Frost

Business Insights

Protecting Your Business from Financial Fraud

WHAT TO WATCH FOR AND WHAT YOU CAN DO

Disheartening as it may be, fraudsters continue to target businesses. According to a 2022 PwC survey of over 1,200 corporate executives, 46 percent of organizations reported experiencing fraud, corruption or other economic crimes in the last 24 months. From low-level con artists to highly sophisticated organized crime rings, fraudsters are everywhere, exploiting every opportunity to fool another unsuspecting victim. And no business is immune to the threat. Each year, scammers steal billions of dollars from mom-and-pop corner stores and global enterprises.

The threat of fraud may be ubiquitous, but businesses can protect themselves. By building awareness among employees and arming them with sound fraud prevention strategies, most companies can dramatically reduce their risk of financial loss.

WHAT TO WATCH FOR

Today's criminals have a long list of tricks. Here are four common types of fraud that impact thousands of businesses every day:

Phishing

Scammers send an email that appears to come from a legitimate company, often a financial institution. The email dupes the reader into visiting a fake website and entering their username and password, which gives account access to the bad guys. Phishing also occurs when users visit a scammer's website that can infect the user's computer with malware and steal sensitive information.

Invoice scams

Criminals may pose as legitimate suppliers or vendors to issue a fake invoice and ask the business to make the payment to an alternate account. Or, real vendors may take advantage of their customer's inattention and create duplicate or artificially inflated invoices.

Business email compromise

A fraudster sends an email as if from an important person within a company. This could include commandeering the email account of a high-ranking executive (or creating an email with a slightly altered name that is easy to interpret as legitimate), using the guise of authority to propel employees into action. Senders often issue urgent wire transfer instructions to a targeted employee in the financial department or urge other employees to do so on their behalf.

Check theft or counterfeiting

A perpetrator will intercept a paper check from the mail and change the payee's information to their own. By the time the intended recipient of the check realizes they haven't been paid, the criminal has long since collected the money and covered their tracks.

WHAT BUSINESSES CAN DO

Aside from the scammers themselves, a business's greatest enemy is complacency. Too many businesses maintain an "it won't happen to us" mindset, leaving their organizations vulnerable. Conversely, recognizing the risks and imbuing the organization with a culture of vigilance can go a long way toward prevention. Here are three concrete measures to put in place:

Require employee fraud training: There are plenty of off-the-shelf training programs available online to teach employees how to spot potential scams to avoid becoming a victim.

Insist on the separation of duties: Ensure that important financial processes aren't completely controlled by one person, so there will always be a second set of eyes to review every action.

Take advantage of tools: Work with the company's financial institutions to utilize fraud prevention measures, such as an approved list of payees, and designate "red flag" events that will prompt the bank to seek additional approvals on certain transactions.

It may not be possible for businesses to completely bulletproof themselves against fraud, but these and other preventive actions can mitigate risk and limit damages when fraud does occur. Frost bankers are committed to working with clients to keep them informed of evolving threats, identify areas of exposure, and take a layered approach to safeguard their business assets.

WE'RE HERE TO HELP

Scan the QR code or visit: FrostBank.com/Protect to learn more.