Protect Your Business from Payment Fraud

Fraud is on the rise as criminals leverage various methods to convince businesses that they are working with known partners or vendors.

One increasingly common method is the use of business email compromise (BEC). It is used to gain the trust of the business by hacking into a business's legitimate email or by creating a "spoofed" email address that varies slightly from a known contact. When BEC occurs, it may look like a request from an established business partner or even a manager or executive at your own company. The individual then requests fraudulent payment or transfer orders. Once sent, the payments are often unrecoverable.

It is important to take time to educate staff on how to avoid falling victim to these scams. Review Your Process for Authorizing Payments.

It is critical for businesses to have strong controls for establishing new vendor payment instructions and changing existing payment instructions. By creating clear and concise procedures, you reduce the likelihood that staff might fall victim to these scams.

Considerations Include:

- Require a callback to the individual making the request using a pre-established or publicly available contact phone number.
- For internal requests, ensure staff know and are comfortable reaching out to verify the requests with members of management and/or executive leadership.
- If possible, consider segregating duties of those who create payments and those who release them.
- Be suspicious of unexpected or unsolicited requests.
- Add steps that include verifying the email contact information, letter by letter. Look for misspellings, additional punctuation, or changes to the email format.
- Be on the lookout for red flags such as spelling and grammatical errors, unexplained urgency, and requests for the communication to remain confidential. Even if the email address appears legitimate, the business may have experienced a security breach.

Develop a Response Plan

In the event fraud does occur, create a plan for staff to follow and respond effectively. Once a plan is developed, train teams to coordinate communication and recovery efforts.

- Notify the Bank and any impacted business partners as soon as possible.
- Scan computers and mobile devices with access to email for malware or viruses to identify where the compromise occurred and take action to repair it.
- Report the incident to the FBI at IC3.gov and local law enforcement.
- Review your insurance policy and notify the insurance company, if applicable.
- After the recovery efforts have been made, review the events leading up to the transmission of the payment. Adjust the process if needed.

Peoples Bank
A higher level of service