Let's talk about ways to help protect your money

There are many convenient ways to send money to people you know. However, if you send your money or give it to a scammer, **there is often little we can do to get your money back**. That's why we encourage you to talk with us about ways to help protect yourself before wiring or withdrawing cash.

Red flags to avoid

No matter the situation, **be cautious when wiring or transferring funds, or giving/sending cash** to people you don't know or businesses you haven't worked with before, especially if any of **the following red flags** are present.

1. You're contacted unexpectedly
2. The communication plays with your emotions
3. You're asked to pay in an unusual way or asked to transfer money to protect yourself
4. You're pressured to act immediately
5. If it seems too good to be true, it likely is

Think carefully if you are:

- Instructed not to trust Bank of America associates or how to respond to questions, **including to say anything other than the truth**
- Contacted out of the blue and told there's an issue that needs immediate attention
- Pressured to act immediately and the request or communication plays with your emotions
- Directed to send a request for money or payment in an unusual way such as a wire transfer, gift cards or pre-loaded debit cards
- Threatened with law enforcement action

Also watch for these:

A phone call, email, text, direct message or pop-up with a request for personal information or money

Scammers will:

- Pose as an employee from a familiar organization and say there's a problem that needs your immediate attention
- Ask for a favor, personal details, money or coach you through steps to complete an action to gain access to your devices and personal information
- Try to confirm your identity with a verification code they send you — even though they called you
- Insist that you download apps or click links to fix issues or confirm information

Remember: Scammers use convincing stories. They can use fake email addresses and caller ID information — don't trust them. Make sure you have verified the identity of the person who has contacted you before acting on any request. Never click a link or attachment from someone you don't know.

See reverse for additional information.

Take precautions in these common situations:

Overpayment scams

If someone offers to send you money through a check but requests that you return extra funds or use the money to buy gift cards, cashier's checks, or other items, be aware. Similarly, be wary if a company claims they mistakenly deposited money into your account and asks for it back. Remember, legitimate transactions rarely involve refunding or redirecting funds in these ways.

Real estate scams

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. Before you send any money, always independently confirm wiring instructions in person or via a phone call to a trusted or verified phone number that you called directly.

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. Always validate requests for money, research investment managers/offers and use caution if asked to provide personal or financial information.

Technology scams

If you get an unsolicited request to remotely access your computer or mobile device, it's most likely 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. 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).

Impostor scams

Scammers may pretend to be familiar businesses or individuals, such as your bank, utility company or even a friend or relative. They can contact you using email, text, or even a familiar phone number. Be cautious if they ask you to send funds to yourself or others to prevent a potential threat. While Bank of America may send you a text to validate unusual activity, we will never contact you to request that you send money using Zelle®[1] to anyone, including yourself. Don't share codes based on a call you receive. We also will never ask you to share a code we text with us over the phone.

Romance scams/Sending funds to a loved one

Scammers may contact you via dating apps or social media and try to establish a trusting, caring and believable relationship — as quickly as possible; or they may tell you that someone you love is in trouble or needs help. 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. Verify the situation by directly calling the person needing help or a trusted contact. If this is an online relationship or someone you have never met in person, perform research on the person or the situation before sending money.

Online sales scams

Scammers set up fake stores selling fake goods, and after you've made your purchase, the store will suddenly disappear. They may use social media platforms to contact you and build a relationship, telling you about an offer that's hard to resist, then instructing you to download an app or send money to take advantage of the offer. Research the seller and products independently, check reviews for possible scam notices, and compare prices with other websites.

Winning prizes and lotteries

If a prize is real, you should not be asked to pay money upfront. Taxes or fees are automatically withheld from rewards or lottery winnings. If you didn't enter a contest, odds are you didn't win it.

To learn more about ways to help protect yourself, talk to an associate or visit the Bank of America Security Center online or on your mobile device at bankofamerica.com/security.

[1] Zelle® should only be used to send money to friends, family or others you trust. We recommend that you do not use Zelle® to send money to those you do not know. Transfers require enrollment in the service with a U.S. checking or savings account and must be made from an eligible Bank of America consumer or business deposit account. Transactions between enrolled users typically occur in minutes and transactions between enrolled consumers do not typically incur transaction fees from Bank of America. We will send you an email alert with transaction details after you send money using Zelle®. Dollar and frequency limits apply. See the Online Banking Service Agreement at bankofamerica.com/serviceagreement for further details. Data connection required. Message and data rates may apply. Neither Bank of America nor Zelle® offers a protection program for any authorized payments made with Zelle®. Regular account fees apply. Zelle and the Zelle related marks are wholly owned by Early Warning Services, LLC and are used herein under license.

00-74-0313NSB | 06/2023

BANK OF AMERICA