



## The Changing Face of Identity Theft

Identity theft is rampant resulting in millions of dollars of damage each year in the United States. Over the last few years, the face of identity theft has changed. Unfortunately, consumers do not realize this change primarily due to the advertising of credit bureaus, some ID theft service companies and lack of news. ID thieves are the one group that understands the changing faces of identity theft. Yet, what can a person do to prevent ID theft when it is misunderstood and changing?

To understand the problem, you must first realize why thieves want your identity. The answer is simple; they want your credit (money), they want to hide their identity, they want certain services, or they desire employment.

Several years ago, the prevalent type of identity theft was "true name" identity theft. This is when a real person's identifying information is used without modification. The thief actually poses as the victim. According to a study by ID Analytics, this accounts for a small portion of all identity fraud; 10 – 15 percent. In these cases, continuous credit monitoring, fraud alerts and credit freezes play a role in keeping the consumer aware of their credit file status.

However as with any theft, once the thief realizes you have caught onto them, they change, modify their actions and come after you wearing a different face. A face harder to detect which credit monitoring, fraud alerts and credit freezes do not readily provide you with protection. These include non-credit theft such as, medical identity theft, criminal identity theft and the fastest growing and hardest to detect synthetic identity theft.

Medical identity theft is when a thief uses a consumer's personal identifying information to acquire medical services. This is non-credit identity theft. This can become a serious health risk since it places erroneous medical information in the consumer's medical records. Based on medical privacy laws, erroneous medical records are more difficult to clean up compared to credit records. Credit monitoring, fraud alerts nor credit freezes will inform you or stop medical identity theft.

Criminal identity theft occurs when certain credentials are presented to law enforcement the results could be criminal record or arrest warrants. This is non-credit identity theft. The consumer may never know until they are stopped for a driving violation and realize there is an arrest warrant in their name. Credit monitoring, fraud alerts nor credit freezes will inform you or stop criminal identity theft.

Synthetic identity theft is the fastest growing type of ID fraud and its occurrences have surpassed "true-name" identity fraud. The ID Analytics study states it currently accounts for 80 -85 percent of all identity fraud.

This is when thieves combine real and fake information to create a brand new and different identity. For example; they use your Social Security number and combine it with a different name, address and phone number. They can then open new accounts, acquires credit cards, cell phones and other goods and services not in your name but because of your social security number.

A problem is that synthetic ID theft creates a fragmented or sub-file to your main credit file. A fragmented file refers to additional credit report information tied to your Social Security number, but someone else's name and address. Negative information entered in the fragmented file that is then linked to you, but doesn't actually belong to you. If you have good credit but there is derogatory information is in the fragmented file, it could negatively impact your ability to get credit. Since this type of ID Theft does not effect your main credit file; it often doesn't hit your credit report nor will a fraud alert or credit freeze help. This means it takes longer to find out you've been victimized, making it harder for you to clear your name. When they run up 1000s of dollars of debt and disappear, the creditors will eventually back track to you.

What we know about criminals that use ID Theft as a way of life is that they will go through certain steps to create a false identity. With just your social security number, they can create brand new identity, an identity that will not be stopped by a fraud alert but will show up in national databases. It is these national databases that hold the key for early detection for possible identity theft. Scanning national databases such as; credit bureau, criminal records, DMV data, public records, large data aggregators (such as Choicepoint), large credit

companies, non-credit loan companies, several large insurance companies that also makes available limited access to medical information for your social security number in conjunction with your other personal identifying information, such as your name, address or date of birth can reveal misuse of your social security number which is signal for possible ID Theft.

The point to remember is that with Synthetic ID Theft is that since it is not your name, address, phone number or credit file.... credit monitoring, fraud alerts or credit freezes will not inform you or stop synthetic ID theft.

In June 2007, a man in Arizona with a fraud alert on his credit file became an ID theft victim. Since then, scanning of the national databases has revealed misuse of his personal identifying information in over 30 cases where his social security number was being used under different names and addresses. A Florida man used the Arizona man's social security number, with the name Gaylord Focker, a different address, date of birth and phone number and received a credit card with a \$9,000.00 limit.

In 2007, a nurse whose personal identifying information became at risk due to the hospital's data breach realized 6 months later that there were 5 convicted sex offenders on the east coast using her social security number. In December 2007, we received two phone calls where each individual had been contacted by a cell phone service, that their social security number was already being used by another cell phone consumer.

Identity theft continues to be a major problem facing citizens of all ages, races and economic status. There is no silver bullet or magic potion that will stop identity theft, early detection by scanning national databases with IDAlert from Identity Theft America.



Lanny Britnell  
'Certified Identity Theft Risk Management Specialist'  
[www.IdentityTheftAmerica.com](http://www.IdentityTheftAmerica.com)  
Phone 334-270-9156  
Cell 334-391-3890  
Email [info@identitytheftamerica.com](mailto:info@identitytheftamerica.com)