Best Practices– Banking Security

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**.

Prepare 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.
- ❑ 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.
- ❑ 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.

Protect Your Systems & Exercise 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 as there are limited timeframes for recovering funds. Leverage reporting and alerts from online banking and Positive Pay services.
- ❑ Restrict online access to authorized personnel. Segregate responsibilities among different employees for payment, approval, deposit, and reconciliation activities whenever possible.
- ❑ Review key employee access regularly and notify Kennebec Savings Bank promptly of any changes to online account 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

New Feature – Payee Emails

What you need to know:

A new service allows you to optionally send email notifications to your payees for ACH and Wire transactions.

- Available for ACH Templates, Quick ACH, and Wire submissions
- **To send email notifications, you must check the box** during transaction processing
- All payees in the batch **with an email address in their payee record** will receive a notification when the batch is processed by KSB
- Payees can be opted out by removing the email address from their payee record
- The email notifications received by the payee will include your business name, the payment type, payment amount, and posting date. The From address on the email is: noreply@kennebecsavings.bank

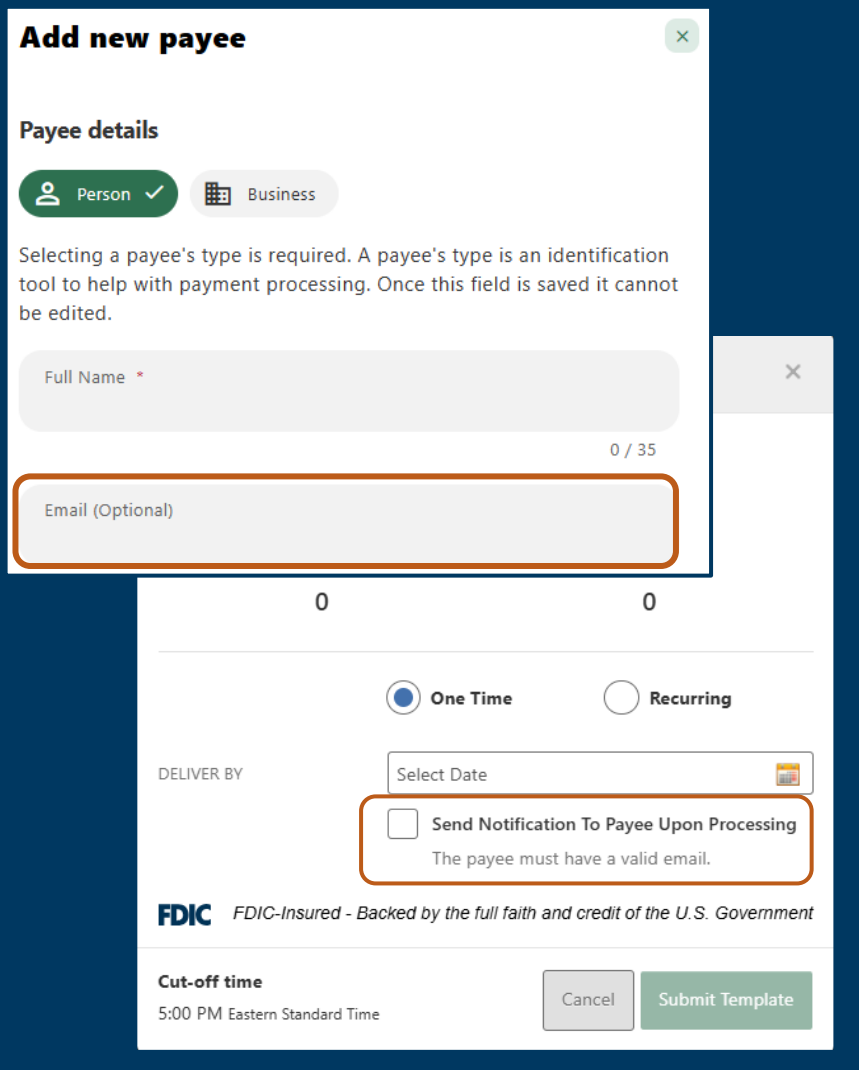
How To:

Add/Remove an Email Address from a Payee

- Business Banking > Business Admin > Payees
- When adding new or editing existing payees, email is an optional field, available on Person and Business records.

Send notifications to eligible Payees for an ACH or Wire

- On the confirmation screen, check the "Send Notification" checkbox and submit

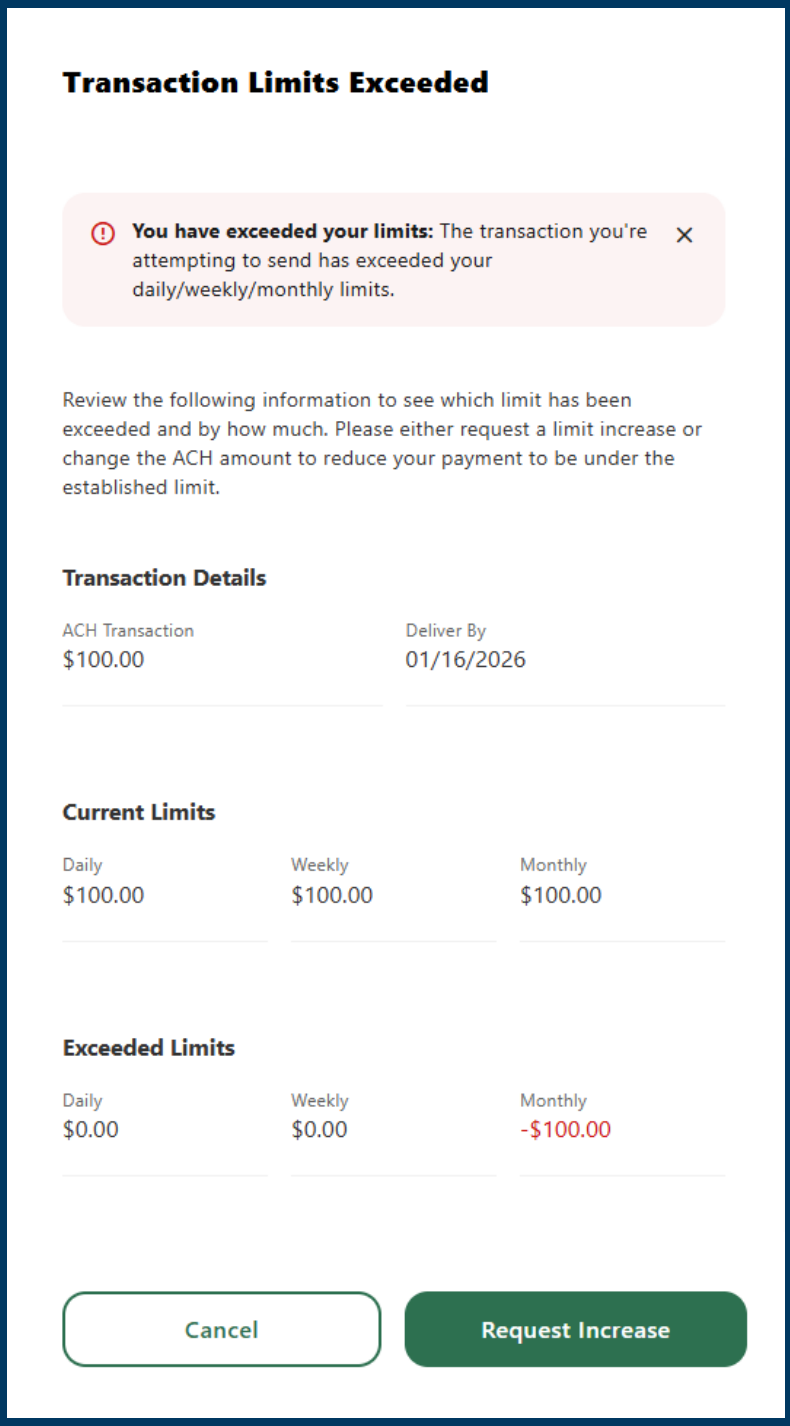


Feature Highlight – Limit Increase Request

What you need to know:

We've streamlined limit increase requests for ACH and Wires to make them easy and trackable!

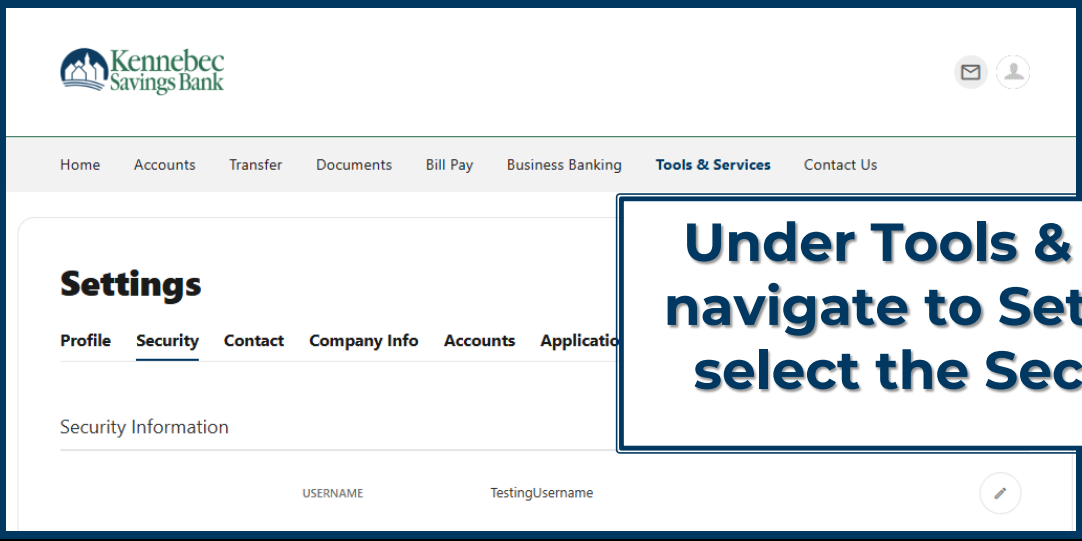
- When a limit (ACH Collections, ACH Payments, Wires) is exceeded, users are prompted to request a limit increase.
- Input the amount of the increase needed and the reason for the increase - BE SPECIFIC.
- The batch is queued while the request is processed.
- KSB's Business Support team will be notified via Digital Banking and we will begin processing the increase.
- When an increase request is granted, the batch will continue through the normal process of dual control and Bank release.
- If the increase request is declined, the batch will be automatically cancelled.



Special Note:

We will always do a security call-back to confirm limit increase requests.

Feature Highlight – MFA Methods



Under Tools & Services, navigate to Settings and select the Security tab

Multi Factor Authentication Set Up

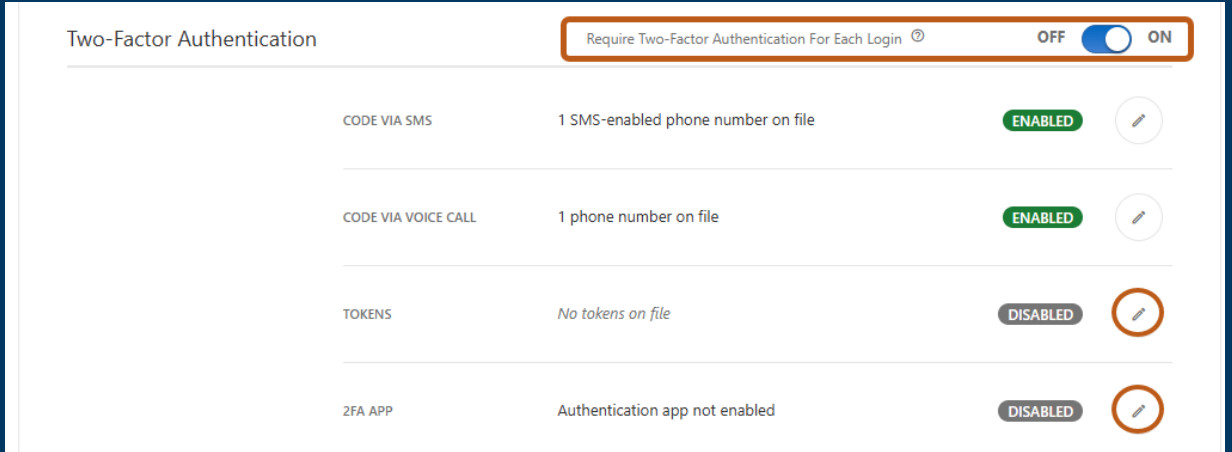
We recommend enabling Two-Factor Authentication for Each Login as a layer of protection in case of compromised username and password.

In addition to SMS Text Messages and Voice Calls for one-time passcodes, we offer:

- Tokens –
  - Request a "**hard token**", a small device that generates one-time passcodes, via online banking or by emailing BusinessSupport@KennebecSavings.Bank.
  - Alternatively, you can download the **Entrust Identity** app and set up a "soft token" on your mobile device to generate passcodes
- 2FA App – 3rd party app that generates one-time passcodes. Supported apps include Cisco **Duo**, Twilio **Authy** and **Google Authenticator**

After receiving your hard token or downloading your soft-token/2FA App, navigate to Tools & Services > Settings > Security and click the Edit pencil beside the method. Users will be guided through on-screen set-up.

Always keep at least two options enabled!



Quick Reference Guide – ACH Rules

Who are the ACH Participants?

1. An **Originator** initiates entries. This is you.
2. 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.
3. The Federal Reserve is the **ACH Operator**, a central clearing facility for ACH transactions.
4. The **Receiving Depository Financial Institution (RDFI)** is the financial institution to which you are sending your entry.
5. The **Receiver** is the individual or company that has authorized you to debit or credit their account at the RDFI.
6. 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 your agreements with Kennebec Savings Bank, as well as the Nacha rules.
- 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 transaction, 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 a 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 or MFA. Don't forget to change passwords periodically.
- 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 and 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

Quick Reference Guide – ACH Rules

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 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**.

Prenotifications (Prenotes)

- A prenote is an optional, non-monetary entry that you can send to verify that a receiver's outing and account number are valid.
- If any errors prevent the entry from processing 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. Refer to your ACH Origination Agreement for more information.

ACH Returns

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

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 the return.

Revised 01/2025

Important– 2026 ACH Rules Updates

New NACHA Rule:

Effective no later than March 20, 2026, Nacha rules require all ACH Originators to use standardized Entry Descriptions for payroll and online purchase transactions. The intention of this new rule is to improve fraud detection and transparency across the ACH network of senders and receivers.

What this means for you:

Anytime you submit payroll for wages, salaries, bonuses, commissions or similar compensation to your employees (Consumer Payments – PPD, Credits), you must use PAYROLL as the entry description.

If you submit entries intended to collect funds from your customers for purchases, they made or authorized online, you must use PURCHASE as the entry description. Though purchases made online are most commonly WEB debits, this may apply to entries you originate using the Consumer Collection – PPD, Debits option.

If you use a third party to generate the ACH files that you upload to Kennebec Savings Bank's ACH Origination service, you may need to contact your vendor. Ensure that they are complying with this new rule and including the appropriate Entry Description into the file you upload to online banking.

New NACHA Rule:

Effective no later than June 19, 2026, Nacha's fraud-monitoring rules require all ACH Originators to have established, implemented, and documented fraud prevention policies and procedures reasonably intended to identify and prevent ACH fraud, including unauthorized transactions and those authorized under false pretenses. This new rule also requires that you internally review your written policies and procedures at least annually and make updates as needed.

What this means for you:

You will need to have written procedures tailored to your company's role, size, and transaction activity, and provide these to Kennebec Savings Bank if requested by Nacha.

Examples of the written policies and procedures for your users related to stopping fraud include practices such as requiring dual control and Multi-Factor Authentication (MFA)and guidelines related to verifying new and changed payment instructions.

Nacha does not mandate that you implement specific tools or new technologies. The new rule allows flexibility for you to decide what is needed for your organization. Your monitoring should be reasonably designed and effectively maintained.

As the implementation date for this new requirement approaches, Kennebec Savings Bank will contact you to ensure your understanding of this rule.

Self Assessment– ACH Originators

Please consider the following questions as you evaluate your ACH origination practices:

Authorization:

- Do you have an authorization agreement on file for each receiver to whom you originate debits? Credits?
- Where and how do you store these authorizations? (In a locked file cabinet, digitally)
    - Who in your office has access the copies?
    - How long do you retain copies of authorization agreements?
    - Upon request, could you provide a copy of an authorization to Kennebec Savings Bank within 10 banking days?

File Transmission Procedures:

- How frequently do you submit files?
- Do you use the template, recurring file, or import option(s)?
- Do you initiate prenotification (prenote) entries?
    - If so, do you wait 3 business days before transmitting a live entry to the account to which you've sent a prenote?
- What are your origination limits (daily and monthly)?
- Which entry types do you originate in your files? (SEC codes such as PPD, CCD, or other)
    - Are all transactions to consumers sent as PPDs?
    - Are all transactions to businesses sent as CCD?
- Who in your office is responsible for ACH origination?
    - Does each responsible party have their own username and security token for Kennebec Savings Bank's Online Banking service?
- Do you originate solely for the benefit of your organization (not on behalf of any other entity)?
- What is your procedure for handling notifications of change (NOCs) and returned entries?

Security & Compliance:

- Do you keep or have access to a copy of the Nacha Rules for reference? Or, do you know how to obtain a copy?
- What Multi-factor Authentication (MFA) options do your users have in place?
    - How regularly do users change login passwords?
- Do you have dual control procedures in place for ACH file origination? For adding or editing payee information?
- How do you protect your receiver's personal and financial information?
    - Where, and for how long, do you store copies of transmitted ACH files?
    - Do you have a process for securely destroying data beyond your retention timeframe?

As usual, we'll be reaching out to several ACH Originators to plan audits/site visits in 2026.