Eastern Bank
JOIN US FOR GOOD®

Keeping Your Business and Employees Safe from Fraud This Holiday Season

By Eastern Bank's Treasury Services Team

SUMMARY

Why Fraud Prevention Matters During the Holiday Season

- ❑ The holiday season is a time of increased consumer activity and emotional vulnerability, making it a prime period for scams and fraud – putting both businesses AND employees at greater risk.
- ❑ Scams and fraud can happen more often during this time due to lack of education, awareness and common misconceptions about fraud. One common belief is that fraud is easy to spot but as technology advances, fraudsters are becoming more sophisticated and harder to detect.
- ❑ Many also believe recovering stolen funds is easy, but it can actually be complex, multi-layered and time intensive.
- ❑ Understanding that the impacts of fraud can be far reaching, affecting both business operations and individual finances, can ground your company's approach to fraud prevention.
- ❑ By educating your workforce and implementing fraud prevention strategies like the ones listed below, businesses can better protect themselves and their employees during the holiday season.

Protecting Your Business During the Holiday Season

IDENTIFY COMMON TYPES OF FRAUD

During the holiday season, several types of fraud become more common, including:

- ❑ **MAIL THEFT**
  Many businesses and consumers experience an uptick in deliveries, making it easier for mail or packages to be stolen.
- ❑ **PACKAGE TRACKING AND MIS-DELIVERY SCAMS**
  When packages are delivered, scammers often use malicious links disguised as delivery package tracking updates to access personal information.
- ❑ **SMISHING SOCIAL ENGINEERING ATTACKS**
  Scammers use deceptive SMS text messages or impersonate businesses to trick recipients into providing sensitive information using the technology behind text messages.
- ❑ **EMOTIONAL MANIPULATION**
  Elevated emotions during the holidays make people more susceptible to manipulation tactics, such as a sentimental story during an increased time of giving, in order to deceive someone and extract funds or information. Beware of "too good to be true" offers that lead to links where scammers gain personally identifiable information and payment from unsuspecting people.
- ❑ **CHECK FRAUD**
  Scammers are increasingly trying to capitalize on check fraud. This can happen when a check is used by someone other than the intended recipient, or when checks the business didn't issue clear the account and result in the loss of funds.

ESTABLISH A STRONG INTERNAL CULTURE AND POLICIES

Businesses can take several proactive steps to safeguard their operations and employees:

- ❑ **ESTABLISH A STRONG INTERNAL CULTURE**
  To ensure employees can distinguish between genuine business needs and impersonators, foster an environment of communication that builds a sense of trust. Flagging any fraud concern – no matter the scope – should be valued and appreciated, including when someone falls victim to what others may deem an obvious fraud.

- ❑ **IMPLEMENT POLICIES**
  Outline clear and specific policies, such as a fraud reporting process and responsibilities reference guide. Have these policies easily accessible, such as in an employee handbook or on an intranet, so they can be quickly referenced by any employee if a suspicious situation occurs.

- ❑ **MONITOR EMPLOYEE ONLINE ACTIVITY**
  To help avoid access to malicious websites, consider monitoring online activities and blocking specific sites from employee work computers and internal equipment.

- ❑ **DISCUSS FRAUD PROTECTION WITH YOUR BANKER**
  Regularly communicate with your banker to understand the latest fraud trends and their insights on prevention and protection measures. Your Bank may even be able to provide you with employee-facing training materials to assist you with this process.

EDUCATE EMPLOYEES ON HOW TO IDENTIFY FRAUD

Employees can also take steps to protect themselves and their employers

- ❑ **TRAIN EMPLOYEES TO RECOGNIZE FRAUD ATTEMPTS**
  Regular training sessions can help employees identify phishing emails, suspicious links, and other common fraud tactics. Consider assigning fraud prevention to an internal role, and leveraging virtual **events and webinars** for training.

- ❑ **HAVE CLEAR GUIDELINES ON WORK PROPERTY USAGE**
  Ensure employees understand the proper use of work devices and networks to prevent unauthorized access.

- ❑ **PROVIDE BEST PRACTICES FOR EMPLOYEES TO REFERENCE**
  Consider creating a quick-reference guide with best practices for fraud prevention and distribute it to your employees.

- ❑ **REMEMBER YOUR TEMPORARY STAFF**
  Train temporary and part-time staff on recognizing and reporting fraud attempts just like you would your full-time workforce.

LEVERAGE TECHNOLOGY

Technology can be useful to detect and protect your business against fraud, including from sophisticated phishing schemes, data breaches and other threats:

❑

SET APPROPRIATE ACCOUNT AND USER ACCESS LIMITS

Restrict access to sensitive information based on employee roles and regularly review these permissions.

❑

USE REAL-TIME FRAUD DETECTION TECHNOLOGY

Implement fraud detection systems that can monitor transactions in real-time and flag suspicious activities. There are many options, including those reliant on AI.

❑

CHECK OUT YOUR STATE'S FRAUD SECURITY POLICIES

Familiarize yourself with your state's fraud security policies and **ensure compliance**.

Business owners play a crucial role in fraud prevention – both for their companies and their employees – and have many options to safeguard their operations. With a few simple steps, you can stay vigilant, implement proactive fraud prevention strategies, and focus on what truly matters during the holidays: upholding a secure and safe environment for your business and employees.

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