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 nor processed 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 can credit or debit checking or savings accounts
- Transactions authorized by phone or internet by the consumer are not permitted
- International ACH transactions are prohibited as well
- PPD credits made for purposes of payroll MUST include PAYROLL in the Company Entry Description field

Authorization

- Authorization to initiate a transaction to the Receiver's account must be received prior to the first ACH transaction
- Depending on the type of transaction (PPD credit, PPD debit, or CCD credit or debit) will determine the required language of the authorization. Sample authorizations may be obtained from the bank.
- 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
- An ACH prenote can be sent at any time, but the first live (money-moving) ACH entry must be sent at least three banking days after the prenote is sent to allow for account verification.
- 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 notify you 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 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 more than the amount of the original transaction, e.g., you cannot add 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 and hasn't been returned more than two times.

- 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.

- Only credits 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 representative noted in your ACH contract's ACH Authorized Signature Form (Schedule D)
- A fee of $100.00 will be 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.
- Reversing entries must be formatted with "REVERSE" in the Company Entry Description field.

OFAC

- To abide by the sanctions of the Office of Foreign Assets and Control (OFAC) you will be 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 **90 days** from the date the entry is transmitted
- Records should accurately reflect the information contained within the original record and should be able to be reproduced for later reference

ACH Fraud Monitoring

- Per the ACH Rules and your ACH Origination Agreement, originators must have established and implemented risk-based processes and procedures in place to identify and act upon ACH entries initiated due to fraud.
- Such procedures include but are not limited to:
    - Annual ACH User Reviews
    - Multi-Factor Authentication (Username, Token Passcode, and PIN)
    - Out of Bank Authentication (Email to Bank 1st Bookkeeping Department)
    - Secure Transmission of ACH Information
    - Receipt of Authorizations from Receivers
    - ACH Data Security (See ACH Fraud Prevention & Data Security Section Below)
    - ACH User Change Notifications (Notify Bank of User Changes ASAP)
    - New Receiver Due Diligence (Call and Verify New Customers/Employees Information)
    - Existing Receivers Changing Account Information (Call and Verify Before Making Changes)
    - Review Your Account Frequently for Unusual Activity (See ACH Fraud Prevention & Data Security Section Below)
    - Secure Systems and Applications (See ACH Fraud Prevention & Data Security Section Below)

- Conduct Fraud Training/Education with Employees (See ACH Fraud Prevention & Data Security Section Below)

- Per the ACH Rules and your ACH Origination Agreement, Company further agrees that established processes and procedures will be reviewed at least annually and updated as appropriate to address evolving risks.

ACH Fraud Prevention & Data Security

Protecting your financial institution, business, employees, and customers requires strong controls over ACH origination. The practices below address common security risks and fraud schemes and are recommended for every business that originates ACH transactions.

1. Secure Computers and Networks

Use the following safeguards for every computer and network involved in ACH activity:

- **Control physical access** - Keep ACH computers in secure areas accessible only to authorized employees.
- **Protect the network** - Use firewalls, antivirus, anti-malware, anti-spyware, and intrusion-detection tools, and review them regularly.
- **Install updates promptly** - Keep servers and workstations current with security patches and software updates.
- **Use individual accounts** - Require a unique user ID for each employee.
- **Enable automatic locking** - Configure inactivity timeouts on computers that store or access sensitive information.
- **Enforce strong password controls** - Require strong passwords, secure storage, periodic changes, lockouts after failed attempts, and automatic locking after inactivity.
- **Limit file access** - Grant access to network files according to job responsibilities.

2. Use Websites and Email Safely

- Limit browsing on computers used for ACH processing to trusted, business-related websites. Avoid high-risk sites such as social media and personal email, which may expose the device to malware.
- Train employees to recognize fraudulent messages, suspicious links, and unexpected attachments.
- Encrypt protected information—including names, account numbers, and other sensitive data—when sending it electronically.

3. Protect Online Banking Access

Protect online banking credentials and promptly remove access when an employee's role changes or employment ends.

- Never write down or share online banking usernames and passwords.
- Keep security tokens where unauthorized individuals cannot access them.
- When an employee with ACH access leaves, immediately reset passwords, delete the user account, recover security tokens, and notify the bank as appropriate.

4. Protect Physical and Digital Records

- Secure all ACH-related data, including customer and employee lists, account information, authorization forms, stored ACH files, and reports containing sensitive information.

- Destroy sensitive records securely by using a cross-cut shredder or a reputable shredding service.

5. Monitor Accounts Daily

Reconcile accounts frequently and review pending and recently submitted ACH files every day. Unauthorized ACH transactions involving non-consumer accounts generally must be returned by the banking day after settlement, leaving very little time to respond.

6. Train Employees to Recognize Fraud

Employees should understand the threats that can cause financial loss or expose business, employee, or customer information. The following schemes are among the most common.

Phishing and Quishing

Fraudulent emails, texts, phone calls, and QR codes are designed to trick recipients into revealing personal or financial information, opening malicious files, or visiting fake websites.

Phishing

Phishing messages imitate legitimate companies or familiar contacts and often create urgency. They may request passwords, account or card information, payment changes, invoice payments, or other sensitive data. Links and attachments may install malware or open fraudulent websites.

Warning signs include:

- Unusual or misspelled sender addresses
- Unexpected requests for money, credentials, or sensitive information
- Suspicious links or attachments
- Generic greetings or vague references
- Poor grammar, spelling errors, or awkward wording

Quishing

Quishing, or QR phishing, uses a QR code to direct someone to a malicious website. Fraudsters may cover a legitimate code with a fake one or pair a code with an urgent or unusually attractive offer.

Scanning a malicious code may lead to malware installation or requests for banking credentials and other sensitive information. A compromised device can expose stored data, browsing activity, and other information accessible from the device.

Protective Steps

Pause before responding to an unexpected message or scanning a QR code. Verify the request through a trusted contact method (e.g. calling them at a number NOT provided through email or QR code), especially when money or sensitive information is involved.

Before you act:

- Check for typos, poor grammar, and unusual wording.
- Be cautious of messages that create urgency or pressure.
- Question unexpected requests and unusual payment methods.
- Do not open suspicious links or unexpected attachments.
- Inspect QR codes for stickers, overlays, or other signs of tampering.

ACH Account and Credential Fraud

Fraudsters may steal an Originator's user ID and password, access the ACH system, and send credits to mule accounts created to receive stolen funds. These accounts are often emptied and abandoned before the fraud is discovered.

Reduce this risk by securing every system used for ACH origination, applying patches promptly, and maintaining current firewall, antivirus, anti-malware, and anti-spam protection.

Website Spoofing

Website spoofing uses a fraudulent site that closely resembles a trusted website to capture usernames, passwords, account information, or other sensitive data.

To reduce the risk:

- Check web addresses carefully for misspellings or altered domains.
- If a site appears suspicious, close it and contact the company through a trusted channel.
- Avoid links from social media, pop-ups, and untrusted websites.
- Enter sensitive information only on secure sites using HTTPS.
- Leave any site that triggers a certificate error or browser warning.

Common Credit-Push ACH Fraud Schemes

Originators should understand evolving fraud tactics and use verification controls before changing payment instructions or releasing funds. Common schemes identified by Nacha include the following:

- ***Business Email Compromise***
  A fraudster compromises or imitates a business leader's email account and directs an employee to send funds to a fraudulent account. The payment is initiated by an authorized employee who has been deceived.
- ***Vendor Impersonation Fraud***
  A fraudster poses as a legitimate contractor or vendor and requests a change to payment instructions. If the change is not independently verified, the next payment may be sent to the fraudster. Public entities may be especially vulnerable because contract information can be publicly available.
- ***Payroll Impersonation Fraud***
  A fraudster impersonates an employee or uses stolen payroll-portal credentials to change the employee's direct-deposit account. Without independent verification, future payroll deposits are redirected to the fraudster.
- ***Account Takeover Fraud***
  A fraudster uses stolen consumer or business banking credentials to access account balances and initiate payments to accounts under the fraudster's control. Because the criminal can see available funds and recent activity, losses can occur quickly.

7. Monitor and Report Suspicious Activity

Monitor ACH activity continuously and report suspicious transactions immediately. Prompt reporting can help stop additional fraud and may improve the chance of recovering funds.

Questions? Contact the bank at (563) 422-3883 for guidance about these practices or other ACH requirements.

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 - NACHA Operating Rules and Guidelines

3 - Fraud Corner taken from Shazam's "2026 Originators Newsletter" – January 2026

Sample ACH Authorizations

These are sample authorization forms for:

- Consumer ACH Debit (Accts Receivable)
- Consumer ACH Credit (Payroll)
- One-time Corporate ACH Debit (Accts Payable)
- Corporate ACH Credit
- Corporate ACH Credit Recurring

Please use these as a guide to ensure your authorizations are NACHA compliant.

Electronic versions are available by request.

CONSUMER AUTHORIZATION FOR DIRECT PAYMENT VIA ACH
(ACH DEBITS)

I (we) hereby authorize _____ ("COMPANY") to electronically debit my (our) account for (select the appropriate box below)

☐ a single (one-time) entry

☐ recurring entries (that recur at substantially regular intervals without my affirmative action to initiate future entries)

☐ subsequent entries (initiated under the terms of this standing authorization) that require my affirmative action to initiate those future entries

and, if necessary, to electronically credit my (our) account to correct erroneous debits or make payment of refunds or other related credits. Please provide account information below.

Account Information

Depository Name ("DEPOSITORY")

_____

Routing Number _____ **Account Number** _____

Select One: ☐ Checking Account ☐ Savings Account

Name(s) on the Account

_____

Amount of debit(s) or method of determining amount of debit(s)

_____

_____

Starting Date: _____ **Frequency of Debit(s)**_____

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 $_____.

I (we) agree that ACH transactions I (we) authorize comply with all applicable laws.

I (we) understand that this authorization will remain in full force and effect until I (we) notify COMPANY [insert manner of revocation, i.e., in writing, by phone, location, address, etc.] that I (we) wish to revoke this authorization.

If requires written notice MUST INCLUDE THIS PART. **Termination notices can be sent to**: Name of Company and Address

I (we) understand that COMPANY requires at least [X days/weeks] prior notice in order to cancel this authorization.

Name _____
(please print)

Signature _____ **Date** _____

CONSUMER AUTHORIZATION FOR DIRECT DEPOSIT VIA ACH
(ACH CREDITS)

I (we) hereby authorize _____ ("COMPANY") to electronically credit my (our) account (and, if necessary, to electronically debit my (our) account to correct erroneous credits). I (we) agree that ACH transactions I (we) authorize comply with all applicable law.

Account Information

Depository Name ("DEPOSITORY") _____

Routing Number _____ **Account Number** _____

Select One: ☐ Checking Account ☐ Savings Account

Name(s) on the Account _____

I (we) understand that this authorization will remain in full force and effect until I (we) notify COMPANY [insert manner of revocation, i.e., in writing, by phone, in person, etc.] that I (we) wish to revoke this authorization.

If require written notice MUST INCLUDE THIS PART. **Termination notices can be sent to**: Name of Company and Address

I (we) understand that COMPANY requires at least [X days/weeks] prior notice in order to cancel this authorization.

Name _____
(please print)

Signature _____ **Date** _____

One-Time CCD ACH Debit Authorization Form

[Your Business Name]
[Your Business Address]
[Your Business Phone Number / Email]

ONE-TIME CORPORATE ACH DEBIT (CCD) AUTHORIZATION FORM

Company Name (Originator): [Your Business Name]
Company ACH ID: [Your 10-Digit ACH Company ID]

By signing this form, the undersigned **Receiver (Customer Business)** authorizes the **Originator (COMPANY)** to initiate a single, one-time ACH debit entry to the corporate bank account indicated below. The Receiver agrees that this transaction complies with all applicable U.S. law and **NACHA Operating Rules**.

1. Customer (Receiver) Business Information

- **Business Name:** _____
- **Authorized Representative Name:** _____
- **Phone Number:** _____ **Email:** _____

2. Corporate Banking Details

- **Depository Bank Name:** _____
- **Account Type (Check One):** [ ] Business Checking [ ] Business Savings
- **Routing Number (9 Digits):** _____
- **Account Number:** _____

3. Payment Details

- **One-Time Debit Amount:** $_____ (USD)
- **Scheduled Date of Debit (on or after):** ____ / ____ / 2026
- **Purpose of Transaction / Invoice #:** _____

4. Authorization & Agreement Terms

This authorization is strictly for a **single, one-time corporate transaction** matching the amount and date specified above. Because this is a corporate (CCD) transaction, the Receiver understands that under NACHA rules, the window to dispute a debit is significantly shorter than consumer transactions.

The Receiver certifies that they are an authorized signor on the corporate bank account listed above and have the explicit authority to bind the company to this agreement. This authorization remains valid until this single transaction has been successfully processed.

5. Binding Signature

- **Authorized Signor Name (Print):** _____
- **Title:** _____
- **Signature:** _____
- **Date:** ____ / ____ / 20XX

Corporate ACH Credit

For a CCD (Corporate Credit or Debit) entry, Nacha does not require a specific standardized form layout, but it does require a commercial agreement or contract between the two business parties that proves authorization and binds both entities to the Nacha Operating Rules.

Sample CCD Credit Authorization Language

ACH CORPORATE CREDIT AUTHORIZATION AGREEMENT (CCD)

Company Name (Originator): [Your Company Name]
Company ID: [10-Digit Company ID / Tax ID]
Contact Info: [Phone Number / Email / Address]

Receiving Company Name (Receiver): [Vendor/Partner Business Name]
Bank Name: [Receiver's Bank Name]
Routing Number (ABA): [9-Digit Routing Number]
Account Number: [Receiver's Bank Account Number]
Account Type: [Checking / Savings]

Payment Terms & Scope:
The Receiving Company hereby authorizes [Your Company Name] to initiate electronic ACH credit entries to the business bank account listed above. This agreement covers [select one: single / recurring] payments for [describe purpose, e.g., invoice disbursements, vendor payments, or service fees].

Timing & Frequency:
Payments will be initiated on [e.g., the 1st of each month / upon invoice approval].

Nacha Compliance & Binding Rules:
Both parties agree to be bound by the Nacha Operating Rules. This agreement acknowledges that originations and receipts must comply with U.S. law and the rules of the National Automated Clearing House Association (Nacha).

Revocation:
This authorization will remain in full force and effect until [Your Company Name] has received written notification of termination from the Receiving Company. Please provide [x days/weeks] prior notice to afford both [Your Company Name] and the bank a reasonable opportunity to act on it. Termination notices can be sent to: [Name of Company and Address]

Authorized Signature:

Print Name: _____

Title: _____

Signature: _____

Date: _____

Corporate ACH Credit Recurring

Here is a sample ACH CCD Authorization Form tailored for recurring business-to-business payments. Under NACHA rules, a **recurring CCD authorization** must clearly state the timing, frequency, and amount (or method of calculating the amount) of the ongoing debits.

RECURRING ACH DEBIT AUTHORIZATION FORM (CCD)

Company (Originator) Information

- **Company Name:** _____
- **Company ACH ID:** _____

Receiver (Customer Business) Information

- **Business Name:** _____
- **Contact Name:** _____
- **Phone/Email:** _____

Payment Authorization Terms

I (we) hereby authorize the COMPANY named above to initiate recurring debit entries to the business account indicated below at the depository financial institution named below. I (we) agree that ACH transactions authorized herein shall comply with all applicable U.S. law and NACHA operating rules.

- **Frequency of Debit:** [ ] Weekly [ ] Bi-Weekly [ ] Monthly [ ] Quarterly
- **Day of Debit:** (e.g., "1st of the month", "Every Friday") _____
- **Start Date:** ____ / ____ / _____
- **Payment Amount:** [ ] Fixed Amount of $_____
- **Variable Amount:** [ ] Itemized billing/invoice amount (Invoice to be sent at least ____ days prior to debit)

Bank Account Information

- **Account Type:** [ ] Business Checking [ ] Business Savings
- **Bank Name:** _____
- **Routing Number (9 Digits):** _____

- **Account Number:** _____

Acknowledgement & Termination

This authorization is to remain in full force and effect until COMPANY has received written notification from the undersigned of its termination in such time and in such manner as to afford COMPANY and the depository financial institution a reasonable opportunity to act on it.

To cancel this authorization, written notice must be submitted to COMPANY at least _____ business days prior to the next scheduled debit date. Written termination notifications can be sent to: [Company Name and Address]

- **Authorized Signatory Name:** _____
- **Title:** _____
- **Signature:** _____
- **Date:** ____ / ____ / _____