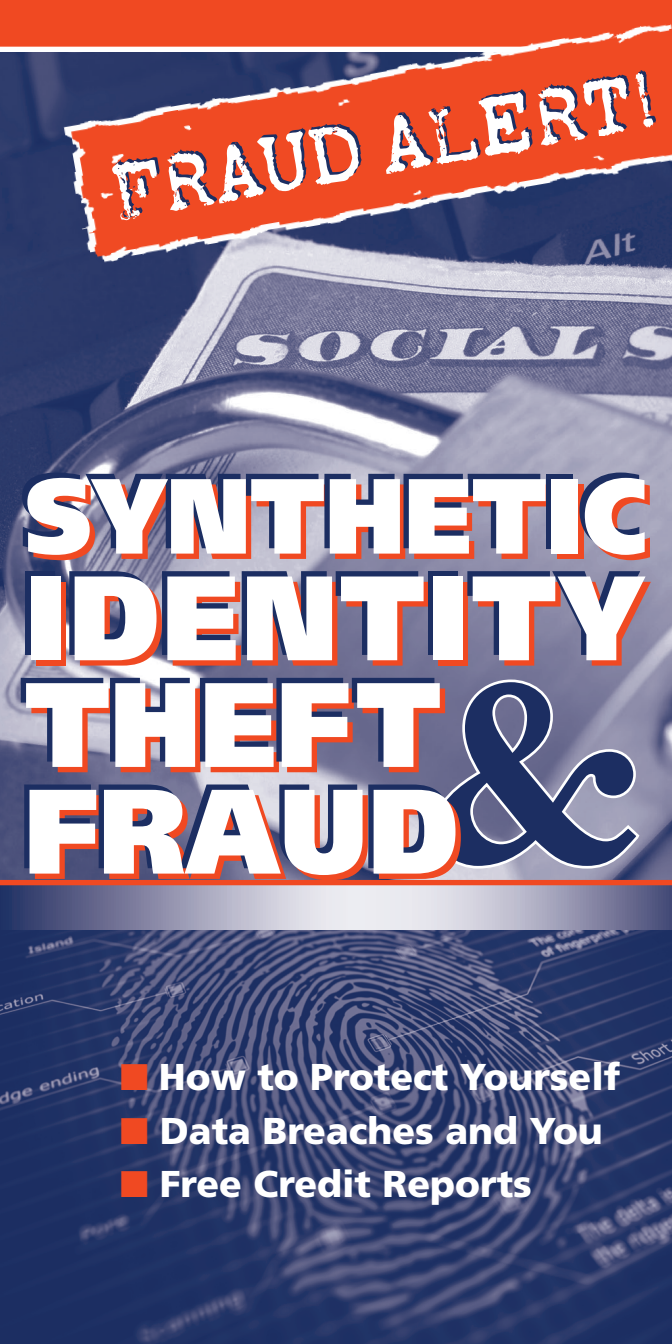
FRAUD ALERT!
SOCIAL S
SYNTHETIC IDENTITY THEFT & FRAUD
How to Protect Yourself
Data Breaches and You
Free Credit Reports

SYNTHETIC IDENTITY THEFT and FRAUD

It is hardly news that identity thieves and cyber-criminals have become more patient, devious and sophisticated. But did you know that they can now ruin your personal credit and even hijack your financial accounts simply by pretending to be someone *similar* to you?

It's called Synthetic Identity Fraud and is now **the fastest-growing type of ID fraud** in the U.S., surpassing "true-name" identity fraud.

Synthetic Identity Theft Is Different From Traditional Identity Theft

Criminals create a synthetic identity by using a combination of fake and real personal information including names, Social Security Numbers, driver's licenses and employee identification numbers to open new accounts or hijack existing accounts. The real personal information that is an integral part of the data used for synthetic identity theft and fraud is most often obtained from one of the many data breaches occurring with increasing frequency. This illegal activity involves millions of records from retail businesses, companies and institutions that have been "hacked" by cyber criminals.

In traditional "true-name" identity theft an individual's actual information is stolen and the criminal pretends to be that individual.

Data Breaches, A Major Impact

Often a news report of a cyber criminal's successful theft of personal information through a hacked data base is ignored or met with a kind of "what's new" attitude. The level of sophistication and patience demonstrated by this new breed of identity thief is astounding and should

cause increased vigilance to your financial accounts. Here are some examples of how personal data is used to build an identity and commit identity fraud.

➜ TRUE-NAME ID THEFT AND FRAUD

A sophisticated criminal enterprise will acquire some aspect of an individual's personal information from one data breach source of stolen information — perhaps a real social security number. The real social security number might then be linked or merged with the same person's real credit and debit card information stolen from a different data breach source. After verification and cross-reference of the data, the criminal can then call the financial institution and use the stolen personal information to impersonate that individual and request that the PIN on an actual card account be changed, produce a duplicate card, go to an ATM and withdraw cash.

➜ SYNTHETIC ID THEFT AND FRAUD

A patient criminal will alter some aspect of a person's real information — not changing the stolen social security number but changing some aspects of the individual's real identity and keeping some real identifiers, such as a name, address, birth date, etc. The criminal will apply for credit cards and maybe cell phone service using the synthetic identity, pay the bills on time and eventually build enough credit to obtain larger loans that will never be paid back.

Although some of the stolen personal information has been changed, a credit reporting agency might not recognize this synthetic identity as fraud because the criminal is patient in building good credit and worse yet—the victim's main credit file will not be affected by the fraud because much of the information is intentionally different. It often won't impact your credit report until a significant amount of debt has been incurred and the criminal is long gone.

As a result, victims often don't learn their identities have been synthesized until they receive unpaid bills, collection notices, or overdue tax bills, or until they notice unusual postal mail patterns.

Children Are Especially Vulnerable

Of particular concern to experts and others is how synthetic identity theft targets children's social security numbers. These real assigned social security numbers tend to stay inactive for long periods and will generally remain unchecked for many years. Unless something unusual happens and the child begins receiving credit card offers in the mail, or the child is denied a driver's license or college loan, the identity fraud may not be discovered.

FREE CREDIT REPORTS YOUR BEST TOOL

When it comes to guarding against cyber-fraud, one of the most important tools at your disposal is your credit report. It details all of your credit transaction accounts, and will be the first place that unusual charges or entirely new accounts will appear. And you can monitor your report for FREE.

Since Federal law permits consumers to a free credit report annually from each of the three major credit reporting agencies, cyber-security experts advise you to get a free report from a different agency every four months. Doing so will allow you to monitor your personal online security all year long.

TO ORDER YOUR FREE CREDIT REPORT, GO TO THE ONLY AUTHORIZED SOURCE:
www.annualcreditreport.com
1-877-322-8228

The true impact of undetected child identity theft is only fully realized when the victimized youngster starts applying for college aid or has difficulty getting their first job after high school because negative financial information pops up on the background screening reports.

Vigilance Is The Answer To Fighting This Growing Threat

1. **Monitoring your bank, credit card and debit card statements is critical.** After all, if an unauthorized transaction appears on your statement, and you do not spot it, you unknowingly end up paying the charges.

2. **Regularly check your credit reports.** Pay close attention to all the detail in transactions using only your Social Security number and report any activity that was unauthorized to the Credit Reporting agencies and the FBI. Your credit score can also indicate a problem, so check those too.

3. **If you suspect a problem, call the Credit Reporting agencies** and place a Fraud Alert or Credit Freeze on your accounts.

4. **Check your annual Social Security statement** that lists your earnings record, work credits and an estimate of future benefits. Double check that your reported income figure is accurate and not above what you actually earned.

5. **Pay attention to reports of data breaches and the hacked companies** that may have gathered a part of your personal information, such as your driver's license number or home address.

6. **Notify your financial institution** if you suspect any sort of unusual activity within your accounts.

Understanding Your Liability

Government regulations and voluntary industry policies will protect you if a credit or debit card is used to make unauthorized purchases. Your card issuer can provide specific details.

- **Credit cards.** Under federal law, if someone steals your credit card you are responsible for the first $50 of unauthorized charges. Some cards carry zero-liability policies. If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use.
- **Debit cards.** Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss. Your liability can range from $50 to as much as $500 (see www.ftc.gov for a full explanation).

Resources

Federal Trade Commission: http://www.ftc.gov
U.S. Treasury Department: http://www.treasury.gov
AnnualCreditReports.com:
http://www.annualcreditreport.com