ACH Origination
Annual Customer Training

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'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 of this type of fraud, it is essential that all computer equipment used by your company to operate Commerce Bank's Cash Management ACH Origination software is regularly updated and patched for security vulnerabilities (including the use of and updating of firewall, virus protection, anti-malware protection, anti-spam protection). You may also want to consider having one computer in your office which is not used to browse the internet or read e-mail to be your sole source of access to the Cash Management system. Limiting access to the computer which is used to house and transmit ACH data may help avoid the accidental downloading of harmful programs/viruses that could potentially compromise your transactions.

The appropriate steps should be taken within your company to ensure that all User ID's, 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 your own internal risk assessment and controls evaluation periodically to be sure you are considering all available security options.

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

Commerce Bank's ACH Origination system utilizes multi-factor authentication by way of a secure token. 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.

Commerce 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 your "Online Activity" and "Transaction History" screens daily within the NetTeller program will ensure that you are aware of all transactions, even when they have not yet posted to your account. The sooner ACH fraud can be detected, the more successful the bank will be in assisting to recover your company's potentially lost funds.

Please keep in mind that we will never ask for or email you requesting your NetTeller or Cash Management password. We may on occasion call to verify other information regarding your online activity should we see something of concern in your login patterns. If you plan to travel and will be logging into your Cash Management while travelling, it is very helpful to call us in advance to avoid your account being temporarily disabled for security purposes.

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 ODFl's, 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 Prenotification (Prenote)?

Prenotifications (prenotes) are non-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 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 prenotes, you are required to do so at least 6 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.

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 should receive prompt advice of ALL return entries from your ODFI with a code 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.
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.
R10 – Customer Advises Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receiver's Account	Originator must stop initiation of entries.
R11 – Customer Advises Entry Not in Accordance with the Terms of the Authorization	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 must maintain a return rate below 1% for entries returned as unauthorized.

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 Commerce Bank via the Cash Management ACH Origination system 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)**

Application (SEC) codes **NOT** accepted by Commerce Bank via the Cash Management ACH Origination system:

ACH Application (SEC) Code	Application Use
ARC	**Accounts Receivable entries (check conversion to ACH)**
BOC	**Back Office entries (check conversion to ACH)**
CTX	**Corporate Trade Exchange**
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)**

If you have any questions relating to this training, please feel free to contact us:

Commerce Bank
Operations Department
700 Taylor Street
Corinth, MS 38834
(662) 286-5577

	ACH Transaction Requirements - Company Understands and Agrees to the following:
√	Company is responsible to ensure adequate funds are in place to cover a related ACH transaction prior to its Effective Entry Date. An ACH transaction can rapidly result in an account being "overdrawn" (reflecting a negative balance.) In the event of an overdrawn account, Company is responsible for any associated overdraft fees and returning the account to a positive balance.
√	Transmission from Company should be received by 2:00 pm CST, two business days before Effective Entry Date for credits and one business day before the Effective Entry Date for debits. Although the Cash Management system will allow ACH transactions to be processed with one day notice, Commerce Bank requests that you allow two days between your Initiation and Effective dates for credits to avoid processing delays due to unanticipated service interruptions. ACH's will not be processed on Federal Holidays, weekends or evenings after 2:00 PM CST.
√	Only PPD (consumer debit/credit) and CCD (commercial debit/credit) transactions are being initiated by our company. Note: Commerce Bank currently does not accept ARC, BOC, CTX, POP, RCK, TEL, WEB or IAT application (SEC) codes – see training material for definitions.
√	All customers, vendors, or employees that are receiving ACH's from our company (either debits or credits) have signed ACH authorization forms on file. Note: Credits for consumers (PPD) can be made via an oral request, however formal authorization forms are recommended by Commerce Bank for quality control. ACH data/record retention is to be kept in secure location.
√	If pre-note authorizations are sent, our company understands that they must be initiated at least 6 (six) banking days before sending the first live dollar entry. If a Notification of Change (NOC) is returned, our company will make the requested changes within 6 (six) banking days of the receipt of the NOC or prior to the initiation of another ACH entry.
√	No ACH transactions originated by my company are being forwarded on to a foreign financial institution. Note: Transactions that have a final destination in a foreign country (IAT) cannot be processed through Commerce Bank's ACH system. Alternative payment methods will need to be discussed.

	ACH Physical Security, Controls, Processes - Company Understands and Agrees to the following:
√	All computer equipment used to operate Cash Management ACH Origination software is regularly updated and patched for security (including use of and updating of firewall, anti-virus protection, anti-malware protection, and anti-spam protection). In addition, such equipment is located in a reasonably secure location that permits access only to authorized personnel.
√	Plans for contingencies and disaster recovery have been considered and processes are in place to implement these plans as needed. In the event of ACH service interruptions, customer should use alternative methods for processing their payments/collections (i.e., delivery of your ACH file via secure means to a designated Commerce Bank location, sending wire transfers, or generation of paper checks for manual delivery).
√	Administrative access is granted to the appropriate company employee to manage all user rights, account access and limits as needed. Cash Management ACH transaction rights are limited to personnel with appropriate business need for functionality. Company ensures that all individuals with access to the Cash Management program received training necessary to understand their responsibilities and utilize the software in accordance with the applicable terms, agreements and ACH Rules.
√	User ID's should never be shared amongst staff, and proper user security, password controls and separation of duties should be maintained. User ID's that are no longer being used should be reviewed and deleted on a regular basis.
√	Appropriate steps are taken 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.
√	Dual control, in which one employee generates the ACH batch and the system requires a secondary employee to log in and approve the ACH batch, is strongly encouraged to ensure adequate separation of duties to assist in preventing ACH origination fraud.
√	Account activity for all accounts accessible through Cash Management is monitored daily by viewing transactions in both the "Online Activity" and "Account History" screens. Company ensures all Secure Messages sent from the Bank are reviewed in a timely manner.

√	Company will notify the Bank immediately of any suspicious activity. Examples include: unexpected password resets, unknown transactions, suspected user credential compromise, suspected embezzlement or other security incident that might compromise your Company's computer or network security.

	ACH Transaction Verification - Company Understands and Agrees to the following:
√	Successful authentication through a valid User ID, Password and Secure Access Codes (or computer browser authentication), constitutes authorization by Company for any activity conducted or transactions originated. Bank does not have liability to detect/prevent activities or transactions that are initiated given successful authentication.
√	Customer written authorization (sent via fax or email) must be executed by an Authorized Company Representative as designated on the Cash Management Authorized ACH Signature Form. The Bank may perform a call-back to the requestor when authorizations are received to validate the authenticity of the request. ACH batches may be cancelled by Commerce Bank if proper authorization cannot be obtained within the required timeframes for processing the file. Customer must notify the Bank if Authorized Representatives listed on the Cash Management ACH Agreement or Authorized ACH Signature Form are deleted or replaced.
√	The designated Cash Management Company Administrator or their secondary backup may contact Commerce Bank staff to request changes to users, the system or transactions. Proper identity verification will be required prior to changes being made. Appropriate verification may include asking identity related questions, requesting code words or secure email communications.

If you have any questions relating to this training, please contact Commerce Bank Operations at (662) 286-5577.

ACH Rules Update 2023

Effective June 30, 2022, Phase 2 of the Supplementing Data Security Requirements Rule modifies the following areas of the *Nacha Operating Rules:*

> Article One, Section 1.6 (Security Requirements) to require each Non-Consumer Originator that is not a Participating DFI, each Third-Party Service Provider, and each Third-Party Sender, whose ACH Origination or Transmission volume exceeds 2 million Entries annually to protect DFI Account Numbers used in the initiation of Entries by rendering them unreadable when stored electronically.
>
> The Rules are neutral as to the methods/technologies that may be used to render data unreadable while stored at rest electronically. Encryption, truncation, tokenization, destruction, or having the financial institution store, host, or tokenize the account numbers, are among options for Originators and Third-Parties to consider.

Effective September 16, 2022, the new Micro-Entries rule will define and standardize practices and formatting of Micro-Entries, which are used by some ACH Originators as a method of account validation.

This Rule will:

- Define "Micro-Entries" as ACH credits of less than $1 and any offsetting ACH debits, used for the purpose of verifying a Receiver's account
- Standardize the Company Entry Description and Company Name requirements for Micro-Entries
- Establish other Micro-Entry origination practices
- Apply risk management requirements to the origination of Micro-Entries

This Rule will become effective in two phases:

> Phase 1 – September 16, 2022
> The term Micro-Entry will be defined, and Originators will be required to use the standard Company Entry Description and follow other origination practices
>
> Phase 2 - March 17, 2023
> Originators of Micro-Entries will be required to use commercially reasonable fraud detection, including the monitoring of Micro-Entry forward and return volumes

Effective September 30, 2022, the Third-Party Sender Roles and Responsibilities rule has the overarching purpose to further clarify the roles and responsibilities of Third-Party Senders (TPS) in the ACH Network by:

- Addressing the existing practice of Nested Third-Party Sender relationships, and
- Making explicit and clarifying the requirement that a TPS conduct a Risk Assessment.

The two Rules will become effective September 30, 2022, with a 6-month grace period for certain aspects of each rule.

Effective March 17, 2023, the Micro-Entries (Phase 2) rule will define and standardize practice and formatting of Micro-Entries, which are used by some ACH Originators as a method of account validation. This phase of the Rule requires Originators of Micro-Entries to use commercially reasonable fraud detection, including the monitoring of Micro-Entry forward and return volumes.