



ACH Origination Services Training Guide

OptimumBank is pleased to provide ACH Origination Services. While we encourage you to read and become familiar with the Nacha Operating Rules, this guide was developed to give you an overview of important information you should be aware of as an ACH originating customer. This guide is to assist you with training, compliance, and risk associated with ACH origination.

ACH FACTS

- ACH entries are categorized as “consumer or corporate”.
- ACH is a batch system (not real time).
- Once sent to the ACH Operator, entries are irrevocable.
- ACH is capable of crediting or debiting checking or savings accounts.
- An ACH Originator is any entity or person that creates an ACH transaction.
- ACH stop payments for consumers may not have an expiration date.

ACH LEGAL FRAMEWORK

You are required to abide by multiple rules and agreements including, but not limited to, the following when submitting ACH transactions. OptimumBank may ask for access to your premises and records to confirm compliance with the Nacha Rules.

- Electronic access to the current edition of the Nacha Operating Rules can be obtained by creating a Login account as a Basic User through Nacha's website.
 - OptimumBank has the right to audit your compliance with the Nacha Operating Rules and your compliance with the origination agreement at any time. OptimumBank has the right to terminate the origination agreement immediately for breach of the Nacha Operating Rules or applicable laws.
- Regulation E (for consumer entries)
- UCC4A (for corporate credits)
- Deposit Agreement with OptimumBank
- ACH Origination Agreement with OptimumBank
- Business Online Banking agreement with OptimumBank
- Customer Authorizations

YOUR RESPONSIBILITIES AS AN ORIGINATING CUSUSTOMER

- Obtain proper authorizations – dependent on transaction type – and retain authorizations for two years past revocation. (See “Consumer Debit Authorizations”)
- Provide a copy of authorization if requested by the Bank.
- Give appropriate notice to debtor if changing amount or date.
- Protect the banking information received.
- Send entries on the proper date.
- Make necessary changes to payee account information within six banking days when notified by OptimumBank.
- Cease subsequent entries when appropriate.
- Monitor your return activity to prevent it from exceeding 0.5% for Unauthorized Debit Returns, 3% for Administrative Debit Returns, and 15% for Overall Debit Returns. (*For more details, reference the Return Rate Reporting Requirements section.*)
- Check payees against OFAC compliance checklists. (This information may be obtained directly from the OFAC Compliance Hotline at 800-540-OFAC or from the OFAC's home page site.)
- Ensure your computer is protected from unauthorized access by use of a “firewall” as listed in the Business Internet Banking Agreement.
- Protect the confidentiality and integrity of protected information until its destruction. Some examples of protected information include customer authorizations, social security number, account number and routing number information, policy numbers, etc.
- Protect sensitive information no matter what form it is stored as, e.g., electronically or paper based, from the point it is collected until it is destroyed. Restrict and limit access to sensitive data. Use locks on doors and file cabinets. Limit employee access to data to those that need it to do their jobs.
- Do not store sensitive information on portable storage devices (e.g., PDA's, USB drives, CD's laptops, iPhones, iPods, etc.) as these devices are frequently lost or stolen.

DIRECT DEPOSIT PAYROLL AUTHORIZATIONS (CONSUMERS)

- Neither ACH Rules, nor Regulation E, require a written authorization for ACH credits or reversals.
- The Bank recommends you use direct deposit authorization forms that allow the company to debit the employee's account for adjustments. The forms may also be used to collect the proper employee account information.

- Obtain a voided check, not a deposit slip, from the employee.
- The most common code for direct deposit is PPD.

CONSUMER DEBIT AUTHORIZATIONS

- For consumers, an authorization to his or her account must be in writing.
- The most common SEC code is PPD (used for debits and credits).
- For debit entries, you must provide the customer with evidence of the authorization and information regarding the manner in which the authorization can be revoked.
- Retain authorizations for a period of two years from the termination or revocation of the authorization. No entries can be initiated after termination or revocation of the customer's authorization.
- Consumer debit authorizations must, at a minimum, include the following:
 - a) Language regarding whether the authorization obtained from the receiver is for a single entry, multiple entries, or recurring entries
 - b) Amount or a reference to the method of determining the amount
 - c) Timing (including the start date), number, and/or frequency of the entries
 - d) Receiver's name or identity
 - e) Account to be debited
 - f) Date of the receiver's authorization and
 - g) Language that instructs the receiver how to revoke the authorization directly with the originator (including the time and manner in which the receiver's communication with the originator must occur). For a single entry scheduled in advance, the right of the receiver to revoke the authorization must afford the originator a reasonable opportunity to act on the revocation prior to initiating the entry.

CORPORATE AUTHORIZATIONS

- For companies, there must be an agreement between the two parties, but the rules do not define what business practices constitute agreements.
- The most common SEC code is CCD (used for debits and credits).

COPIES OF CONSUMER OR CORPORATE AUTHORIZATIONS

- Upon request, you must provide a copy of the customer's authorization to OptimumBank within five banking days.
- At any time, OptimumBank may test your ability to provide a copy of an authorization.

CHANGING DATE OR AMOUNT OF DEBITS

- ACH Rules require you to notify your debtors of any changes in date or amount debited under the following circumstances:
 - 7 calendar days' notice for a change of date (consumer and corporate).
 - 10 calendar days' notice for a change in the amount (consumer only).
- Sending the notice via U.S. Mail is acceptable.

PRENOTES

- Prenotes are zero-dollar entries that precede the first live entry. The purpose of a prenote is to verify the account information.
- Prenotes are optional for you to send. However, if sent, prenote rules must be followed. A prenote must precede the first live entry by at least three banking days.
- If a Return or a Notification of Change related to the prenote is received timely, you must not transmit subsequent entries to the receiver's account until you have remedied the reason for the return entry or made the correction requested by the Notification of Change.
- The Receiving Bank is not required to validate the name of the payee on the prenote, although many do; they are only required to check the account number. You must understand there is still a risk if the subsequent entry debits or credits the wrong account (this is true for all originations, not just prenotes).

NOTICE OF CHANGE

- When ACH information is incorrect, a Notification of Change "NOC" is sent by the Receiving Bank requesting that future entries contain correct information. ACH Rules require you to make the change within six banking days of receiving the information from OptimumBank.
- The Receiving Bank warrants that the information they provide is correct.
- OptimumBank will notify you of any NOCs received on your behalf.
- OptimumBank will pass any fines received to you for non-compliance.

RECEIPT OF RETURN ENTRIES

- Returns must be processed by the Receiving Bank within 24 hours of settlement. Returns that are unauthorized beyond the 24 hours are the company's liability and any disputes may have to be settled outside the banking network. The Bank recommends that you view your account activity daily.
- An exception to the 24-hour rule is consumer unauthorized returns, which may be returned 60 days of posting.
- The use of consumer (PPD) or corporate (CCD) entry codes determines applicable ACH return rules.
- If the Receiving Bank receives a dispute claiming a debit was unauthorized, the Receiving Bank must get a signed Written Statement of Unauthorized Debit for the account holder. You may obtain a copy of that statement by requesting a copy through OptimumBank.
- The *Rules* established an Unauthorized Entry Fee that is designed to improve the ACH Network quality by reducing the number of ACH debits that are returned as unauthorized. The Originating Bank will be required to pay a fee to the Receiving Bank for any ACH debit returned due to a reason of unauthorized (return reason codes R05, R07, R10, R11, R29, and R51).
 - Upon the receipt of an R05, R07, R10, R11, R29, or R51, we may request a copy of the associated authorization.

RETURN RATE REPORTING REQUIREMENTS

- OptimumBank is required to track the types and volume of incoming return entries for each originating customer.
- For customers that originate debit entries, OptimumBank is required to also track return percentages for various return categories which include:
 - Unauthorized Returns cannot exceed a return rate threshold of 0.5%, which include debit entries returned as R05, R07, R10, R11, R29, and R51.
 - Administrative Returns cannot exceed a return rate level of 3.0%, which include debit entries returned as R02, R03, and R04
 - Overall Returns cannot exceed a return rate level of 15%, which include all debit entries returned for any reason (excluding RCK entries).
- If any of the above listed return rate threshold/levels are exceeded, OptimumBank may contact you and request additional information to determine the reason for the high levels of debit entries being returned.

REINITIATION OF RETURNED ENTRIES

- Reinitiation is the method permitted in the *Rules* by which a Returned Entry may be resubmitted. You may reinitiate a debit entry that was previously returned, only if:
 - the entry was returned as R01-Insufficient Funds or R09-Uncollected Funds,
 - You must not reinitiate an entry that was returned as R01-Insufficient Funds or R09-Uncollected Funds more than two times following the return of the original entry. This gives the Originator a total of three attempts at debiting an account.
 - the entry was returned as R08-Payment Stopped and you received approval from the payee to re-send the entry, or
 - corrective action has been taken to remedy the reason for the return.
- The reinitiation must occur within 180 days of the date of the original entry.
- Reinitiated entries must be submitted as a separate batch that contains the words "RETRY PYMT" in the Company Entry Description field of the Company/Batch Header Record. The use of this description in the field notifies the payee that the entry relates to a previously returned entry.
- The contents of the Company Name, Company Identification, and Amount fields must be identical to the contents of the original entry. The contents of other fields should be modified only as necessary to correct an error or facilitate proper processing of the reinitiated entry.
- It is a violation of ACH Operating Rules to reinitiate the debit entry if a return is received for any other reason.
 - You are prohibited to reinitiate a transaction that was returned as unauthorized. A new authorization must be obtained.

REVERSALS (con only be made under certain conditions)

- Reversals may only be made for the following reasons: (1) wrong dollar amount, (2) wrong account, (3) duplicate transaction, (4) unintended receiver, or (5) debited earlier than intended/credited later than intended.
- If a reversing entry must be made, please contact the Bank for instructions.
- When processing a reversal, the complete ACH file that was originally submitted must be reversed. The reversing entry must be for the full amount, must be sent within five banking days of original entry within 24 hours of discovering the error.
- For wrong account amount or wrong account reversing entries, a correcting entry must also be sent.
- The Receiving Bank is under no obligation to post the reversing debit if it overdraws the payee's account or if the payee's account is closed.
- A payee must be notified if a reversing entry debits his or her account. However, a payee does not need to authorize the reversing entry.

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.

Prevention Tips:

- 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 different domain.
- 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 when your browser displays certificate errors or warnings.

PHISHING

Phishing is when 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).

Prevention Tips:

- 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.

Fraud Prevention Measures

- Limit user access to ACH Origination System (business online banking).
- Use a dedicated computer for your online financial transactions. Do not allow checking email or web browsing.
- Enforce segregation of duties:
 - The same person should not be allowed to create and approve ACH Batch transactions.
- Prohibit sharing user logins, passwords, or tokens
- Monitor all transaction activity daily
- Immediately contact the bank when any suspicious transactions are found

OFAC

- You are required to check payees against OFAC compliance checklists.
- The Office of Foreign Asset Control (OFAC) lists countries, groups, and individuals that U.S. companies are not allowed to send funds to or receive funds from.
- The Bank must protect itself by informing every customer that it is against the law to send debit or credit entries to OFAC blocked entities.

BUSINESS DAYS

OptimumBank will be closed on the following standard holidays observed by the Federal Reserve Bank. We will not accept any ACH Origination files for processing on these days or on Saturdays and Sundays.

New Year's Day (January 1)
Martin Luther King's Birthday (Third Monday in January)
Presidents Day (Third Monday in February)
Memorial Day (Last Monday in May)
Juneteenth (June 19th)
Independence Day (July 4)
Labor Day (First Monday in September)
Columbus Day (Second Monday in October)
Veterans Day (November 11)
Thanksgiving Day (Fourth Thursday in November)
Christmas Day (December 25)

Note: If January 1, June 19, July 4, November 11, or December 25 falls on a Sunday, the next day (Monday) is a Federal Reserve Bank holiday. In general, if one of these holidays falls on a Saturday, OptimumBank will be open the preceding Friday.