Steps You Can Take to Protect Yourself from Identity Theft

1. **Review your account statements/credit reports and notify law enforcement and us of suspicious activity.**
We recommend that you regularly review statements from your bank, credit card, and other accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
1.800.685.1111	1.888.397.3742	1.800.916.8800

When you receive your credit reports, look them over carefully. Look for accounts that you did not open and/or inquiries from creditors that you did not initiate. Also check to see if your personal information on the credit report is accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you remain vigilant in your review of your account statements and credit reports. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission. A copy of a police report may be required by creditors to clear up your records.

2. **Consider placing a fraud alert or a security freeze on your credit files.**
If you suspect that you may be a victim of identity theft, consider placing a fraud alert or a security freeze (also called a credit freeze) on your credit file. Security freeze laws vary from state to state. For more information about fraud alerts and security freezes, please see the Federal Trade Commission's guidance at http://www.consumer.ftc.gov/articles/0279-extended-fraudalerts-and-credit-freezes.

3. **Protect your Passwords.**
You can minimize the threat of identity theft by improving your password practices. Use different passwords for all your accounts. Make those passwords strong with at least eight characters, including a mix of letters, numbers, and symbols ($%#!*@). Change your passwords from time to time. For additional guidance on passwords and securing your accounts, see http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/passwordsand-securingyour-accounts.

4. **Fight "phishing" – don't take the bait.**
Scam artists "phish" for victims by pretending to be banks, stores, government agencies, or other trusted sources. They do this over the phone, by email, and by postal mail. Do not respond to any request to verify your account number or password. Legitimate companies do not request this kind of information in this way. If an email looks suspicious, don't click on any links in that email.

5. **Learn more about how to protect yourself from identity theft.**
You may wish to review the Federal Trade Commission's guidance on how to avoid identity theft and what to do if you suspect your identity has been stolen. For more information, contact the Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580; www.ftc.gov/idtheft; 1.877.ID.THEFT (1.877.438.4338).