

Protecting Yourself from Identity Theft and Fraud  
by: Kim Douglas Sherman, Esquire

When your personal identification information, such as your name, social security number, birth date, credit card number, and driver's license number, have been used without your consent or permission to open credit accounts, to open bank accounts, to obtain loans, or to obtain goods or services—you are a victim of identity theft. It can be a devastating experience; the commercials on television do not even touch the feeling of violation. If you are a victim of this crime, your entire financial world can be thrown into turmoil. This article is just a brief summary of how you can protect yourself and what you should do if you find yourself victimized.

As soon as you become aware that you are a victim of identity theft, the Broward County Sheriff's Office recommends that you immediately contact the company or financial institution's fraud department where your information was used to alert them of the fraud and have the account close or canceled. Immediately file a police report where the fraudulent activity occurred; the Broward Sheriff Office will assist you to determine the proper place for making the report. The Federal Trade Commission [(877) 438-4338] investigates interstate and internet fraud. You can download a copy of an identity theft affidavit from the FTC's website at: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) to assist you in notifying merchants, financial institutions and the credit bureaus. Contact the three major credit reporting companies [Equifax (800) 525-6285; Experian (888) 397-3742; TransUnion (800) 680-7289] to report the identity theft and have them confirm that a **Fraud Alert** is placed on your personal credit file. The Fraud Alert will help prevent any future acts of fraud involving your personal identification where a credit check would be conducted with the three major credit bureaus.

The best practice is to protect yourself. Here are some recommendations that are easy and effective. Always promptly review your monthly banking, brokerage, and credit card statements for accuracy—and report any questionable matters immediately. Watch your credit by getting the free annual reports that each of the three major credit agencies will provide to you upon your request. Report any errors you find in the reports immediately and in writing. Keep your guard up, and do not be casual about disclosing your private information. Never disclose your Social Security number, birth date, or mother's maiden name unless you initiated the transaction and unless you know that you are dealing with a reputable merchant or website. Guard your card! Try not to bring any identification of credit cards which are not necessary. When you give out your credit card in a restaurant or business, keep the card in sight to prevent the fraudulent use of handheld readers—a practice called “skimming.” Use firewalls on your home computer as a deterrent to hackers. Use a shredder at home before throwing away papers, like bank statements and credit card bills, that have your personal information on them. Just avoid using strange Automated Teller Machines [ATMs], cell phones, and wireless or public computers for conducting your personal business. The thieves have the means to listen in to such communications.

The “con” in the word “conman” refers to confidence. Be alert and use good common sense in whom you trust and how you conduct your personal business.