Eastern Bank
JOIN US FOR GOOD®

Checklist For Protecting Your Business Against Fraud

As organizations embrace online operations and remote work, the fraud-threat landscape becomes more complex. Fraud losses or cyberattacks can cause more than financial damage — they can hurt your reputation and erode consumer trust.

At Eastern Bank, we know business fraud is a serious issue. And while no organization is immune to fraud and cyberattacks, taking precautions can help reduce risk. Use this checklist to help keep your business secure.

CONDUCT TRAINING SESSIONS

- ❑ Hold regular sessions on network security and cybersecurity best practices.
- ❑ Demonstrate examples of phishing and social engineering to help employees identify threats.
- ❑ Update employees on common scams and provide industry resources to stay informed.
- ❑ Build a culture of verification so employees take time to verify and feel comfortable reporting suspicious activity.

FOLLOW BEST PRACTICES FOR INTERNAL CONTROLS

- ❑ Establish written internal procedures for your organization, including guidelines for determining verification of payment instructions. Review and update them annually.
- ❑ Set policies about payment procedures, detailing what is and isn't allowed within the business and with vendors (e.g., it is a common practice for businesses to not accept payment instructions via email).
- ❑ Create a dual system for the setup and authentication of monitoring, approving and verifying payment information.
- ❑ Regularly review employee administrative rights and access privileges to limit the number of employees with access and to "right-size" access based on role.
- ❑ Use multiple channels to review and validate payment requests from vendors and company personnel.
- ❑ Review accounts payable and receivable daily.
- ❑ Avoid sharing sensitive or personal information via email; truncate account numbers for additional security.

COMBAT CHECK FRAUD

- ❑ Reduce paper check payments, relying on ACH transfers instead.
- ❑ Create a separate bank account for check issuance to segregate check activity from other important transactions.
- ❑ Steer clear of pre-signed checks or a signature stamp; consider preapproval instead.
- ❑ Sign up for Positive Pay, which verifies checks and approves vendors, notifying you if records don't match.

PROTECT WORKSTATIONS

- ❑ Keep passwords and IDs safe; update them regularly and use multifactor authentication for logins.
- ❑ Limit computer use to work-related needs and avoid for personal use.
- ❑ Update devices with the latest software, malware and antivirus protections.
- ❑ Install a network firewall to protect remote and in-office users.
- ❑ Consider policies for remote workers to limit the ability to print sensitive information, and restrict access to financial systems to in-office employees.

REVIEW POTENTIAL THREATS

- ❑ Conduct regular audits to ensure guidelines are followed as well as to identify red flags, weak access points and bottlenecks.
- ❑ Work with IT to review security needs and determine if upgraded firewalls and anti-malware tools can offer additional protection.
- ❑ Assess whether current anti-spam tools should be strengthened.

Eastern Bank
JOIN US FOR GOOD®

Checklist For Protecting Your Business Against Fraud

BUILD A READY TEAM

- ❑ Discuss cyber coverage with your insurer and ask for recommendations to improve security.
- ❑ Consider contacting outside firms to conduct cyber threat assessments to find potential weaknesses.
- ❑ Form a closer relationship with your banking partner and ask for guidance around systems and reporting tools to help stay safe.
- ❑ Bookmark and reference industry resources for current threat trends and educational resources, such as the:
  - ❑ FBI's Internet Crime Complaint Center (www.ic3.gov)
  - ❑ Financial Crimes Enforcement Network (www.fincen.gov), or
  - ❑ Your local payments association (in New England, www.neach.org).

IF YOU'VE BEEN COMPROMISED

If you suspect you've been a victim of business fraud, immediately:

- ❑ Contact your banker.
- ❑ Notify your insurer.
- ❑ Report the crime to the authorities.
- ❑ Alert vendors and customers.

Business fraud can happen to any organization, so regular training and monitoring, adhering to internal controls and increasing cyber awareness can help reduce risk.

For more information, **get in touch with us today.**