GUARD
YOUR PERSONAL INFORMATION...

- ✓ NEVER provide financial or other personal information by text, email, postal mail, other Internet apps or voice call unless YOU initiated the contact for a legitimate reason. And when you must share, 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. Don't lend your debit or credit cards 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. You can also establish $ limits and other restrictions with Brella™.
- ✓ Carry only the ID you need. Put other ID (Social Security number, birth certificate, passport) in a safe place. Audit your wallet and purse frequently and remove unnecessary items that could compromise your personal information if lost or be a hassle to replace.
- ✓ Shred documents with personal information, including debit and credit card receipts, preferably with a cross-cut shredder. Destroy pre-approved credit card applications if you aren't going to take advantage of them.
- ✓ Don't let delivered mail sit in your mailbox. Grab it as soon as possible. Be cautious about outgoing mail, too.
- ✓ Notify your Southeastern Bank branch if newly ordered checks or routine bank statements don't arrive in a timely manner. Better yet, use online Bill Pay and sign up for e-statements.
- ✓ With check orders, make sure you received the quantity you ordered and confirm the accuracy of the information on the checks.
- ✓ If personal checks (or any checks payable to you) are stolen, notify your Southeastern Bank branch immediately and close the compromised account.
- ✓ Monitor your bank and other financial accounts by going online every few days to review balances and transactions.
- ✓ Never release your Social Security number to make a purchase; offer other identification instead.
- ✓ Do not talk about your confidential banking information where others may overhear you.
- ✓ Periodically check your credit report for unusual activity.
- ✓ Visit the following websites for additional tips on guarding your ID and avoiding scams:
  - Federal Trade Commission: ftc.gov
  - AARP®: aarp.org
- ✓ Trust your instincts, especially if being pressured to divulge personal information or act hastily. If something doesn't seem right, discuss it with someone you trust and take extra time to think about it.

SIGNS OF ID THEFT

- ✓ The balances in your bank or other financial accounts drop unexpectedly or unusual transactions appear.
- ✓ 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 or 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 unique passwords for different sites & apps and turn on two-factor authentication. Don't share login IDs, passwords, secure access codes 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 – and DON'T click on links or attachments in emails or texts unless you trust the sender and were expecting them.
- ← 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 use 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 biometric identification or at least a 6-digit passcode on your device. Set the device to automatically lock when not in use.
- ← 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.
- ← Adjust your profile on social media so only your friends can see your page. Don't accept friend requests from people you don't know or respond to random messages from strangers.
- ← When disposing of hard drives, use overwrite software or destroy the drive.

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