Protecting Yourself from Fraud

You should stay vigilant and cautious to protect yourself against fraud. Below are a few steps you can take to reduce your risk and make yourself less of a target to scammers.

- Monitor your accounts regularly to guard against unauthorized transactions or account changes.
- Create strong passwords, and don't share your passwords with anyone.
- Passwords should:
    - Include a combination of letters and numbers.
    - The longer the password the harder for a fraudster to identify it.
    - Add numbers in multiple places both in the middle and ends of the password.
    - Avoid names, birthdates, social security numbers, or other personal information, as these can be easily guessed.
    - Use unique passwords for each account, so that a scammer would not be able to log in to multiple accounts if they identify your password.
- Usernames should be unique for each account. This way, if a scammer compromises one account, it will be more difficult for them to compromise other accounts.
- Use two-factor authentication whenever it is available. Two-factor authentication requires you to enter a unique security code, that is provided to you via email or SMS messaging. This adds a layer of security to your account and makes it harder for scammers to break into your account.
- Do not use public Wi-Fi to access your account information. Use your home Wi-Fi or a secured Wi-Fi connection to access accounts online.
- Update your devices regularly and use updated operating systems. Make sure your devices all have reputable anti-virus software installed. This helps prevent scammers from installing malware on your devices.
- Don't provide personal or account information via email, text, or to an unsolicited caller. If you receive an unsolicited call from someone asking for your personal or account information, or if something just doesn’t feel right, it’s a good practice to end the call and contact the company directly. Find the company's contact information online or on a trusted source, such as an account statement, rather than clicking a link or calling a number provided in an unsolicited communication.
- Similarly, don’t click on unsolicited links or attachments sent via email or text. These can be phishing attempts or could introduce a virus or malware onto your machine. Instead, go to the company's website to locate the information, or contact the company directly to confirm if the email or text you received was legitimate.