12 Steps to Personal Security

1) Do not give out your Social Security number to people or companies that you do not know. Under no circumstances should you give out personal information on the phone to someone you do not know, or if you did not initiate the call. If someone calls looking for personal information to "update records," get their name, phone number, and address. Call them back at the number you have on file, or use one that is printed on your billing statements. Do not disclose personal information until you know why it is required and how it will be used.

2) Review your credit report from each of the three major credit reporting agencies (TransUnion, Equifax, and Experian) at least once per year. Check the information and dispute any inaccuracies. Ascertain that there have been no inquiries by people with whom you have not initiated business. (Beginning December 1, 2004, consumers will be entitled to one free credit report from each agency once per year.)

3) Review all monthly credit card statements and bank statements as soon as they arrive each month. Be sure there are no charges you did not make. Also make sure you actually receive the statement each month. If it is late, contact the card issuer and make sure no one has changed the address on the card.

4) Shred all paperwork which contains your personal information. When shredding, cross-cut so that no numbers remain in readable rows. Destroy any and all unwanted credit card and refinancing offers. Shred any documents you no longer need which contain personally identifiable information and account numbers.

5) Guard your mail from theft by collecting it regularly. Forward it to a post office box if you will be out of town. Always take bills or documents with personal data to the post office or an official postal service mailbox; never leave them for pickup in your personal mailbox.

6) Store any personal information you keep at home and at work in a safe place. Do not put any information other than your name or address on your checks.

7) Guard deposit slips as closely as checks. Not only do they have your name, address, and account number, but they can also be used to

withdraw money from your account. (They can simply deposit a bad check and use the “less cash received” line to get money out of the account.)

8) If you are ever denied credit, find out why immediately. This is particularly important if you have not reviewed your credit reports lately. If you get a call from a merchant or card issuer about charges you did not make, react quickly. This may be the first warning that your identity has been stolen or compromised.

9) Do not carry your birth certificate, passport, or any other cards which display your Social Security number in your wallet. Only carry as many credit cards as necessary. Photocopy everything that you carry in your wallet / purse to make canceling and replacing items easier if your wallet / purse is stolen.

10) Create unique passwords and personal identification numbers (PINs). Avoid using easily available information, such as mother’s maiden name, date of birth, or the last four digits of your Social Security number.

11) Do not answer email requests for personal or account information unless you are able to verify their legitimacy. Initiate the visit to the requestor’s website yourself through a known valid link, or make a phone call to the business regarding the inquiry.

12) Protect your name**.** Get an unlisted phone number, or drop your address from the listing. Do not use titles such as "Dr." or "Atty" in your listing.