Originator ACH Reference Guide

The following information has been provided so that customers know their responsibilities under the NACHA Operating Rules (The Rules) and the Bank 1st ACH Origination Agreement. This quick reference guide was developed to give customers an overview of important information you should be aware of as an originator of ACH transactions. This document does not cover all the NACHA Operating Rules and is not intended to be legal advice.

ACH Participants

"There are five key participants that contribute to the successful completion of an ACH transaction:

- ***Originator***: The company or business that has been authorized by the Receiver to either credit or debit their account. Your company is the Originator when you are initiating credit transactions to an employee's account for payroll or when you are initiating debit transactions to a consumer or business account for payment of goods or services.
- ***Receiver***: An individual that has authorized the Originator (your company) to credit or debit their account. E.g., an employee is the Receiver if your company is initiating a payroll credit.
- ***Originating Depository Financial Institution (ODFI)***: The financial institution (Bank 1st) with which your company has a contractual relationship for ACH Services. The ODFI is responsible for sending ACH entries to the ACH Operator on your behalf.
- ***ACH Operator***: The central clearing facility for ACH transactions. The ACH Operator is responsible for accepting files of ACH entries from ODFIs, 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.
- ***Receiving Depository Financial Institution (RDFI)***: 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."

Processing Deadlines

ACH files must be submitted to Bank 1st through ACH Business Online Banking using the following guidelines:

Deadline	Day of Delivery to Bank
3:00 p.m.	1 Business Day Prior to Effective Entry Date

- Effective Entry Date (aka the Settlement Date) = the date your company intends the ACH entries to post to the accounts of the Receivers (employees or customers).

- The Federal Reserve and Bank 1st will be closed on most holidays. Refer to the bank's website (www.bank1stia.com/hours) or our Facebook page for the holiday schedule. Please keep in mind that ACH files cannot be delivered on these dates.

Initiating ACH Transactions

- ACH entries are categorized as either consumer (PPD) or corporate (CCD)
- Consumer and corporate entries must be sent in separate batches
- ACH is capable of crediting or debiting checking or savings accounts
- Transactions authorized by phone or internet by the consumer are not permitted
- International ACH transactions are prohibited as well

Authorization

- Authorization to initiate a transaction to the Receiver's account must be received prior to the first ACH transaction
- Sample authorizations may be obtained from the bank upon request.
- If you are **debiting** accounts, the customer must be provided a copy of their authorization prior to initiating the first debit transaction
- All authorizations must be kept for at least two years after the transaction has been revoked
- At any time, an RDFI may request to view a copy of the Receiver's authorization. If they do, you MUST provide it.

Exposure Limits

- Prior to initiating your first ACH file, the bank will notify you of what your exposure limit will be.
- An exposure limit is a set dollar limit that your business cannot exceed in ACH files per effective date.
- If you need this limit to be increased, please contact the bank at 563-422-3883.

Prenotifications

- Prenotifications (prenotes) are zero-dollar entries used to verify that the account number on an entry is for a valid account at an RDFI
- Prenotes are optional
- If you wish to originate pre-notes, please notify the bank so the proper transaction codes can be turned on for you
- Prenotes must be sent at least three banking days before the first live dollar entry
- If there are any errors in a prenote entry or it cannot be processed, you will be contacted by Bank 1st
- Any errors must be corrected prior to submitting the live dollar entry

Micro-Entries

- Micro-entries are credit or debit entries used by an originator for the purpose of verifying a Receiver's account
- Credit micro-entries MUST be in an amount less than $1.00

- One or more debit Micro-Entries must not exceed, in total, the amount of the corresponding credit Micro-Entries
- Micro-entries MUST be submitted as a separate batch of entries with the word "ACCTVERIFY" placed in the company entry description field
- Originator's name should be displayed in the company name field of the entry and should be a name readily recognizable by the Receiver
- Originators must send the debit and the corresponding credit micro-entries simultaneously for settlement at the same time

Notification of Change (NOC)

- When ACH information is incorrect, a notification of change (NOC) is sent by the receiving bank requesting that future entries contain corrected information
- Bank 1st will notify you of any NOCs received on your behalf
- You are required to make the changes noted in the NOC within six banking days or prior to the initiation of the next entry, whichever is later

ACH Returns

- An ACH return is an ACH entry that the RDFI is unable to post for a particular reason
- An RDFI may use the return process for valued ACH entries as well as prenotifications
- Bank 1st will send you a notification if a return entry is received for your account
- If you initiate an ACH transaction and it is returned for one of the reasons listed below, you cannot reinitiate the transaction without a subsequent authorization from the customer.
    - The return reasons include:
        1. Authorization Revoked by Customer
        2. Payment Stopped
        3. Customer Advises Not Authorized
- If a debit transaction is returned due to Insufficient Funds or Uncollected Funds:
    - You cannot reinitiate the transaction for a dollar amount in excess of the amount of the original transaction, e.g., you cannot add on a return fee to the original dollar amount
    - You can only reinitiate the transaction a maximum of two times in an attempt to collect funds
- If you choose to initiate a return fee via ACH, you must do so using the directions listed in the return fee section below

Reinitiation of Returned Entries

Reinitiation of a returned item is allowed under the rules if:

- The entry was returned for insufficient or uncollected funds
- The entry was returned for stopped payment and reinitiation has been separately authorized by the Receiver after the Originator or ODFI receives the Return Entry
- The Originator has taken corrective action to remedy the reason for the return

You have 180 days after the settlement date of the original entry to reinitiate the entry.

A debit entry will not be treated as a reinitiated entry if:

- The debit entry is one in a series of preauthorized, recurring debit entries and is not contingent upon whether an earlier debit entry in the recurring series has been returned
- The originator obtains a new authorization for the debit entry after it receives the original return entry

Format Requirements for Reinitiated Entries

- Reinitiated entries must be submitted as a separate batch that contains the word "RETRY PYMT" in the Company Description field.
- The contents of the Company Name, Company Identification, and Amount fields of the Reinitiated entry 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.

Return Fee Entries

Per NACHA rules, a return fee may be assessed for ACH debits to CONSUMER accounts that are returned insufficient funds (NSF) or uncollected funds (UCF).

Authorization

Before you can initiate such an entry you must receive authorization in one of two ways:

1. Authorization by Notice: You provide notice to the consumer at the time the underlying ACH debit is authorized.
    - Sample Language: "If your payment is returned unpaid, you authorize us to make a one-time electronic fund transfer from your account to collect a fee of $____."
2. Authorization by Person: You may also receive the authorization in person.

Creating the Fee Transaction

- All fees must be in a separate batch (i.e., they cannot be comingled in a batch with your other debits)
- In the company description field when creating your batch, you must put the following RETURN FEE (it must be in all caps). This will show up on your customer's bank statements.

Timing

- An Originator may only originate one Return Fee Entry in relation to an underlying transaction returned NSF, regardless of the number of times the underlying transaction is returned.
- A Return Fee Entry that is itself returned NSF may be re-initiated, but there cannot be a Return Fee Entry initiated on an NSF Return Fee Entry.
- The Effective Date of a Return Fee Entry authorized by notice cannot be later than 45 days after the Effective Date of the ACH return entry, or the receipt of the return of the underlying check transaction.

Return Rates

NACHA Rules require that bank's monitor their ACH Origination customer's return rate level.

- Unauthorized Entry Return Rate must be .5% or less. This includes returns made to you for the following reasons:
  - R05 – Unauthorized Debit to Consumer Account using Corporate SEC
  - R07 – Authorization Revoked
  - R10 – Customer Advises Not Authorized, Improper, or Ineligible
  - R29 – Corporate Customer Advises Not Authorized
  - R51 – Item is Ineligible, or RCK Entry is Improper

- Administrative Return Rate of 3.0% or less. This includes returns made to you for the following reasons:
  - R02 – Account Closed
  - R03 – No Account/Unable to Locate
  - R04 – Invalid Account Number

- Overall Return Rate must remain at 15.0% or less

Exceeding these limits can cause NACHA to assess fines. In such an event, the bank will discuss action plans with the ACH Originator including but not limited to terminating the contract.

Same Day ACH

Originators have the ability to initiate and deliver ACH transactions on the same day, i.e., the effective entry date is the same banking day as the date on which the entry is transmitted by Bank 1st to the ACH Operator.

- Both credit and debits can be submitted for same day processing
- Both consumer and corporate ACH transactions can be submitted for same day processing
- Ineligible entries include:
  - Individual transactions > $999,999.99
  - International ACH Transactions
- Files must be received by 12:30pm to qualify for same day processing
- Same day files will NOT be processed until a notification call is received from an authorized party noted on your ACH contract's ACH Authorized Representative Form and the same day ACH passcode is confirmed
- A fee of $100.00 will assessed per ACH file submitted for same day processing

Reversals

While not encouraged, if you ever need to reverse a file or single entry originated by your company, the reversal must be completed in a timely manner so as to transmit or make available to the RDFI the corrected entry within five banking days following the settlement date of the erroneous entry or file.

OFAC

- To abide by the sanctions of the Office of Foreign Assets and Control (OFAC) you will required to provide us initially and periodically thereafter a list of all individuals/entities that you initiate ACH transactions to through Bank 1st Online Banking
- If this list changes (i.e., you add or remove someone from your list) it is your responsibility to notify the bank promptly
- The bank reserves the right to audit the provided list for accuracy at any time

Retention Requirements

- You must keep records of your ACH entries, including returns and adjustments, in either paper or electronic form for **six** years from the date the entry is transmitted
- Records should accurately reflect the information contained within the original record and should be reproduced for later reference

ACH Fraud Prevention & Data Security

In order to protect the financial institution, your business and your employees/customer's sensitive information it is imperative that your business take extra precautions in regards to originating ACH transactions. The following are sound business practices that the bank recommends to address the risks associated with originating ACH transactions, including but not limited to Corporate Account Takeover (CATO) and other fraud.

What is Corporate Account Takeover?
"It is a type of business identity theft in which a criminal entity steals a business' valid online banking credentials[1]" (e.g., username, password, or one-time token password). "Small to mid-sized businesses remain the primary target of criminals, but any business can fall victim to these crimes[1]" Once this information is obtained criminals can send fraudulent ACH transactions from your account.

How do CATO attacks occur?
"Attacks today are typically perpetrated quietly by the introduction of malware[1]" "Malware is short for "malicious software." Malware is any kind of unwanted software that is installed without your adequate consent. Viruses, worms, and Trojan horses are examples of malicious software[2]" Such software can lead to your sensitive information being stolen.

What can you do to prevent ACH fraud?
Each business should evaluate its risk in regards to CATO as well as other frauds and implement security measures to prevent and mitigate this risk[1]" Please review the following sound practices and implement those that may be applicable to your business' size and complexity.

Computer Security

It is recommended that a business:

- Ensure physical security of the computer that it uses for ACH transactions. Ensure this computer is kept in an area that can only be accessed by authorized employees and cannot be tampered with by non-authorized individuals.
- Use appropriate tools to prevent and deter unauthorized access to its network and periodically review such tools to ensure they are kept up to date. These tools include:
    - Firewalls
    - Anti-malware and anti-spyware programs
    - Anti-virus software
    - Intrusion Detection Systems
- Keep all network servers and PC workstations current with the latest security updates and patches.
- Require unique User IDs to sign into workstations.
- Enable time out features on all computers that house sensitive data.
- Practice password controls including but not limited to strong password requirements, secure password storage, periodic changes in passwords, lockout features after a certain number of invalid login attempts and automatic lockout after defined amount of no activity.
- Restrict access to files on network by job duties.

Websites/Email

- It is recommended that a business be selective of the websites visited on the computer used for ACH submission. Unnecessary and "high-risk" websites (e.g., social networking or personal email) can unintentionally download malware.
- Educate all employees on how to identify fake emails and to be wary of website links and file attachments. Many times, clicking unknown links or unknown attachments can lead to malware.
- Ensure when electronically transmitting protected information, i.e., names, account numbers, etc., that the information is sent securely, i.e., encrypted.

Online Banking

It is recommended that a business:

- Protect your online banking login credentials.
    - Do NOT write your username and password down.
    - Do NOT reveal your password to another person.
    - Do NOT leave your token accessible to unauthorized individuals.
- Ensure procedures are established to properly handle terminated employees with ACH abilities, e.g., reset online banking passwords, delete user, obtain token, etc.

Physical/Digital Security

- Ensure all ACH data including lists of customers/employees and their account information, authorization forms, stored ACH files and any other reporting containing sensitive ACH data is kept secure at all times.
- Dispose of all sensitive data in a secure method, e.g., use of a shredder or a shredding service.

Account Security

It is recommended that a business reconciles their accounts frequently, at a minimum reviewing pending or recently sent ACH files[1]. **NOTE: Unauthorized ACH transactions to non-consumer accounts have a very short**

time frame in which they can be returned. Basically, the bank must return an unauthorized ACH by the day after settlement. PLEASE REVIEW YOU ACCOUNTS DAILY!!

Reporting Suspicious Activity

It is recommended that a business monitor and report suspicious activity. Ongoing monitoring and timely reporting of suspicious activity are crucial to deterring or recovering from these frauds[1].

What is Bank 1st doing to protect your sensitive data from CATO or other ACH fraud?

- Data sent via our Bank 1st ACH Business Online Banking product is sent securely and encrypted.
- We require all Business Online users to login using multi-factor authentication, i.e., username, password, and a one-time token password.
- We conduct a comparison of received files to businesses' sent emails. Any files received without an email will not be processed until the business is contacted and the file is verified.
- Establish, implement, and monitor exposure limits. These limits are set to accommodate your business's activity level but prevent files of excessive dollar amounts.
- Process ACH files under dual control.

If you have any questions pertaining to these rules or any other requirements, please contact the bank at (563) 422-3883.

References

1 – National Automated Clearing House Association. (2011). Sound Business Practices for Businesses to Mitigate Corporate Account Takeover. *Corporate Account Takeover Resource Center*. Retrieved February 27, 2013, from www.nacha.org/Corporate Account Takeover Resource Center.

2 – Microsoft. (2013). What is malware? *Safety and Security Center*. Retrieved March 4, 2013, from http://www.microsoft.com/security/resources/malware-whatis.aspx.

3 - NACHA Operating Rules and Guidelines