



*Issued 3/11/18*

## **Newest ID Scam Creates Fake People**

Synthetic identity fraud creates, in effect, a new person by selecting the right social security number (SSN). This is a new twist to identity fraud, which typically uses an existing person's identity to apply for credit or government benefits. A new kind of identity fraud creates phony identities out of fake people and the U.S. government is expressing concern that this could become a go-to scheme for terrorists and organized crime.

The most common plan here is to randomly choose a SSN that wasn't issued prior to 2011, when the [Social Security Administration] changed the rules on how SSNs were issued. By choosing a number from this range, they can have reasonable confidence that there won't already be a history of another person using that SSN. Unfortunately, many sites on the internet provide guidance on how to do this.

While the schemes vary and the steps to establish a synthetic ID are different, very basically it can go something like this: the bad guy applies for a line of credit at a financial institution. While this can be rejected, the resulting credit inquiry generates a credit profile for the synthetic ID in the credit bureaus' databases. Once the synthetic ID is established via the generated credit profile (or credit file), the criminal gain applies for credit, gets credit established, and then applies for multiple credit cards. The criminal in the final "bust out" stage waits until the credit score is high enough to yield a large payout, then charges the maximum on the

card, as spelled out in a report from the Government Accountability Office (GAO). The key to a large payoff is patience. Patient fraudsters will try and mimic the patterns of young people or new immigrants – accepting poor credit offers at first and paying them off, to build up their credit score – with the ultimate goal of accessing big credit lines and charging off for large financial gain. Since the scammers are using the SSN of a young child, they can use the number for several years before anyone looks at the credit report to notice this activity.

While individuals are the most common offenders, large-scale schemes are also used by bad guys to fund organized crime and terrorism, according to the GAO report. The problem is, terrorists – or any kind of organized crime – can potentially use synthetic identities to enter and move around the U.S. undetected, the GAO said. “We’ve seen synthetic identity fraud rings which have seemingly obvious associations to organized crime – so that is a significant issue,” ID Analytics’ King said.