Security

Protect Yourself From Fraud

Have a Question?

safe & secure

Arm yourself against fraud
with these important tips.

Protecting your finances and privacy has always been a top priority of Rollstone Bank & Trust. The links on this page will help you arm yourself with the knowledge needed to avoid fraud and loss. One of the best ways to protect yourself is to be aware – if something seems suspicious, it probably is.

Remember that Rollstone Bank will NEVER call, email, or text you and ask for confidential financial information. If you are ever unsure of something that has our name on it, please call us for verification at 800.640.1166. If you think you have become a victim of fraud or identity theft, please report it to us immediately by phone at 800.640.1166 or by email.

Scammers follow the headlines. *Expand*

The coronavirus has prompted a new wave of fraud. Criminal actors are using a variety of means to contact potential victims. We remind you to:

- **NEVER** give your account numbers, Social Security number, or other personal information over the phone or via electronic means.
- **REGULARLY** check your account activity, via online or mobile banking, or open your paper statement immediately upon receipt.

- **REPORT** any questionable activity.

Be vigilant and advise friends and family to be mindful of this new fraud variation, as many people are depending on the stimulus relief payments and may fall victim to these cybercrimes.

Please contact us if you have any questions.

Monitor your credit report. *Expand*

You are entitled to a free copy of your credit report EVERY WEEK through December 2023 from the 3 major credit bureau agencies, in addition to your free annual copy. Take advantage of this opportunity and stay on top of your credit. More information is available at AnnualCreditReport.com

The Federal Trade Commission (FTC) provides some great information about credit reports on their website. Learn more at consumer.ftc.gov.

The importance of updating your devices *Expand*

“One of the best ways you can protect yourself is to ensure the technologies you use have all the latest updates, making it much harder for cyber attackers to break into them.”

Read this very informative article on “The Power of Updating”. https://www.sans.org/security-awareness-tr…/…/power-updating

Email fraud – against consumers & businesses *Expand*

There are a variety of email scams going on every day, targeting individuals as well as C-level employees at businesses. Learn more about phishing, work-from-home scams, business email compromises and more.

Federal Trade Commission
Commonwealth of Massachusetts Fake check scams *Expand*

If you receive a check in the mail that you were not expecting, it may be a scam that could cost you thousands of dollars. There are many variations of check scams, such as someone offering to:

- Buy something you advertised for sale;
- Pay you to work at home;
- Give you an "advance" on a sweepstakes you've won; or
- Give you the first installment on the millions you'll receive for agreeing to transfer money in a foreign country to your bank account for safekeeping.

Fraudulent checks look real. You can protect yourself from being victimized with these simple steps:

- Call the bank the check is drawn on to verify its authenticity.
- Monitor your account regularly through online banking
- Report fraud attempts to the Bank, and keep the check to aid in the investigation.

Educate yourself at these websites:

- National Consumers League
- Office of the Comptroller of Currency
- Commonwealth of Massachusetts

Identity theft *Expand*

Identity theft is a crime in which an impostor obtains key information about you, such as your driver's license and Social Security numbers, and impersonates you. The information can be used to obtain credit, merchandise and services in your name. It can ruin your credit and take substantial time and money to rectify. Learn how to protect yourself at these sites.

Federal Trade Commission
Commonwealth of Massachusetts Stay safe at the ATM & Night Depository. *Expand*

At Rollstone Bank & Trust, we want to make banking convenient for our customers, but we also want you to be safe. When using the ATM or Night Depository, please keep the following tips in mind:

- Prepare your transactions at home.
- Be mindful of surroundings.
- Use well-lighted facilities.
- Take someone with you.
- Don’t proceed if anything looks suspicious.
- Don’t accept assistance from anyone you don’t know.
- Don’t resist a robbery; try to remember details and call the police immediately.
- Count your money in a secure area.
- Keep car doors locked at drive-up ATMs.
- Protect your PIN
    - Don’t write it down where it can be easily discovered.
    - Don’t tell anyone your PIN.
    - Prevent others from seeing your PIN when you enter it.
- Don’t lend your card to anyone.
- Don’t leave receipt in or near the ATM.
- Record each transaction and compare to your statement.
- Notify the bank as soon as possible if you lose your card.

Protecting our customers & employees *Expand*

The safety and welfare of our customers and employees is very important to us at Rollstone Bank & Trust. To help ensure this, we have adopted a policy supported by our local Police Departments and the Massachusetts Bankers Association that requires customers entering our banking facilities to remove their hats, hoods, headgear and sunglasses. At this time, we also ask that you adhere to protocols we have put in place to mitigate the spread of coronavirus.

We are asking for your cooperation in supporting this policy and apologize for any inconvenience that it may cause. Our commitment is to provide safe working conditions for our employees and a safe banking environment for our customers. We believe this policy will help us do both.

To learn more about bank robberies in Massachusetts, and see just why it's so important for us to enforce this policy, please visit the Mass Most Wanted website.

If you have any questions at all regarding this policy, please contact us. Thank you for your understanding and for banking with Rollstone Bank & Trust.

Best online banking practices for businesses *Expand*

Rollstone Bank & Trust is committed to providing convenient eBanking tools to you while maintaining strict security procedures throughout our organization. To help you keep your online transactions safe and secure, here are a few recommended best practices to help mitigate fraud.

Computer and Mobile Device Security

- Obtain and install security suite software – Anti-Virus software alone is not enough.
    - Use caution selecting product – free online software often is malware.
    - Keep software updated.
- Use a dedicated computer for online banking that is restricted from general internet browsing/surfing and email.
- If you must use a multi-purpose machine and will be checking mail, avoid clicking links in email. Also, set email to display without HTML formatting, if possible.
- If you install it, patch it! Keep the operating system up-to-date with patches. It is also important to update

third-party software on your system.
- Establish regular automated backups of key systems.
- Have a plan in place to respond to a security incident, such as ransomware.
- Always use current, supported browsers.
- Always lock your computer when stepping away.
- Avoid saving passwords to your computer or mobile device.
- Never access a financial institution website for online banking (or any privileged or sensitive system) from a public computer at a hotel/motel, library, coffee house, or other public wireless access point.
- Install a VPN on mobile devices.
- All devices should be set to logoff automatically after a few minutes of no activity.

Users

- Restrict access to appropriate employees and always keep current.
- Implement transaction limits.
- Create unique login credentials for each user (no "group" access).
- Educate all company personnel on good cyber security practices.
- Protect against Business Email Compromise (BEC) and Email Account Compromise (EAC). Exercise caution when given instructions via email from your CEO, Manager, or another employee to perform a transaction or provide information.
- Do not allow remote access to your PC unless you initiated the call with a trusted partner.

Login

- Never share user IDs, passwords, PIN numbers, etc. with anyone. Do not leave them in an area that is not locked/secured.

- Do not use an email address as User ID.
- Do not use the same login or password on any other website or software.
- Use complex password phrases with special characters.
- Ensure mobile devices used to obtain one-time passcodes are secure.

Accounts

- Monitor accounts frequently (daily as a best practice).
- Take advantage of Alerts in BeB to notify you of online activity.
- Utilize dual control for transaction processing.
- When implementing changes for destination of funds (i.e., employee's direct deposit of payroll, payment of invoice, etc.), be sure to confirm the changes with the appropriate individual(s) and positively identify them; do not accept email requests.

OPERATIONAL CONTROLS FOR CCX (remote deposit)

- Make sure employees are appropriately trained with respect to CCX and equipment.
- Each user that accesses the system should have a unique User ID and Password.
- Keep user IDs and passwords confidential.
- Endorse items deposited via CCX as follows: "For Remote Deposit at RBT Only 211370736."
- Restrict access to processed checks to only those employees involved in deposit processing.
- Ensure processed checks are appropriately endorsed and stored in a secure location for 60 days from the date of deposit.
- Promptly destroy processed checks at the end of the 60-day period.
- Have a method in place for secure destruction of processed checks.

Best online & mobile banking practices for consumers *Expand*

Rollstone Bank & Trust is committed to providing convenient eBanking tools to you while maintaining strict security procedures throughout our organization. To help you keep your online transactions safe and secure, here are a few recommended best practices to help mitigate fraud.

Computer and Mobile Device Security

- Obtain and install security suite software. Anti-Virus software alone is not enough.
    - Use caution selecting product – free online software often is malware.
    - Keep software updated.
- Install software patches and operating system updates promptly.
- Secure your home wireless network.
- Be sure all security features on mobile device are enabled.
- Use a password on all mobile and electronic devices.
- Install a VPN on mobile devices.
- Mobile devices should be set to logoff automatically after no more than two minutes of non-use.
- Report lost/stolen mobile phones.
- Only download mobile applications from trusted sources.
- Refrain from storing sensitive information (including passwords/passphrases) on a mobile device.
- Never access a financial institution website for online banking (or any privileged or sensitive system) from a public computer at a hotel/motel, library, coffee house, or other public wireless access point.
- Never leave your computer or mobile device unattended when using online banking services.
- Do not allow remote access to your device unless you initiated the call with a trusted partner.

- Always use current, supported browsers.

Authentication to Secure Site

- Choose a sufficiently complex passphrase and change it regularly. Every 3 – 6 months is the recommended frequency.
- Do not write passwords/passphrases down.
- Never use obvious passwords, such as zip code, year of birth, or social security number.
- Create different passphrases for different sites.
- Do not share your login credentials with anyone.
- Always use Sign Off or Log Off when exiting a secure session.

Monitor Your Accounts

- Monitor accounts frequently.
- Set-up alerts for notification of transaction/balance information.
- Enroll in eStatements to eliminate paper statements from mailbox theft.
- Periodically review your credit bureau or enroll in a service that monitors your credit.

Email

- Always use caution when opening email from unknown sources.
    - Poor grammar/spelling may indicate fake email.
- Never provide personal, sensitive data via unsecure email.
- Do not open links or attachments from unknown senders.
- Change your password often.