## **IDENTITY THEFT FACT SHEET**

Source: FTC's NCPW 2005. Quiz – Identity Theft: When Fact Becomes Fiction

- 1. ID theft is the fastest growing white-collar crime in the U.S. 27 million Americans have been victims of the crime in the past five years, nearly 10 million people last year.
- 2. Identity thieves can get personal information from you by:
  - Stealing your wallet or purse
  - Stealing your mail
  - · Rummaging through your trash, and
  - Using personal information they find on the Internet about you.

For additional information on how ID thieves can steal your identity, go to: <a href="https://www.consumer.gov/idtheft/understanding\_idt.html#2">www.consumer.gov/idtheft/understanding\_idt.html#2</a>.

- 3. If you are getting rid of your computer, it is not enough to delete files using mouse and keyboard commands. Use a "wipe" utility program to overwrite the entire hard drive. This makes files unrecoverable.
- 4. ID thieves that obtain your personal information can: (1) call your credit card issuer and change the mailing address on your card; (b) open a new credit card account or bank account in your name; (c) file for bankruptcy under your name to avoid paying off debts they've incurred; and (d) counterfeit checks or drain your bank account.
- 5. Here are some ways for you to minimize your risk of becoming a victim of ID theft::
  - Don't give out personal information by email, Internet, phone or mail unless you initiated contact and you are certain you know who you are dealing with
  - Don't carry your social security card with you
  - Carry only the identification information and credit/debit cards that you actually need
  - Password protect your credit card, bank and phone accounts.
  - For additional tips, go to: www.consumer.gov/idtheft/protect\_againstidt.html#5.
- 6. If you are a victim of ID theft, place a fraud alert on your credit report. This will help prevent If thieves from opening additional accounts in your name.
- 7. If you think someone has stolen your personal information or identification, do the following:
  - Immediately close all your credit card or bank accounts
  - Place a fraud alert with any one of the three national consumer reporting companies
  - Contact the Social Security Administration to get a new Social Security number
  - Alert issuing agencies for your driver's license and other identification documents
- 8. If you have high speed Internet connection, such as DSL or cable modem, get a firewall program to prevent uninvited guests from accessing your computer.
- 9. Signs you could be a victim of ID theft:
  - Fail to receive bills or other mail
  - Receive credit cards for which you did not apply
  - Are denied credit for no apparent reason
  - Get calls or letters from debt collectors or businesses about merchandise or services you didn't buy
- 10. Don't tape computer and website passwords to your computer. Safeguard these passwords. Also, when creating passwords, use a combination of letters (upper and lower case), numbers and symbols.