Kennebec Savings Bank

WELCOME TO BUSINESS ACH ORIGINATION!

We're glad you've chosen Kennebec Savings Bank's digital services to help you move money quickly and securely in the Automated Clearing House (ACH) network.

As an ACH Originator, you are responsible for complying with the rules set by the National ACH Association (Nacha), the organization that oversees the ACH network. As your Originating Depository Financial Institution (ODFI), Kennebec Savings Bank is here to support you.

This guide will help you understand some of your primary responsibilities as an Originator.

AUTHORIZATION

- You must have a **written and signed authorization** from each receiver before sending ACH transactions.
- Keep all authorization forms on file. You must be able to provide copies to the receiver, their financial institution, or Kennebec Savings Bank if requested.
- Make sure each transaction matches what the authorization allows.
- Without proper authorization, a receiver may dispute and reverse a transaction for up to 60 days (or more in some cases).

See page 2 of this guide for a sample authorization form.

TRANSACTION QUALITY & RULE COMPLIANCE

- Consider ACH payments to be **final**. Sending money to the wrong account or to an unknown party can create delays, returns, or losses. To protect yourself, you may use prenotes ($0 test entries) to confirm account information before sending monetary transactions.
- Use the correct Standard Entry Class (SEC) Codes - **PPD for consumer** transactions and **CCD for business** transactions.
- For all employee payments such as wages and salaries, use "**PAYROLL**" as your Company Entry Description. For debit transactions tied to online purchases, use "**PURCHASE**."
- Monitor and respond to:
  - **Returns**, which are sent when a transaction cannot be processed (such as invalid account, insufficient funds, suspected fraud, stop payment).
  - Notifications of Change (**NOCs**), which indicate that account information needs to be updated before your next transaction.

See pages 3–4 of this guide for a Quick Reference to the Nacha rules.

FRAUD PREVENTION

- Scammers often target businesses to trick them into sending money electronically. Nacha requires you to have documented, risk-based procedures to help detect and prevent fraudulent ACH activity, including scams involving false pretenses.
- Your fraud-prevention measures should include:
  - Dual control (two people approving transactions)
  - Guidelines for verifying and confirming payment instructions with your customers or vendors
  - Other internal security training and practices applicable to your business risk

See pages 5–8 of this guide for recommended security best practices, an originator self-assessment, and a risk management guide template.

ACH AUTHORIZATION AGREEMENT

This **Agreement** authorizes (Company Name) to initiate individual or recurring electronic transactions to the **Receiver** named below using the **Payment Information** and **Payment Details** designated below. This **Agreement** will remain in effect until a termination request is received in writing by (Company Name) in such time and manner as to allow reasonable opportunity to act on it. Further, both parties agree to comply with Nacha Operating Rules and all applicable U.S. law.

Receiver:

Receiver Name	
Address	
City, State Zip	
Telephone	
Email Address	

Payment Information: *Please provide a canceled check, if available.*

Financial Institution Name	
Financial Institution City, State	
Receiver Name on Account	
Routing Number	
Deposit Account Number	
Type of Account	☐ Checking ☐ Savings

Payment Details:

ACH Transaction Type	☐ Credit (Payments) ☐ Debit (Collections)
Frequency (if variable, describe)	
Amount (if variable, describe)	

I authorize (Company Name) to initiate ACH Credits and/or Debits to the deposit account indicated above, provided that each transaction is initiated according to the terms of this **Agreement**. I certify that I am the **Receiver** (or have authority to enter into this **Agreement** on the **Receiver's** behalf, if Receiver is a company).

Receiver / Authorized Signer Date

Printed Name Title, if applicable

ACH QUICK REFERENCE GUIDE

WHO ARE THE PARTICIPANTS?

- An **Originator** initiates entries. This is you.
- The **Originating Depository Financial Institution (ODFI)** is the financial institution with which your company has a contractual relationship for ACH services. This is Kennebec Savings Bank.
- The Federal Reserve is the **ACH Operator**, a central clearing facility for ACH transactions.
- The **Receiving Depository Financial Institution (RDFI)** is the financial institution to which you send your entry.
- The **Receiver** is the individual or company that has authorized you to debit or credit their account at the RDFI.
- The **National ACH Association (NACHA)** is the governing body for the ACH rules.

YOUR RESPONSIBILITIES

- Protect your and your receivers' banking information.
- Follow guidelines listed in the Nacha rules and your agreements with Kennebec Savings Bank.
- Obtain and keep all records of authorization for two years from the date of revocation of authorization or the date of the last entry.
- Ensure entries are sent on the dates and for the amounts authorized in your agreements.
- Be mindful of return rates; make necessary changes to payee information within six banking days of notification by Kennebec Savings Bank and ensure that recurring transactions are ceased in a timely manner when necessary.

ACH REVERSALS

- Reversals may only be made for: 1) duplicate transactions, 2) debit of incorrect amount, account or date, or 3) credit for employment that was also paid via check.
- A reversing entry must be for the full amount originally sent, be sent within 24 hours of discovering the error, and reach the receiver within five banking days of the original entry's settlement.
- If the reversing entry is sent due to incorrect amount or account, a correcting entry must be sent at the same time as the reversal.
- A reasonable attempt must be made to notify the receiver of the reversal.

FRAUD PREVENTION MEASURES

- Limit access to the ACH origination system to designated personnel only.
- Prohibit the sharing of usernames, passwords, and security tokens. Never provide this information to anyone, even if they represent themselves as calling on behalf of Kennebec Savings Bank.
- Use a dedicated computer for your online financial transactions; do not allow email or web browsing on this machine.
- Implement dual control procedures.
- Monitor your account transaction activity daily. Immediately contact Kennebec Savings if a suspicious transaction is identified, as there is a limited recovery window for unauthorized transactions.

GOVERNING RULES & AGREEMENTS

This Quick Reference Guide is not intended to serve as a comprehensive list of the rules, rights, and responsibilities of ACH originators. Originators are required to abide by several rules and agreements including (but not limited to) the following, which are subject to change:

- NACHA Operating Rules (www.nacha.org)
- Regulation E for consumer entries
- Uniform Commercial Code 4A (UCC4A) for corporate credits
- Kennebec Savings Bank's Deposit Account Agreement
- Kennebec Savings Bank's Business Internet Banking Services Master Agreement
- Kennebec Savings Bank's ACH Origination Agreement
- Customer Authorizations

AUTHORIZATIONS

- An **authorization is required** before originating a debit to a consumer's account. However, neither the ACH Rules nor Regulation E require an authorization for ACH credits or reversals.
- As a best practice, Kennebec Savings Bank recommends that you obtain some form of authorization before originating credits as well. For credit authorizations, the authorization should provide you with the right to debit the receiver's account for adjustments or corrections.
- An authorization agreement must exist between you and a business receiver as well, but the NACHA rules do not specifically define what constitutes such agreement.
- You must retain copies of authorizations for **two years** after revocation or transmission of the last live entry, and, upon request, provide them to Kennebec Savings Bank within **ten business days**.

PRENOTIFICATION ENTRIES (PRENOTES)

- A prenote is an optional, non-monetary entry that you can send to verify that a receiver's financial institution and account information is valid.
- If any errors prevent the entry from being processed correctly, a Notification of Change (NOC) or return will be sent to notify you of the problem. Kennebec Savings Bank will notify you of any NOCs or returns received on your behalf.
- If used, a prenote must be sent to the receiver's account prior to a future credit or debit entry by at least **three banking days** to provide time for the RDFI to respond.
- Below are the most used Notification of Change Codes:

NOC Code	Description
C01	Incorrect Account Number
C02	Incorrect Routing Number
C05	Incorrect Transaction Code (transaction code identifies account type as checking or savings)

STANDARD ENTRY CLASS (SEC) CODES

- Below are the payment types you will use to identify ACH debit and/or credit entries transmitted to the RDFI:

SEC Code	Application Use
PPD	Business to consumer transfers for payroll, expense reimbursement, dues, etc.
CCD	Business to business transfers

- Use of other SEC Codes will require pre-approval from Kennebec Savings Bank. For more information, contact our Business Support team.

ACH RETURNS

- Entries that post can be returned. A few of the most common return codes are outlined below:

Return Code	Explanation
R01	Insufficient Funds – available balance not sufficient to cover the debit entry
R02	Account Closed – previously active account has been closed
R03	No Account – the account number structure is valid, but doesn't match an open account
R04	Invalid Account – the account number structure is not valid

- If the RDFI has mishandled an entry or returned it in error, you and the ODFI have the right to dishonor said return.

SECURITY BEST PRACTICES

Safeguarding your accounts is a top priority for Kennebec Savings Bank. We assign unique usernames and passwords, provide security tokens and multi-factor authentication (MFA) options, establish limits for Automated Clearing House (ACH), Remote Deposit Capture and Wire transactions, and monitor for suspicious login and file activity to help protect you and your data. However, despite our best efforts, we cannot control what is most often the initial point of compromise – the computer you use and the staff who process your transactions.

Review the checklists below and implement best practices to strengthen your security posture. You can also visit the resources on Kennebec Savings Bank's website for more tips and information at **www.KennebecSavings.Bank/Security**.

PROTECT YOURSELF AND YOUR TEAM

- ☐ Attend regular security training from consultants, vendors, and Kennebec Savings Bank on topics like strong passwords, MFA, and avoiding scams.
- ☐ Promote a culture of verification by ensuring employees understand their role in preventing fraud and rewarding those who question or report suspicious activity.
- ☐ Never share or reuse passwords; use secure password management tools to track multiple logins.
- ☐ Review, update, and retrain on procedures annually and anytime there is a change in staff.
- ☐ Consider adjustments to policies and procedures for remote workforce, such as limiting access to financial systems to in-office employees.
- ☐ Establish internal procedures and controls. A few "must have" guidelines include:
  - Acceptable use of work devices: define who can install software, etc. Limit computer use to work-related activities. Avoid personal email use on business-owned devices.
  - Authorities and limits with dual control and signoffs, especially with transaction processing.
  - Expectations to verify payment requests by confirming instructions verbally with a known contact, especially for email requests.

PROTECT YOUR SYSTEMS & USE CAUTION WITH EMAIL

- ☐ Assess the measures you have in place to safeguard against unauthorized access to the computers used for online banking activities.
- ☐ Verify every email's authenticity; avoid unknown links or attachments, be cautious with unknown senders, and strengthen anti-spam tools if needed.
- ☐ Install and update software, firewall, malware and antivirus protection on your systems.
- ☐ If possible, avoid accessing financial services websites on open Wi-Fi networks.

PROTECT YOUR ACCOUNT INFORMATION

- ☐ Review account activity daily and immediately report unauthorized transactions. Timeframes are limited for recovering funds. Leverage reporting and alerts from online banking and Positive Pay services.
- ☐ Restrict online access to authorized personnel. Segregate responsibilities for payment, approval, deposit, and reconciliation activities when possible.
- ☐ Review employee access regularly and notify Kennebec Savings Bank promptly of any changes to online access.
- ☐ Store check stock, signature stamps, monthly statements, online banking tokens and other account-sensitive items securely and with access control.

USE YOUR RESOURCES

- ☐ Contact Kennebec Savings Bank ASAP if you have concerns regarding your accounts or online banking access. We can assist you with navigating challenges, disabling access, and updating signers.
- ☐ Obtain insurance to protect you against fraud losses.
- ☐ Bookmark and reference key industry resources for training, education and reporting incidents:
  - FBI Scams & Safety: www.fbi.gov/scams-and-safety
  - FBI's Internet Crime Complaint Center: www.ic3.gov
  - Financial Crimes Enforcement Network: www.fincen.gov
  - Your local payments association (NEACH): www.neach.org

ACH ORIGINATOR RISK MANAGEMENT GUIDE

Scammers often target businesses to trick them into sending money electronically. Nacha requires all ACH Originators to have **documented, risk-based procedures** in place to help detect and prevent fraudulent ACH activity, including scams involving false pretenses.

False Pretenses: Entries "authorized" by you but induced by deception (i.e.: business email compromise, vendor impersonation, payroll diversion).

In short, how do you protect yourselves from falling victim to a scammer? The prompts in this guide are designed to help you evaluate your current practices and develop risk management procedures.

1. SECURITY TRAINING

How often do you meet with staff to address fraud prevention and security best practices? What topics do you cover and who is required to attend?

Best practice:

- Keep records of your meetings, attendees, and topics covered.
- Keep a record of any updates to this document or other internal policies/procedures on at least an annual basis, or whenever key staff changes occur.
- Require your staff to sign off on procedure reviews and training.

Procedure Key Content:

- ☐ Training dates/frequency
- ☐ Topics covered
- ☐ Staff required to complete training
- ☐ Procedure review frequency
- ☐ Causes for more frequent updates (staff changes, etc.)

2. VERIFICATION OF PAYMENT INSTRUCTIONS

What procedures do you have in place for verification of new or updated payment instructions?

Best practice:

- Keep all authorization forms and documents on file.
- Use $0 prenote entries to verify receiver account information before sending "live" transactions.
- Require call backs, multiple-sign offs or other controls when updating existing payment information, especially if received via email.

Procedure Key Content:

- ☐ Steps taken to verify suspicious payment instructions
- ☐ Payment instruction verification steps
- ☐ Phone verification process
- ☐ Dual-control requirements
- ☐ ACH approval process

3. ACCOUNT REVIEW & CONTROL PROCEDURES

How often do you review the current signers, digital banking users and permissions for your organization? How often do you reconcile account transaction activity? Do you have proper segregation of duties?

Best practice:

- Review account signer and digital user information with Kennebec Savings Bank at least annually or whenever key staff changes occur.
- Always keep accounts and online banking access up to date to mitigate the risk of internal fraud.
- Reconcile account transaction activity daily to reduce the risk of loss.
- Document the checks and balances you have in place within your organization.

Procedure Key Content:

- ☐ Account activity review frequency
- ☐ Responsible reviewer(s)
- ☐ Actions when unusual activity is detected
- ☐ Staff with online access
- ☐ Payment initiator(s)
- ☐ Payment approver(s)
- ☐ Reconciliation staff

4. PASSWORD PRACTICES

How do your users access digital banking? What controls or requirements do you have in place for users? Do you have a password management solution (LastPass, Keeper, etc.) or procedures related to storing password information?

Best practice:

- Never allow users to share login information.
- Require MFA for all logins to digital banking.
- Do not store login information by unsecured means, such as writing them in notebooks or on sticky notes.

Procedure Key Content:

- ☐ Password sharing policy
- ☐ Password management tools used
- ☐ Multi-Factor Authentication requirements

5. COMPUTER SECURITY & WORKPLACE CONTROLS

What policies and procedures do you have related to the security of your computer systems, allowed devices and access points, and remote work?

Best practice:

- Review and document your Human Resources or Information Security/Technology team requirements as related to digital banking and staff access.

Procedure Key Content:

- ☐ Acceptable use of devices
- ☐ Policy for open Wi-Fi use
- ☐ Remote work policies
- ☐ Procedure for evaluating unknown emails
- ☐ Anti-spam tools used
- ☐ Suspicious email reporting contact

6. SECURE STORAGE

How do you store documentation, such as authorization forms? Would you be able to provide these in a timely manner upon request?

Best practice:

- Securely store all online banking tokens, documents, payment information, etc. in locked cabinets or vaults and organize them for efficient retrieval.

Procedure Key Content:

☐ Online banking tokens stored at

☐ Other sensitive documents stored at

7. BANK CONTACT INFORMATION

Who and how would you contact Kennebec Savings Bank in the event of suspected fraud or questions about the Nacha rules? Who at your organization is authorized (per the business resolution) to request information and authorize changes to your ACH program?

Best practice:

- *Update this information regularly and ensure that it is available to all applicable staff.*
- BusinessSupport@KennebecSavings.Bank
- Online Banking Message Center secure message
- (207) 622-5801

Procedure Key Content:

☐ Kennebec Savings Bank key contact name

☐ Phone/email

☐ Authorized contact(s) at your organization (on the resolution)

8. INSURANCE COVERAGE

Do you have fraud protection insurance for your organization? If so, list the policy information and insurance provider contact information below.

Best practice:

- Review your current levels of business insurance, investigate options and fully understand responsibilities and limitations.
- Ensure that the most updated information is available to staff in the event of fraud.

Procedure Key Content:

☐ Insurance provider

☐ Policy type/coverage