KeyBank

protect your business from fraud

At KeyBank, the security of your accounts is our top priority. We're always looking for new technologies and ways to help you keep your accounts safe and secure.

When it comes to business, fraud prevention requires a coordinated effort from all employees. Arming yourself with the latest guidance is crucial to protecting company financials and sensitive information — and we're committed to keeping you apprised of the latest fraud trends and preventive measures.

Here are a few guidelines to help you safeguard your accounts against fraud.

Use online banking and account alerts to catch suspicious activity quickly.

Business accounts and transactions should be reviewed *every day*. Online banking makes this easier by providing 24/7 access to your accounts. And once enrolled, you can set up account alerts[1] for automated, around-the-clock monitoring of your business accounts. Here's how:

KeyBank Business Online

Sign in, then scroll down to the *I want to …* section. Then choose *Manage Alerts*.

KeyNavigator

Sign in, then click *Message Center* in the upper right corner. Then select *Manage Alerts*.

Beware of check fraud.

With mail and check theft on the rise, consider using digital payment platforms when possible — which are more secure than checks *and* can help lower payment costs. You can also use ACH or wire transfers to make electronic payments securely. And when check payments are unavoidable, be sure your business is enrolled in Key Positive Pay[2] — our fraud detection reporting service that verifies items presented for payment against your original check details.

Fraudsters often impersonate banks.

Be cautious of unexpected requests by phone, text, or email for full Social Security number, login ID, or other personal information when the communication was not initiated by you.

If KeyBank initiates a call or text to you

We'll never ask for your log-in credentials, passwords, PIN, or one-time passcode. We'll also never ask you to send money to yourself via any electronic method such as Zelle,® account transfers, or wire payments.

If you initiate an interaction with KeyBank

We may ask for information such as the last four digits of your Social Security number, login ID, or a one-time passcode to verify your identity.

Play it safe and verify any questionable requests by contacting a *known* KeyBank resource — like your Relationship Manager, 1-888-KEY4BIZ,® or your local branch — before providing any sensitive information.

There's no harm in verifying a request. In fact, we'll be glad you did.

[1] Message and data rates may apply from your wireless carrier.
[2] Terms, conditions, and fees may apply.

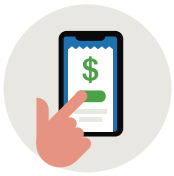
protect your business from fraud

When in doubt, don't click!

Whether in a text message or email, you should never click on a link unless you are 100% certain it is legitimate. Fraudsters often use embedded links to try to collect your company's sensitive data or install harmful malware on your computer.

Make sure all employees know to:

- Be skeptical of any unexpected text or business email containing a link.
- Look for red flags such as a request to verify or unlock your account, a sense of urgency, or grammatical errors.
- Report all suspicious business communications ASAP.



Implement a secure accounts payables policy.

When targeting businesses, fraudsters often pose as a vendor or supplier your company is known to work with. They may spoof (create a close replica of) the vendor's email or website. They will then send an imposter message saying their payment information has changed and directing you to pay invoices to a new bank and/or account number. To combat this, it's important that businesses have a clear policy for paying invoices that includes:

- Never changing vendor payment information without first contacting the vendor through a known phone number or email address to verify that the change request is legitimate. Never use the vendor contact information provided in the initial request — it could be spoofed.
- Requiring the approval of two authorized employees before vendor payment information can be revised.

Stay informed.

When it comes to fraud, knowledge is power. Staying up to date on the latest trends and emerging scams is your greatest defense. And KeyBank is here to help you do just that. We'll continue to share information, guidelines, and best practices that will help you identify and potentially avoid fraud attempts. For additional information on trending fraud tactics and how to avoid them, visit banksneveraskthat.com.[3]

We're here to help.

If you think you may be a victim of fraud, report the matter to KeyBank **immediately** through a known channel or by calling the KeyBank Fraud Hotline at 1-800-433-0124. Dial 711 for TTY/TRS.

KeyBank

[3] The links provided in this email are not owned or operated by KeyBank. KeyBank is not responsible for the products, services, and content on the third-party website.