: We recommend that Originators use an authorization agreement (credits) with their Receivers that states they are authorized to debit/ reverse any entries made in error. This is good business practice and will help with any disputes in the future.

Understanding your role regarding the security of Non–Public Personal Information

The *Nacha Operating Rules* require that each Originator and Third–Party Sender must have policies and procedures in place regarding the initiation, processing, and the storage of personal, non-public information, entries and files. Your security and the policies and procedures you have in place should accomplish the following three requirements:

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

OFAC

Do Originators have to comply with OFAC requirements?

- You are required to check payees/ACH recipients against Office of Foreign Asset Control ("OFAC") compliance checklists. OFAC checklists contain lists of countries, groups and individuals with which U.S. Companies are not permitted to send or receive funds.
- The financial institution helps protect our clients by informing them that it is against the law to send debit or credit entries to OFAC-blocked entities.

You may check the OFAC SDN list here

Notification of Change (NOC) (COR)

If the information on a transaction you originated is incorrect, you may receive a non-dollar correction transaction called a Notification of Change (NOC). It specifies information such as:

- Correct account number
- Correct routing/transit number
- Correct account type (checking/savings etc.)

For example, if a receiving bank (also called Receiving Depository Financial Institution or RDFI) has been through a merger, it may send you a NOC to provide new information that should be included on future transactions you originate.

The financial institution will notify you of any NOCs received. Changes need to be made before originating future transactions. This is important to avoid disruption of payments or fines for uncorrected information which your financial institution may pass on to you. By following the NOC process, the receiving bank ensures the information provided on future ACH transactions will be correct. By complying with the NOC, your business can originate future transactions without having to obtain a new authorization.

Authorizations

As an Originator, you are required to adhere to certain rules and agreements when initiating ACH transactions. An authorization is a document that is received by the Originator from the Receiver which authorizes the Originator to initiate a transaction on behalf of the Receiver.

- Consumer authorizations must be in writing and signed or similarly authenticated by the receiver.
- The receiver must also receive a copy of the written authorization.
- The terms of the authorization must be clearly stated and understandable.
- Must contain instructions for termination.
- Originators are required to retain the authorization for two years from the termination or the revocation of the authorization.
- You must obtain authorization from a customer when making a one-time/recurring ACH debit and must indicate very clearly to the customer that they are authorizing a one-time/recurring ACH debit.
- You must take reasonable steps to ensure customers' routing numbers are valid.
- You must take steps to verify a customer's identity, without regard to whether a transaction is authorized online or by phone.
- You must be vigilant about possible fraud and do whatever is "commercially reasonable" to ensure the ACH transactions you initiate are not fraudulent.
- Ensure that you cancel a subscription promptly and stop making debits if a customer asks to cancel.

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.

Ensuring you are 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 code. The most commonly used SEC codes:

PPD — Pre-arranged Payment or Debit

- Most commonly used for direct deposit
- For business to consumer use only
- Written authorization 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
- Agreements are handled by contract authorization between companies

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

Example: You cannot generate an "ACH Batch" that contains employees for weekly payroll and also businesses you are paying for invoices or other payment needs. You would need to originate one PPD batch containing all of the employee transactions, and one CCD batch containing all of the B2B transactions.

Company Name

To ensure clear identification of the source of an ACH transaction, the Rules contain specific requirements on how an Originator must identify itself within an ACH record. *The Rules* require the Originator to populate the Company Name Field with the "name it is known to and readily recognized by the Receiver". This name could be the Originator's "doing business as" name or "trading as" name.

The inclusion of a readily recognizable Originator name ensures that the Receiver is able to identify a transaction appearing on their periodic statement. The clear identification of the Originator of an ACH transaction improves overall network quality by reducing the number of unrecognized entries requiring investigation and possible returns.

Common notification of change (NOC) codes:

C01	Incorrect bank account number
C02	Incorrect transit/routing number
C03	Incorrect transit/routing number and bank account number
C05	Incorrect payment code
C06	Incorrect bank account number and transit code
C07	Incorrect transit/routing

Fraud Corner

What are the fraud risks for ACH?

Fraud challenges all participants in the ACH Network. Originators must remain vigilant to prevent and defend against fraud risk. There are certain common fraud schemes of which you should be aware. In one fraud scheme, fraudsters hack into an Originator's 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 this type of fraud presents, it is essential that all computer equipment your company uses to operate treasury management and ACH Origination applications is regularly updated and patched for security vulnerabilities (including use of and updates to firewall, virus protection, anti-malware protection and anti-spam protection).

What is website spoofing?

Website spoofing is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoof websites are typically made to look exactly like a legitimate website published by a trusted organization. **To prevent fraud related to website spoofing:**

- Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a slightly different domain name.
- If you are suspicious of a website, close it and contact the company directly.
- Do not click links on social networking sites, pop- up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.
- Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://".
- Avoid using websites for which your browser displays certificate errors or warnings.

What is phishing?

Phishing is a method of fraud by which an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication.

Phishing messages often direct the recipient to a spoof website. Phishing attacks are typically carried out through email, instant messaging, telephone calls, and text messages (SMS). **To prevent fraud related to phishing:**

- Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don't ask for sensitive information through email or text messages.
- Beware of visiting website addresses sent to you in an unsolicited message. Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
- Try to independently verify any details given in the message directly with the company.
- Utilize anti-phishing features available in your email client and/or web browser.

You may also want to consider having one computer in your office which cannot be used to browse the internet or read emails and is your sole source of access to the treasury management system. Limiting access to the computer which is used to house and transmit ACH data may help avoid accidental downloads of harmful programs/viruses that could potentially compromise your transactions. Appropriate steps should be taken within your company to ensure that all User IDs, passwords, authentication methods and any other applicable security procedures issued to your employees are protected and kept confidential. All staff should be aware of 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.

Fraud Corner

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 make those orders. Business email compromise is classified as Relationship and Trust Fraud by the Federal Reserve's FraudClassifier Model because an authorized party was manipulated into initiating a payment.

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 contract information is often in the public record. Vendor impersonation fraud is classified as Relationship and Trust Fraud by the Federal Reserve's FraudClassifier Model because an authorized party was manipulated into initiating a payment.

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. Payroll impersonation fraud is classified as Compromised Credentials or Impersonated Authorized Party depending on whether the fraudster uses stolen credentials to access the employer's HR portal or impersonates the employee when contacting the employer's HR department.

Account Takeover Fraud

Account takeover fraud occurs when a fraudster obtains the credentials of a consumer or a business bank account and pushes credits to their own accounts. The fraudster is active in the victim's online bank account, knows the account balances, and can quickly deplete entire accounts. Account takeover fraud is classified as Compromised Credentials because an unauthorized party initiates payment using stolen credentials.

Additional information can be found here:
Protecting Against Cyber Fraud

Federal Reserve FraudClassifier Model

The Federal Reserve worked with the payments industry to create the FraudClassifier model to help organizations classify fraud consistently. Nacha participated in the development of the FraudClassifier model and encourages the model's use. The model supports a common fraud language across payment types and fraud methods that can help all parties work together to identify and fight fraud. Applying the model across organizations and the industry ensures greater consistency in fraud classification, more robust information, and better fraud tracking.

Additional information can be found here:
Federal Reserve FraudClassifier model