Synthetic Identity Fraud Talking Points

November 1, 2007

Background

Many people are familiar with the concept of "**new account fraud**" in which an imposter opens lines of credit using personal information of another; this could include utilities, credit card accounts, mortgages, etc. This type of fraud poses an immediate problem for victims because these new accounts will appear on the victims' credit history, making it more difficult for them to obtain new credit such as mortgages and even sometimes impacting their ability to get a new job. Luckily, consumers have long had easy access to immediate alerts when this fraud has occurred through credit monitoring services such as Privacy Guard and others. Credit monitoring can serve as an early warning mechanism for new account fraud, enabling victims to take quick action to dispute the accounts and restore their good name.

Fewer consumers are aware of an important variation of new account fraud that is called "**synthetic identity theft**" in which an imposter creates a new identity using some information from a victim but altering it in such a way that causes the credit agencies to create "subfiles" for the new accounts. This means the new accounts won't appear on the victim's credit report, making synthetic identity fraud much harder to detect.

Synthetic identity theft is often undetectable because of the way credit bureaus store data and release it to consumers. Credit reports ordered by consumers don't reveal all credit history entries connected to a Social Security number. Only entries that exactly match a consumer's name, Social Security number and other personal information appear on these reports. Accounts that are opened using the consumer's number but a different name are often omitted, according to the bureaus.

So, the original information holders will never know about the new accounts until bill collectors come looking for them.

How can this fraud happen?

In the rush to issue a new account, errors can be made (and the credit granting system expects that errors will be made), and fraudsters have learned how they can scam the system. There are two main ways that fraudsters are scamming the system to create synthetic identities:

1) Using a victim's real social security number, but a different name that is not actually attached to that social security number
2) Obtaining a victim's name and social security number, but manipulating the information on their account application slightly (such as misspelling the victim's name slightly and/or transposing some of the digits in the Social Security number)

In either case, the fraudster will likely do this several times without the victim becoming aware it is happening. So, in synthetic identity theft, the bad guy doesn't merely create a new account in your name only, the bad guy establishes multiple new personalities. This means it takes longer for you to find out you've been victimized, making it harder for you to clear your name once you do find out.

Why is this a problem for consumers?

Accounts used by identity thieves eventually become delinquent. A few industry insiders argue that synthetic identity fraud mainly hurts creditors since the creditors will get hit with a loss from

the delinquent accounts. However, synthetic identity fraud can and does affect consumers in two important and very devastating ways:

1) **Debt collectors can come after innocent consumers.** Collection agencies have the ability to perform "social searches" on Social Security numbers to find current addresses for delinquent debtors. A Social search will also turn up names associated with that Social Security number, which means the innocent consumers whose original Social Security numbers and identities were modified to create synthetic identities will hear from debt collectors. Then, it will be up to the victim to prove that these accounts and debts are fraudulent. This process is very time consuming and potentially more difficult to dispute than new account fraud that is caught early on, especially since the debt collection industry often pursues debtors very aggressively.
2) **Subfiles can turn up in certain types of credit checks, which means that the derogatory information from these fraudulent accounts can impact a victim's ability to obtain a mortgage or other loan.** Banks, auto dealers and other lenders have special relationships with the credit bureaus that allows them to run a full background report on a Social Security number, called a "Social Search", to turn up all the accounts that are linked to that Social Security number. Consumers cannot run this type of report not even on their own Social Security number. When there's more than one name attached to a Social Security number at the credit bureaus, some call the extra files "sub-files." Consumers cannot see sub-files but creditors can.

What can consumers do?

1) Monitor your Social Security number. Experts agree that credit monitoring doesn't help to detect synthetic identity fraud. Credit monitoring won't catch instances where the fraudster uses a different name, date of birth or address along with the consumer's real Social Security number.

Checking annual Social Security earnings reports for mistakes is a good idea – particularly if you are not getting credit for your earnings. **But misuse of your Social Security number another person will not appear on this report**, **because only wages reported using the correct name and number are credited to your account**. Believe it or not, there are literally millions of millions of workers who pay taxes using the wrong Social Security number every year. Much of this comes from illegal immigrants looking to get work, a phenomenon that some people are calling "immigrant identity theft". If your Social Security number is used illegally to gain employment you could end up owing taxes on wages you didn't earn, have a lien placed on your assets if federal income taxes are not paid, and much more.

2) Enroll in an identity monitoring service. Be sure to select a program that will search public records for evidence of variations in your name and Social Security number AND evidence that you number has become associated with different names. Consumers should still continue to monitor their credit reports periodically, but no one should feel completely safe if that is all that they do to protect themselves and their financial identity. An excellent service that provides this type of monitoring and notification is called ID Secure which will monitor billions of account records and alert you when it spots potentially suspicious use of your name and Social Security number. Plus, ID Secure's specialized resolution service can help you to understand the magnitude of the fraud that has occurred and advise you of the steps you can take to restore your good name.

Given the patchwork nature of a synthetic identity, it can take years to unravel the tangled mess of this type of crime. If victims ever actually discover the crime, clearing one's name can be much more complicated than it would have been in the case of true-name identity theft, so consumers need to do all that they can to protect themselves.