FCC
Computer Security
Notice

IDENTITY THEFT PROTECTION

These days the simple act of throwing out your trash can lead to financial disaster. Identity Theft is not a new crime; it has been around for decades. With the overabundance of information on the Internet such a crime has become even easier to commit.

What is Identity Theft? Identity Theft, for the most part, is credit card fraud or bank fraud where a thief plots to steal from you. Simply by gaining access to your Social Security number (SSN) or an existing account number the thief can create new credit, bank and store accounts for which they never intend to repay ruining your good name and your credit.

How Identify Theft Occurs. There are several conventional methods employed to gain access to your personal information. The thief seeks out credit card or bank statements in your trash. They steal incoming or outgoing mail. They may steal your purse or wallet. They also commit phone or email scams. The truly bold simply break into you residence.

How the Internet Fuels the Identity Theft Crime Spree. Unlike the methods noted above the truly savvy thieves have gone high tech. The Internet can be used much more easily to steal someone's information. An information broker employed by the thieves can get just about anything. In the past information brokers were used primarily to get information for lawyers, corporations or private investigators. This is no longer the case and their practices may be unscrupulous.

With a few dollars an identity thief can look up your DMV records. They can also look at the header file in your credit report which includes your name, address and sometimes your SSN. A phony signature can get an entire credit file from an information broker. Your property records are publicly accessible and may be an indication of your level of wealth or income. SSNs are often accessed directly under the guise of official business and are the most valuable to thieves.

What Law Enforcement is Doing to Help. A million complaints about ill gotten credit and goods in 2001 have *not* forced corporations and credit card companies to crack down.

The Identity Theft and Assumption Act of 1998 made identity theft a crime but the Act has no *preventative* measures. The Social Security Number Confidentiality Act of 2000 prevents the use of SSN on mailed checks while the Internet False Identification Act of the same year prevents the sale of "novelty" SSN cards. Currently both Acts are being updated to restrict SSN use for records-keeping purposes only.

Four Things You Can Do to Prevent Identity Theft From Affecting YOU.

• Consider purchasing a personal shredder and shred *everything* that may contain SSN, banking or credit information before discarding it;

• Don't give out your SSN unless you *know* the person/company you're offering it to;

• Consider the use of a post office box, which is more secure than receiving your mail at home; and

• Periodically review your credit reports and bank statements to detect unauthorized purchases or accounts.

What to Do IF You Become a Victim of Identity Theft.

• Report fraud to the Social Security Administration and the Federal Trade Commission (FTC). Also file a police report;

• Request a fraud alert through the credit reporting agencies for each of your credit accounts;

• Review your check writing history with a check recovery agency; and

• Use the Internet to get help. It is a great resource to get advice on how to recover from identity theft.

COMPUTER SECURITY
TIP OF THE MONTH

COMPUTER SECURITY DAY WILL BE CELEBRATED WORLDWIDE ON NOVEMBER 30TH, 2002. LIKE MANY OTHER FEDERAL AND CIVILIAN AGENCIES, THE FCC WILL OBSERVE COMPUTER SECURITY DAY AS A WEEK LONG CELEBRATION DECEMBER 2ND-6TH. ALL FCC STAFF WILL BE ASKED TO SIGN A "RULES OF BEHAVIOR" FORM WHICH OUTLINES PROPER ETIQUETTE WHILE USING FCC COMPUTERS.

YOU CAN REFERENCE ADDITIONAL INFORMATION ABOUT IDENTITY THEFT AT:

• FTC's Complete Guide to ID Theft: http://www.consumer.gov/idtheft

• Identity Theft Prevention And Survival Website: http://www.identitytheft.org