## **DON'T FALL FOR IT!**

## Stay safe this Fall from fraud and scams

Scammers are becoming increasingly sophisticated, but sometimes, a simple defense is your best shield. They employ various tactics, including technology, impersonation, and couriers, all aimed at swindling you out of your hard-earned savings. Despite their high-tech methods, you can safeguard your accounts by following these simple guidelines:

- Legitimate individuals won't pressure you. If someone urges you to act quickly, Stop, hang up, and reach out to a trusted friend or family member.
- Not all internet search results lead to authentic business websites. To ensure you're logging into the right site, check your statements or bills and manually type in the website. If you're uncertain, Stop what you're doing and call the company directly.
- Sharing personal identifiers with anyone can put your identity at risk. If someone requests your one-time password, PIN, online credentials, or Social Security Number, Stop, hang up, and contact your bank.
- FBOG will never ask you to send money to anyone (such as through Zelle®, wires, etc.). If someone claiming to be from FBOG requests money, Stop, hang up, and call FBOG for verification.
- Banks, government agencies, and utilities will never solicit payment through unconventional methods. If you're asked to do something out of the ordinary (like purchasing gift cards, precious metals, or digital currencies), keep your funds secure:
  Stop. Hang up. Contact your bank and report the issue to the authorities.
- Trust your instincts. If something feels off, it likely is. Stop, hang up, and consult with a trusted friend or family member.
- Check your statements. Review your bank and credit card statements regularly for unfamiliar or suspicious transactions. If something doesn't look right, contact your bank right away.

## Stay alert to safeguard your accounts.

Bookmark our site, greenwichfirst.com/security-tips/, and visit regularly for the latest updates on prevalent scams and tips on recognizing them.

If you suspect a scam has targeted you, report it to the FTC at reportfraud.ftc.gov/ and alert your bank.

When contacting your bank, always use the number on the back of your card. If your card is lost, go to the bank's website or mobile app and call the number found under "Contact Us."



