Cache Valley Bank provides ACH origination services for its approved customers who utilize the ACH network to initiate electronic payments. This document contains information regarding the duties of the ACH Originator (your company), an overview of the ACH network, and key information regarding ACH origination rules and responsibilities.

What are the Fraud Risks for ACH?

ACH Origination fraud is a challenge for Financial Institutions and ACH Originators like your company. Fraud can occur in a variety of ways. One hijacking scheme involves a perpetrator using compromised login credentials to access an originator's online banking system. The perpetrator then originates ACH transfers from the true originator's account to accounts controlled by the perpetrator. 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.

Another common scheme occurs through email when an originator receives an email from someone they believe to be one of their customers or vendors. The email directs the originator to change the bank information to which they send payments for that customer/vendor, which is a fraudulent account controlled by the perpetrator. Again, these funds are generally irretrievable by the time the fraud is discovered.

Due to the risk of this type of fraud, it is **essential** that all computer equipment used by your company to operate Cache Valley 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.

It is also **crucial** that you verify email correspondence by talking directly to your customers/vendors anytime you receive a request to update their bank information. Compromised or spoofed email accounts are very common, and email **should not** be relied upon as the sole source of validation for banking 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. For additional information on protecting your business from Internet fraud, please visit the usa.gov website at https://www.usa.gov/online-safety.

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

Cache Valley Bank's ACH Origination system utilizes multi-factor authentication by way of a secure access code that is sent out to a pre-determined phone number (voice or SMS text) when access is requested from an unknown computer. 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.

Cache Valley Bank strongly 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-approval procedures such as these go a long way in preventing ACH origination fraud. If you don't currently have the Dual-approval security feature in place, the Cash Management administrator can request to enable it by contacting Cache Valley Bank's customer service department.

Administrative access is granted to the appropriate company employee to manage all user rights, account access and limits as needed. Your 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.

It is also very important for your company to make it a practice of monitoring your accounts online daily. Reviewing both the "Activity Center" and transaction history daily within the Cash Management system will ensure that you are aware of all transactions, even when they have not yet posted to your account. The sooner account or ACH fraud can be detected; the more successful the bank will be in assisting to recover your company's potentially lost funds.

Cache Valley Bank also utilizes real-time transaction monitoring that scans all ACH batches, wires, and external transfers generated through our online banking system. Any anomalous activity is flagged and reviewed. If one of your transactions is flagged, we may contact you to verify the validity of the transaction(s).

Cache Valley Bank has automatically enabled Security Alerts to send notifications when a new user or recipient is added, when your login id is changed or disabled, when your password or security alert preferences are changed, and when your user profile is updated. We also offer optional Security Alerts to send notifications when an outgoing ACH transaction has been generated, when invalid passwords or secure access codes are entered, when the forgot-password process is successful or unsuccessful, and notifications for when valid passwords and secure access codes are entered for better monitoring of your Cash Management profile. To set up additional security alerts, in Cash Management, select Settings then Alerts.

Please keep in mind that we will **never** email you requesting your Cash Management password or token credential. 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 outside of the USA 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.

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. Anytime your company generates an ACH transaction to either debit or credit a receiver's account, your company is considered the originator. This could be a credit transaction to your employee's account for payroll or to a business customer's account for payment of goods and services. This could also be a debit transaction to pull funds from 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 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 with whom your company has a contractual relationship for ACH services and is responsible for sending ACH entries into the ACH Network on your behalf. In this case, Cache Valley Bank serves as your company's ODFI.
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, 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 monetary 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 (three) 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 return codes below). An RDFI may use the return process for prenotifications as well as for monetary 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/Unable to Locate 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	Effective 4/1/2020 R11 is used to return a debit in which there is an error, but for which there is an authorization. Originator must resolve the error with the Receiver before reinitiating the entry.
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. May be used by an RDFI for entries it thinks may be fraud with the descriptor QUESTIONABLE in the return addenda.
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.

Important notes regarding returned items:

- Disagreements regarding authorization should be handled OUTSIDE of the ACH Network
- Originators must maintain an Unauthorized Return Rate Threshold below .5% for entries returned as unauthorized. This includes returns for authorization revoked, customer advises unauthorized, and corporate customer advises not authorized.
- Originators must maintain an Administrative Return Rate Threshold below 3% of your total debit entries returned due to administrative or account data errors. This includes returns for account closed, no account/unable to locate, and invalid account number.
- Originators can have no more than 15% of your total debit entries returned for any return reason, known as the Overall Return Rate Threshold.

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 three (3) 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 Cache Valley 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)**
CTX	**Corporate Trade Exchange**

Application (SEC) codes **NOT** accepted by Cache Valley 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)**
POP	**Point-of-Purchase (check conversion to ACH)**
RCK	**Re-Presented check collection**
TEL	**Telephone Initiated entries**
IAT	**Cross Border International entries**

Reversals

Per the NACHA Rules, reversals previously were only allowed due to wrong dollar amount, wrong account number, or duplicate transaction. The rule was expanded on June 30, 2021 to extend the permissible reasons for a reversal to include a "wrong date" error – 1) the reversal of a debit Entry that was for a date earlier than intended by the Originator, or 2) a credit Entry that was for a date later than intended by the Originator. Reversals may only be sent within 5 banking days of effective date of the original entry. The NACHA Rules state that your company must make a reasonable attempt to notify the Receiver of the reason for the reversal before the effective date of the reversing entry.

Reinitiated Entries

Effective September 18th, 2015, this Rule change stipulated that when reinitiating, or resubmitting, an ACH Collection or ACH Single Receipt of an ACH entry for the same dollar amount that was previously returned as R01 Insufficient Funds, that entry must contain the words 'Retry Pmt' in the addenda information. In addition, the reinitiated entry must contain the same content in the Company Name, Company ID and amount fields as the original entry. Please note: the rule is not applicable to debit entries in a recurring series or for debits returned as R07 Authorization Revoked. Effective August 18, 2016, there was a clarification made to this Rule that an originator wouldn't use "Retry Pmt' following a return for reason R03 (No Account – Unable to Locate) or for reason R04 (Invalid account number).

Proper Use of SEC Code

The ODFI warrants that every transaction complies with the Rules. Specifically, Subsection 2.4.1.2: The Entry Complies with The Rules, and states "The Entry Complies with these Rules, including the use of the proper Standard Entry Class Code." It is the responsibility of the Originator to use the appropriate SEC code for the transaction to ensure that the transaction complies with the Rules. In addition, transactions submitted with an incorrect SEC code may have different rights that are not appropriate for the transaction. For example, a transaction sent as a PPD to a business account has extended return rights that should not be afforded to a business transaction and increases the risk of the transaction.

Same-Day ACH

Same-day ACH became available through the ACH network in 2016, which allows for transactions submitted within a same-day processing window to be settled on the same day as the processing date. Cache Valley Bank offers Same-day ACH services on a per-request basis. Batches submitted for same-day processing must be received by Cache Valley Bank by 1:30 PM MT. Applicable transactions must be made available by the RDFI by 5:00 PM RDFI local time. A rule change was made effective on March 18, 2022 that raised the per-transaction limit from $100,000 to $1,000,000. Increased fees are associated with same-day transactions.

Third-Party Sender Registration

This rule requires Originating Depository Financial Institutions (ODFIs, like Cache Valley Bank) to identify and register Third-Party Sender clients. The registration process promotes consistent customer due diligence among all ODFIs, and serves as a tool to support NACHA's continuing efforts to maintain ACH Network quality.

A Third-Party sender is defined as an intermediary between the Originator and the ODFI (Cache Valley Bank) when there is no signed ACH Agreement between the ODFI (Cache Valley Bank) and the Originator. For example: if you process ACH transactions for another company with whom we do not have an ACH Agreement, you are considered a Third-Party Sender for that company. Third-Party Senders are required to perform a Risk Assessment annually and provide a copy of the Risk Assessment to their ODFI.

ACH Rule Changes and Rules Awareness

The National Automated Clearing House Association (NACHA) is the rule-making body governing the ACH network and therefore all participants of the ACH network must comply with the NACHA Operating Rules. Each company sending ACH entries through Cache Valley Bank must comply with the NACHA Operating Rules as stated within the ACH agreement between Cache Valley Bank and the Customer.

Cache Valley Bank will annually communicate applicable Operating Rules changes to ensure that our Originators are educated on those Rules and make any necessary changes to its daily process as a result of these changes. Annually, you may purchase a copy of the updated NACHA Operating Rules & Guidelines by visiting www.nacha.org or you may obtain free limited access to the basic NACHA Operating Rules in read-only format by visiting www.nachaoperatingrulesonline.org.

2025 Applicable Rule Changes

Response to ODFI Request for Return. The Response to ODFI Request for Return rule will require the RDFI to respond to an ODFI's request to return any entry, regardless of whether the RDFI complies with the ODFI's request for the return. The RDFI must advise the ODFI of its decision or the status of the request within 10 banking days of the receipt of the ODFI's request. The objective of the Rule is to improve the recovery of funds when fraud has occurred. The Rule is effective April 1 , 2025.

2026 Upcoming Applicable Rule Changes

Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs. The Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders, and ODFIs Rule will require each non-consumer Originator, Third-Party Service Providers/Third-Party Senders, and ODFI to establish and implement risk-based processes and procedures reasonably intended to identify ACH entries initiated due 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 risk. The objective of the Rule is to reduce the incidence of successful fraud attempts through regular fraud detection monitoring.

The Rule will be implemented in two phases: Phase 1 – March 20, 2026 – On this date the Rule will apply to all ODFIs, and those non-consumer Originators, Third-Party Service Providers, and Third-Party Senders with an annual ACH origination volume that exceeds 6 million entries in 2023. Phase 2 – June 19, 2026 – The Rule will apply to all other non-consumer Originators, Third-Party Service Providers, Third-Party Senders on this date.

RDFI ACH Credit Monitoring. The RDFI ACH Credit Monitoring Rule mirrors the Fraud Monitoring by Originators, Third-Party Service Providers/Third-Party Senders and ODFIs Rule in that it will require RDFIs to establish and implement risk-based processes and procedures reasonably intended to identify credit ACH entries initiated due to fraud. As with other entities, RDFIs 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 and better enable the recovery of funds when fraud has occurred. The Rule will be implemented in two phases: Phase 1 -March 20, 2026 – On this date, the Rule will apply to RDFIs with an annual ACH receipt volume exceeding 10 million entries in 2023. Phase 2 – June 19, 2026 -The Rule will apply to all other RDFIs.

Standard Company Entry Descriptions – Payroll and Purchase. The Standard Company Entry Descriptions Rule 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 goes into effect on March 20, 2026.

Holiday Schedule for 2025

Below is the Holiday Schedule that Cache Valley Bank will observe in 2025. This schedule may be subject to change. Changes will be posted on the Bank's online banking system prior to the change taking place.

January 1, 2025 – New Year's Day	Closed
January 20, 2025 – Martin Luther King Jr. Day	Closed
February 17, 2025 – Presidents Day	Closed
May 26, 2025 – Memorial Day	Closed
June 19, 2025 – Juneteenth	Closed
July 4, 2025 – Independence Day	Closed
July 24, 2025 – Pioneer Day	Offices closed, ACH processing open with adjusted hours
September 1, 2025 – Labor Day	Closed
October 13, 2025 – Columbus Day	Closed
November 11, 2025 – Veterans Day	Closed
November 27, 2025 – Thanksgiving Day	Closed
December 25, 2025 – Christmas Day	Closed

Right to Audit / NACHA Enforcement Authority

Upon written request, Cache Valley Bank shall have the right to examine your ACH Operations to ensure that ACH data is being processed correctly and that processing is adequate to meet the terms of our agreement and all NACHA Operating Rules. Cache Valley Bank may voluntarily provide to NACHA information such as return data that may be indicative of a potential Rules violation by any of our customers.

If you have any questions relating to ACH Origination Rules, please contact Cache Valley Bank Customer Service at 435-753-3020 or your relationship manager.