FNB South Customer Awareness Program

FNB South's Commitment to Security

FNB South will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential customer information. Fraudulent emails may be designed to appear as though they are originated by FNB South. Do not respond to any email communications which request any type of personal or confidential information and do not go to any links listed on that e-mail. These communications are not originated by FNB South! Never give out any information that the Bank already has to a caller, texter, or e-mail sender. If you contact us we may verify the last 4 digits of your SSN to confirm your identity but we will never contact you and ask for your debit/credit card number or your full SSN. If we need to contact you, it will always be done in a manner that protects your personal, confidential information and we will clearly identify ourselves. One of our top priorities is to safeguard YOUR confidential information and we work diligently to do so. We always work with the local regulatory and law enforcement departments to be certain any type of illegal activity is stopped as soon as possible. We have multi-layer security to protect your confidential information and will continue to be vigilant in protecting it. You should immediately report any suspicious emails or websites to FNB South.

If you suspect identity theft or have any questions regarding this notice, please contact FNB South at (912) 632-7262 and ask to speak to a customer service representative.

Online Banking Security

FNB South is committed to protecting your personal information. Our Online Banking uses several different methods to protect your information. All information within our Online Banking uses the Secure Socket Layer (SSL) protocol for transferring data. SSL is a cryptosystem that creates a secure environment for the information being transferred between your browser and FNB South. All information transferred through Online Banking has a 128-bit encryption. In addition to the security features put in place by FNB South.

Here are some tips on keeping your information secure.

- Never give out any personal information including User Names, Passwords, SSN, and Date of Birth
- Create difficult passwords which include letters, numbers, & symbols
- Don't use personal information for your user names or passwords like Birth Dates & SSN
- Avoid using public computers to access your Online Banking
- Don't give any of your personal information to any web sites that does not use encryption or other secure methods to protect it

What is Identity Theft?

Identity theft involves the unlawful acquisition and use of someone's identifying information, such as:
Name

- Address
- Date of Birth
- Social Security Number
- Mother's Maiden Name
- Driver's License
- Bank or Credit Card Account Number

Thieves then use the information to repeatedly commit fraud in an attempt to duplicate your identity which may include opening new accounts, purchasing automobiles, applying for loans, credit cards, and social

security benefits, renting apartments and establishing services with utility and telephone companies. It can have a negative effect on your credit and create a serious financial hassle for you.

How do I protect myself?

You should report lost or stolen checks or credit cards immediately. Never give out any personal information including birth date, SSN or Passwords Shred all documents containing personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices. Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it. For more information about identity theft and other tips on how to protect yourself and your information please visit the websites listed below.

Debit Card Protection

Debit card usage has increased dramatically in recent years and fraudulent use of debit cards has also increased. We at FNB South have some suggestions for you for the care and usage of debit cards. NEVER give your debit card information when requested by phone, email, or texting. We at neither FNB South nor any other bank we know of will ever request information from you in this manner. Please contact us if you receive any such request. It is a good idea to pay by credit card if your card leaves your sight. An example might be when a waiter takes your card from your table in a restaurant or when ordering online. Debit cards are easier to process illegally vs. credit cards.

What You Can Do

- Install and keep up to date antivirus software protection.
- Be sure and use a firewall when surfing.
- Don't click on links in emails.
- Don't surf to pages you are unsure of.
- If you are a commercial account you should perform your own risk assessments and evaluations on all online accounts.

Federal Trade Commission:
http://www.ftc.gov/bcp/edu/microsites/idtheft/
FDIC Consumer Alerts:
http://www.fdic.gov/consumers/consumer/alerts/index.html
United States Department of Justice:
http://www.usdoj.gov/criminal/fraud/websites/idtheft.html
Equifax:
P O Box 105069
Atlanta, GA 30349-5069
www.equifax.com
To order a report: (800) 685-1111
To report fraud: (800) 525-6285
Experian:
P O Box 2002
Allen, TX 75013-0949
www.experian.com
To order a report: (888) 397-3742
To report fraud: (888) 397-3742
Trans Union:
P O Box 1000
Chester, PA 19022
www.transunion.com
To order a report: (800) 916-8800
To report fraud: (800) 680-7289