Testimony by
Jeffrey Brown
Deputy Assistant Inspector General
Office of Audit, Office of the Inspector General
Social Security Administration
to the
United States House of Representatives
Committee on Ways and Means
Subcommittee on Social Security in the Hearing titled
"Social Security Administration's Role in Combatting Identity Fraud"
on May 24, 2023

Good afternoon, Chairman Ferguson, Ranking Member Larson, and members of the Subcommittee on Social Security. I commend you for holding this important hearing today on the Social Security Administration's (SSA) role in combatting identity fraud.

Social Security touches the lives of every American no matter where one is in their life's journey. With very few exceptions, all United States citizens, permanent residents, and temporary or working residents have a Social Security number (SSN). Even non-working residents (citizens and non-citizens) are required to obtain an SSN due to its use by businesses and government entities. Today, about 175 million people work and pay Social Security taxes and nearly 67 million Americans receive a Social Security benefit each month. Most Americans are either receiving a benefit from or contributing to the Social Security system.

Notwithstanding its original narrowly drawn function for use in recording Social Security earnings, the SSN has become a de facto national identifier. The SSN has essentially become the cornerstone of the identity framework. Individuals are often required to use their SSN as identifiers to open bank accounts, apply for loans, apply for unemployment, and for many other routine matters requiring proof of identification.

Unsurprisingly, the expanded use of SSNs as a national identifier has given rise to individuals using other people's SSNs for illegal purposes. Stolen SSNs have been used to obtain benefits and services, establish credit, gain employment, and hide identities to commit other crimes. The SSN has become the lynchpin to identity theft.

Identity theft is one of the fastest-growing crimes in America, affecting millions each year. According to the Federal Trade Commission (FTC), in 2022, individuals reported identity theft more than any other type of complaint. Of those, the FTC received 441,882 reports from people who said their information was misused with an existing credit card or when applying for a new one.

SSN misuse and identity theft has a real impact on the American public. Victims of SSN misuse face significant harm when others obtain benefits in their names: victims may be unable to rightfully receive critical benefits or be left to deal with the ramifications of damaged credit and other issues. The states with the most reported identity theft cases per capita include the Chairman's state of Georgia, along with Louisiana, Florida, Delaware, and Nevada.[1]

The Office of the Inspector General (OIG) plays a vital role in combating SSN misuse and identity theft. Throughout SSA OIG's history, SSN misuse and identity theft have been a priority in our oversight efforts. SSA OIG has specific authority to investigate SSN misuse violations under Title 42 U.S.C. §408. Additionally, based on shared jurisdiction, we also assist in addressing identity fraud by conducting investigations related to violations under Title 18 U.S.C. § 1028.

Our SSN misuse investigations encompass a range of fraud schemes. To facilitate these schemes, perpetrators rely heavily on their ability to acquire and misuse another individual's SSN to commit crimes. Examples of those crimes and our work include:

- Identity document fraud (driver's licenses / passports)
- Bank, credit card and wire fraud
- Disability fraud, such a work concealment
- Deceased payee fraud
- Fraudulent benefit applications and account takeovers
- Stolen Identity Refund fraud and Earned Income Tax Credit fraud
- Synthetic identity theft

Synthetic identity theft is one of the more troubling forms of identity theft and has been a focus of some of our recent investigations. It is a unique form of fraud that combines SSNs of real people with fraudulent information, such as false names and dates of birth to create new identities. Synthetic identity theft is one of the most difficult forms of fraud to catch because fraudsters build good credit over a period time using a fake profile before making fraudulent charges and abandoning the identity.

The combination of a fraudulently obtained identity document, such as a picture ID, and an SSN enhances an individual's ability to commit certain crimes while concealing their true identity. This type of fraud has a particularly damaging impact on vulnerable populations such as older individuals and children, who are less likely to use their SSNs for work and therefore less likely to discover the fraud.

One example of our synthetic identity fraud investigations involved individuals who participated in a scheme to defraud a bank in San Antonio, Texas. The individuals were charged with using approximately 700 synthetic identities, in addition to stolen identities, to create bank accounts and shell companies. The perpetrators used complex computer data storage and virtualization machines to manufacture synthetic identities, combining

[1] Federal Trade Commission Consumer Sentinel Network Data Book 2022 (ftc.gov)

the personal information of real people (such as stolen SSNs) with fraudulent information, such as false names and dates of birth.

They used the identities to falsely and fraudulently open credit cards and bank accounts for those identities. They also registered shell companies with the State of Florida Division of Corporations, using the companies as part of the scheme. The companies appeared to be associated with service industries, such as yachting, technology, and landscaping, but conducted no legitimate business and had no legitimate employees. Fraudulent payments were made from accounts registered to these synthetic identities to accounts registered to the perpetrators.

After the passage of the Coronavirus Aid, Relief, and Economic Security ("CARES") Act their scheme evolved to utilize the already-established synthetic identities and associated shell companies and accounts to fraudulently apply for assistance under the CARES Act's Paycheck Protection Program (PPP), which was intended to help small businesses financially survive the pandemic. Between $20 and $25 million in PPP relief was paid to companies registered to the perpetrators, and to companies registered to synthetic identities they controlled. This multifaceted scheme not only harmed and misused the benefits of the PPP and the CARES Act, but it also harmed the integrity of the SSN as an identifier. One of these individuals recently pled guilty for his role in stealing millions in COVID relief money through a synthetic fraud scheme.

SSA OIG has established a multidisciplinary team of professionals that develop and implement innovative approaches to combat identity theft and scams through audits, criminal investigations and prosecution, civil enforcement, public outreach, and education. I want to outline some of those efforts.

The SSA OIG Office of Audit (OA) is a key player in identifying vulnerabilities in SSA programs and operations that may result in identity theft. We report these vulnerabilities to SSA for their attention and refer the data from our audits to the SSA OIG Office of Investigations (OI) to investigate identity fraud and disrupt organized groups from manipulating this system.

Our audits found fraudsters may steal identities to work or to claim earnings-related benefits. For example, in one audit, we found fraudsters improperly used the SSNs of 37 older adults to acquire $4.6 million during a five-year period.[2] During the same timeframe, OA found fraudsters misused 817 SSNs of deceased individuals to earn approximately $29 million in wages.

In another audit, we reported SSA removed from its Master Earnings File $742 million in self-employment earnings originally reported on approximately 50,000 numberholders' Federal income tax returns during a four-year period.[3] In approximately 59 percent of those cases, SSA removed the earnings because the numberholders alleged other individuals stole their identities and used their SSNs to file fraudulent tax returns. At our

[2] SSA OIG, Improper Use of Elderly Individuals' Social Security Numbers (A-03-16-24028), January 2017

[3] SSA OIG, Self-employment Earnings Removed from the Master Earnings File (A-06-12-12123) in January 2015

request, the U.S. Department of the Treasury Inspector General for Tax Administration (TIGTA) determined tax filers had used the self-employment earnings to claim the earned income tax credit.

Another audit found in one three-year period, about 37,700 employers reported approximately $1 billion in wages using the names and SSNs assigned to 36,546 children ages 13 and younger.[4] This group included 365 deceased children. Although the earnings for the living children were legitimate in all but eight percent of the cases, nearly all (362) of the deceased children's cases involved SSN misuse. These children had about $9 million in wages reported by employers that did not typically employ children.

Another focus of our audit work examines the Internet services the SSA offers. SSN numberholders can create my Social Security accounts to transact business with SSA, including reviewing their earnings records or changing their direct deposit information.

In January 2013, SSA began allowing individuals to change their direct deposit bank information using the *my Social Security* Internet application. Shortly thereafter, SSA and the OIG began receiving allegations of fraud related to unauthorized changes.

Our audits found from January 2013 through May 2018 fraudsters redirected $33.5 million in benefits intended for 20,878 beneficiaries by making unauthorized direct deposit changes through *my Social Security*.[5] Fortunately, an additional $23.9 million to 19,662 beneficiaries was prevented from misdirection because SSA corrected the unauthorized direct deposit changes before a payment was released.

During the COVID-19 pandemic, SSA closed its field offices to the public, resulting in a dramatic increase in the utilization of SSA's online services. As the use of eServices increased, so did the opportunity for fraudsters to manipulate SSA's online platforms.

Scammers use stolen personable identifiable information (PII) to file fraudulent online applications, establish or take over online accounts, or redirect benefit payments to alternate bank accounts. Since the start of Fiscal Year 2021, OIG has received more than 41,000 eServices-related allegations, including fraud schemes that misuse or are facilitated by SSA's online platforms, such as *my Social Security*. It is critical SSA employ effective controls to obtain sufficient assurance users of its online services are who they claim to be.

Additionally, bad actors exploited some of SSA's public-facing systems to validate SSNs and potentially use that information to commit identity fraud. These incidents underscore the need for SSA to thoroughly evaluate applications for potential vulnerabilities—including the risk the applications could be misused for purposes for which they were not designed. As more Americans utilize online platforms, fraud schemes will increase.

[4] SSA OIG, Improper Use of Children's Social Security Numbers (A-03-12-21269), March 2014

[5] SSA OIG, Unauthorized my Social Security Direct Deposit Changes Through May 2018 (Limited Distribution) (A-01-18-50669), September 2019

Our OI is currently developing an OIG-wide strategy to address identity theft related to eServices, including the analysis of real-time agency data to proactively identify the potential fraud. In addition to investigating identity theft related to eServices for prosecution purposes, OI also identifies vulnerabilities in systems and processes and reports them timely to SSA.

As you can imagine, beyond eServices, our OI also receives and evaluates allegations of fraud, waste, abuse, and mismanagement in SSA's programs and operations, and takes appropriate action in coordination with federal, state, and local prosecutors on matters of SSN fraud. Like the synthetic identity fraud case highlighted earlier in my testimony, many of our investigations involve SSN misuse. This work has led to many successful convictions.

For example, to highlight a few, in a recent joint investigation with the U.S. Department of State Diplomatic Security Service (DSS) and other federal and state law enforcement agencies, a man was found to have stolen the identity of another individual. Following the joint investigation, the man pleaded guilty to passport fraud, aggravated identity theft, and possession of a firearm by a convicted felon. In February 2022, a U.S. District Court judge sentenced him to 22 years of imprisonment.

In 2021, as a result of our investigation, an employee of a car dealership in the State of Connecticut was sentenced to 21 months in prison and five years of supervised release for a scheme involving fraudulent auto loan applications and identity theft. For a period of almost a year, the man falsified documentation for auto loans, including SSA benefit verification letters, and in some instances used others' identities to apply for loans without their authorization.

In 2020, a former U.S. Postal Service letter carrier was sentenced to 27 months in prison. Our investigation found she had misrepresented her living arrangements and income in applying for government benefits in her own name and applied for and received additional benefits using the identities of multiple friends and family members, including minor children. She also stole and deposited checks from the mail she was assigned to deliver.

Our OI in collaboration with private sector partners, conducts imposter scam investigations, often jointly with law enforcement agencies. In some instances, these partnerships have allowed OI to identify victims quickly and recover funds before they were lost. For example, on November 18, 2021, SSA OIG and the FBI arrested five individuals pursuant to an indictment from the Northern District of Georgia. The indictment resulted from an investigation led by SSA OIG investigators that uncovered a telephone imposter scam originating from overseas call centers. The twelve-count indictment charged the five defendants with wire fraud, conspiracy to commit wire fraud, money laundering, and conspiracy to commit money laundering.

In addition to the arrests, agents executed one residential search warrant and five account seizure warrants. The operation took place in five states: Georgia, Florida, Massachusetts, New Jersey, and New York, with approximately 100 law enforcement officers and support staff involved. In addition to SSA OIG and the FBI, DHS Homeland

Security Investigations, the TIGTA, and Wood-Ridge (New Jersey) Police Department provided substantial assistance to the investigation and operation. The investigation has identified and seized nearly $2 million in proceeds of the scam's criminal activities.

The development of Artificial Intelligence (AI) provides a new tool to create official-looking deception scam messages intending to steal personal information. AI will utilize algorithms that can recognize, summarize, and generate fraudulent texts and contents based on massive datasets. AI can even generate scam messages and produce a transcript in which a scammer impersonates federal government employees. AI will prove valuable to criminals and challenging for investigators. Aware of this developing technology, SSA OIG is working towards countering AI-generated scams and educating Social Security recipients of AI-generated scams.

The emergence of the COVID-19 pandemic resulted in criminals finding ways to fraudulently take advantage of the infusion of trillions of dollars in federal funding. SSN misuse, including identity theft, is a common thread running through many investigations related to the misuse of pandemic relief funds.

Since the start of the pandemic, SSA OIG has participated in the National COVID-19 Fraud Enforcement Taskforce, led by the Deputy Attorney General of the United States, 25 COVID-19 fraud workgroups and in 159 investigations related to COVID-19 pandemic relief programs, funds, and scams.

Further, SSA OIG has issued nearly a dozen COVID-19-related audits. SSA OIG and collaborated in joint investigations working with federal, state, and local law enforcement entities to pursue SSN misuse and other crimes involving federal pandemic relief funds including Unemployment Insurance (UI) fraud and PPP fraud.

Since the outset of the COVID-19 pandemic, SSA OIG has received over 31,740 fraud allegations referencing Pandemic-related relief programs and funds. At present, we have over 70 active investigations involving COVID-19 pandemic fraud. Our investigative efforts to date, both solely and in joint investigations with our law enforcement partners, have resulted in 32 defendants convicted, over $34 million in identified fraud loss, court-ordered restitution of over $24 million, and over $6.5 million in funds recovered.

In FY 2023, SSA OIG anticipates expending approximately $2.3 million on Pandemic-related investigative workloads and audits. Though SSA OIG has a critical role in combatting COVID-19 pandemic fraud, SSA OIG has never received dedicated funding for pandemic oversight.

These COVID-19 challenges required additional resources not accounted for in our budget and took away from resources generally devoted to our bread-and-butter investigations, such as Social Security program fraud. Nonetheless, SSA OIG continues to make data-driven decisions to prioritize these workloads. Even in Fiscal Year 2022, SSA OIG identified $15 in returns to the government for every $1 it received through its appropriation.

Further, as recommended by the Pandemic Response Accountability Committee in testimony provided to the Committee on Ways and Means and included in the recently passed H.R. 1163, Protecting Taxpayers and Victims of Unemployment Fraud Act, the extension of the statute of limitations for criminal charges or civil actions for prosecuting fraud from five to ten years means SSA OIG will continue focusing on fraudulent Unemployment Insurance payments further into the future.

SSA OIG also plays an important role in disrupting Social Security-related and other government imposter scams. For over a decade, the American public's have been plagued by widespread robocalls and live callers impersonating government agencies to steal money or personal information, including SSN's, from victims. At a basic level, the scams are all the same: a victim is contacted by a criminal pretending to be from a government agency, the criminal tells the victim about a problem or prize, the criminal uses specific payment methods that are difficult to track, and the criminal pressures the victim to act immediately.

These scam calls appear to originate from within the United States and, more maliciously, often "spoof" caller identification from a government or law enforcement agency. Callers may ask for personal information, demand payment, or make threats. These scams occur primarily via telephone but may also occur via misleading postal mailings, emails, internet websites, blogs, radio and television ads, and social media accounts.

These scams have caused untold anguish and financial harm, with criminals sometimes stealing hundreds of thousands of dollars from victims. In response, a team from across SSA OIG developed and implemented a multipronged approach to combat these scams, harnessing its workforce's diverse skills and experience and collaborating with other public and private entities as a force-multiplier.

The SSA OIG's Office of the Counsel (OC) is responsible for enforcing Section 1140 of the Social Security Act, which, in part, protects consumers from misleading SSA-related communications (including through Internet websites and scam telephone calls) may convey the false impression SSA approved, endorsed, or authorized the communication, and may lead people to provide money or PII.

Our OC educates U.S. telecommunications companies about Section 1140 and secures compliance and seeks penalties against U.S. telecommunications companies, acting as gateway carriers, who profit by accepting these scam calls into the U.S. telecommunications system and passing them to unsuspecting consumers.

OC has initiated 36 cases against gateway telecommunications companies and have imposed penalties against 16 gateway carriers. As a result, many of these companies have begun to take more proactive steps to prohibit scam calls from entering the United States or have decided to discontinue operations and/or the gateway carrier segment of their operations.

Our OC also proactively and continuously protects consumers by shutting down fraudulent SSA-related websites and social media accounts. For example, since the

start of this Fiscal Year, the SSA OIG has successfully requested the removal of 20 fraudulent SSA-related social media accounts on platforms including Facebook and Pinterest. These fraudulent and imposter accounts frequently take the form of pages masquerading as official agency resources or and even agency officials. They can trick members of the public into revealing their PII to scammers. In sum, our education, investigative, and enforcement efforts have yielded meaningful results. Since fall of 2020, there has been an 87.4% decrease in SSA-related imposter allegations.

While safeguarding the public from financial fraud and scams is a daily goal, one of our major initiatives, in collaboration with SSA, is the National Slam the Scam Day. The campaign encourages the public to hang up or ignore suspicious calls or messages – in other words, to “Slam the Scam”.

On Slam the Scam Day we amplify our outreach efforts to protect the American public. This year on March 9, 2023, we marked our fourth annual National Slam the Scam Day, which brought together Federal, state, and local government agencies, nonprofit organizations, and private companies to encourage the public to hang up or ignore criminals impersonating government employees.

We appreciate the support of the United States Congress with a U.S. Senate Resolution marking National Slam the Scam Day and the Members of Congress who shared messages on social media and through press releases. This outreach expanded scam information and how your constituents can protect themselves from Social Security-related and other government imposter scams. This combined effort on Slam the Scam Day’s media coverage garnered an approximate audience of over 86 million people.

In conclusion, I want to thank the Subcommittee for inviting me today to highlight the SSA OIG’s oversight and outreach efforts in combatting and preventing the misuse of SSNs. This hearing is an important reminder to the American public we all need to remain vigilant to protect our SSNs and PII and be mindful to slam the scam.

Thank you, and I would be pleased to address any questions.