Keeping Your Money Safe: Wire Fraud Scams

Denise Owens, CFE, SVP, Fraud Department Manager

Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.

Wiring someone money is not as common as it used to be, given technological advances in banking that allow you to send and receive money faster. However, it is still an activity that criminals can exploit. According to the Federal Trade Commission, criminals defrauded victims out of $423 million using wire fraud in 2018. Just as with other types of fraud, criminals attempt to pose as a person with whom you have gained trust; for example, a relative, an executive at your company, your bank, an attorney, or a government agency. They send a fake request instructing you to wire funds immediately using payment instructions they provide – and they reiterate the urgency of their request. This is meant to pressure you into making a mistake that is difficult to correct. Once the money has been wired, it is nearly impossible to recover the funds.

How Does the Scam Work?

Wire fraud is a form of criminal activity that makes use of electronic communications or digital networks. This type of crime makes use of any and all forms of electronic media, including telephone or fax machine, email or social media, or SMS and text messaging. The criminal typically tries to deceive you into sending money to an account to prevent an emergency, rescue a stranded relative, or avoid a penalty from a government entity, such as the IRS.

Another form of wire fraud is known as business email compromise. This type of fraud is when a criminal hacks into a corporate e-mail account and impersonates the real account owner to defraud the company, its customers, partners, and/or employees into sending money or sensitive data to the criminal's account.

How to Protect Yourself from Wire Fraud Scams

The following scenarios and responses will help you protect yourself and your funds from wire fraud scams:

1. Someone you have never met in person is asking for money. This is the biggest red flag for wire fraud. Criminals will pose as long-lost relatives, IRS officials, or even someone you may think you know well, like a new long-distance relationship. If you haven't met them in person, you should think twice before sending your money.

2. You receive an email from a high-level company executive instructing you to transfer money from the corporate account. This is a classic example of business email compromise where a criminal is using a

spoofed email account in an effort to get you to send them money or proprietary company information. Check to make sure names and domains aren't misspelled. You should also contact the executive directly to verify the request is valid.

3. You see an ad online for a great deal, but you're required to transfer the money right away to receive the product. The reality is the product probably doesn't exist and the criminal just wants your money. While many people use wire transfers to pay for luxury items, it's worth checking the reputation of the seller, if you're transferring a large sum.

4. You receive an email from someone pretending to be your bank or other service provider saying you need to update your security information. Remember, as soon as you click the link, you're vulnerable to malware. Phishing emails that try to steal your information or get you to wire money will often contain a lot of spelling and grammatical errors. The email might not address you by name, and likely comes from a suspicious and unrecognizable source. It will probably ask you to provide financial information or to verify it, but if you hover over a URL, you'll see that it will take you to a suspicious and unknown website. Don't click on any links within these emails; instead, just delete them and block the sender.

5. You receive an email or a phone call that claims the IRS wants you to pay back taxes, and you need to transfer your money, or you'll be arrested. In reality, the IRS will formally contact you by mail rather than by phone, and they won't be asking for your payments by credit card or by wire transfer.

Keeping Your Money Safe

As always, the "Keeping Your Money Safe" fraud prevention series is designed to help you thwart cyber criminals trying to acquire your personal information or infiltrate your devices. The key to protecting yourself is education and awareness. PlainsCapital Bank's Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, visit our fraud resources page.