ADVICE ON WAYS TO AVOID SEASONAL SCAMS

The Virginia State Attorney General's office had previously developed a program to help prevent Identity Theft criminals during the holiday season. The program has been called "Campaign STOP".

The letters in "STOP" represent the four steps that consumers should take in protecting their identity:

- **"S"afeguard your Social Security number. You should not carry your Social Security card with you. You need to memorize the number and keep the card in a safe place. Do not give the number for unverified requests.**
- **"T"reat trash and mail properly. Always shred credit card pre-approval applications and bills containing personal information such as credit card numbers, account numbers, birth dates, and Social Security numbers before throwing them in the trash.**
- **"O"rder credit reports. You should check your credit report at least once a year and look for suspicious activity. Credit reports are available for free - you can visit http://www.annualcreditreport.com or call (877)322-6226 for more details.**
- **"P"rotect identity information. Do not give out personal information to incoming callers or in response to incoming emails.**

Here are some other tips for avoiding scams during the holiday season, provided by the Attorney General's Office, the Better Business Bureau, and the National Cyber Security Alliance:

- **Gift cards. You should not purchase gift cards on internet auction sites. You are taking a risk because the cards may be stolen and have no value. Buy gift cards from reputable sources - directly from the store if you can. When buying a gift card, keep the original purchase receipt with the card as proof of purchase.**
- **Fraudulent Emails or pop-ups. On your computer, delete Emails or pop-ups that ask for personal information, such as account numbers or passwords. This is happening more frequently and criminals have become skilled at sending Email messages that appear to be from legitimate businesses with the actual logos. Always remember - legitimate businesses do not send unsolicited Email messages asking for such information.**
- **Safe web sites. When buying something online, look for signs that the Web site is secure. These signs include a closed padlock on the browser's status bar. When you are asked to provide payment information, the beginning of the Web site's URL address should change from "http" to**

"https", indicating that the purchase is encrypted or secured. If these two items are not seen, do not proceed with the purchase.

- **Charitable giving. Do not respond to unsolicited Email messages for charitable giving. Call the organization and ask for written information and verify the charity's registration with the State Office of Consumer Affairs at (804)786-2042.**