Let's Work Together to Protect Your Business.

Here are some steps to help keep your business secure.

At Kennebunk Savings, we want you to know that we use industry-leading technology to keep your business and personal information safe and secure.

Here's how Kennebunk Savings helps keep your information secure

Online Account Security: Kennebunk Savings' approach to security extends beyond a unique user ID and password. We use strong encryption, firewalls, technology updates, multiple validations and regular security testing of our online systems.

Account Alerts: Online and mobile banking offer alerts that you can activate to help you monitor your account activity.

Fraud Services: Our Fraud Services monitor for suspicious activity on your debit card 24/7. When a transaction is not consistent with your usual card activity, you will receive a text and/or a phone call from Fraud Services to verify the authenticity of your card transaction. We will never ask for your full card number, full social security number, expiration date on your card, your card PIN, or the CVC code when identifying you. Instead we will use our standard identification procedures: we'll ask only for the last 4 digits of your card, plus the last 4 digits of your social security number. If you cannot provide these details, we'll ask you to verify your date of birth and your mother's maiden name. You will also have the option to be verified using a One Step Authentication. This simple process sends a five-digit passcode via SMS text to your cell phone, allowing for a quick and convenient verification without asking standard identification questions. Important steps you should take to be sure Fraud Services can work on your behalf:

- Make sure Kennebunk Savings has your most current phone number(s).
- Always notify us when you plan to travel.

To update your personal contact information or notify us of your travel plans, call Customer Care at 1.800.339.6573 or visit your local banking office.

Controls for secure account access with Online Cash Management: Manage your business accounts online with Online Cash Management for multiple levels of security.

- The Security Token adds another layer of security with a one-time password that not only verifies the identity of the person logging in, it also confirms that they are logging into a trusted site.
- Multi-level permission controls let you define and limit employee access to your online banking accounts.

Help protect your business from fraud

- Protect your user ID, password, token (if applicable) and security challenge questions. Use different and strong passwords for different websites and consider changing your PINs/passwords regularly.
- Do not share your PINs, debit card numbers, passwords or social security number with anyone.
- Do not give personal information (such as birthday, email or address) to anyone via email or over the phone unless you verify the source.
- Beware of emails, pop-up requests and text messages that require an urgent reply. Don't ever open attachments, click on links, or respond to emails from unknown senders.
- Always log your computer off and close your browser to prevent any unauthorized access.
- Install operating system (Windows and Mac OS) and application "updates" when you receive them.
- Install anti-virus software and keep it current daily.
- Use a secure connection when providing confidential information online.
- Scan for spyware and adware.
- Never leave your laptop/device unattended.
- Back up important files.
- Keep all your information up-to-date with the Bank. This includes your current phone numbers and mailing and email addresses.

Key things to remember

Do not send money or give out personal information in response to any unexpected request(s)—whether it comes as a text, a phone call, or an email. If you do receive a suspicious request, always verify who is contacting you before responding. Here's how:

- **Phone:** Hang up the phone and call back using a number you know to be legitimate, from your bank or other reliable source, and ask for more information.
- **Email:** Do not respond until you authenticate the sender. Call the company to confirm the sender's identity and the legitimacy of the company's offer.
- **Internet Offers:** You can check out other companies and offers with the Better Business Bureau, Federal Trade Commission and National Fraud Information Center.

Guidance for you and your employees

- Establish clear policies and procedures for employee use of your company information technologies.
- Require complex passwords, using a combination of numbers, symbols, and letters.
- Change passwords regularly (i.e. every 30 days).
- Do not give user names or passwords, or other computer/website access codes to anyone.
- Do not open emails, links, or attachments from strangers.
- Do not allow employees to install or connect any personal software or hardware to your network without permission.
- Limit which office computers have access to social networking sites to help safeguard your company from online threats, like malware and viruses.

Report fraud and suspicious cyber incidents

Report Immediately: Call Kennebunk Savings at **1.800.339.6573** or visit your nearest branch if you suspect fraud or identity theft involving your Kennebunk Savings accounts or debit/ATM cards. We provide 24/7 debit card fraud assistance. Even if you suspect fraud or identity theft that does not involve your Kennebunk Savings accounts or cards, call us so that we can monitor your accounts.

Document Your Communications: Keep a log of all conversations related to the suspicious incidents, including dates, names, and phone numbers. Keep copies of all communications and send correspondence by certified mail, return receipt requested.

Contact the Credit Bureaus: Contact the toll-free fraud numbers of any of the three credit bureaus to have a fraud alert placed on your credit report. Request a credit freeze, which is now available by law for free.

Equifax	www.equifax.com	1.888.766.0008
Experian	www.experian.com	1.888.397.3742
TransUnion	www.transunion.com	1.800.680.7289

Contact the Federal Trade Commission: File a complaint with the Federal Trade Commission (FTC) by phone: 1.877.ID THEFT (1.877.438.4338); online: www.ftc.gov/idtheft; or by mail. The ***FTC's Identity Theft website*** is a national resource that provides information to help people protect themselves and helps victims of identity theft repair damage to their credit records.

Contact Your Local Police Department: Report suspected theft of business or personal financial information. If there is a monetary loss, contact your regional U.S. Secret Service office in addition to your local police department.

Kennebunk Savings
800.339.6573 • kennebunksavings.com
Member FDIC Equal Housing Lender

950-040 10/18