Identity Theft Assistance Guide – Southern First Bank

The checklist below is designed to assist you with steps to take, if you believe you have been a victim. Always keep track of contact names and telephone numbers of the individuals you have contacted for future reference.

Contact your Southern First Bank relationship team.

- Report any fraudulent activity on your Southern First accounts by calling a member of your relationship team at 864.679.9000 or 1.877.679.9646, or via email.
- Review activity on all of your accounts, including checking, savings, credit card, debit card, and loans. Check for changed addresses and changed Personal Identification Numbers (PINs).
- Close accounts which have been compromised. Fraudsters may or may not immediately begin using your account information. Open new accounts, passwords, and (PINs).
- Change your online banking username and password. Create a "strong" password with at least 8 characters that includes a combination of letters and numbers. Avoid using an automatic login feature that saves usernames and passwords.

Contact the major Credit Bureaus, and request a "fraud alert" to be placed on your credit file.

- Equifax: 1.800.525.6285 or www.equifax.com
- Experian: 1.888.397.3742 or www.experian.com
- TransUnion: 1.800.680.7289 or www.transunion.com
- Request a free copy of your credit report. This can be conducted online at: www.annualcreditreport.com

Contact other creditors or financial institutions.

- Include credit card companies, utility service providers, financial institutions and lending agencies.
- Send a letter or email to the company referencing the contact person's name and discussion. Retain copies of all documents provided.
- Close any compromised or suspected compromised accounts. Open new accounts with new passwords or PINs.

Contact your local police agency and file a report.

- Depending upon your location, you may have to contact either city or county police. A police report will provide creditability to your case when dealing with creditors who may require proof of criminal activity

Report the criminal activity to the Federal Trade Commission (FTC) or other agencies as needed: Call 1.877.ID.THEFT (1.877.438.4338) or file a complaint online.

- If you believe your mail was stolen or redirected, notify the US Postal Inspection Service at www.usps.com.
- If you believe your Social Security number is being used fraudulently, call the Social Security Fraud Hotline at 1.800.269.0271.
- If you believe someone has stolen or is using your state issued Driver's License, contact the Department of Motor Vehicles or you may contact them at the SCDMV Hotline, 803.896.9688.

Diligently review your accounts and statements, and continue to report any suspicious activity.

- Do not use public or other unsecured computers for logging into Online Banking.
- Check your last login date and time, and transfer history every time you log in.
- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to your financial institution.
- Take advantage of and regularly view system alerts; examples include: balance alerts, transfer alerts, password change alerts, ACH Alerts (for Cash Management users) and Wire Alerts (for Cash Management users).