United States Government Accountability Office

HIGHLIGHTS OF A FORUM

Combating Synthetic Identity Fraud

Accessible Version

GAO-17-708SP

July 2017

GAO Highlights

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

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.

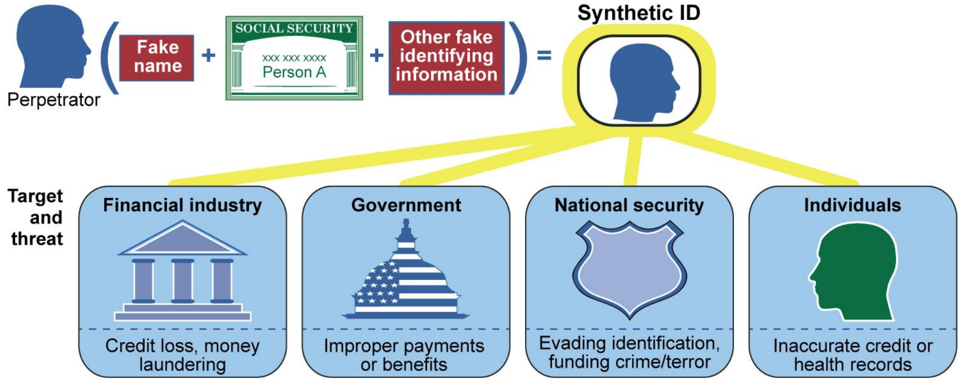
GAO convened and moderated a diverse panel of 14 experts on February 15, 2017 to discuss: how criminals create synthetic identities; the magnitude of the fraud; and issues related to preventing and detecting SIF and prosecuting criminals. With assistance from National Academy of Science, GAO selected 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


Perpetrator
Fake name
+
SOCIAL SECURITY
xxx xxx xxxx
Person A
+
Other fake identifying information
=
Synthetic ID
Target and threat
Financial industry
Credit loss, money laundering
Government
Improper payments or benefits
National security
Evading identification, funding crime/terror
Individuals
Inaccurate credit or health records

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.

Contents

Table

Figures

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

Introduction

Synthetic identity fraud (SIF) is a crime in which perpetrators generally combine real and/or fictitious identifying information, such as Social Security numbers (SSN) and names, to create new identities with which they defraud financial institutions, government agencies, or individuals. As such, the resulting identity and credit profile is not associated with a real person. In contrast, traditional identity fraud is a crime in which perpetrators obtain personally identifiable information belonging to an individual and assume that individual's identity to commit fraud. Criminals and other fraudsters rely in large part on the credit reporting system to create and use these synthetic identities. According to experts we interviewed as the financial industry has developed tools to combat traditional identity fraud, criminals have increasingly turned to SIF. These experts agreed that financial institutions and government agencies have been affected by SIF. However, 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.

To advance the national dialogue on combating SIF, we convened and moderated a diverse panel of 14 experts from government, law enforcement, credit bureaus, data brokers, financial institutions, and academia on February 15, 2017.[1] With assistance from the National Academy of Sciences, we identified prospective panelists with a variety of perspectives. We selected panelists based on their publications, referrals from other experts, and their specific skills and knowledge of SIF.[2] We also conducted a literature review and interviewed experts who have researched and written about SIF or are involved in combating SIF. (See app. I for a list of forum participants and their affiliations; app. II for a copy

[1] Credit bureaus are companies that collect and sell information about the credit history of individuals and businesses, and include Experian, Equifax, and Transunion. Data brokers are companies with a primary line of business of collecting, aggregating, and selling personal information to third parties. A data broker is different from a credit bureau in that a data broker does not focus on consumer trade lines but instead collects other individual information from public records such as date of death and real estate purchases.

[2] We invited officials from the Social Security Administration (SSA) to participate, but they were unable to attend. However, we held separate discussions with SSA officials that helped to inform this report.

of the forum agenda; and app. III for details on our objectives, scope, and methodology.)

This report summarizes the discussion by forum participants, highlighting their answers to key questions we asked during the forum. The questions related to how criminals create synthetic identities; the magnitude of the fraud; and issues related to preventing and detecting SIF and prosecuting criminals. This report concludes the first in a series of planned GAO engagements on SIF.

The information and viewpoints summarized here do not necessarily represent the views of all participants or the views of their organizations or GAO. We did not independently assess the accuracy of the statements expressed by participants. We structured the forum so that participants could openly comment on the issues discussed, and not all participants commented on all the discussion topics. To ensure the accuracy of our summary, we provided participants the opportunity to review a summary of key points from the forum and incorporated their comments, as appropriate, prior to publishing this report.

We conducted our work from July 2016 to July 2017 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for the findings and conclusions in this report.

This report is available at no charge on the GAO website at http://www.gao.gov. If you or your staff have any questions about this report, please contact Lawrance Evans at (202) 512-8678 or evansl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

I want to thank again all of the forum participants for their time and their thoughtful contributions to the forum discussion. The range of perspectives we heard enhanced our understanding of SIF, how criminals create synthetic identities, the magnitude of SIF, challenges related to combating such fraud, and potential steps the nation can take to address this important issue. GAO will continue to undertake additional work in this area in the future.

Lawrance L Evans, Jr.

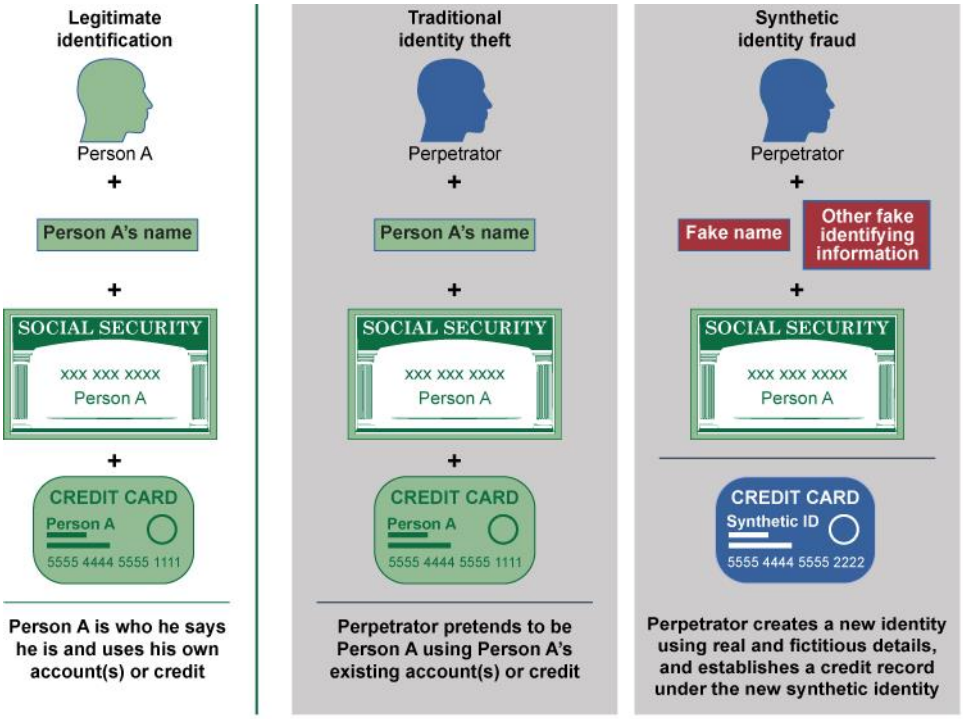
Lawrance L. Evans, Jr.
Director, Financial Markets and Community Investment

Background

Traditional Identity Fraud Compared to Synthetic Identity Fraud

In traditional identity fraud, criminals may, for example, use a person’s credit card information to make unauthorized charges or use another person’s established identity to apply for credit or government benefits for which he or she would not be eligible, such as Social Security benefits. In SIF, criminals do not take over existing identities; instead, they create new identities (see fig. 1). Based on discussions with experts and articles we reviewed, for the purposes of this report, we defined SIF as the combination of real or fake information, such as a SSN, with nonmatching personal information, such as a name or date of birth, for the purposes of creating a new identity with intent to defraud or evade government or private-sector entity safeguards. While synthetic identities are fabricated, an individual can face negative ramifications if the perpetrator uses his or her real SSN (as illustrated below).

Figure 1: Traditional Identity Fraud versus Synthetic Identity Fraud


Legitimate identification
Person A
+
Person A's name
+
SOCIAL SECURITY
XXX XXX XXXX
Person A
+
CREDIT CARD
Person A
5555 4444 5555 1111
Person A is who he says he is and uses his own account(s) or credit
Traditional identity theft
Perpetrator
+
Person A's name
+
SOCIAL SECURITY
XXX XXX XXXX
Person A
+
CREDIT CARD
Person A
5555 4444 5555 1111
Perpetrator pretends to be Person A using Person A's existing account(s) or credit
Synthetic identity fraud
Perpetrator
+
Fake name
Other fake identifying information
+
SOCIAL SECURITY
XXX XXX XXXX
Person A
CREDIT CARD
Synthetic ID
5555 4444 5555 2222
Perpetrator creates a new identity using real and fictitious details, and establishes a credit record under the new synthetic identity

Source: GAO. | GAO-17-708SP

Panelists generally agreed with this definition and cited three general categories of SIF: (1) fraud for nefarious activities, (2) fraud for living, and (3) fraud for credit repair.

- Fraud for nefarious activities is the category that results in most of the financial losses and poses the greatest threat to the financial system, government programs, and national security, according to panelists and our research. Fraud for nefarious activities refers to a deliberate, organized, and sometimes large-scale scheme to liquidate credit accounts, launder money, or fraudulently obtain government benefits. According to panelists, criminals use these large-scale schemes to fund organized crime, terrorism, and other illicit activities.
- Another category is fraud for living, in which an individual assumes a created identity to live or work in the United States. The perpetrator who commits fraud for living may be someone who is in the United

States as an undocumented immigrant and seeks, for example, work authorization or utility accounts.[3]

- The third category is fraud for credit repair, in which an individual creates a false identity using a stolen or fake SSN combined with his or her real name to build an alternate credit history.

According to panelists, some criminals have shifted to SIF as financial institutions improved how they prevent and detect traditional identity fraud. For example, financial institutions now use data analytics (that is, qualitative and quantitative techniques and processes) to detect and stop transactions that are not consistent with customers' typical purchasing patterns. In addition, in October 2015, major credit card companies began to use Europay, MasterCard and Visa or "chipped" cards. Chipped cards are more difficult to counterfeit than traditional credit cards because they are encrypted.

Federal Agencies' Roles in Identity Fraud Investigations

Financial institutions and government agencies that administer benefits programs may contact various federal agencies to investigate suspected identity fraud. The jurisdiction of these federal agencies varies depending on the type of fraud. For example, the United States Postal Inspection Service has jurisdiction over crimes that involve the use of U.S. Mail (that is, mail fraud). Mail fraud relates to identity fraud in instances where, for example, criminals fraudulently obtain credit cards from financial institutions via the mail. Table 1 details selected federal agencies that investigate traditional identity fraud and SIF and their jurisdictions.

Table 1: Select Federal Agencies and Their Role in Investigating and Prosecuting Identity Fraud

Agency	Role
Offices of the United States Attorneys	• Prosecutes a broad range of complex white collar crimes, including fraud and violations of the Bank Secrecy Act and the Foreign Corrupt Practices Act. • Works closely with law enforcement agents in specialized areas such as health care fraud and cybercrimes.

[3] One expert told us that a parent may use the SSN of their child to, for example, open a utility account.

Agency	Role
Federal Bureau of Investigation	• Investigates criminal activities such as public-sector corruption, identity theft, money laundering, corporate fraud, securities and commodities fraud, mortgage fraud, financial institution fraud, bank fraud and embezzlement, fraud against the government, election law violations, mass marketing fraud, and health care fraud. • Generally focuses on investigations with a nexus to organized crime activities that are international, national, or regional in scope.
United States Secret Service	• Investigates and analyzes information in support of financial analysis, infrastructure protection, and criminal investigations. • Safeguards nationwide payment and financial systems by, for example, fighting against counterfeiting, financial fraud, and forged identity documents, and combating transnational organized crime and technology-based threats that target the citizens and financial institutions of the United States.
United States Postal Inspection Service	• Investigates all allegations of fraud within the Postal Service's programs and operations, including identity theft and mail fraud, as well as allegations that become national or multi-jurisdictional. • Investigates any crime in which the U.S. Mail is used to further a scheme—whether the crime originated via mail, telephone, or Internet; use of U.S. Mail in furtherance of the scheme constitutes mail fraud.
Federal Trade Commission	• Hosts a database that identity-theft victims use to self-report complaints. • Supports law enforcement by, for example, providing sample indictments, programmed data searches, and access to key databases.
Inspectors General	• Investigates the administration of federal programs and operations to prevent and detect fraud and abuse. • Investigations can include criminal, civil, and administrative matters; and are based on information received from a variety of sources, including Office of Inspector General's fraud, waste and abuse hotline; federal agencies program offices, GAO, and Department of Justice referrals; congressional requests, and referrals from the Office of Special Counsel regarding whistleblower disclosures.

Source: GAO. | GAO-17-708SP

Social Security Administration's Role in Social Security Number Verification

The Social Security Administration (SSA) began issuing nine-digit SSN in 1936 to track workers' earnings and to pay future benefits. The SSN used to be composed a three-digit geographic number, a two-digit age group number, and a four-digit serial number. The agency maintained a list of all SSN geographic and group numbers issued, which could be used to determine if a social security number had actually been issued. In 2011, SSA began randomizing SSNs, in part, in response to concerns that criminals could reconstruct SSNs from public information such as records of births and property records. According to experts with whom we spoke, under the original SSN-assignment system, financial institutions and others generally could determine if the place and date of birth that customers provided in credit applications matched the three-digit geographic and two-digit age group numbers of their SSN. With random numbers, financial institutions cannot pair the SSN with credit applicants' place and date of birth to help verify applicants' identities. Further, financial institutions cannot verify if the SSN is valid since SSA no longer publishes a list of all SSN geographic and group numbers ever issued.

SSA verifies SSNs under certain circumstances. For financial institutions, SSA will verify SSNs as part of a mortgage application or credit check, for example. SSA requires customers to provide a form (SSA-89) that authorizes the agency to verify the customer's SSN for the financial institution. The financial institution first provides the SSA-89 form to the customer for signature (often through the mail), waits for the customer to return the signed form, and then submits the form to SSA. In addition, law enforcement may contact SSA for SSN verification as part of investigations of identity fraud. A panelist said that, from his perspective, SSA recently centralized the process and requires require law enforcement to contact SSA headquarters for certain SSN verification requests. Previously, according to panelists, law enforcement could informally contact the local SSA field office and obtain the information more quickly.

According to SSA officials, the agency has formal agreements to share information with some federal government agencies to help them administer their programs, such as determining program participant eligibility. SSA may share information with agencies that administer certain benefit programs. For example, SSA has sharing agreements with the Department of Veterans Affairs, Department of Labor, Department of Education, Centers for Medicaid and Medicare Services, and the Internal Revenue Service (IRS). SSA may also provide information to other agencies, but SSA officials told us they first consider SSA resources and priorities before responding to ad-hoc requests.

How do perpetrators create synthetic identities?

Perpetrators combine stolen or fake Social Security numbers with fabricated identifying information.

A typical process to create and build a synthetic identity involves the steps below (see fig. 2):[4]

Step 1: Perpetrators make up or obtain a real SSN and add non-matching identifying information such as name, date of birth, and address to create a synthetic identity. According to panelists, SIF perpetrators prefer to steal randomized SSNs, those issued since 2011, which cannot be verified. Panelists also said hackers, for example, often breach public or private databases that contain personally identifiable information and sell stolen SSNs over the Internet.[5]

Step 2: Perpetrators use the synthetic identity to apply for a line of credit, typically at a bank. The bank submits an inquiry to credit bureaus about the applicant's credit history. The credit bureaus initially report that an associated profile does not exist and the bank may reject the application; however, the credit inquiry generates a credit profile for the synthetic identity in the credit bureaus' databases.

Step 3: According to our interviewees and panelists, once the synthetic identity is established via the credit profile, the perpetrator again applies for and ultimately receives credit. At this stage, the perpetrator will typically apply for multiple credit cards and other products marketed to consumers who are new to credit.

[4] Steps may vary somewhat when commiting fraud for living or credit repair. For example, with fraud for living the perpetrator may use the Social Security number of his or her own child and thus not need to acquire one. Moreover, in fraud for credit repair, often there is no planned "bust-out" in step 5, and instead the accounts may or may not remain in good standing based on the perpetrator's personal financial situation.

[5] A SIF criminal may also combine their real name with a Credit Protection Number (CPN) or Credit Privacy Number. These numbers are fictitious Social Security numbers (SSN) that are used to facilitate credit transactions. In the case of credit repair, panelists told us that a person who uses a CPN may not realize that he is commiting synthetic identity fraud. For example, an Internet site we reviewed falsely claimed that using a CPN rather than a SSN is legal. Panelists informed us that this process is illegal because providing a number other than one's SSN when asked on a credit application is a false statement and is considered fraud.

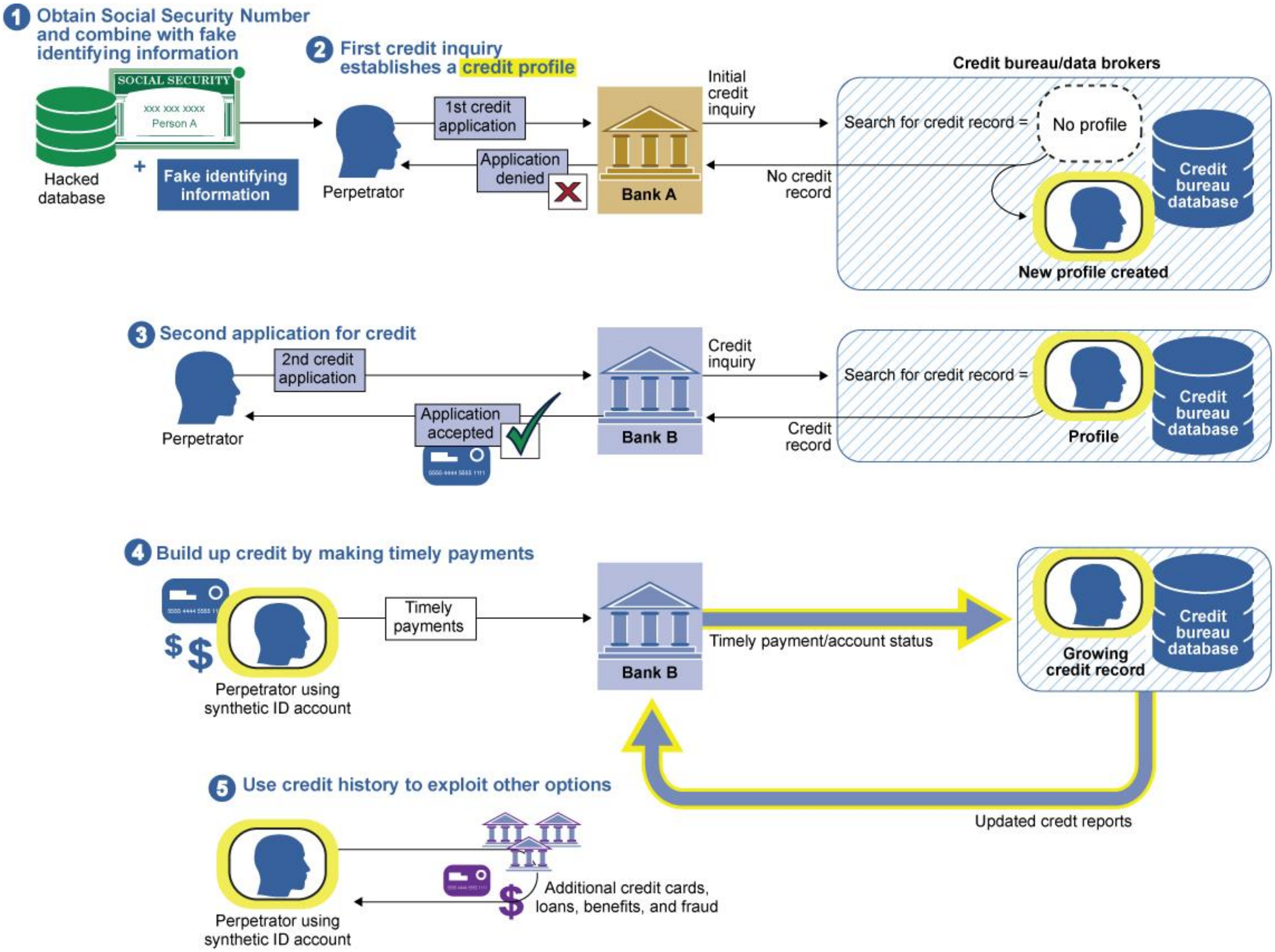
Step 4: SIF perpetrators maintain good credit over time to build up credit limits and apply for more cards. They also exploit credit bureau procedures to improve their credit history by getting legitimate credit users to act as accomplices and add synthetic identities as “authorized users” on accounts in good standing. Criminals may also build credit history by adding the synthetic identities as “authorized users” to other credit accounts they have obtained using different synthetic identities.

Step 5: Eventually SIF perpetrators exploit financial institutions by, for example, charging the maximum amount on credit cards and not paying the bill. This stage of the fraud is known as the “bust-out.”[6] Perpetrators may also launder the money between multiple accounts. They may also use the synthetic identities to fraudulently obtain government benefits or illegally obtain work.[7]

[6] This type of fraud, in which the fraudster established a positive repayment history and maxed-out the line of credit before defaulting, is sometimes referred to as bust-out fraud.

[7] According to an expert, some government agencies may use credit bureaus and data brokers to verify certain identity information for participants in government programs. We did not identify the specific agencies that use information from credit bureaus or data brokers during this engagement.

Figure 2: Typical Process to Create a Synthetic Identity


1 Obtain Social Security Number and combine with fake identifying information
SOCIAL SECURITY
XXX XXX XXXX
Person A
Hacked database
+
Fake identifying information
2 First credit inquiry establishes a credit profile
Perpetrator
1st credit application
Application denied
Bank A
Initial credit inquiry
No credit record
Credit bureau/data brokers
Search for credit record =
No profile
Credit bureau database
New profile created
3 Second application for credit
2nd credit application
Application accepted
Perpetrator
Bank B
Credit inquiry
Credit record
Search for credit record =
Profile
Credit bureau database
4 Build up credit by making timely payments
Timely payments
Perpetrator using synthetic ID account
Bank B
Timely payment/account status
Growing credit record
Credit bureau database
Updated credt reports
5 Use credit history to exploit other options
Perpetrator using synthetic ID account
Additional credit cards, loans, benefits, and fraud

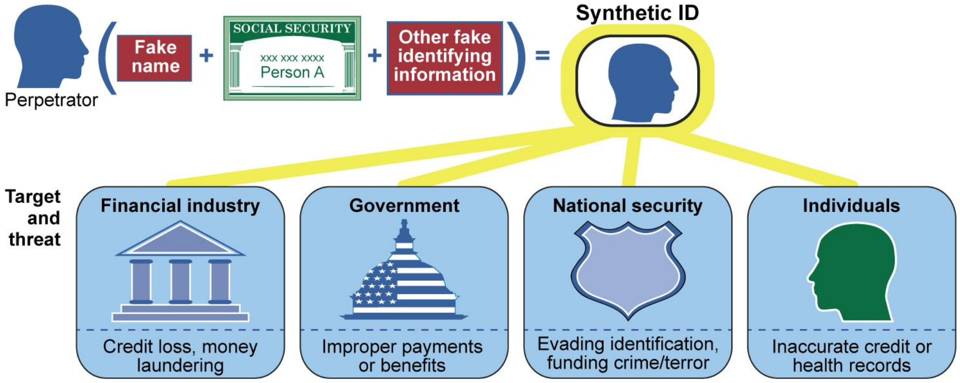
● According to CG Forum panelists, financial institutions do not routinely verify Social Security numbers (SSN) with the Social Security Administration (SSA) when new customers apply for credit. While financial institutions have the option of verifying a customer's SSN directly with SSA, the current SSA verification system requires the financial institution to obtain an executed Form SSA-89 signed and returned by the applicant. Panelists stated that the process could take up to a week and that the financial industry considers that wait too long for a credit decision; the industry has a business interest in making the process efficient and expeditious for the customer. Panelists noted that financial institutions may use this method when they suspect fraud or for loans that have greater underwriting requirements to gain assurance of the customer's identity.

Source: GAO. | GAO-17-708SP

What threats does SIF pose to the private sector, government, national security, and individuals?

The magnitude of the threat that SIF poses is unknown, but panelists shared their views about potential threats. As shown in figure 3, SIF poses threats to the financial industry, government, national security, and individuals. Each of these is discussed in greater detail below.

Figure 3: Threats Posed by Synthetic Identity Fraud


Perpetrator
Fake name
SOCIAL SECURITY
xxx xxx xxxx
Person A
Other fake identifying information
Synthetic ID
Target and threat
Financial industry
Credit loss, money laundering
Government
Improper payments or benefits
National security
Evading identification, funding crime/terror
Individuals
Inaccurate credit or health records

Source: GAO. | GAO-17-708SP

Financial Industry Financial Losses

Although the full extent of losses to the financial industry is unknown, the threats posed by SIF may be significant, according to our panelists. Panelists said it is difficult to estimate losses related to SIF because SIF-related losses often look like a typical credit loss (that is, a loss made by a financial institution on its lending activities). For example, when a customer commits a bust-out, a bank may initially view it as a customer who can no longer pay his bills on time and will ultimately charge-off the debt (that is, stop trying to collect the delinquent account, typically after 180 days, with the option to sell the account to a debt collector who continues to try to collect the debt). While the full extent of financial losses due to SIF cannot be determined, some panelists were able to offer estimates of the financial sector’s losses. For example, one panelist estimated, based on his experience, that many financial institutions likely experience $50 million to $250 million in financial losses each year due to SIF. Another panelist estimated 10-15 percent year-over-year growth in

SIF from 2011 through 2016, with approximately $1 billion in credit card losses across all financial institutions in 2016.

As described above, SIF against the private sector typically results in bust-outs and/or money laundering.[8] One panelist described a bust-out scheme in 2013 that involved a syndicate of 19 perpetrators managing 7,000 identities and more than 25,000 credit cards with losses that exceeded $200 million. Synthetic identities may also be used in money laundering schemes where accounts are established with synthetic identities to hide the illicit source of funds.

Benefits Fraud against the Government

According to panelists, the government's total exposure to SIF is unknown; however, based on their experience, many panelists described how synthetic identities could and had been used to commit fraud against the government and likely cause significant losses. Panelists said that any program that relies on paying a benefit when a claim is made and then performing enforcement afterwards may be vulnerable to SIF. According to panelists, the following programs are among those potentially vulnerable to SIF: Medicare, Medicaid, Unemployment Insurance, and Supplemental Nutrition Assistance Program (SNAP) (formerly known as the Federal Food Stamp Program). For example, Medicare and Medicaid providers may use synthetic identities to create false patient records and bill for supplies never used or services never performed or establish fully synthetic offices and conduct both of these activities. One panelist noted that his organization had detected $200 million in improper Unemployment Insurance payments due to SIF in one state.[9] Another panelist discussed recently discovered SNAP-related fraud, which involved criminals using synthetic identities to systematically apply for and receive improper SNAP benefits. They also stated that state tax refunds are susceptible to SIF as well. A panelist noted that his investigation prevented $500 million dollars in improper state tax refunds directly related to SIF since 2012. Panelists also said that local, state, and federal government agencies may not be able to recover the losses because the perpetrators are unknown.

[8] Money laundering is generally the process of converting proceeds derived from illicit activities into funds and assets in the financial system that appear to have come from legitimate sources. See 18 U.S.C. § 1956.

[9] Improper payments can include, but are not limited to, fraudulent claims. In this instance, the improper payments are due to fraudulent claims.

National Security Threats

The use of synthetic identities against national security programs is less well-known and understood; however, panelists expressed concerns about potential threats to the nation's security. The panelists did not provide any details about national security programs that were compromised due to SIF, but they expressed concern with national security programs that rely on verifying a purported identity against a list of suspected bad actors or terrorists. They noted that terrorists, and any other type of criminal, may use synthetic identities to enter or move around the United States undetected. Panelists noted that SIF criminals have used synthetic identities to obtain state-issued identity documents necessary to acquire passports. Panelists also noted that SIF has been used to finance terrorists over long periods of time without being detected by law enforcement. Synthetic identities obscure the actual perpetrators. (Panelists spoke generally about cases related to SIF and terrorist financing and did not provide any detailed information.)

Challenges for Individuals

Panelists stated that when criminals use stolen SSNs, they typically steal them from individuals who are less likely to use their credit actively, and these victims may face difficulties obtaining credit or other related problems in the future. According to panelist and the literature we reviewed, perpetrators target children's SSNs because criminals can commit SIF for long periods of time until the individual begins to apply for credit.[10] Further, children born after 2011 have randomized SSNs, which are preferred by SIF criminals because financial institutions are no longer able to independently determine whether the SSN is valid. According to panelists, this can cause problems for victims when they begin to use their SSNs because the first user of a SSN is generally assumed by financial institutions to be the "owner of that SSN." As such, the victim may face difficulties in establishing credit and proving that he or she is the true owner of the SSN. Other vulnerable populations include the elderly, people who do not have bank or credit accounts, and homeless.

Further, panelists said that victims whose SSNs are stolen for SIF may face potential health risks if their health records are connected to

[10] The Federal Trade Commission publishes information on protecting a child's identity information. This can be found at: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

someone else. Panelists said that the healthcare industry is increasingly relying on SSNs as unique identifiers for patients. Consequently, if a patient's identity is linked with a SIF perpetrator's medical information, the patient may be placed in a life-threatening situation. The panelists did not provide any examples of cases where SIF victims encountered this type of challenge, but they noted that the implications of SIF on the healthcare industry are emerging concerns.[11]

How do private- and public-sector entities prevent and detect synthetic identity fraud?

Private- and public-sector entities employ mechanisms or controls to prevent and detect traditional identity fraud, but these efforts may be ineffective for detecting SIF. These mechanisms and controls used by financial institutions, data brokers, credit bureaus, and government agencies are discussed in greater detail below.

Financial Institutions

Panelists noted that methods used by financial institutions often are designed to prevent traditional identity fraud and may miss SIF. Specifically, panelists and other experts we interviewed stated that when a customer makes an application for credit, financial institutions typically rely on third parties, such as credit bureaus and data brokers, to verify the purported identity information during their assessment of the applicant's credit history. In addition, financial institutions may rely on the information provided by third parties to develop knowledge-based questions to confirm identities (e.g., mother's maiden name). However, this process is vulnerable because criminals insert fictitious identity information into credit bureau and data broker databases to create synthetic identities and can therefore use that information to respond accurately to authenticating questions. While financial institutions have the option of verifying a customer's SSN directly with SSA, the current SSA verification system requires the financial institution to obtain an executed Form SSA-89 signed and returned by the applicant. Panelists stated that the process could take up to a week and that the financial industry considers that wait

[11] We discussed this issue in the context of traditional identity theft. See GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud,* GAO-17-254 (Washington, D.C.: Mar. 30, 2017).

too long for a credit decision; the industry has a business interest in making the process efficient and expeditious for the customer. As such, panelists did not believe the Form SSA-89 process reflected current business processes and that revision to this process may make verifying identity information more efficient. Panelists noted that financial institutions may use this method when they suspect fraud or for loans that have greater underwriting requirements to gain assurance of the customer's identity.

According to panelists, after an applicant is approved for credit, financial institutions continue to rely on data analytics or information provided by third parties to detect identity fraud. Data analytics typically focused on suspicious activity, such as accounts with large transactions, transactions made in geographic areas deemed high-risk, and patterns of insufficient payments or bounced checks. Financial institutions often also look for rapid changes in customer behavior, which is consistent with traditional identity fraud. However, SIF is typically a much slower process and often the institution may not realize an account is fraudulent until after the bust-out or other fraud has already occurred, if at all. Panelists indicated that the use of advanced data analytics, such as data mining that flags seemingly unconnected accounts based on the same customer phone number, for example, could be more effective at detecting SIF accounts.

Credit Bureaus and Data Brokers

Panelists indicated that credit bureaus and data brokers employ data analytics to identify potential identity fraud; however, panelists stated that credit bureaus and data brokers do not proactively share this information with financial institutions because of legal and other challenges. Credit bureaus and data brokers employ data analytics that enable them to, for example, flag individuals with limited collaborating information such as utility accounts or other account history. They can identify active accounts associated either with the SSN of a deceased person or with multiple names. Credit bureaus and data brokers can also identify seemingly unconnected active accounts that share some of the same customer information (for example, customer phone number or address).

Panelists said that credit bureaus and data brokers were often positioned to have the best information overall on possible SIF because they have data from a cross-section of accounts and financial institutions. In addition, credit bureaus and data brokers can often trace identities back to an original source. However, because credit bureaus and data brokers may not be able to state definitively that the person is using a synthetic identity, only that he or she might be, they face concerns, such as reputational risk, about incorrectly flagging an account as fraudulent and reporting that information to financial institutions. In addition, according to panelists, credit bureaus and data brokers are concerned that they may violate Fair Credit Reporting Act (FCRA) rules if they proactively notify financial institutions about individuals they suspect may be using a synthetic identity.[12] Panelists indicated that clearer guidance on FCRA and other related laws and regulations concerning the extent to which private sector entities could share information to combat SIF could help to facilitate more effective collaboration.

Government Agencies

Panelists told us that federal agencies' internal investigators (e.g., Office of Inspectors General) do not specifically look for SIF and agencies often do not view themselves as vulnerable. According to SSA officials and panelists, some federal agencies try to prevent identity fraud by verifying program participants' SSNs, often through agreements with SSA.[13] For example, SSA provides information to officials that administer worker's compensation and income-maintenance programs (e.g., Temporary Assistance for Needy Families program). SSA also provides information to IRS, for example, so that IRS can verify the SSN of individuals who submit tax returns.

For agencies that do not have an agreement with SSA, panelists said the agencies likely use controls that are designed to detect traditional identity fraud and not specifically designed to detect SIF. These tools rely on victim self-reporting (that is, an individual whose identity has been stolen will report the crime to the authorities). With SIF, however, the fraud can run for long periods of time before a person realizes his or her SSN has

[12] The Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x), promotes the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies, which may be used to determine individuals' eligibility for such products as credit or for insurance or employment. The act also allows individuals to access and dispute the accuracy of personal data held on them. The FCRA sets rules for access and reporting of credit information and provides for fines in cases where these rules are violated. Additionally, as amended in 2003, FCRA imposes safeguarding requirements designed to prevent identity theft and assist identity theft victims.

[13] SSA may coordinate with and provide SSNs to a wide cross-section of federal agencies, including agencies that administer benefit programs and law enforcement. See 20 C.F.R. pt. 401, subpt. C.

been compromised, or it might not involve a real person's identity leaving, no one to report SIF, which undermines the victim-reporting control. We have previously created a framework for managing fraud risks in federal programs.[14] This framework calls for federal agencies to commit to combating fraud, assessing their risks to fraud, and then designing and implementing controls aimed at preventing fraud. The panelists could not speak in any detail on all federal agencies' implementation of the framework, so it is not clear to what extent federal agencies in total have been using it to assess their exposure to SIF. Panelists did not discuss the extent to which agencies apply the risk framework to assess their risk of exposure to SIF. This is an area that we plan to follow up on, as discussed below.

How do private- and public-sector entities investigate and prosecute synthetic identity fraud and what are the associated challenges?

Private- and public-sector entities provide information to law enforcement for further investigation; however, gathering timely evidence and obtaining convictions is challenging. These processes and associated challenges are discussed in greater detail below.

Financial Institutions, Credit Bureaus and Data Brokers, and Government

Panelists indicated that when private-sector entities and government agencies suspect identity fraud, they will often conduct their own internal investigations before referring the case to law enforcement. Once a financial institution identifies a potential SIF account using data analytics tools, an internal investigator will examine the case and attempt to determine whether or not the account is likely to be fraudulent or a credit loss. Like financial institutions, credit bureaus and data brokers conduct their own investigations when they identify or are contacted by a financial institution, for example, about fraudulent transactions or accounts. (While panelists acknowledged that government agencies conduct some type of internal investigations, they were not aware of specific activities agencies perform.) If internal investigators at private-sector entities and

[14] GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015).

government agencies determine that accounts are likely fraudulent, panelists told us that the investigators will alert law enforcement agencies and provide them with account and transactional records, photographs, and audio and/or video recordings.

Financial institutions, similar to credit bureaus, tend not to share results of their internal investigations with each other or the credit bureaus or data brokers, which can limit the effectiveness of their internal investigations and the evidence they provide to law enforcement. Under the Financial Crimes Enforcement Network's regulations, in instances of suspected money laundering or terrorist financing, financial institutions may share certain information about customers that would otherwise be prohibited under privacy regulations.[15] However, panelists told us that they do not believe financial institutions have interpreted the regulations as applicable to SIF.

Panelists also told us that financial institutions are willing to accept a certain amount of credit and fraud loss as a cost of doing business. They also stated that, based on their experience, financial institutions would rather accept additional risk than target resources to their internal investigative departments.

Law Enforcement

According to the panelists, law enforcement conducts identity fraud investigations and any subsequent prosecutions usually after they receive referrals from private and public sector entities, but they face challenges obtaining needed information. During identity fraud investigations, law enforcement collects additional information from private or public entities and coordinates with SSA to verify SSNs. According to one panelist, investigating SIF cases is difficult because perpetrators go to great lengths to hide themselves. When law enforcement is able to identify video footage or other evidence, one panelist said that they face significant challenges in obtaining cooperation from merchants to provide the needed information in a timely way for successful prosecutions of criminals. For example, as reported by panelists, a department store may require a subpoena before store representatives provide video footage,

[15] These provisions create a safe harbor from liability that allows financial institutions to share information for certain permissible purposes (that is, when money laundering or terrorist activity is suspected). See 31 C.F.R. § 1010.540.

and by the time law enforcement obtains the subpoena, the video has been automatically erased.

Panelists also stated that law enforcement investigators have faced more difficulties in obtaining assistance from SSA in recent years. During investigations, law enforcement often contacts SSA to verify SSNs. According to panelists and our discussions with SSA officials, SSA is now primarily focused on traditional fraud related to SSA benefits such as false claims for disability benefits.[16] As such, panelists noted that the assistance SSA provides to law enforcement has become more difficult to obtain and is more time-consuming in recent years. For example, one panelist from law enforcement stated that it took 4 months for SSA to verify a list of 2,400 SSNs. According to the panelist, previously he could contact his local SSA field office and provide SSA field staff with a spreadsheet of numbers to be verified, a process that typically was completed in 1 day. However, now it appears that SSA has centralized its verification process for law enforcement and now requires investigators to make formal requests through headquarters, which has introduced delays.

According to panelists, SIF perpetrators have little disincentive to commit these crimes because of typical limited penalties and possible limited interest by prosecutors to indict alleged perpetrators. Law enforcement told us that the associated penalties for committing SIF are often relatively light. According to one panelist, a judge has discretion to impose the sentence he or she believes is sufficient but not greater than necessary under the sentencing guidelines and typical sentences for SIF have been probation or 1 year imprisonment.[17] According to the same panelist, prosecutors have attempted to increase sentences by trying to obtain a conviction for aggravated identity theft, which adds a two-year mandatory minimum sentence.[18] According to the panelist, with aggravated identity theft, however, the prosecution must prove that the SIF criminal knew, for example, that the stolen SSN belonged to a real

[16] SSA's Inspector General's Office (OIG) began shifting resources to comply with the Social Security Benefit Protection and Opportunity Enhancement Act of 2015, which mandated that SSA expand efforts to combat disability fraud. See Bipartisan Budget Act of 2015, Pub. L. No. 114-74, tit. VIII, § 811, 129 Stat. 584, 601 (codified at 42 U.S.C. § 421).

[17] Some criminals' sentences are more severe. In 2016, a New York man was convicted of committing bust-outs with a synthetic identity and was sentenced to 80 months and fined $25,000.

[18] See 18 U.S.C. § 1028A(a).

person. This can be difficult with SIF because often the criminal will either make up a SSN or use a SSN he purchased via the Internet. As such, the criminals likely know little about the person whose SSN was stolen. A panelist said that they believed the light sentences associated with SIF encourage criminals to commit this type of crime. Panelists indicated that changing the law to remove the requirement that the defendant knew that the identity belonged to a real person could make it easier to obtain conviction for aggravated identity theft in SIF cases and could increase the punishments for those convicted of SIF.

What is needed to help public and private institutions combat SIF?

Panelists raised a number of challenges associated with SIF including inefficiencies associated with SSA's SSN verification process, limited information sharing by the private sector, ineffective SIF detection methods used by the private sector and government agencies, and weak penalties for committing SIF. Panelist also proposed potential actions to help address these challenges that are discussed below.

Inefficient SSN Verification Process

Panelists said SSA's response to requests for identity verification is too slow, and the process to make a request is inefficient. To address this challenge, panelists proposed that SSA review its policies and procedures to determine the extent to which the agency needs to shift how it responds and accepts inquiries by law enforcement, other government agencies, and private-sector entities. Panelists noted that greater collaboration with public and private entities could help combat SIF as SSA is ultimately the best source of information on SSNs.

Limited Private Sector Information Sharing

Panelists said financial institutions' application of regulations may hinder private sector entities from sharing information to combat SIF. To address this challenge, panelists believed that greater information sharing would make it easier to prevent and detect synthetic identities. Panelists indicated that clearer guidance on FCRA and other related laws and regulations could help to facilitate more effective collaboration among private-sector entities and help prevent, detect, and aid the prosecution of SIF.

Ineffective Private-Sector and Government-Agency Detection Methods

Current detection tools and internal controls are not designed to detect and prevent SIF. To address this challenge, panelists suggested that advanced data analytics and biometrics are among existing and emerging technologies that could be useful in combating SIF. Advanced data analytics involve a variety of techniques to identify patterns or exposure to SIF. Biometrics is another tool panelists identified to address SIF. Biometrics is automated recognition of individuals based on their biological and behavioral characteristics. For example, one biometric approach discussed by a panelist involved a computer program that electronically compared pictures provided by an applicant to pictures on the person's passport as a method of verifying identity. Biometrics may have limited effectiveness if financial institutions rely on biometric information provided by perpetrators. There may also be privacy concerns raised related to the use of biometrics. Implementing GAO's framework for managing fraud risks in federal programs could also help federal agencies combat SIF. This framework could enable federal agencies to develop controls that help prevent and assess their risks to various types of fraud, including SIF.

Weak Penalties for Committing SIF

Penalties for SIF are not sufficient to deter SIF criminals. To address this challenge, panelists suggested that the penalties for SIF could be increased. They suggested changing the law to remove the required element that the defendant knew that the identity belonged to a real person, which would make it easier to obtain conviction for aggravated identity theft in SIF cases, and would increase the punishments for those convicted of SIF.

Appendix I: Panelists from the Comptroller General Forum on Synthetic Identity Fraud

Panelist	Relevant Experience
Damon Asper, Internal Revenue Service	Identity theft prevention, data modeling, and analytics.
Duen Horng (Polo) Chau, Georgia Institute of Technology	Machine-learning techniques (that is, an artificial intelligence that allows computers to handle new situations via analysis, self-training, observation, and experience with minimal direction by humans) and human-computer interaction to address challenges with large data analytics.
Lee Cookman, TransUnion	Fraud analytics and monitoring tools related to synthetic identity fraud.
Robert Delaney, Discover Bank	Investigation of synthetic identity fraud case and other financial crimes.
Tamera Fine, United States Department of Justice	Prosecution of synthetic identity fraud.
Ben Johnson, Ten Eleven Ventures	Industry solutions (that is, companies that financial institutions hire to resolve issues related to fraud, for example) experience related to addressing security technology issues.
Ken Meiser, ID Analytics	Fraud mitigation, compliance, and authentication services related to synthetic identity fraud.
John O’Neil, IBM Corporation	Big data and analytics to combat money laundering, synthetic identity fraud, and other fraud-related issues.
Marian Oster, LexisNexis	Experience working with federal agencies on data-related issues.
Robby Perry, Chase Bank	Investigation of synthetic identity fraud case and other financial crimes.
Marco Piovesan, InfoMart	Risk mitigation concerning identity verification and due diligence.
Scott Robbins, United States Postal Inspection Service	Investigation and assisting in the prosecution of synthetic identity fraud cases.
Scott Straub, LexisNexis	Data-related solutions for governments concerning fraud, waste, and abuse prevention including synthetic identity fraud.
Amy Walraven, Turnkey Risk Solutions	Detection of synthetic identity fraud and credit bust-out.[a]

Source: GAO. | GAO-17-708SP

[a] Bust-out fraud occurs after the SIF criminal establishes a solid repayment history and maxes out the line of credit before defaulting.

Appendix II: Comptroller General Forum Agenda

Comptroller General's Forum on Synthetic Identity Fraud

February 15, 2017, 8:30am-4:30pm
National Academies, Room 105
500 5th Street NW Washington, DC 20001

AGENDA

Facilitator: Pamela Davidson

8:30-9:00am	**Opening Remarks by GAO**
	Lawrance L. Evans, Jr., Financial Markets and Community Investment Director, GAO • Describe goals for the session • Define synthetic identity fraud • Set ground rules for discussions
9:00-9:30am	**Opening Remarks by Panelists**
	Provide one to two minutes per panelist to discuss backgrounds related to synthetic identity fraud.
9:30-12:30pm	**Panel I: Causes and Prevention of Synthetic Identity Fraud**
	• What information do perpetrators often rely on to commit synthetic identity fraud? • To what extent do perpetrators use the following to commit synthetic identity fraud: • Operational or internal processes used by private and public sector entities in their operations (e.g., sharing identity information) or • Regulatory processes, compliance with various laws and regulations (e.g., statutes related to privacy protections)? • What steps could be taken, and by whom, to prevent synthetic identity fraud? *Break at facilitator's discretion*
12:30-1:30pm	**Lunch** (Keck Cafeteria; 3rd Floor)
1:30-4:30pm	**Panel II: Detection and Consequences of Synthetic Identity Fraud**
	• How is synthetic identity fraud typically detected? • What are the consequences and magnitude of synthetic identity fraud related to: • Private industry, • Federal programs, • National security, or • Other potential areas. • What steps could be taken, and by whom, to make improvements in the detection of synthetic identify fraud? *Break at facilitator's discretion*

Working Definition of Synthetic Identity Fraud: For the purposes of this forum, we define Synthetic Identity Fraud as the combination of real information (e.g., a legitimate Social Security number) with fictitious information (e.g., fictitious name, date of birth) for the purposes of creating a new identity with intent to defraud or evade government or private-sector entity safeguards.

Appendix III: Objectives, Scope, and Methodology

To advance the national dialogue on combating synthetic identity fraud (SIF), we convened and moderated a diverse panel of 14 experts from government, law enforcement, credit bureaus, data brokers, financial institutions, and academia. This report examines key topics related to how criminals create synthetic identities; the magnitude of the fraud; and issues related to preventing and detecting SIF, and prosecuting SIF criminals.

To define SIF, understand how it is committed and combated, determine the extent of the fraud and related implications, and to identify potential panelists for the forum, we conducted a literature review and interviewed a non-generalizable sample of knowledgeable stakeholders. We conducted a literature search based on key terms (for example, identity theft, identity verification, SIF). We searched various relevant databases, such as PR Newswire, Business Wire, and American Banker. We also asked knowledgeable stakeholders to recommend additional authors, articles, and studies. From these sources, we identified 38 relevant studies that appeared in academic journals and newspapers between February 2005 and December 2016. We chose this time period because according to knowledgeable stakeholders the prevalence of SIF has been greatest in that time period. To conduct interviews with a non-generalizable sample of knowledgeable stakeholders, we used the “snow-ball approach.” We chose the “snow-ball” approach to identify additional experts not found in our initial literature review. This approach began with referrals from subject matter experts at GAO to identify potentially knowledgeable stakeholders. During our interviews with these knowledgeable stakeholders we then asked them to recommend other people who they felt were experts about issues related to SIF. We then interviewed those people and asked for additional referrals. We continued with that approach until we identified a list of potential experts.

To determine which experts to invite to our forum, we assessed the experience of 56 people that included 20 from the relevant studies we identified, 14 from referrals we obtained during interviews with knowledgeable stakeholders, and 10 identified by the National Academy of Sciences (NAS) based on requirements we outlined in our contract with the academy. We ranked each knowledgeable stakeholder based on their publication history, participation or presentations at SIF-related conferences, and if they were referred to us by other knowledgeable stakeholders. To ensure we had an expert panel that represented a range of key stakeholders involved in addressing SIF, we selected panelists based on whether they represented government, credit bureaus, data brokers, financial institutions, law enforcement, legal professionals, and academics. For each key stakeholder group, we started at the top of the ranking list and reviewed each knowledgeable stakeholders to assess the extent to which they could substantively address each of our researchable objectives. Based on our selection criteria and process and in consultation with NAS, we identified 18 experts to invite to be on the panel. Four of the 18 experts that we invited declined our invitation. The 4 that declined included 1 official from a credit bureau, 1 from an industry solutions provider, and 2 from the Social Security Administration (SSA), who were not available on the day of the forum. To ensure that we obtained and included SSA's perspective on the issues discussed during the forum, we met with SSA officials and obtained their responses to questions relevant to this report. That information has been included, as appropriate.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Lawrance L. Evans, Jr., (202) 512-8678 or evansl@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Triana McNeil, Assistant Director; Robert Lowthian, Analyst-in-Charge; Shaundra Patterson; Bethany Benitez; Pamela Davidson; and Tovah Rom. Additional assistance was also provided by Johana Ayers, Daniel Bertoni, Wayne McElrath, Toni Gillich, Kathleen King, Nancy Kingsbury, Diana Maurer, Jonathan Oldmixon, Neil Pinney, Matthew Valenta, Helina Wong, and Carolyn Yocom.

(101041)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548