Citizens National Bank

The Power of Local℠

Power of Insights

Do you have a plan in place to protect your business from payments fraud?

In a recent survey of 700 treasury and finance professionals, a record 74% reported being hit by payments fraud last year.*

While checks continue to be the subject of more fraud that any other payment method, wire fraud is the second most common type. For example, in 2017, incidents of wire fraud tripled in the U.S., from 14% to 48%, and 92% of these businesses report that it cost their companies ½ percent of total revenue.

According to Shane Callahan, Chief Operating Officer for Citizens National Bank, "The Bank has seen several instances of wire fraud recently that have had a significant impact on our customers. It's really important for businesses to take preventive measures to protect their payments and implement products and processes to protect their corporate assets and data from fraud," he said.

What is wire fraud? Wire fraud is an act of fraud in which someone uses electronic communications, such as telephone or e-mail to make false representations so they can obtain money. For example, you may receive wire instructions which appear to be from someone that you do business with, when in fact, they are from a criminal.

We sincerely care about you and your business, so we strongly recommend that you follow these tips to safeguard your accounts as much as possible:

- Be especially skeptical of any sudden change in wiring instructions, and always confirm that the number which you are wiring money to is in the name of the party entitled to the funds.

- Business email compromise (BEC) is also one of the primary ways that fraudsters may try to communicate with your business. Be sure and confirm wire and other disbursement instructions you may have received via e-mail by calling the number of the business that you have on file instead of calling a phone number listed in an e-mail that you may question.

- Many criminals are smart and do careful research to know when the President of a company may be out of town. Then, they will call or e-mail an office staff member and make it appear as if the company official is in a rush for funds to be wired somewhere while he or she is away.

Don’t fall for this trap. Talk directly to the person by phone to confirm that it is a legitimate request.

- Take caution when responding to e-mails from free public e-mail account domains, as they are often a source of risk; and watch out for phishing e-mails with embedded links, even when they come from a trusted source.

- Don't share your online banking Log In credentials (User ID and password) with anyone.

- Monitor your accounts regularly for unauthorized transactions and report any to your bank immediately.

- Install a firewall on your computer to prevent unauthorized access.

- Separate wire and ACH initiations and approval responsibilities within your office staff, and review the list on a regular basis.

As you guard against wire fraud, it's also important to take precautions against check fraud.

- Be sure to store your checks, deposit slips and bank statements in a secure location.

- Implement dual controls over account reconciliation.

- Utilize available check fraud protection solutions such as positive pay with payee name verification.

If you need further guidance on protecting your business, or have additional questions, we invite you to contact Lance Hall, Bank Operations Manager, at **601.484.5235** today. We have a strong team of experts in this area who are eager to be of service to you.

**2017 Payments Fraud and Control Survey published by the Association for Financial Professionals.*