GUARD

YOUR PERSONAL INFORMATION...

- ✓ Never give financial or other personal information by phone (voice or text), Internet or mail unless you initiated the contact for a legitimate reason.
- ✓ Be careful about sharing personal information and don't give out more than necessary.
- ✓ Shield your PIN at ATMs or when using a debit card for a purchase.
- ✓ Immediately report lost or stolen credit or debit cards. Do not lend your debit or credit card to anyone.
- ✓ Sign up for Brella™, the free mobile app that helps protect you from fraud by sending alerts when your debit card is used so you can quickly detect unauthorized activity.
- ✓ Carry only the ID you need. Put other ID (Social Security number, birth certificate, passport) in a safe place.
- ✓ Shred documents with personal information, including debit and credit card receipts.
- ✓ Never preprint your driver's license number or Social Security number on your checks.
- ✓ Notify your Southeastern Bank branch if newly ordered checks or routine bank statements don't arrive in a timely manner.
- ✓ Know how many checks you ordered and also verify your order and the accuracy of the information on your checks.
- ✓ If personal checks (or any checks payable to you) are stolen, notify your Southeastern Bank branch immediately and close the compromised account.
- ✓ Promptly review and reconcile your bank statements for accuracy and fraud.
- ✓ Never release your Social Security number to make a purchase; offer other identification instead.
- ✓ Destroy pre-approved credit card applications if you aren't going to take advantage of them.
- ✓ Do not talk about your confidential banking information where others may overhear you.
- ✓ Visit the following websites for additional tips on guarding your ID and avoiding scams:
  - Federal Trade Commission: ftc.gov
  - AARP®: aarp.org

SIGNS OF ID THEFT

- ✓ Purchases not made by you appear on your monthly bills.
- ✓ Bills arrive on accounts you don't own.
- ✓ Collection agency calls about unknown debt.
- ✓ Credit card/bank statements don't arrive.
- ✓ Your credit report shows mystery debts.

WHAT TO DO IF YOUR IDENTITY HAS BEEN STOLEN

- ✓ Call your Southeastern Bank branch.
- ✓ Put a fraud alert on your credit report by contacting:
  - Equifax: 1-800-525-6285
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289
- ✓ Keep records of steps taken to clear your name and re-establish your credit.
- ✓ Consider filing a police report.

GUARD YOUR DEVICES & THEIR INFORMATION

Select a complex password of letters, numbers and symbols. Make your Internet banking password long and complex so it is hard to crack. Between 8 to 20 characters is recommended.

Use different passwords for different sites & apps and take advantage of layered security options whenever possible. Don't share login IDs, passwords or other credentials used to access mobile banking or other apps with anyone.

Install firewall, anti-virus, anti-spyware and security software updates often.

Delete spam or emails that ask for bank or other sensitive information. This includes not clicking on links or attachments sent in emails or texts as doing so may download a virus or other malware onto your device.

Pay attention to a website's URL. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

When shopping online, use well-known, reputable sites. Also look for https://, a closed lock or an unbroken key icon.

Don't stay permanently signed into accounts. When you've finished using an account, log out.

Adjust the settings on your mobile device so it doesn't automatically connect to nearby Wi-Fi. That way, you have more control over when and how your devices uses public Wi-Fi. Never use public Wi-Fi to conduct financial transactions.

Bluetooth is also vulnerable to interception. Be sure to turn Bluetooth off when you're not using it.

Lock your phone. Use at least a 6-digit passcode on your device or facial recognition. Set the device to automatically lock when not in use.

When disposing of hard drives, use overwrite software or destroy the drive.

Use the current version of your Internet browser so web pages display quickly and make sure you have the latest security updates.

Take advantage of any anti-phishing features offered by your email provider and Internet browser.

With your identity, thieves can open new bank accounts, take out a mortgage on your property, buy cars and more.