Synthetic Identity Theft: The Silent Swindler

Peter Silva, 2010-03-12

As a brief follow up to yesterday's Got a SSN I Can Borrow, I came across this story from The Red Tape Chronicles saying the odds that someone else has used your Social Security Number is One in 7. ID Analytics, a data collection and customer behavior analytics firm, works with organizations, including the US Social Security Administration, to detect Identity-Based fraud; separating the true customers from the impostors. They've analyzed 290 million Social Security numbers and found that 40 million of those numbers have been connected to more than one name; basically, 40 million of us are sharing identities with someone else. They also indicated that 6% of the total population, or 20 million Americans, have multiple SSNs associated with their name. Often, it might just be an incorrect entry or typo into a system, but it can also be when criminals apply for credit at multiple banks changing 1 digit with each application – around 20% are deliberate misrepresentations. When the system propagates either the error or intentional entry, that second SSN is forever associated with the individual and thus Synthetic. Synthetic Identities are created when an unassigned number gets attached to someone and a new entity is created within the credit system. Some people have 4-5 SSNs connected to their name and 5 million SSNs are connected to three or more people.

Synthetic Identity Theft is typically when a criminal uses either totally fake or a mixture of fake and real information to create a new identity. Usually, a fraudster will use a real SSN with a fake or different name that is associated with that number. Synthetic Identity Theft is difficult to track, detect and report since individuals are usually not aware it is occurring since it doesn't appear on a credit report and because a combination of names, addresses, SSNs and so forth are used, it is usually does not match up with a single, individual consumer to claim fraud. Most go unreported and become 'charge-offs' within the financial institution well before anyone is aware of the problem.

Protect yourself by shredding mail and sensitive documents since thieves will dig through trash to find pieces of information they can use; review your Social Security benefits booklet every year to check if the income reported is actually what you made; and stay on top of your credit, reporting any discrepancies. The free AnnualCreditReport.com is the official site to help consumers to obtain their free credit report each year. I tend to grab all three at once since I subscribe to a credit monitoring service, but if you don't – stagger each of three reporting agencies reports throughout the year to see any changes since the last credit file disclosure. If necessary, you can also put a Security Freeze on your credit report. Finally, don't give out your Social Security number if you don't have to – if someone asks, like a doctor's office, just respectfully decline. I have never had a problem telling someone that I prefer not to give out that sensitive information. Heck, you could probably even say you've been a victim of Synthetic Identity Theft.

ps

twitter: @psilvas

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113