

How Identity Theft Can Affect You

By Jordan Buschmohle, iSekurity

Identity theft is the fastest growing crime in the United States, claiming millions of new victims each year. Every three seconds, someone's identity is stolen. Everyone is vulnerable. Identity theft is devastating and can take, on average, 330 hours to reverse the damage done to its victims and cost, on average, \$4,500 per year, per incident.

Although the crime of identity theft has been around for many years, it has only been within the last five years that the reported incidents have grown to a rate deemed a national crisis. The Federal Trade Commission has declared identity theft an epidemic, and predicts that every US resident will be affected by identity theft at least once by year end 2010.

Most people believe that identity theft is simply about credit fraud. Identity theft is actually about a breach of your personal information and the subsequent use of that information to:

- Gain employment
- Open new credit or accounts in your name
- Buy homes or vehicles in your name
- Gain access to your personal banking accounts
- Open utility accounts
- Use your health insurance
- Commit crimes in your name

Identity theft can happen in numerous ways. Some of the most popular means are:

- Dumpster Diving:** Rummaging through trash for bills or other papers with your personal information
- Skimming:** Using a device to illegally capture credit and debit numbers
- Phishing:** Sending email fraudulently presented as coming from financial institutions, that ask for personal information
- Using a Change-of-Address Form:** to divert your billing statements to another location
- Old Fashioned Stealing:** Stealing wallets, purses, mail such as pre-approved credit card offers, tax statements, and personal records.

- **Cyber Crimes/Stealing of Intellectual Property:** Stealing of digital backup data, hacking into corporate servers, stealing laptops and downloading information onto your computer and grabbing sensitive data.

Medical Identity theft has also spiraled out of control, claiming more than half a million victims each year. Unlike traditional identity theft, medical identity theft is very difficult to detect and, if you are a victim, it's much more difficult to repair its damage. Every time a thief uses your medical identity to obtain medical care, records are created with his medical information that could be mistaken for yours—a different blood type, a history of drug or alcohol abuse, test results that aren't yours, or a diagnosis of an illness you don't have. Unlike credit reporting agencies, health care providers are not required to delete or correct incorrect information on your medical records.

Crimes relating to Identity theft have accelerated in 2008, and are expected to worsen in 2009. In addition to traditional methods, criminals are using more sophisticated schemes targeting the unemployed, consumers with poor credit and homeowners facing foreclosure, especially in our troubled economy, according to a report issued by the Identity Theft Resource Center, a national advocacy group of experts based in San Diego, CA.

Once you become a victim, it is your responsibility to pick up the pieces and put your life back together, one step at a time. This process can take years. Statistics from the United States Secret Service show that, on average, once your identity is stolen, it is used up to 30 times. This is due to the simple fact that no one is pursuing the criminal. Yet, the only way to truly stop the identity theft is to attack the problem at its source by investigating the crime and locating the perpetrator. Local, State and Federal government authorities do not have enough resources or manpower to actively combat the crime. Without the proper law enforcement in place or the appropriate amount of resources allocated to fighting it, identity theft will remain the fastest growing crime in America.

What You Can Do

In addition to protecting your personal information carefully, you can also take advantage of two free resources to deter identity theft crime: credit monitoring services and fraud alerts.

- **Monitor your credit** by visiting annualcreditreport.com. (You can also pay a service provider between \$10-\$30/month to monitor your credit for you.) Credit monitoring will not stop identity theft from occurring. It's an after-the-fact notification that you already have a problem.

- **Fraud alerts** were created by the Federal Government and the three major credit bureaus. You can set these up free of charge by visiting one of the three major credit bureau websites. A fraud alert can be helpful in preventing new credit accounts from being opened in your name for: a credit card, car or home loan, line of credit, cell phone or utility account, etc. The system is not foolproof, because it is the merchant's responsibility to follow through on what the alert is intended to do. When attempting to open a new account, the merchant should see the fraud alert and stop the transaction before it takes place. Unfortunately, because this alert is located near the back of your credit report, and the system does not legally obligate the merchant to halt the transaction, fraud alerts do not always work.

Keep in mind that even if credit monitoring or fraud alert systems worked perfectly, they don't prevent all forms of identity theft. They do not stop an individual from using your information to obtain medical procedures, liquidate your savings account, gain employment and subsequently leave you with IRS debt, or commit insurance fraud or other crimes.

iSekurity is a new Oklahoma Pharmacists Association member benefit partner, and a national provider of identity theft protection. The company employs the largest team of former federal agents from the United States Secret Service, FBI, DEA, ATF, IRS, Customs, and Postal Inspector agencies, and is committed to aggressively investigating crimes of identity theft against its members.

For more information on iSekurity, please contact the company at: (877.838.5734) or visit <https://isekurity.com/opha>.