



Fraud awareness is fraud protection

How to defend your business



CLASSIFICATION: PUBLIC

Table of Contents

Current Fraud Schemes



How to React to Fraud or
Suspected Fraud



Attempting to Recover Funds




Best Practices

Corporate Account Takeover

This is a phone-based scam where callers pose as a reputable organization and use pressure tactics to obtain login credentials and passwords.

Best Practices

-  NEVER provide your password to anyone.
Never give out sensitive login information.

If something sounds suspicious, it probably is.
Don't respond. Call our fraud hotline and report.



Text Message Fraud

Text Message Fraud, or smishing, is the practice of sending text messages that appear to be from a reputable source to induce individuals to reveal sensitive information.

Red flags to help you identify smishing

- Suspicious URL
- Urgent situation requiring immediate response
- Unknown phone number
- Link to verify, authenticate, or unlock your account



If you or someone in your organization has provided sensitive information during an unsolicited call from KeyBank, call us immediately.

Key Fraud Hotline
800-433-0124

Dial 711 for TTY/TRS



If you think you've been exposed to Business Email
Compromise within your organization, call us immediately.

Key Fraud Hotline
800-433-0124
Dial 711 for TTY/TRS

Recovering Funds

The best defense against fraud is prevention, because once fraud occurs it's very difficult to recover funds.



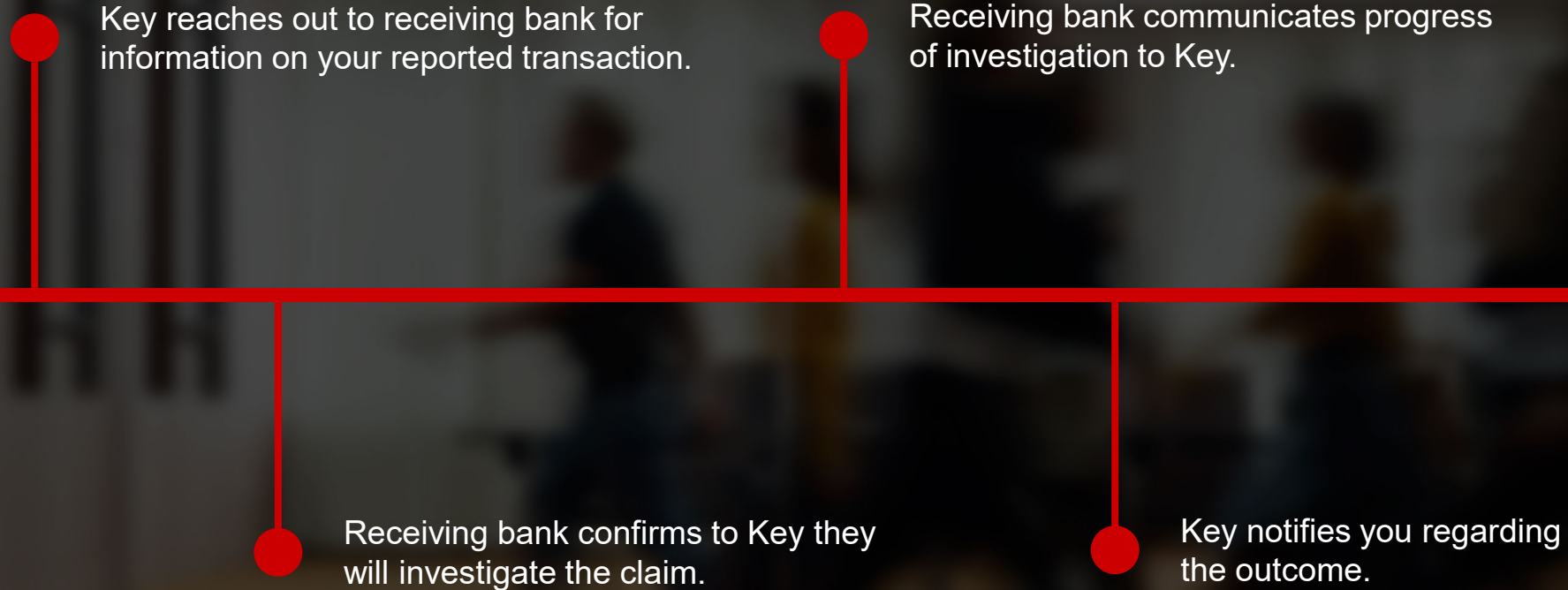
Once notified of suspected fraud, KeyBank is limited in terms of helping you recover funds. Time is critical. Please call us immediately if you suspect fraud.



Everyone can be fooled. Don't let embarrassment prevent you from reporting fraud. Immediate action is your best chance of recovering funds.



Attempted Funds Recovery Timeline





Best Practices



CLASSIFICATION: PUBLIC

Best Practices Summary



Proactively monitor your account and report suspicious transactions.



Set up account alerts.



Never take immediate action.



Never share your login credentials.



When in doubt, contact Key.



Notify us of any suspicious changes to your online profile



Invest in continuous fraud education for everyone in your organization.



As always, if you've been exposed to or are a victim of suspected fraud, call us immediately.

Key Fraud Hotline
800-433-0124

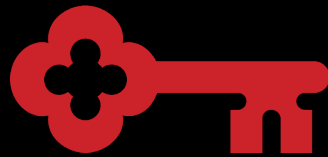
Dial 711 for TTY/TRS

**Report all
suspected fraud
immediately**

Call the KeyBank Fraud Hotline
800-433-0124

Dial 711 for TTY/TRS

- Contact your banker about anything suspicious
- Email a screenshot of any fraudulent text to **reportphish@keybank.com**



The information and recommendations contained here have been compiled from sources believed to be reliable and represent the best current opinion on the subject. No warranty, express or implied by KeyBank, is made as to the absolute correctness or sufficiency of the information contained. This is meant as general information only; particular situations may require additional actions.

CFMA # 240422-2550280

©2024 KeyCorp. All rights reserved.

CLASSIFICATION: PUBLIC