Protecting Your Information

Identity theft and account fraud are attracting more attention these days. These crimes are committed when someone steals personal information such as your bank account number or Social Security number, uses that information to take funds from your account or borrow in your name.

What can I do to protect myself?

- **Don't give out your social security, checking account or credit card number over the telephone unless you initiate the call and trust the person or vendor.**
- **Don't carry social security numbers in wallets or write them on checks.**
- **Report lost or stolen checks immediately. Promptly review all checks when you receive new ones to be sure none have been stolen in transit.**
- **Protect your purse or wallet at all times. Keep personal information, cancelled checks and new checks in a safe place.**
- **Always shred or tear up financial statements, invoices, charge receipts, ATM receipts and other personal documentation you wish to discard.**
- **Notify your financial institution immediately if you receive a suspicious phone call from someone pretending to represent the bank and asking for account information to "verify a statement" or "award a prize" or any other unusual purpose.**
- **Call the customer service number 256-543-3860 or report to your branch office if you receive a suspicious e-mail or telephone call from someone who says he or she represents The Southern Bank Company.**
- **Don't respond to any e-mail that asks for your password, Social Security number or other personal information. Open e-mails only when you know the sender and be especially careful about opening an e-mail with an attachment.**

What can be done if I think that my identity has been stolen?

- **Contact companies, including banks, where you have accounts. Inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions. Close accounts so future charges are denied.**
- **File a report with the local police so there is an official record of the incident. You can also file a complaint with the Federal Trade Commission (www.ftc.gov).**

- **Contact the main credit reporting companies and place a "fraud alert" in your file. Once you place the fraud alert, you are entitled to order one free copy of your credit report from each of the three credit reporting companies.**

  Equifax: 1-800-525-6285; www.equifax.com; P. O. Box 740241, Atlanta, GA 30374-0241

  Experian: 1-888-397-3742; www.experian.com; P. O. Box 9532, Allan, TX 75013

  Transunion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P. O. Box 6790, Fullerton, CA 92834-6790

- **Check your credit report to see if there has been unexpected or unauthorized activity. Request a "fraud alert" for your file and a "victim's statement" asking creditors to call you before opening new accounts or changing existing ones.**
- **Watch for stolen mail. If you suspect that any mail is not being delivered to you, confirm this with the sender and contact the local post office and police.**
- **Keep written records of all incidents. Include what happened, what was lost or stolen, and what steps you took to report the incident to law enforcement and the various agencies, banks, and firms involved. Be sure to include the date, time, telephone numbers called, the name of the person you spoke to, and any other relevant information.**

We hope you find this information useful. At The Southern Bank Company, we believe that being informed and taking the right precautions can go a long way to help you avoid becoming a victim of identity theft and account fraud.