GAO Highlights

Highlights of GAO-17-708SP, a report to Congress

July 2017

HIGHLIGHTS OF A FORUM

Combating Synthetic Identity Fraud

Why GAO Convened this Forum

According to experts, SIF has grown significantly in the last five years and has resulted in losses exceeding hundreds of millions of dollars to the financial industry in 2016. A key component of synthetic identities is SSNs—the principal identifier in the credit reporting system. There are many questions about SIF; the threat it poses to the financial system, government programs, and national security; and the most effective partners and methods for combating SIF.

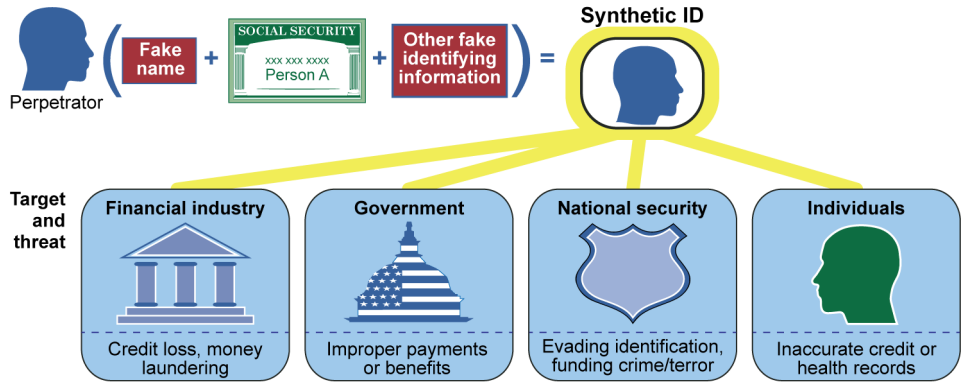
GAO convened and moderated a diverse panel of 14 experts on February 15, 2017 to discuss: how criminals create synthetic identities; the magnitude of the fraud; and issues related to preventing and detecting SIF and prosecuting criminals. With assistance from National Academy of Science, GAO selected panelists (private sector and government) based on their publications, referrals from other experts, and their specific skills and knowledge of SIF. The viewpoints in the report do not necessarily represent the views of all participants, their organizations, or GAO. GAO provided participants the opportunity to review a summary of the forum and incorporated their comments as appropriate.

View GAO-17-708SP. For more information, contact Lawrance Evans at (202) 512-8678 or evansl@gao.gov

What Forum Panelists Said

Synthetic identity fraud (SIF) is a crime in which perpetrators combine real and/or fictitious information, such as Social Security numbers (SSN) and names, to create identities with which they may defraud financial institutions, government agencies, or individuals. As of July 2017, the magnitude of SIF was unknown but panelists agreed that this type of fraud has widespread ramifications. For example, one panelist noted that banks can lose an estimated $50-$250 million in a year from SIF-related unpaid debt. Government agencies may face losses, too. For example, one panelist said that a state paid an estimated $200 million in fraudulent SIF-related unemployment insurance claims. Panelists also described instances where SIF criminals funded terrorism through money laundering.

Threats Posed by Synthetic Identity Fraud



Source: GAO. | GAO-17-708SP

Panelists identified a number of challenges that public and private institutions face when combating SIF and identified options to address some of the challenges.

- **Prevention:** Financial institution's interpretations of privacy laws limit information sharing with each other and law enforcement about fraudulent activity. Additional regulatory guidance clarity could improve information sharing.
- **Detection:** Private and public institutions tend to use traditional fraud detection methods (e.g., victim self-reporting) to identify SIF. With SIF, there may not be a victim to report a crime. Advanced data analytics that detect, for example linkages between seemingly unconnected bank accounts (e.g., data mining that identifies different accounts with the same customer phone number) could be more effective at detecting SIF than traditional methods.
- **Prosecution:** The Social Security Administration (SSA) prioritizes its resources on fraud cases related to SSA benefits over outside requests for SSN verification which can slow law enforcement's efforts.