SECURITY & FRAUD PREVENTION BUSINESS HEALTH CHECK

Businesses lose billions of dollars every year due to Business Email Compromise (BEC), and this number continues to increase. BEC occurs when a fraudster poses as a business owner by spoofing an email address to deceive employees into transferring money or sensitive information. Strong security, operating, and accounting practices can help protect the health of your business and lower the risk of fraud or even a security breach. Check the health of your business. Utilize this checklist to confirm practices you already have in place and identify areas for further improvement:

Fraud Prevention

- ☐ Online Banking tools are used to make electronic payments, requiring two people to make any changes.
- ☐ Requests to change vendor addresses and/or bank information of vendors and other payees are verified directly with the phone numbers that you have on file for those vendors (do not accept changes via email or fax and do not call the phone number listed in the email or fax).
- ☐ Checks used for payments are brought directly into local post offices (not left in mailboxes to be picked up).

Information Security

- ☐ Passwords are required to access company systems, and they must be complex and unique to each employee (capital letters, lowercase letters, symbols, numbers).
- ☐ Passwords are required to be changed periodically and they are kept private and secure.
- ☐ Two or more verification factors are required to gain access to online sites, accounts, and other company resources (“mulitfactor authentication”).

System Health

- ☐ Anti-virus software and malware detection are installed on every computer and updated periodically.
- ☐ Emails are electronically pre-screened for potentially fraudulent attachments and links.
- ☐ Operating systems are periodically updated when vendors send updates or “patches” to fix security vulnerabilities.

SECURITY & FRAUD PREVENTION BUSINESS HEALTH CHECK

Employee Education

- ☐ Employees are periodically trained on your IT security policies, standards, or expectations.
- ☐ The accounting department specifically reviews your IT security policies, standards, or expectations, as well as this health check.
- ☐ Information Security Programs are in place and comply with Massachusetts regulations. Scan the QR code to learn more.

Scan to Learn More

Protect Yourself Using Our Services

Needham Bank understands the need to protect employee, business, and financial information—that's why we offer many products and services to secure your business from fraud.

- ☐ Use NB Business Online & Mobile Banking to monitor your account activity in real-time and ensure all transactions posted are authorized and accurate.
- ☐ Set up account alerts to keep tabs on your account activity and receive notifications when things don't seem right.
- ☐ Establish permissions and restrictions to control which employees have access to your accounts. Restrict access by user and by account.
- ☐ Use our secure online Bill Pay to receive business bills electronically so you know what is due and when without having to shuffle through a pile of papers.
- ☐ Take advantage of remote deposit capture to deposit checks. You can use a scanner and ensure your deposits never leave the confines of your business.
- ☐ Implement Positive Pay to match information from checks presented for payment to a list of checks authorized and issued by your company.
- ☐ Consider ACH Positive Pay to manage ACH debits and credits by determining the electronic payments you have previously authorized to clear.

Visit **NeedhamBank.com/BusinessFraudPrevention** for additional resources and helpful information on types of fraud, how to prevent and protect your business and what to do if you fall victim.

If you suspect that your business has become a victim of fraud, call **781-444-2100**, your local branch, or your relationship manager at Needham Bank as soon as possible.

Scan for More Helpful Info

10/24