

PINNACLE BANK

How Do You Protect Yourself Against Payment Fraud!?

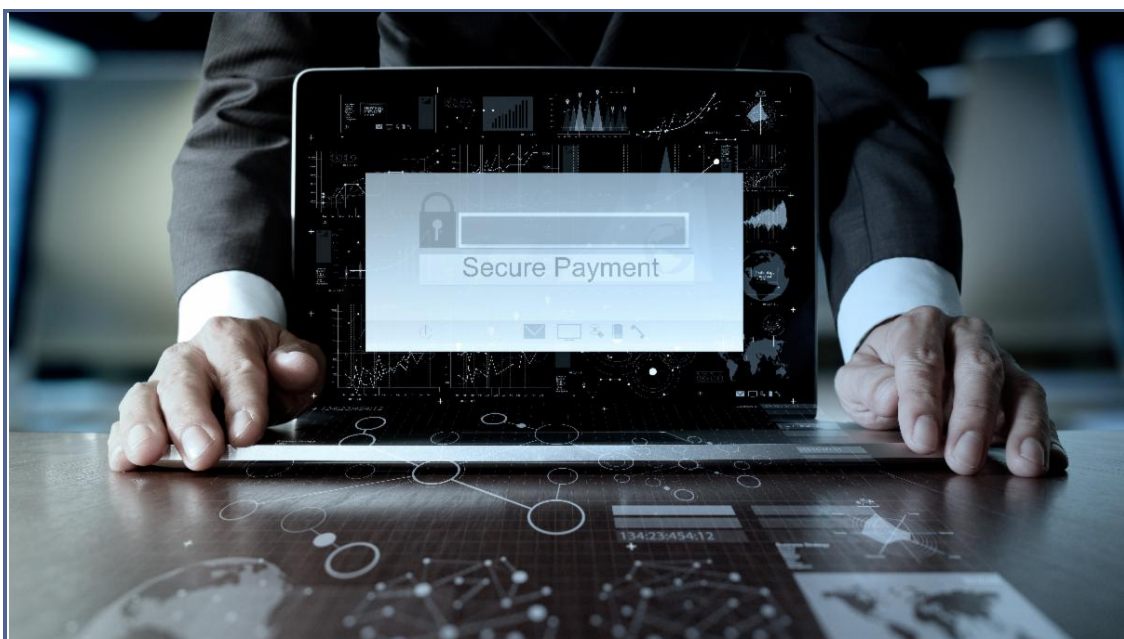


Pinnacle Bank takes payment fraud and client data protection seriously. Part of our efforts in combating fraud is educating our clients on how to recognize fraud attempts, particularly payment fraud, which has been on the rise.

Below are 4 types of scams that can lead to payment fraud; as well as payment verification best practices that can be easily implemented to ensure you avoid becoming a victim.

Best Practices

- Always verify the identity of the person requesting funds; if the request is via email or text, call the person on a KNOWN number.
 - Question urgent requests, and authenticate change of payment information, even if received from a known email address, as the individual email may have been compromised.
 - Take advantage of our dual control and assigned limits for all payment types when available.
 - Sign up for payment alerts when available.
 - Engage and never disable multi-factor-authentication, stay mindful of data that is shared online and via social media sites.
-



How Does Payment Fraud Happen?

Payment fraud can come in many different forms, from the theft of a debit card to malicious fake emails requesting funds. Below are the most common fraudulent payment attempts.

Electronic Transfer Scams

Wire and ACH fraud is when a scammer poses as a trusted source, usually a vendor, company, or family member, and requests an immediate transfer of funds.

No matter what reason they give, always authenticate who the funds are being sent to, and never send money to a non-trusted source, who pressures you to pay immediately, or who says an electronic transfer is the only way to pay.

Be Careful!

One of the best ways you can prevent electronic transfer fraud is to never send funds to someone you don't know. Don't send funds to someone unless you can confirm their identity, give them a call! Even if this person claims to be a family member, it is best to call that family member directly and ask if they recently requested an electronic payment. Double-checking who you are sending funds to will help protect your money.

Phishing

Many fraudsters send phishing emails warnings, such as "your account is about to be suspended", and that the account holder must enter their password in a phishing webpage or pay a subscription fee to continue to access the service.

Be Careful!

Be cautious when clicking links or opening attachments from unknown or suspicious sources. Stay alert for common tactics used by fraudulent actors, such as urgent or threatening language, misspelled words, or suspicious links. Using antivirus software can also help protect against phishing attacks.

Online payment scams

An online payment scam can involve a scammer who poses as someone you trust and demands a fast payment using Zelle, Venmo a money transfer company, or cryptocurrency.

Be Careful!

Always question unusual payment requests. The common thread in these scams is that they often demand immediate payment. By forcing you to act quickly, you are less likely to question the request. When you receive an unexpected text, email, or voice message requesting a payment, do not reply, click links, or call phone numbers included in that communication, only contact the individual with a known number.

Online shopping scams

Online shopping scams can be difficult to spot because scammers often create realistic websites and social media ads with great deals, fake assurances, and bogus warranties for

their products.

Typically, the scammer requests payment through a mobile payment app or wire transfer because they are usually irreversible.

Be Careful!

Know that anyone can set up a realistic-looking website or social media ad. Online scammers will sometimes purchase ads to direct you to their scam website, so research the seller or product before you buy. Watch out for deals that are too good to be true. A deep discount could be the sign of a scammer trying to lure you in.

To learn more about how to protect you and your business click on:

[Online Banking Fraud Prevention Best Practices](#)

Contact us right away if there's a problem!

If you believe you are the victim of an online payment scam, had fraudulent activity, or something just doesn't seem right — contact us immediately.

We will work with you to review your transactions to understand the extent of the issue.

Pinnacle Bank

(888) 485-7050



Get in
Touch

PINNACLE BANK