QUICK TIPS ON PROTECTING YOURSELF AGAINST ID THEFT!

- **Do not put your Social Security number (SSN) on any documents, unless it is <u>legally</u> required.**

- **Talk with your attorney regarding documentation to be submitted to the Register of Deeds office for recordation. Make sure you follow-up so personal information like social security numbers and financial accounts are not placed on public record.**

- **Social Security numbers (SSN) are not mandatory for example on the following documents: NC General Warranty Deeds; Certificates of Satisfaction; Deeds of Subordination; Deeds of Trust; Separation and Property Settlement documents; Powers of Attorney.**

- **Personal checks. No longer order checks including your Social Security Number or Driver's License Number.**

- **Check your credit report several times a year to make sure it doesn't have unfamiliar accounts.**

- **Shred or burn papers with credit card or bank account numbers, Social Security numbers, etc.**

- **Don't carry your Social Security Card.**

- **Avoid using easily available information (Date of Birth-DOB; Last 4 digits of the SSN; personal phone number)**

- **Secure personal information in your home.**

- **Ask about information security procedures in your workplace**

- **Don't give out personal information on the phone unless you've initiated contact or are sure of whom you are dealing with.**

- **Guard your mail and trash from theft**

- **Deposit outgoing mail in a secured mailbox.**

- **If you go on vacation, call the United States Postal Service at 1-800-275-8777 to ask for a vacation hold on your incoming mail.**

GUARD PERSONAL INFORMATION ON YOUR HOME OR BUSINESS COMPUTER!

- **Update virus protection software regularly.**
- **Update your operating system regularly with security patches**
- **Don't open e-mail, download files, or click links that you don't know who the sender is. Much spam is considered "phishing," the act of deception to acquire sensitive personal information by IM, e-mail, etc.**
- **Use a firewall, especially if you have broadband connections.**
    - **If your computer is using the latest version of Windows XP, you have a built-in firewall.**
- **When doing eCommerce or online banking, assure yourself that you're using a Secure Sockets Layer (SSL) encrypted connection. Your browser indicates that websites use it with a small "lock" icon in the status bar, or that your URL has changed to "https://". The website's privacy policy will also explain what encryption it uses to protect your information.**
- **Avoid storing important financial information on laptops and use strong passwords (8 or more characters, including numbers, both lower and uppercase, without dictionary words).**
- **Delete any personal information on your computer before you dispose of it. This can be achieved with "wipe" programs that will write 1's and 0's over all data, making it unrecoverable.**
- **Never give out your passwords to anyone. Your ISP does not need to know your password to reset it, nor does your business' tech support, nor does any website. They should reset your password instead, and then you should immediately change it.**

IDENTITY THEFT TELEPONE HOTLINE NUMBERS

If you are a victim of identity theft, call the fraud hotline for one of the three major credit-reporting agencies to check your credit. By law, you are allowed one free credit report a year. As part of a new plan, the other two will be notified:

• Equifax -- (800) 525-6285

• Experian -- (888) 397-3742

• TransUnion -- (800) 680-7289

You can file a complaint

• Federal Trade Commission -- (877) 438-4338;

Other government ID theft hotlines

• Social Security Administration -- (800) 269-0271

• Internal Revenue Service -- (800) 829-1040

• SCAN – 1-800-262-7771

International Check Services

• 1-800-631-9656

OTHER RECOMMENDED ACTIONS FOR VICTIMS OF IDENTITY THEFT

- **Close any accounts that have been tampered with or opened fraudulently.**
    - **Credit accounts, such as from banks, credit card companies, phone companies, utilities, and ISPs.**
    - **If you open new accounts, use different passwords and pin numbers.**
- **File a report with your local police in the community where the identity theft took place, and keep a copy of the report.**