Combating Synthetic Identity Fraud

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

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.