Equity Bank 5/9/2024 [Edition 1, Volume 1]

ACH NEWSLETTER

IMPORTANT REMINDERS

Notification of Change (NOC)

It is important that you review your NOC notifications and make appropriate changes in timely matter.

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transmitted by an RDFI to notify your ODFI that previously valid information contained in a posted entry has become outdated or is erroneous and should be changed.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.

Deadline Reminders

The deadline for processing ACH files to be effective the next business day is 5:00 pm. CT. This is a hard cut-off therefore we recommend having your ACH files completed and submitted by 4:00 pm, CT to allow time for troubleshooting and/or corrections to be made, if needed. If you have questions, concerns or troubleshooting needed – please don't hesitate to contact our Treasury Support Team at 833-249-7658. We can assist you with your ACH file, Online Banking, Wires, RDC, and much more! If you would prefer to email, you can send your questions/concerns to treasury@equitybank.com.

NOC Code	Description of Error
CO1- Incorrect Account Number	Account number is incorrect or is formatted incorrectly.
C02- Incorrect Routing Number	Due to a merger or consolidation, a once valid routing number must be changed.
C03- Incorrect Routing Number and Incorrect Account Number	Due to a merger or consolidation, the routing number must be changed, and account number structure is no longer valid.
C05- Incorrect Transaction Code	Transaction Code is incorrect and is causing entry to be routed to the wrong type of account (checking, savings, general ledger, or loan).
C06- Incorrect Account Number and Incorrect Transaction Code	Account number is incorrect, and Transaction Code is incorrect causing entry to be routed to the wrong type of account (checking, savings, general ledger, or loan).
C07- Incorrect Routing Number, Incorrect Account Number, and Incorrect Transaction Code	Due to a merger or consolidation, a once valid routing number must be changed, account number structure is no longer valid, and the transaction should be routed to another type of account.

Educational Corner:

This document is provided as a quick reference guide to assist with the more commonly asked questions and answers regarding ACH processing. It is not intended to take the place of the ACH Operating Rules. Equity Bank strongly recommends that each ACH Originator purchase the ACH Operating Rules – Corporate Edition annually which will provide a complete and up to date version of the Rules that, as a participant in the ACH Network, you have agreed to abide by. This is available electronically at www.nachaoperatingrulesonline.org Please contact Treasury Support at 833-249-7658 with any questions.

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 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 Equity Bank's Online 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.

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

Equity Bank's Online Banking system utilizes multi factor authentication by way of a secure access code that provides a one-time passcode via phone, e-mail or SMS message. While this 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.

Equity Bank also establishes a File Limit as an additional security measure. This limit will be established by the bank based on your company's needs and risk assessment.

Equity 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. 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 both the Activity Center and Account History daily within the Online Banking system will ensure that you are aware of all transactions, even when they have not yet been processed or posted to your account. The sooner ACH fraud is detected, the more successful the bank will be in assisting to recover any potentially lost funds.

Please see the Fraud Patrol Guide at the end of this newsletter for other best practices to protect your account.

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 ODFI's, which are then sorted and 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 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 and transaction description (i.e. 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, weekend, or holiday, the ACH Operator will apply a Settlement Date of the next business day.

What is a Prenotification (Prenote)?

What is Micro deposit

Prenotifications (prenotes) 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.

Prenotes are optional and can be sent with any ACH application. Prenotes 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 prenotes, you are required to do so **at least 3** banking days before sending the first live dollar entry. If there are any errors in a prenote 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 before a live-dollar entry is initiated.

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 prenotifications 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 will receive prompt advice of ALL return entries from your ODFI with a code that describes the reason for the return.

What is Reinitation of Entries

An Originator or ODFI may reinitiate an entry, other than RCK, that has previously been returned, only if:
• The entry was returned NSF/UCF.
• The entry was returned stop payment and authorization to reinitiate has been received by the Originator; or
• The Originator or ODFI has taken corrective action to remedy the reason for return, such as obtaining new account information for an entry returned account closed.

The entry must be reinitiated within 180 days after the Settlement Date of the original entry. For debits returned NSF/UCF, a maximum of 2 reinitiated entries may be transmitted following the return of the original entry. This results in a total of 3 presentments (i.e., original entry plus 2 reinitiated entries). Additionally, 'RETRY PYMT' must be specified within the Company Entry Description field of the Company/Batch Header Record for all reinitiated entries regardless of SEC code.
Improper reinitiation practices are defined in the *ACH Rules* as:
• Initiating an entry for an amount greater or less than the original entry, which was returned
• Initiating an entry that was returned unauthorized prior to obtaining a proper authorization
• Initiating an entry that Nacha reasonably believes represents an attempted evasion of the reinitiation rules (e.g., changing the Company ID or Company Name from the original entry)

A debit entry is not to be treated as a reinitiated entry when:

• The debit is one in a series of recurring entries and is not contingent upon whether an earlier debit has been returned (e.g., the monthly insurance premium scheduled in May would be a new entry even though the April payment was returned)
• The Originator obtains a new authorization for a debit returned
• The original entry is returned R03 – No Account/Unable to Locate Account or R04 – Invalid Account Number Structure
• The original entry is returned R11 – Customer Advises Entry Not in Account with the Terms of the Authorization and the error has been corrected to conform to the authorization (e.g., entry returned R11 because it was authorized for $50 and not $500; when Originator corrects the entry to be $50, it is not considered a reinitiated entry)

Reason for Return	Action by Originator
R01 – Insufficient Funds	Originator may initiate a new ACH entry within 180 days of original Settlement date.
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.
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.
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.
R11 – Customer Advises Entry Not in Accordance with the Terms of the Authorization	Originator must contact Receiver to identify the reason for the return. New authorizations may be required prior to reinitiating the entry.
R13 – Invalid ACH Routing Number	Originator must stop initiation until routing number is corrected
R16 – Account Frozen	Originator must stop initiation of 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.

- Disagreements regarding authorization should be handled OUTSIDE of the ACH Network
- Originators must maintain a return rate below 0.5% for entries returned as unauthorized.

What is an ACH Application (SEC) Code?

ACH applications are payment types used by Originators, such as
entries transmitted to a corporate or consumer account at the
recognized by a specific Standard Entry Class (SEC) code, whic
code also identifies the specific record layout that will be us
information.

Application (SEC) codes accepted by Equity Bank:

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**
WEB	**Internet Initiated entries**
ARC	**Accounts Receivable entries (check conversion to ACH)**
BOC	**Back Office entries (check conversion to ACH)**
POP	**Point-of-Purchase (check conversion to ACH)**
RCK	**Re-Presented check collection**
TEL	**Telephone Initiated entries**

Fraud Patrol

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 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 Equity Bank's Online 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.

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

Equity Bank's Online Banking system utilizes multi factor authentication by way of a secure access code that provides a one-time passcode via phone, e-mail or SMS message. While this 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.

Equity Bank also establishes a File Limit as an additional security measure. This limit will be established by the bank based on your company's needs and risk assessment.

Equity 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. 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 both the Activity Center and Account History daily within the Online Banking system will ensure that you are aware of all transactions, even when they have not yet been processed or posted to your account. The sooner ACH fraud is detected, the more successful the bank will be in assisting to recover any potentially lost funds.

Recognizing & Mitigating Credit Push Fraud: Different Ways of Credit Push Fraud:

- **<u>Business Email Compromise – What Is It?</u>**

With Business Email Compromise, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business' officers and monitor his or her account for patterns, contacts, and information. Using information gained from social media or "out of office" messages, the fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions.

How It's Done

- Fraudster monitors officer's accounts for patterns, contacts, and information.

- After identifying the target, ploys are conducted such as spear-phishing, social engineering, identity theft, email spoofing, and the use of malware to either gain access to or convincingly impersonate the email account.
- Fraudster uses the compromised or impersonated account to send payment instructions.
- Payment instructions direct the funds to an account controlled by the fraudster or a money mule.

Vendor Impersonation Fraud – What Is It?

Vendor Impersonation Fraud can occur when a business, public sector agency or organization, e.g., a municipal government agency, a school district, receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payment along with routing and account information. This type of request could come from fraudsters and not the contractor or construction-related company. Although any business entity could be the target of this type of social engineering attack, public sector entities seem to be specifically targeted because their contracting information is oftentimes a matter of public record.

How It's Done

- Fraudster monitors a business, public sector agency or organization for publicly available contractor or vendor information.

- The fraudster poses as a legitimate vendor or contractor to request updates or changes to payment information or change of payment method.

- Then the fraudster sends an email, form, or letter resulting in the business or agency transferring funds to an account controlled by the fraudster or a money mule.

Payroll Impersonation Fraud – What Is It?

Fraudsters target individual employees by directing the employees to update or confirm their payroll information via a fake payroll platform that spoofs their employer's actual payroll platform. In some cases, the fraudster may claim the employee must do one of these: view a confidential email from human resources or the payroll department, view changes to the employee's account, or confirm that the account should not be deleted. In any case, when the employee logs in from a link or attachment in the email, the fraudsters then use the stolen employee credentials to change payment information in the real payroll platform.

How It's Done

- Fraudster targets an employee by sending a phishing email that impersonates the employee's human resources or payroll department, as well as the company's payroll platform. The email directs the employee to log in to confirm or update payroll information, including bank account information.
- Employee clicks the link or opens the attachment within the email and confirms or updates the payroll information.
- The fraudster then uses the stolen login credentials to change payment information to an account controlled by the fraudster or a money mule.

Ransomware Attacks – What is It?

Ransomware is a type of malware that will prevent you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

How It's Done

- The fraudster successfully installs ransomware onto a computer by sending an email attachment, ad, link, or website that's embedded with malware.

- Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More nefarious versions can encrypt files and folders on local drives, attached drives, and even networked computers.
- You usually discover it when you can no longer access your data, or you see computer messages letting you know about the attack and demanding ransom payments.

Ways to fight and prevent Fraud – Avoid being a Victim: Treat any change of payment information as a brute-force attack.

- Be old-fashioned! Call the requestor to confirm the payment initiator has not been spoofed.
- Call the payee/receiver at the number on file (not the phone number that accompanied the request to change account information).
- Validate account ownership and review your accounts frequently. By reconciling daily, you are able to quickly catch any erroneous transactions and limit loss.
- Initiate payments using Dual Controls. By utilizing dual controls, if your computer is infected with malware and your online banking compromised, the unauthorized person would not be able to complete a transaction with just the one online banking user profile.
- Never provide password, or account information when contacted.
- Don't provide nonpublic business information on social media.
- Avoid free web-based email accounts for business purposes. A company domain should always be used for business emails.
- Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book.
- Sign up for ACH Positive Pay – Fraud prevention and review of ACH items debiting your account.
- Dedicate a computer or system for online banking.
  By dedicating a computer solely for the purpose of sending your files, you reduce the risk of downloading a virus on your computer, in turning giving an unauthorized person access to your online banking.
- Use a system that has multifactor authentication with an independent mechanism.
- Log and monitor key computer or systems.
- Remember – the bank will never ask you for your password or secure access codes.

What are the Fraud Risks for Checks?

- The 2022 Association for Financial Professionals (AFP) survey noted that 63% of respondents reported being impacted by check fraud.

- Be Proactive internally and with your clients. Employee training and increased awareness

  - Learn to spot counterfeit items.
  - Avoid poor image quality items or checks that are not signed/endorsed properly.
  - Exercise caution avoiding of redeposit of items/duplicate presentment. Proper disposal of deposited items within 60-90 days
  - Use proper authentication when accessing RDC system – don't share user credentials/passwords
  - Safety and integrity of deposit items held in locations (i.e., protection of personal information).

- ***What types of controls are in place to help us combat check fraud on your deposited items?***
- Our RDC system uses username and passwords to access it.
- Equity Bank also establishes a File Limit as an additional security measure. This limit will be established by the bank based on your company's needs and risk assessment.

- Periodic self assessment or customer audit required for all customers.

- **Positive pay**
- **Payee Validation (Payee Positive Pay) – 50% more effective than Positive Pay alone**
- **Reverse Positive Pay**
- **Daily Reconciliation and Check Image Review**
- **Segregation of accounts**
- Have an actionable plan in place to respond in case of a fraud attack.
- Tamper resistance features on checks
- Review of returned items

If you have any questions, please contact your Treasury Sales Officer or a member of our Treasury Support team at 833-249-7658 or by e-mail to treasury@equitybank.com