Always you. csb Cambridge SAVINGS BANK

FRAUD AWARENESS & PREVENTION CHECKLIST

Cambridge Savings Bank strives to be your partner in protecting you and your business from fraudulent activity. Use these helpful tips to strengthen your ability to protect yourself, your employees and your business from becoming a victim of fraud.

ACCESS CONTROL & SECURITY

- ☐ Create a strong password or passphrase[1] with at least 8 characters that includes a combination of mixed case letters, numbers and special characters.
- ☐ Prohibit the use of "shared" usernames and passwords for online banking systems.
- ☐ Use a different password for each website that is accessed. Consider using a secure password manager to help manage unique passwords.
- ☐ Never give your password to anyone, even a bank employee.
- ☐ Disable, expire or delete user accounts when employees leave your organization.
- ☐ To protect privacy, use secure, up to date email software and mobile applications when communicating or collecting confidential/sensitive information.
- ☐ Ensure separation of duties by assigning appropriate permissions and access to users. Users should not create two profiles for themselves to bypass dual control requirements.
- ☐ Update passwords regularly to improve security.

INTERNET USAGE

- ☐ Employ multi-factor authentication options such as hardware tokens, PIN codes, authenticator apps, and/or SMS codes where possible to reduce the risk of credential theft.
- ☐ Do not download software from unknown sources.
- ☐ Employ a firewall to limit the potential for network intrusion. Consult with IT security experts to assess your network security infrastructure, as your network security needs may or may not exceed what your internet service provider offers.
- ☐ Employ an email filtering solution to examine and apply controls to all email flowing into your organization, and to help block various types of malicious content and SPAM.
- ☐ Install and keep up to date anti-virus and anti-malware software.
- ☐ Do not open web advertisements or "pop-ups".
- ☐ Do not post financial, nonpublic personal, or other sensitive information to social media websites, as they are often utilized by malicious fraudsters to gather information on potential targets.

ACCOUNT ACTIVITY & BALANCES

- ☐ Review and reconcile all accounts daily or weekly - maintain segregation of duties.
- ☐ Protect the account numbers and electronic access devices we provide you for your accounts. Do not discuss, compare or share information about your account numbers.
- ☐ Only share your financial information with others for valid business reasons.
- ☐ Cambridge Savings Bank will never ask you to send financial information (including passwords, usernames, PINS, account numbers, or Social Security numbers) by unsolicited texts, phone calls, emails, or via links

PAPER CHECKS

- ☐ Safeguard check stock and use pre-printed numbers to identify missing checks.
- ☐ Incorporate security features into your check design.
- ☐ Never sign checks in advance.
- ☐ Monitor check orders – contact supplier if checks are not delivered within a reasonable time.
- ☐ Use secure storage with controlled access for your checks, check printing equipment, endorsement stamps, cancelled and remote deposited checks.
- ☐ Discard/Shred checks that have been remotely deposited after 30 days.
- ☐ Use a gel or rollerball pen with quick-drying ink to fill out checks. Using ink that bleeds into the paper protects against smudging and alterations.

[1] "A passphrase is a memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is like a password in usage but is generally longer for added security." (from NIST Special Publication 800-63 "Digital Identity Guidelines")

ACH & WIRE TRANSACTIONS

- ☐ Be vigilant when reviewing and confirming email payment instructions, especially those containing new beneficiary banks, account names or account numbers. New instructions received via email should be verified by phone.
- ☐ Maintain and periodically review ACH and wire transfer limits for your organization and authorized employees to ensure limits match your business needs.
- ☐ If you are requested to initiate instructions fast or due to an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- ☐ Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- ☐ Know the habits of your customers, including the reason, detail, and amount of payments. Beware of any significant changes.

ORGANIZATION & EMPLOYEES

- ☐ Educate employees on ways they can protect themselves from online fraud attempts.
- ☐ Implement a comprehensive information security policy that defines clear security objectives for preserving the confidentiality, integrity and availability of information. Review and update annually.
- ☐ Document business processes that require periodic risk assessments and control evaluations.
- ☐ Conduct periodic risk and control assessments and implement processes to mitigate risks and strengthen controls.
- ☐ Regularly train employees on proper handling of sensitive information.
- ☐ Segregate duties between employees that can initiate financial transactions and those that reconcile accounts.
- ☐ Rotate banking duties among employees to mitigate collusion.
- ☐ Establish a policy to confirm email requests from other employees to initiate financial transactions using a known telephone number or in-person.

FRAUD MITIGATION—BEST PRACTICES USING BANKING SERVICES

Online Banking—Secure portal to manage your accounts, reconcile balances and view activity in real time. Use online banking daily to check for alerts and to monitor accounts for unusual activity.

Wire Transfers—A safe and secure method of payment. Set up dual control and wire alerts for approvals. Call back verification is available to confirm wire transfer activity for online wires of $250,000 or more. Utilize a multifactor authentication method such as a token or One Time Password as additional security when approving payments online. Receive incoming wire notifications so you know when your funds are received. Be suspicious of wire transfer payment requests for secrecy or pressure to act quickly.

ACH—Use ACH to increase efficiency and lower costs by reducing the need to process paper items. Use ACH debit blocks and filters to guard against fraudulent ACH debits.

Business Bill Pay—Schedule single, recurring, or future-based payments to any person or business and set up alerts to be notified when a bill arrives or has been paid. Companies using the business bill pay service are encouraged to utilize the dual control functionality.

Check Positive Pay—Use Positive Pay to help prevent losses and catch fraudulent activity before the money ever leaves your account.

Remote Deposit Capture & Lockbox Services—Use remote deposit and lockbox services to gain greater control over your accounts receivable process and reduce the risk of lost or stolen checks.

ADDITIONAL RESOURCES

Here are additional resources to consider when developing an information security program:

- Visit the National Cybersecurity Alliance's Resource Center at https://staysafeonline.org/resources/
- Visit the Federal Trade Commission's Business Guide for Protecting Data at www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

If you believe you are a victim of a fraudulent activity or access to your accounts has been compromised reach out to your Relationship Manager or the Customer Service Center at 888.418.5626. If you receive a suspicious email regarding your CSB account, forward the email as an attachment to the Customer Service Center team at info@cambridgesavings.com (add "CSB BOB" in the subject line).