How To Safeguard Your Business Accounts From Payment Fraud

Alvin Shenk, CTP, SVP, Central and South Texas Sales Manager

Business owners face a host of challenges, but perhaps none are more worrisome than protecting themselves against payment fraud. According to the Association for Financial Professionals' 2019 Payments Fraud and Control Study, 82 percent of organizations surveyed were victims of attempted or actual payment fraud last year.

Payment fraud can cover a variety of scams, but typically involve dishonest individuals impersonating legitimate customers. Fortunately, there are steps you can take with your bank to protect your money, your information, and your customer relationships. Following are tips for recognizing and preventing three common types of payment fraud to safeguard your business accounts from payment fraud.

Check Fraud

Even with the massive growth of online shopping and the ubiquitous use of credit and debit cards, check fraud remains a common problem for many businesses. Check fraud includes forgery and theft, where criminals steal checks and sign or endorse them without authorization. But, new technology has made other forms of check fraud easier. Today's high quality graphics software and color printers allow counterfeiters to create fake checks that are almost indistinguishable from the real thing. Whether writing checks on behalf of your business, or accepting check payments, business owners remain vulnerable to check fraud.

So how can you stay ahead of today's criminals? One of the best defenses against check fraud is Positive Pay. Positive Pay is an automated cash management system that allows you to monitor your paid check activity. When you issue checks, you provide your bank with a file containing all of the check information, and your bank verifies it against checks presented for payment. If there's a discrepancy, your bank will alert you to confirm whether the check is legitimate.

To protect yourself from accepting fraudulent checks, there's no substitute for vigilance. Scrutinize checks closely and look for any inconsistencies or printing irregularities to help spot counterfeits. When accepting checks in person, ask for an ID. There are also check verification services available that can help determine the validity of a check, or the account holder's payment history.

ACH Fraud

While generally more secure than checks, Automated Clearing House payments are still not immune to fraud. As more businesses and individuals utilize ACH networks to make and receive electronic payments, criminals are also stepping up their efforts to commit fraud using these systems.

ACH fraud usually entails a scammer gaining access to a victim's banking

credentials and then initiating bogus transactions to electronically transfer money into their own account. This can happen in a variety of ways, most commonly through email or voice phishing. The best way to prevent falling victim to ACH fraud is by protecting your banking credentials. Learn to identify phishing emails and calls and never provide your credentials through email or over the phone. Instead, if you receive a request for this information, contact your bank directly.

You should also look into the fraud protection measures offered by your bank. If your business uses ACH transfers, ask about filtering options that enable you to set criteria to determine which ACH transfers will be approved. With these filters in place, your bank will alert you if suspicious activity occurs on your account, giving you an opportunity to reject the transaction. Account and ID blocks are also effective, allowing you to specify which companies or accounts can make debits from your account.

Wire Transfer Fraud

Wire transfer fraud is less common than check or ACH fraud, but often involves larger dollar amounts that can be more difficult to recover. As with ACH fraud, wire transfer fraud often begins with phishing emails, but these scammers tend to put additional time and effort into researching their target company. Once they gain access to a company's network, they may spend months monitoring communications to learn how the business operates and better understand its key executives and procedures. Then, by impersonating a senior executive or trusted business partner, they request a large-dollar wire transfer into their own account, often stressing the need to expedite the payment. Once the payment is made, they quickly move it to another account, making it difficult or impossible to recover.

Once again, the key to preventing this type of fraud is through training and vigilance. Employees should learn to recognize phishing scams and fully understand your business' procedures and protocols for making wire transfers. Any suspicious requests should be reported and verified. You should also require multi-factor identification for large wire transfers. This means confirming the requestor's identity through at least two different forms of identification. For instance, an email request for a wire transfer should also be confirmed by a follow-up telephone call you initiate using a verified phone number. This also applies when a vendor requests a change to their address or bank information.

Protecting Your Business

As a business owner juggling countless responsibilities, you can't let your guard down when it comes to the potential of payment fraud. That's why it is important to have a trusted banking partner who can help you protect your business' finances, relationships, and reputation. To learn more about how PlainsCapital can help you safeguard your business accounts from payment fraud or PlainsCapital Bank's fraud prevention services, call 214.252.4005.