

**IDENTITY THEFT –
WHAT YOU NEED TO KNOW**
Anne R. Moses

Identity Theft is our fastest growing crime. More than 15M people have been victims.

There are 3 basic types of identity theft:

1. *True Name Identity Takeover* - Someone gets your personal information and assumes your identity at a different address to open new accounts. This is the most serious type.
2. *Synthetic Identity Theft* - The thief combines different elements of real identities to create a fictitious person – his name, your SS# and birthday.
3. *Account Takeover* – The thief gains access to your debit or credit card account information (or other assets) and makes purchases or withdrawals. This is the most common type.

In 2003, a law was enacted to provide remedies. Beginning in November, all creditors must have a program in place using specified identity theft “red flags” to verify the identity of anyone applying for credit. This applies to new applicants as well as existing credit accounts.

Here are some steps you can take – for free -- to protect yourself:

1. Get a free copy of your credit report from Equifax, Experian and TransUnion annually at www.annualcreditreport.com. Every 4 months request a report from a different credit bureau. Review each report carefully and challenge any inaccurate information.
2. If you think you are or may become a victim, place an “initial fraud alert on your credit file by calling any one of the 3 credit bureaus. This lasts for 90 days but can be renewed.
3. Shred all discarded tax returns, SS earnings histories, bank or brokerage statements. If you are discarding a computer, physically destroy the hard drive or use a program that deletes hidden data files.
4. Opt out of pre-approved credit solicitations by calling 1-888-5-opt-out.
5. If you are not actively seeking credit, freeze your credit file with each national credit bureau.
6. Don't go to Internet links you don't know and trust

7. Don't share your card information with anyone – most thieves are people you know.
8. Never give personal information in response to an unsolicited phone call or email.
9. Trust your instincts.
10. When making online purchases, set your PC security options at “high” and check that the site shows a high level of security such as “https” or a VeriSign or other security logo on the check out page.

Good luck and be careful!