Frost

Business Insights

PROTECTING YOUR BOTTOM LINE:

Strategies to Safeguard Your Business from Payments Fraud

Six in 10 businesses reported their organizations were victims of payments fraud in 2022. It's essential for modern-day businesses to understand the various forms of payments fraud as well as the financial and reputational risks involved.

Payments fraud has become an increasingly common threat to businesses of all sizes in recent years. Simply put, payments fraud occurs when scammers make unauthorized payments from your business accounts or trick an employee into doing it for them. If your company has yet to be victimized, consider yourself lucky. According to a recent Association for Financial Professionals survey, 65% of businesses fell prey to payments fraud in 2022. And the consequences can be severe. Data from the FTC revealed that incidents of payments fraud led to $8.8 billion in reported direct losses in 2022. Those losses don't include indirect costs such as increased insurance premiums and customer churn.

No business is invulnerable, so it's critical for owners and employees to be aware of the most common types of payments fraud and know how to stop them.

Protect your business from payments fraud by recognizing the telltale signs of an attack, which may come in one of these forms:

Business Email Compromise (BEC) is a common scam where attackers send emails appearing to originate from familiar individuals, such as colleagues, supervisors, senior executives or business partners. In many cases, the messages come from legitimate email accounts, but which have been compromised. These messages may include specific details to appear authentic, sometimes including genuine marketing materials and real contact information for whomever they are impersonating. Once trust is established, the attackers may manipulate victims into taking uncharacteristic actions, such as revealing sensitive information, initiating unusual transactions or even redirecting funds to a new (fraudulent) account.

Phishing is a tactic used to obtain sensitive information, such as credit card details, log-in credentials and other personal information. Scammers tend to launch phishing attacks through email, social media and search engines with messages or ads that include links containing malicious software or redirecting users to fake websites that appear legitimate. Phishing websites often prompt users to enter confidential details like usernames, passwords, credit card information or other personal data, allowing scammers to gain unauthorized access to their accounts.

Vendor impersonation is another con in which attackers target businesses by posing as legitimate suppliers or service providers. Scammers may trick unsuspecting employees into paying a fraudulent invoice, changing billing account details such as bank account and routing numbers, or providing personal information about their own customers. This tactic can be easier to execute because fraudsters only need to use an email address that appears similar to that of the legitimate vendor, rather than taking over legitimate email. By exploiting employees' knowledge of, and trust in, existing business relationships, scammers can quickly inflict significant financial losses on targeted businesses.

TAKE PREVENTATIVE MEASURES TO STOP PAYMENTS FRAUD — BEFORE IT'S TOO LATE.

There are many ways to minimize the risks of payments fraud to your business. Here are six basic strategies any company can implement:

1. **Pick up the phone.** Nothing is as simple and effective as making a quick call to verify a payment. If something feels even a little off, pick up the phone and call. Don't use the phone number given to you by the requestor, find the contact another way and verify the payment transaction before proceeding.

2. **Insist on safe email and online practices.** Ensure every employee completes at least a rudimentary training module on how to prevent fraud. The content should cover how to spot scam emails, phishing web sites and fake invoices. Basic awareness and vigilance can ward off most would-be attackers.

3. **Question unusual activity.** If you're in a position to review financial transactions, don't assume all of them are legitimate. If something causes you to raise an eyebrow, take the time to investigate, knowing the threat of fraud is ever-present.

4. **Ensure the separation of duties.** Structure payment processes so they aren't completely controlled by one person. This way, there will always be a second set of eyes to review every transaction.

5. **Take advantage of tools.** Work with your bank to utilize fraud prevention measures such as an approved list of payees, automatic payment alerts on certain types of transactions, or "red flag" events that prompt the bank to seek additional approvals.

6. **Implement two-factor authentication.** For enhanced security, require employees and customers to do more than enter a username and password. Two-factor authentication involves one extra step, such as verifying the user's identity through SMS, email or a token system, before they can make transactions.

In addition to these fraud prevention measures, some companies may also want to explore more sophisticated safeguards such as data encryption protocols, secure payment gateways and real-time fraud monitoring software.

Regardless of your industry or the size of your budget, taking steps to prevent payments fraud should be a top business priority. By understanding different payments fraud tactics, implementing reasonable controls and partnering with trusted financial institutions like Frost, you can greatly reduce your risks.

Sources:

- Association for Financial Professionals, April 18, 2023. Survey: 65% of Organizations Report Being Victims of Payments Fraud in 2022
- Federal Trade Commission, February 23, 2023. FTC crunches the 2022 numbers. See where scammers continue to crunch consumers.
- The Federal Reserve, February 10, 2017. Regulation E: Electronic Fund Transfers

WE'RE HERE TO HELP

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