GUARD
your personal information...

- Never give personal information by phone, Internet or mail unless you initiate the contact.
- 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.
- Carry only the ID you need. Put other ID (Social Security number, birth certificate, passport) in a safe place.
- Shred documents with personal information.
- 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 driver's license number 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.

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
  Trans Union: 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 and applications.

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

Don't try and don't reply to spam or emails that ask for bank information. This includes not clicking on links or attachments sent in emails.

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).

For online transactions, 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 device uses public Wi-Fi.

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, order cell phones, take out a mortgage on your property, buy cars or furniture and more.