



THE MANY FACETS OF IDENTITY THEFT

By Sheyna Steiner

Synthetic ID theft refers to fraud perpetrated with a fabricated identity. Mike Cook, co-founder and chief operating officer of ID Analytics, a company that analyzes fraud risks to businesses, coined the term. Synthetic ID theft is thought to be one of the most prevalent forms of identity theft and is difficult for business to detect and recognize.

Synthetic ID theft

What is it?

"Synthetic ID theft is when a fraudster just creates an identity and that identity gets through the traditional data checks that are done for fraud," says Mike Cook, co-founder and chief operating officer of ID Analytics. "They are able to acquire goods and services in a name that isn't real and is manufactured and doesn't really exist."

The identity may be completely fabricated or it might use parts of an existing identity pasted together with fictitious elements. "They can use any parts of an identity that is available to them," says Cook.

One of the key ingredients is a realistic Social Security number. "It has to be in a valid range and it needs to go with a date of birth that corresponds with that Social Security number," Cook says.

The identifying numbers are released in batches at various points throughout the year. The middle two numbers of the Social Security number represent the group to which that particular batch was issued.

One way that thieves formulate their bogus Social Security numbers is by tumbling a valid one.

"If I were going to do it, I would take my Social, and let's say it ends with 9831. I would change it to 9832, 9833, 9834, 9835 and continue on that way and create 1,000 identities as long as they are all the same age," says Cook.

How to prevent

In general, businesses, more than consumers, suffer from synthetic identity theft.

Nonetheless, individuals can experience some harm if part of their identity is used to commit fraud. By taking the same steps used to protect themselves from other categories of identity theft, consumers can somewhat protect themselves from synthetic ID theft. But nothing is foolproof.

"By following those steps, you're trying to mitigate the risk," says Evan Hendricks, editor of Privacy Times and author of "Credit Scores and Credit Reports."

Unfortunately, more often than not, the situation is out of the hands of consumers. There's nothing you can really do, says Mike Cook, co-founder and chief operating officer of ID Analytics.

How to recognize

Experts disagree on the impact financial fraud using partial identifiers can have on a victim's credit file. For instance, if a criminal uses your Social Security number to get financing for \$10,000 worth of furniture at the local home store but doesn't use your name or address with it, the transaction may not make it to your credit file.

According to Evan Hendricks, author of "Credit Scores and Credit Reports," and editor of Privacy Times, credit reporting agencies often create subfiles for Social Security numbers in cases of fraud.

A consumer can only find out about them after applying and getting denied for credit because the credit report sold to subscribers could include the fraudulent information associated with the Social Security number.

Then, if you ask for your own report, the erroneous information won't show up, says Hendricks.

"There's a very precise matching to make sure that they only give you your information, but when they sell a credit report they use a looser algorithm, so more information is included," he says.

"This whole thing of having two separate files, one you sell and one you give to the consumer, is not supposed to happen," Hendricks says. "But it does and affected consumers are forced to sue under the Fair Credit Reporting Act to find out the truth."

Mike Cook, co-founder and chief operating officer of ID Analytics, says synthetic ID theft shouldn't affect your credit at all due to the way credit reporting agencies pull together information and display it.

"I've seen it reported before that synthetic fraud does affect consumers in that way, but it really doesn't. I've worked in the credit bureau system for 20 years. The information won't be added to the file. There might be a fraud indicator added to your file that says someone else might be using your Social, but it won't affect your credit," says Cook. "It might have someone stop you in the credit process and ask questions."

Even your address can be commandeered for fraud.

"Fraudsters can look in the phone book and get your last name and then go to an actual physical location and try to get credit or finance something that they would buy from a retail lender or get a wireless cell," says Cook. "Say Mike Cook lives at the certain address that they have; they will say that their name is John Cook at that address."

If the perpetrator is declined credit, the declination letter will be mailed to your address.

"If that happens, they (the victim) should contact the company that sent the letter and they should also contact the Identity Theft Resource Center and they'll be able to explain to them what happened," says Cook.

How to recover

Because there is no injured party reporting the crime in most cases, the statistics on its prevalence vary.

"It's hard to understand. We've done analysis in the past, and we know that in some industries synthetic ID fraud happens at a higher rate than others," says Mike Cook, co-founder and chief operating officer of ID Analytics. "For instance, we know in wireless industries that synthetic fraudsters tend to attack wireless accounts more often than a large bank."

The reason for that is the verification effort, he says.

"Synthetic fraudsters try to attack places they can get through the verification process a little faster," says Cook.

ID Analytics works with businesses to manage identity risk and weed out fake identities. When businesses are better able to authenticate the identities of their customers, the risk to industry and individuals decreases.