What you need to know about

Electronic Payments Fraud

Cybercriminals can commit theft by exploiting the online and electronic payment systems of merchants, platforms like Zelle and PayPal, and more. This is known as Electronic Payments Fraud. Here are the different types of fraud to watch for — plus ways to help protect your accounts.

Stolen Online Card Information

What is it? A fraudster steals a victim's debit or credit card information online and uses it to get cash advances or make purchases for themselves.

How does it happen? The fraudster may hack directly into an online platform where the card has been used or use tactics such as phishing, social engineering, or card skimming to steal or manipulate the victim into sharing their card account information.

Wire Fraud

What is it? A fraudster tricks a victim into sending money directly to them via wire transfer. It's particularly dangerous because wire transfers are among the fastest ways to send money.

How does it happen? The scammer often impersonates trusted businesses or individuals and usually invents some sort of urgent situation to deceive victims into sending funds quickly to the fraudster's personal account.

Account Takeover

What is it? A fraudster gains unauthorized access to a victim's account and uses it to commit fraud. While typically a financial account, it could also be a victim's email, e-commerce, or even social media account.

How does it happen? The fraudster tricks victims into sharing their login credentials through phishing scams, malware, or other deceptive tactics, or the victim uses the same credentials for multiple websites (including for a site that was hacked.)

Payment App Fraud

What is it? These scams occur when victims are conned into sending money via apps like Zelle or PayPal to fraudulent accounts, believing they are trusted individuals or businesses.

How does it happen? Scammers may pose as legitimate contacts or use fake profiles to trick users into transferring funds.

Helpful tips

Never share sensitive data such as passwords or credit card numbers with unknown sources.

Create strong passwords with 15+ characters and use a mix of upper/lowercase letters, numbers, and symbols.

Enable two-factor authentication whenever possible.

Regularly monitor your bank accounts for any unauthorized transactions.

Check your credit report regularly.

Only use known websites when making purchases or entering payment data.

Don't click on pop-ups, ads, links, or email attachments that appear suspicious or if you don't know the source.

Only use secure Wi-Fi.

Shred personal documents with sensitive information.

Educate yourself on the latest security threats and best practices.

For KeyBank clients: Set up account alerts in online and mobile banking.

We're here to help.

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.**

Learn about more resources and safe practices to help you fight fraud by visiting our Fraud Protection Center at Key.com/fraud.

KeyBank

This document is designed to provide general information only and is not comprehensive nor is it legal advice; particular situations may require additional actions. 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. All rights reserved. All trademarks, service marks, and trade names referenced in this material are the property of their respective owners.

Zelle and the Zelle-related marks are wholly owned by Early Warning Services, LLC, and are used herein under license. Venmo is a registered trademark of PayPal, Inc.

©2025 KeyCorp®. All rights reserved. KeyBank Member FDIC 250306-3067428