NEW SCAM ALERT

Know the red flags

Be wary of requests to Zelle® money to resolve for fraud layer

The most common types of scams will target you through fake emails, text messages, voice calls, letters or even someone who shows up at your front door unexpectedly. No matter which technique the scammer uses, you may be:

- Contacted unexpectedly by phone, email, text, direct message or pop-up with a request for personal information or money. Never click a link or download an attachment from someone you don't know. Bank of America will never text, email or call you asking for personal or account information.
- Pressured to act immediately with an alarming phone call, email or text that plays with your emotions. Scammers may pose as an employee from a familiar organization, such as Bank of America and say there's a problem that needs immediate attention. Do not act unless you have verified the person who has contacted you and the story or request is legitimate.
- Asked to pay in an unusual way, like gift cards, bitcoin, prepaid debit cards or digital currency, including Zelle® to resolve fraud. Bank of America will never ask you to transfer money to anyone, including yourself and will never ask you to transfer money because we detected fraud on your account.
- Asked to provide personal or account information, such as an account verification code, bank account number or PIN. When in doubt, don't give it out. Bank of America will never text, email or call you asking for an account authorization code.
- Offered a free product or 'get rich quick' opportunity that seems too good to be true? If something sounds too good to be true, it probably is. Never cash a check for someone you don't know.

If you authorize a transfer or send money to a scammer, there's often little we can do to help get your money back.

Mobile and Online Banking. Increase your meter level by reviewing the *5 Red Flags that Signal a Scam* — and learn more about scams and how to stay safe. Know the scams

Scammers use different tactics to get victims to fall for their schemes. In some cases, they can be friendly, sympathetic and seem willing to help. In others, they use fear tactics to persuade a victim. Select the scam type from the following list to see a typical message from a scammer and the red flags that should cause you concern.

Imposter Scams

- Scammers may pose as businesses or people you know — like your bank, utility company, phone provider or even a friend or relative. They may ask you to send funds to yourself or others using Mobile or Online Banking. They may spoof legitimate phone numbers to call or text you to make the request more convincing.
- **How to help protect yourself:**
  -
  - Be cautious if being pressured to respond immediately — this is what scammers want you to do.
  - Be wary of unfamiliar calls, computer messages, texts or emails requesting money or personal information. Verify you are sending to a trusted recipient by calling a trusted or verified phone number from a recent bill, receipt or by visiting an official website.
  - Remember that Bank of America will never request that you transfer money to anyone for any reason, between accounts or to your own account.

Online sales scams

- Whether you're thinking about purchasing event tickets, adopting an animal or just browsing the web, be cautious if you see an online promotion that sound too good to be true - it probably is. Scammers set up fake stores selling fake goods, and after you've made your purchase, the store will suddenly disappear.
- **How to help protect yourself:**
  -
  - Research the seller and products independently, and compare prices with other websites. Make sure they have a refund policy, information on privacy terms and conditions and ways you can contact them.
  - Use caution if asked to pay using untraceable means such as a wire, money transfer or gift card. If you do, you may not receive your purchase or get your money returned.
  - Verify the website by carefully looking at the URL address bar or domain name to ensure you are at the correct site. Look for secure URLs (https://) and check reviews for possible scam notices for the site.

Real estate scams

- Whether you are looking for a vacation rental or are purchasing or refinancing a home, you may still be a target for scammers. Scammers can take over a rental or real estate listing by changing the email address or other contact information, then listing it on another site. They may send you an email that appears to be from your real estate agent, title company, or settlement agent/attorney with last minute updates to wiring instructions. Or you could get a quote for moving your items to your new place that turns out to be significantly higher and they'll hold your belongings until you pay.
- **How to help protect yourself:**
  -
  - Before you send any money, always independently confirm wiring instructions in person or via a phone call to a trusted or verified phone number. Once the money is gone, there's almost no way to get it back.
  - Be cautious if pressured to urgently send a security deposit or make a payment to hold the property before you even see it or sign a lease.
  - Pay attention and do your research on the companies, owner(s) and/or listing: Is it vague? Do the photos have watermarks? Does the rent amount sound too low? Are there any scam warnings or complaints about them online? Remember: If it sounds too good to be true, it usually is.

Investment Scams

-
- Be wary if you are contacted by "investment managers" or receive an unsolicited request (via social media, pop-up, text, email or phone call) that presents a "great investment opportunity." Offers that promise guaranteed returns, or the chance to get rich quick or double your money are likely a scam.
- **How to help protect yourself:**
  -
  - Think twice if you're asked to send money through digital currency/crypto currency or instant money transfers. Remember, once you send the money, there is very little we can do to get that money back.
  - Always validate requests for money, research investment managers/offers and use caution if asked to provide personal or financial information.

Romance Scams

- Romance scammers may contact you online via dating aps or social media and try to establish a trusting, caring, and believable relationship — as quickly as possible. Then, scammers make an emotional plea, telling you a story that ends with a request to transfer money through untraceable means like a wire transfer or gift cards. Be vigilant — if it sounds too good to be true, it probably is.
- **How to help protect yourself:**
  -
  - Be careful when posting personally identifiable information on social media. Enable security settings on your social media profiles to limit what you share publicly.
  - Never send money, provide financial information or other sensitive information to anyone whose identify you cannot independently verify.
- Research who you are talking to. See if their images, name and details have been used elsewhere.

Technology Scams

- If you get an unsolicited request to remotely access your computer or mobile device, it's probably a scam - and you could lose money. Scammers often pose as employees of familiar companies and ask you to provide remote access or download an app. They may call, use pop-up screens or email to convince you that your device has a virus or that you're owed money.
- **How to help protect yourself:**
  -
  - No matter what reason you're given, never grant device access or download any app at the request of unknown companies or individuals.
  - Always confirm the identity of someone requesting access by calling a trusted and verified phone number (the one they provide could be part of the scam).

Compromise Scams

- Scammers may try to target you through a fake business, social media or email account. The cyber-criminal may use a hacked or fake account that looks legitimate to trick you into sending funds.
- **How to help protect yourself:**
  -
  - Never trust unknown individuals. Verify everything they claim and do not send sensitive information to anyone whose identity you can't confirm.
  - Give all requests for funds a second look. If an email looks strange, look up the sender and email or call them (don't use the number they provide).
  - Invest in antivirus software and other cyber security software that can flag suspicious emails and websites

IF YOU HAVE ANY SUSPICIONS ABOUT CALLS, EMAILS OR TEXTS; TERMINATE THE CONTACT IMMEDIATELY AND CALL YOUR FINANCIAL, CREDIT OR BUSINESS INSTITUTION DIRECTLY.