KeyBank

Electronic payment fraud:

What every business should know.

Using a technique called electronic payment fraud, cybercriminals commit theft by exploiting online electronic payment systems of companies and banks. Find out how electronic payment fraud works and how you can help protect your business from it.

ACH and Wire Fraud

A scammer impersonates a business's trusted vendor. They typically invent an urgent situation to deceive victims, who are usually employees authorized to make payments, into quickly sending funds by ACH or wire transfer to the fraudster's account.

Real-Time Payment Fraud

The scammer uses social engineering tactics such as phishing to gain a victim's trust, and then requests money through apps like Zelle or PayPal. Regardless of how the funds are sent, real-time payment fraud is a type of authorized payment fraud, invoice fraud, or push-payment fraud, used to trick victims into authorizing payment to a fraudster.

Account Takeover

The fraudster accesses a victim's financial, email, or e-commerce account by stealing their sign-on information or by using phishing scams, malware, or other deceptive tactics to trick the victim into sharing it. Once the fraudster gains access to a victim's account, they use it to commit fraud.

Mobile Payment Fraud

Fraudsters use sophisticated tactics like account takeover, phishing, SIM swap, or fake apps to access a victim's device or con a victim into revealing sensitive data. The fraudster can then exploit mobile payment systems and steal financial data, manipulate payments, or make transactions.

Continued on reverse.

Helpful Tips

- **Enforce two-factor authentication.** This should be required for all employees.
- **Always validate payment requests.** Confirm payment requests and payee or account information by verifying the details through a known channel. This is especially important for urgent requests or if the payment account has changed. Look out for misspellings or transposed letters in email addresses or URLs.
- **Implement secure payment policies.** Restrict payment capabilities to authorized personnel and require two authorized employees to validate and approve all payments before releasing funds.
- **Establish digital security protocols.** Require secure Wi-Fi connections and payment platforms.
- **Enable account alerts.** Use these to automate around-the-clock monitoring of your business accounts and receive immediate notification of unusual or suspicious activity.
- **Trust your instincts and pause.** If it seems suspicious, be extra vigilant in verifying the request.
- **Educate employees.** Share the latest security threats and best practices. Knowledge is the best defense against fraud.

See important disclosures on page 2.

Electronic payment fraud: What every business should know

We're here to help.

KeyBank is committed to arming you with the latest information on cybercrime and payments fraud. For more information, visit key.com/businessfraud. To learn more about KeyBank's Core Fraud Solutions, connect with your payments advisor or relationship manager.

If you think you may be a victim of fraud, call the KeyBank Fraud Client Service Center at 1-800-433-0124. Dial 711 for TTY/TRS.

KeyBank