Protecting your business from fraud

KEY TAKEAWAYS

> Understand the most common types of fraud and how to identify them.

> What to do if you uncover fraudulent activity or suspect you are a victim of fraud.

> A checklist of fraud detection and prevention techniques and how to employ them in your organization.

The threat of fraud often centers on the continually evolving technologies used to conduct business and online banking. According to the 2014 Association for Financial Professionals (AFP) Fraud and Control Survey,* 60% of respondents experienced actual or attempted payments fraud in 2013. At KeyBank, our goal is to provide our clients with fraud awareness tips and actionable suggestions that can help you stay one step ahead of financial criminals.

BACKGROUND: UNDERSTANDING FRAUD

Cyber criminals continue to target online banking and electronic payment transactions. Fraud committed against business bank accounts generally occurs by writing unauthorized checks, through wire fraud, or through ACH fraud. With two bits of information, your business checking account number and bank routing number, a criminal can make a payment for goods or services either by phone or online.

How Fraud Originates

The usual starting point for fraud is social engineering, which is the practice of obtaining sensitive information by tricking people into breaking normal security procedures to:

- Divulge your passwords or other sensitive financial or personal information
- Direct you to a website to download something malicious
- Ask for remote access to your computer
- Secretly install malicious software on your computer

KeyBank

*Data from page 6 of the 2014 AFP Payments Fraud and Control Survey, Introductions and Key Findings.

Types of Social Engineering Fraud

One of the most common strains of social engineering is called phishing (pronounced “fishing). Phishing usually involves a spammed email, phone call, voicemail, or text message sent by criminals who intend to capture personal information (e.g., Social Security number, credit card information, user IDs, and passwords).

Phishing emails often appear to come from legitimate sources you know, or a company you specifically do business with.

Phishing emails often contain malware that can be installed on your computer when you take the action requested in the email. These emails may also attempt to steal your banking credentials or other personal information by asking you to confirm data.

Malware can cause a wide range of problems, from system disruptions to the loss of personal data or identity theft.

Your computer could also be infected when a user:

- Visits less-than-trustworthy websites (e.g., gambling, adult content)
- Downloads and installs “free” software
- Visits a website that has been compromised
- Responds to a malicious advertisement on a website

Another type of social engineering is account hijacking, whereby your email or any other account you have associated with a computing device or service is stolen. For example, an employee may receive an email that appears to be sent from a manager requesting transactions to be initiated or a change in account information. Employees should be sure to confirm via phone or in person if a change out of the ordinary is being requested.

Safeguarding Electronic Payments

To help protect against fraudulent wire transactions, organizations need to carefully monitor all electronic payments, and especially wire activity.

- Never send funds to unknown individuals. Completely understand and verify crisis or urgent requests.
- If you receive an unexpected, urgent message from any known senders asking you to wire funds to them, call them at a trusted phone number to ensure they truly sent the request.

WHAT KEY IS DOING ABOUT ONLINE FRAUD

Because phishing emails are not coming from Key or passing through any of Key's systems – even if they are good imitations that may look like they came from Key – there is nothing Key can do to stop you from receiving a phishing email. However, if we learn of a phish, we will work with the authorities to try to take down the fraudulent site. This makes it even more important for KeyBank customers to recognize fraud attempts and know how to protect themselves.

As part of our ongoing efforts to increase fraud awareness, Key alerts and educates clients and employees about phishing emails and methods. Those alerts are updated as new and changing methods of fraud appear.

Key has various systems and procedures in place to monitor accounts and identify potential fraudulent transactions. However, Key's monitoring is an enhancement to – not a substitute for – your own monitoring.

Key is committed to continued investment in prevention and detection, using both technical and non-technical advancements. We are focused on new authentication advancements and behavioral analytics as well.

As part of Key's due diligence, we will work closely with you when setting up your company's accounts and your user authorizations to ensure entitlements are accurate and up to date.

Your business benefits with early detection

> Losses are reduced since you can prevent unauthorized transactions before they occur

> Identify potential fraudulent items quickly as opposed to waiting for your monthly statement and then identifying a problem

> Preventing losses saves you the time and effort associated with attempting to recover lost funds

WHAT TO DO IF YOU SUSPECT YOU ARE A VICTIM OF FRAUD OR MALWARE

- Call Key's Fraud Hotline directly at 1-800-433-0124 for an analysis of the situation and further direction. After calling the Fraud Hotline, contact your Relationship Manager to make them aware of the issue.
- If you are unsure whether an email is an authentic message from Key, please call us right away to verify. Do not respond to the message. Instead, forward the message to emailfraud@keybank.com. You can also visit key.com/security for additional information on fraud protection. If you responded to the fraudulent email or have specific questions, call Key at 1-800-433-0124.
- If you have any security questions related to your use of Key Total Treasury,® please call our Key Total Treasury Security Support team at 1-800-539-9039, and select *option 1*. If you suddenly do not have access to Key Total Treasury, please call Key immediately and inform us. This may be a result of malware or phishing attempts.
- If you have discovered malware on your computer, or clicked a link or opened an attachment and are not sure if your computer is safe, immediately disconnect your computer from the Internet and your company's network. Please contact Key to inform us of the malware concern and consult with a qualified IT professional to scan for and/or remove any malware and viruses.

  Unfortunately, depending on the type of malware, any networked computer is at risk of infection from any other computer on the same network. This is why removing the computer from the network and internet is so important.
- Remember, if you or your business are a victim of fraud, it's important that you report it to the proper law enforcement authorities.

To learn more, contact your Relationship Manager to determine which solutions are right for your organization, or visit key.com/phishing or key.com/security.

PROTECTING YOUR ACCOUNTS FROM FRAUD

While we can't completely eliminate fraud, we can prevent and detect it.

Be vigilant

- ☐ Monitor your accounts daily and closely
- ☐ Work with IT/Security to develop a plan for responding to fraud
- ☐ Be suspicious of any unsolicited emails, phone calls, or text messages with an urgent request for personal or company financial information, from both known and unknown senders

Browse safely

- ☐ Never log in to your online banking account via a link or internet address provided in an email or text message
- ☐ Never use "favorites" to access a website where you plan to disclose private information – type the URL into your browser's address bar
- ☐ Only enter financial or account information on sites that have the lock icon displayed in the browser and https preceeding the URL

Review computer security

- ☐ Use strong passwords and change them often
- ☐ Ensure that anti-virus programs are updated daily
- ☐ Maintain and review your computer operating systems and web browsers; and install any of the recommended security updates as they become available
- ☐ Limit administrative rights
- ☐ Ensure employees lock their computers when away from their desk
- ☐ Consider using a dedicated computer for all banking transactions

Set up online banking controls

- ☐ Limit the use of your ACH system to employees who need to use the system
- ☐ Use dual controls and ensure separation of duties
- ☐ Verify employee access rights and credentials regularly

Be suspicious

- ☐ Do not open unsolicited, suspicious emails, or emails from unknown senders – delete them. If you do open one, never click on links or open attachments
- ☐ If you receive a message from a known sender, do not open an attachment before checking with them through a known phone number/email address
- ☐ Email appearing to come from a trusted source could be fraudulent and contain a virus, Trojan horse, worm, or other malware
- ☐ Do not share your email address with random sources
- ☐ Never provide personal information requested via pop-up windows or email

Communicate with and educate your employees

- ☐ Routinely discuss how to identify fraud
- ☐ Develop/evaluate internal fraud policies
- ☐ Discuss a contingency plan for operations with your banker in the event of a payment disruption
- ☐ Read Consumer Affairs reports as they often post alerts about new scams
- ☐ Provide ways for your employees to report suspected fraud

If you suspect you are a victim of fraud or malware, call Key's Fraud Hotline directly at 1-800-433-0124, and then contact your Relationship Manager to make them aware of the issue.

To learn more, contact your Relationship Manager, or visit key.com/phishing or key.com/security.

KeyBank

This document is designed to provide general information only and is not comprehensive nor is it legal advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought. KeyBank does not make any warranties regarding the results obtained from the use of this information.
Key.com is a federally registered service mark of KeyCorp. ©2014 KeyCorp. **KeyBank is Member FDIC.** ADL7164.01