HOUSE WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

UNITED STATES HOUSE OF REPRESENTATIVES

MAY 24, 2023

STATEMENT FOR THE RECORD

SEAN BRUNE

DEPUTY COMMISSIONER FOR SYSTEMS and CHIEF INFORMATION OFFICER

SOCIAL SECURITY ADMINISTRATION

Chairman Smith, Chairman Ferguson, Ranking Member Larson, and Members of the Subcommittee:

Thank you for inviting me to discuss the Social Security Administration's (SSA's) role in combating identity theft, as it relates to misuse of Social Security Numbers (SSNs). I am Sean Brune, the Deputy Commissioner for Systems and the Chief Information Officer for SSA. Today I will talk about our efforts to prevent and mitigate the harm resulting from bad actors who try to misuse SSNs for their own gain. These issues extend beyond our agency. Identity theft is a collective problem. All of us play a role in finding the solutions. I greatly appreciate your concerns about this important topic and acknowledge the Subcommittee's many years of work on this issue.

The SSN and Our Programs

The Social Security Act of 1935 (Act) does not mandate the use of SSNs, but authorizes the creation of a record-keeping system for accurate wage reporting. We designed the nine-digit SSN to allow employers to uniquely identify and properly report an individual's earnings covered under the new Social Security program, and to help us track earnings, determine eligibility for benefits, and pay the correct benefit amount.

Today, almost 90 years later, the SSN remains at the core of our recordkeeping and is essential to carrying out our mission. We use the SSN to administer the Old-Age, Survivors, and Disability Insurance programs, commonly referred to as "Social Security." We also use the number to administer the means-tested Supplemental Security Income program, which provides monthly payments to people with very low income and resources who are aged, blind, or disabled.

Expansion of SSN Use for Other Purposes

While we designed the SSN solely for administering our programs, over time the universality and ready availability of the number made the SSN a convenient means of record-keeping in other large systems of records, including other parts of the Federal government. In 1943, for example, Executive Order 9397 required Federal agencies to use the SSN in any new system for distinguishing individuals. Then, beginning in the 1960s, SSN use expanded quickly with advances in computer technology, as government agencies and private organizations began using automated data processing and record keeping.

In 1961, the Federal Civil Service Commission began using the SSN as the identification number for all Federal employees. The next year, the Internal Revenue Service began using the number as its taxpayer identification number. In 1967, the Department of Defense adopted the SSN as the service number for military personnel.

In the 1970s, Congress enacted legislation requiring an SSN for applicants to receive assistance under the Aid to Families with Dependent Children program (succeeded by Temporary Assistance for Needy Families), Medicaid, and the Supplemental Nutrition Assistance Program (SNAP). Additional legislation authorized States to use the SSN in the administration of taxes, general public assistance, driver's licenses, or motor vehicle registration laws within their jurisdiction. In the 1980s and 1990s, legislation required the use of the SSN in employment eligibility verification and military draft registration, among other things.

The 1996 welfare reform law required the SSN to be recorded in a broad array of records—including applications for professional licenses, marriage licenses, divorce decrees, support orders, and paternity determinations—to improve child support enforcement. The 1996 law also included SSN requirements for purposes of obtaining the Earned Income Tax Credit, and in recent years, Congress has enacted SSN requirements for eligibility for additional tax credits, such as the Child Tax Credit. These examples are not exhaustive but illustrate the growth of the use of the SSN within all levels of government.

Use of the SSN by the Private Sector

Use of the SSN for computer and other accounting systems spread, not just throughout State and local governments, but to banks, credit bureaus, hospitals, educational institutions, and other parts of the private sector. Generally, there are no restrictions in Federal law on the use of the SSN by the private sector, and in certain cases the law requires these organizations to use the SSN. In one common practice, businesses may ask for a customer's SSN to apply for credit cards, obtain medical services, and apply for public utilities. In most cases, customers may refuse to provide the number; however, a business may decline to furnish the product or service.

Businesses use the SSN to track and identify and exchange information about individuals. Over time, additional advances and trends in technology fostered the growth of data aggregators who amass and sell large volumes of personal information, including SSNs, collected by businesses.

Responding to the External Use of the SSN

SSA cannot control how other entities use the SSN for outside purposes. To an extent not originally intended, the SSN has become frequently used as a personal identifier by both government and the private sector to establish and maintain information about individuals. Before the widespread use of the SSN outside of Social Security programs (for purposes such as establishing credit), there were few incentives to obtain fraudulent SSNs or counterfeit cards. However, as the use of the SSN expanded, so too did incentives to obtain fraudulent SSNs, giving rise to concerns about the integrity of the number and card.

At one time it may have been helpful to use the SSN as "secret information" – something that would only be known by the person to whom the SSN was assigned. That is no longer

acceptable and has not been for many decades**. The SSN never was – and never will be – evidence of someone's identity**. The SSN is simply a number associated with a specific individual in our records, as the combination of a name with an SSN allowed for correctly crediting earnings and paying benefits. Even if it was secret at some point, it most likely is not now. Neither knowing the SSN nor having possession of an SSN card verifies that the person using them is the individual to whom we issued the SSN. SSN verifications can nonetheless be an important tool to prevent and detect identity theft.

Identity Theft and the SSN

Unfortunately, SSN misuse and identity theft—including synthetic identity theft, where the claimed identity is made up and does not involve an actual person, continue to persist. Identity thieves may target children because their credit histories are clean, and their records may be used for years before anyone realizes someone has stolen their identities or misused their SSNs. We continue working to protect people's SSNs through actions in our control, such as by protecting customer data by removing SSNs from mailed documents where needed.

We understand the frustration, distress, and economic hardship SSN misuse and identity theft cause victims. As a matter of practice, online and in our offices, we provide individuals who suspect their identities have been stolen with up-to-date information about steps they can take to work with credit bureaus, law enforcement agencies, and the Federal Trade Commission. We also encourage such individuals to consider contacting the IRS because an identity thief might use a stolen SSN to file a tax return. Information about tax-related identity theft is available at www.irs.gov/uac/Identity-Protection. We develop cases of possible SSA-program related fraud and refer them to our Office of the Inspector General for investigation as appropriate. When individuals report misuse of an SSN to SSA, we can only correct SSA program-related issues, because, as I noted earlier, we do not have control over how other entities use SSNs.

Public Education

Education is key. In recent years, we strengthened our efforts to educate the public about how best to protect their sensitive information from fraudsters. We released public service announcements, worked with external groups and agencies to raise awareness, and partnered with the United States Postal Service to display identity scam prevention posters in Post Offices around the country. We provide our employees with the latest information to ensure they can help individuals who call and visit our offices. We ask them to help educate their friends, families, and communities. We use social media to reach individuals, advising them to "guard their card" and sensitive information.

We collaborate closely with our Office of Inspector General to keep our customers and our employees informed of developing threats against their personal information. This year, working with our OIG, we observed the fourth annual "Slam the Scam" day during the Federal Trade

Commission's National Consumer Protection Week, continuing our work to ensure the public is able to identify fraud attempts, understands how to respond, and stays up to date on best practices to protect their information.

SSN Verifications

Public education is only part of the answer. Even though we advise people to keep their SSN confidential, public and private data leaks have greatly reduced the likelihood that SSNs are private information. This is why SSA's lawfully authorized electronic SSN verifications have become so important. Annually we perform over 2 billion automated SSN verifications through more than 3,500 data exchanges. As the issuing authority for SSNs, we are the only entity that can authoritatively validate SSNs. Unlike other entities, we can validate any SSN we assigned, regardless of when we assigned it or whether there is financial activity associated with it. Importantly, our verification services only verify that the name, SSN, and other information presented match the combination present in our records. We cannot verify that the individual presenting that information is the correct individual.

Our Social Security Number Verification Service, or SSNVS, is a free service employers can use as part of the wage-reporting process to verify an employee's SSN using an online verification system on our website. By using this service, employers can increase the accuracy of their wage reports by verifying names and SSNs on W-2 wage reports. SSNVS also reduces processing time and costs, and allows us to give proper credit to employees' earnings records.

In 1984, Congress added a new income and eligibility verification system aimed at reducing improper payments of Federally funded benefits (e.g., Medicaid, SNAP, and Unemployment Insurance). Verification of the SSN is a key aspect of this system; we confirm whether the name, SSN, and, in most cases, date of birth, provided by an individual match the information in our records.

Since then, Congress has mandated the verification of SSNs for such varied purposes as the Department of Homeland Security's E-Verify program, health care programs, voter registration, drivers' licensing, and many others. As a result, the use of electronic SSN verifications has grown dramatically. These verifications help to reduce or prevent improper payments and ensure better program integrity.

We provide SSN verifications to private entities with consent of the SSN holder in certain circumstances. For financial organizations, we use our Electronic Consent Based SSN Verification Service (eCBSV). Congress enacted eCBSV in 2018. Using eCBSV, financial institutions can submit their customers' SSN information to us, so that we can compare it against our records and provide 'match/no match' results. eCBSV helps prevent synthetic ID theft. Again, eCBSV verifies only that the name, SSN, and other information presented match the combination present in our records.

Given the importance of our electronic SSN verifications in defending against synthetic identity fraud, we are working to expand the ability of Federal benefits programs to use this service as part of their identity verification processes. We intend to enable Federal benefits programs to verify SSNs, directly or through other Federal agencies, using real-time verification requests.

Keeping the SSN Secure

It is critical that we protect sensitive information in our possession from unauthorized disclosure and manipulation. It is also critical that we ensure that our electronic services are accessible to all segments of the public. We have made strides to expand options for SSN card replacement, reducing the need for people to visit offices, such as by offering online internet replacement card services in most states, and by increasing the ability in some states for people to request new cards due to marriage name changes. We also introduced the ability for US citizens and non-citizens to begin applications for original or replacement cards online before visiting an office to finish the process. Additionally, we have worked with Federal partners to expand the Enumeration Beyond Entry process to help eliminate in-person visits to SSA in certain circumstances.

We hold most seriously our responsibility to protect program integrity and personal information in our possession. At the same time, we must be able to conduct operations in a practical manner without placing undue burden on the public or our service channels. We continue to work on security enhancements, as well as partner with others to address misuse.

Planning for the Future

We understand the significant challenges associated with fully addressing the dangers posed by identity theft, which remain a collective challenge across government and the private sector. As long as the SSN remains key to accessing things of value—credit, loans, and financial accounts, and thus numerous common goods and services—the SSN itself will have commercial value, and it will continue to be targeted for misuse. We take the integrity of the SSN very seriously. We will continue to do what we can to prevent and mitigate the effects of SSN misuse and identity theft. We stand ready to work with Congress as it considers ways to protect Americans' personal information.