COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

U.S. HOUSE OF REPRESENTATIVES

May 17, 2018

STATEMENT FOR THE RECORD

NANCY A. BERRYHILL
ACTING COMMISSIONER
SOCIAL SECURITY ADMINISTRATION

Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee:

Thank you for inviting me to discuss the Social Security number (SSN) and card. I am Nancy Berryhill, Acting Commissioner of the Social Security Administration. My testimony today describes the development of the SSN for the administration of Social Security programs and our ongoing efforts to ensure its integrity.

As you know, use of the SSN as an effective record-keeping tool has expanded far beyond its original and primary purpose. I hope our efforts show that we are committed to doing what we can to mitigate the harm resulting from SSN misuse and identity theft. But these issues extend beyond our programs, and solutions require commitment from the public and private sectors. I commend you for holding this hearing today.

The SSN and Our Programs

When the Social Security program was enacted under the Social Security Act of 1935 (Act), the Act did not mandate the use of SSNs but authorized the creation of some type of record-keeping system. Names alone could not ensure accurate wage reporting. We designed the nine-digit SSN to allow employers to uniquely identify and 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. We also developed the SSN card to show the SSN assigned to a particular individual to assist employers in properly reporting earnings.

Today, over 80 years since the program's inception, the SSN remains at the core of our record-keeping processes and is essential to carrying out our mission. We use the SSN to administer the Retirement, Survivors, and Disability Insurance programs, commonly referred to as "Social Security." We also use the number to administer the Supplemental Security Income (SSI) program, which provides monthly payments to people with limited income and resources who are aged, blind, or disabled.

Through the use of the SSN, in Fiscal Year (FY) 2017, we posted 279 million earnings items to workers' records. Based on wages reported using the SSN, on average, each month we pay Social Security benefits to over 62 million individuals. We also pay SSI benefits to over 8 million individuals. In total, during FY 2017, we paid about $934 billion to Social Security beneficiaries, and about $55 billion to SSI recipients. That same year, we assigned over 5.8 million original SSNs and issued nearly 10.6 million replacement SSN cards. To date, we have issued around 505 million unique numbers to eligible individuals.

Expansion of SSN Use for Other Purposes

Many factors led to the expanded use of the SSN 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. 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 due to 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 food stamps. 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 just the last few 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 the Federal 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. For example, businesses may ask for a customer's SSN to apply for credit cards, obtain medical services, and apply for public utilities. A customer may refuse to provide the number; however, a business may, in turn, decline to furnish the product or service.

The SSN not only allows businesses to track and identify individuals, it also allows them to exchange information about these individuals. Over the last decade, 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. Generally, data aggregators use the SSN to store and retrieve information about an individual because it is such an easy, universal method to maintain individual records.

Responding to the External Use of the SSN

While not intended, the SSN has become the personal identifier most broadly used 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. Working with Congress, we have made changes to protect the integrity of the number. These efforts focus on increasing the

security of the SSN and card, confirming the authenticity of the SSN and card through SSN verifications, and educating the public. The following are examples of some of our key efforts.

Strengthening the SSN and Card

In the beginning of the program, and for many years thereafter, we assigned SSNs and issued cards based solely on the applicant's allegation of name, date of birth, and other personal information. We required no documentation to verify an individual's identity. We began adding documentation requirements in the 1970s as a result of statutory changes to the Act. By 1978, we required evidence of age, identity and citizenship/alien status from all applicants for original SSNs, as well as evidence of identity for replacement cards.

Today, we use a robust application process requiring SSN applicants to submit evidence of age, identity, and United States citizenship or current work-authorized immigration status. Generally, individuals (other than newborns) must come into an SSA field office or Card Center to apply for an original SSN and card. We require an in-person interview for all applicants age 12 or older. During the interview, we attempt to locate a prior SSN to help ensure that we do not assign an SSN to an individual assuming a false identity.

These policies comply with requirements enacted in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, which include:

- New, rigorous minimum standards for verification of documents submitted in connection with an SSN;
- The addition of death and fraud indicators to SSN verification routines for employers and for State agencies issuing driver's licenses and identity cards; and,
- Limiting individuals to 3 replacement SSN cards per year and 10 per lifetime (with limited exceptions).

We have also established programs to ensure the accurate and timely assignment of SSNs, and to provide convenient public service options. Through these programs, we coordinate with other government agencies—the custodians of the very records we use to assign SSNs—to obtain the information they collect and verify electronically. Because we work directly with the custodians of the evidence records we need, individuals who choose to use these programs do not need to visit our offices to present their documents in person.

- The Enumeration at Birth (EAB) program allows parents to obtain SSNs for their newborns as part of the birth registration process. The evidence required to process an SSN application is the same evidence gathered by hospitals and birthing facilities and verified by bureaus of vital statistics (BVS) during the birth registration process. Through EAB, BVSs electronically send us the information we need; we assign the number and issue the card. Today, all 50 States plus Puerto Rico, New York City and the District of Columbia participate. In FY 2017, we assigned over 3.8 million SSNs through EAB.

- The Enumeration at Entry (EAE) program allows lawful permanent residents (LPRs) to obtain SSNs as part of the immigrant visa process. Once the Department of State approves the visa, it transmits identifying information from the visa application to the Department of Homeland Security (DHS); DHS, in turn, transmits to us the data we need when the person enters the country. In FY 2017, we assigned over 271,000 SSNs and issued about 7,600 replacement cards through EAE.

- The Enumeration Beyond Entry (EBE) program—our newest program—allows lawfully present noncitizens to obtain an SSN when DHS provides them work authorization. DHS sends us the information it collected and verified when approving the request for work authorization. We implemented this process in October 2017, and have used it to assign about 106,000 SSNs and issue about 14,000 replacement cards through April 2018.

Like evidence requirements, at the inception of the program, there were no specific requirements regarding the SSN card. However, as use of the SSN and card increased and technology improved, so too did counterfeiting concerns. In 1983, Congress amended the Act to require that SSN cards be made of banknote paper and be counterfeit-resistant to the maximum extent practicable. In 2007, pursuant to IRTPA, we implemented additional changes to the card based on interagency taskforce recommendations. The new security features include:

- A guilloche background pattern, which is a unique, computer-generated, non-repeating spiral design;
- A latent image, visible only when viewed at specific angles;
- Color shifting inks, like those in the Nation's currency, that create a noticeable color shift when moved in front of a light source; and
- The card issuance date, reflecting the date we processed the card application.

SSN Verifications

In 1984, shortly after amending the Act to require a banknote paper card, Congress added a new income and eligibility verification system aimed at reducing improper payments of Federally-funded benefits (e.g., Medicaid, Supplemental Nutrition Assistance, 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 DHS's E-Verify program, health care programs, voter registration, drivers' licensing, and many others. So, the use of SSN verifications has grown dramatically. Today, we perform over 2 billion SSN verifications a year.

Public Education

We also focus on educating the public about how they can protect their SSNs. We advise individuals to avoid sharing their SSNs. We encourage them to keep their cards in a safe place

and not to carry them, or any documents displaying their SSNs, with them unless an employer or service provider insists on seeing it.

In addition, we:

- Post Frequently Asked Questions on our website that address questions related to identity theft and the various ways we protect SSNs[1];
- Post publications that specifically address identity theft and how an individual can protect his or her SSN[2];
- Provide articles for publication in local newspapers nationwide urging people to protect their SSNs and cards;
- Broadcast best practices, such as "Tips to Prevent Identity Theft," on televisions in field office lobbies, to explain how individuals can protect themselves from identity theft; and,
- Collaborate with the Federal Trade Commission (FTC) to educate the public through local seminars and public information materials.

Identity Theft

Unfortunately, SSN misuse and identity theft—particularly pairing fraudulent identity information with valid information, known as synthetic identity theft—continue to increase. As DHS has advised us, part of this problem results from the use of stolen or made-up SSNs to secure work by individuals, for example, who are not authorized to work (such as aliens without work authorization) or are attempting to underreport earnings. In addition, according to our Office of the Inspector General, identity thieves often 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.[3]

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 up-to-date information about steps they can take to work with credit bureaus, law enforcement agencies, and the FTC. We develop cases of possible fraud and refer them to our Office of the Inspector General for investigation as appropriate.

In certain circumstances, we will assign new, different numbers to victims of SSN misuse who suffer disadvantage due to the misuse of their SSNs. It is important to note that assigning a new number is often a last resort because, unfortunately, given the pervasiveness of the SSN in daily life, a new number may cause the victim greater problems than the ones they are trying to solve. For example, the absence of history under the new SSN may itself cause difficulties—particularly a lack of credit history under the new number, which may make it more difficult to obtain credit, buy a car, or get a mortgage.

---

[1] e.g., https://faq.ssa.gov/link/portal/34011/34019/Article/3790/Can-I-get-a-different-Social-Security-number-if-I-am-a-victim-of-identity-theft

[2] e.g., "Identity Theft and Your Social Security Number," at www.socialsecurity.gov/pubs/EN-05-10064.pdf

[3] *See* SSA Office of the Inspector General, *Potential Misuse of Foster Children's Social Security Numbers*, A-08-12-11253 (Sept. 25, 2013).

In the past, our policies required that evidence of disadvantage resulting from SSN misuse be recent, occurring within the year preceding the request for a new number. In recognition of the devastation identity theft poses, and the fact that it may not manifest immediately, we re-evaluated this policy and made several key changes. First, we lengthened the look-back period; we now allow for evidence of disadvantage within the two years preceding the request for a new number. This timeframe covers the majority of requests, and technicians may extend the two-year window further depending on the circumstances. Second, we advise frontline employees to consult regional office specialists regarding complex cases. This allows us to better serve the needs of victims of misuse and identity theft by ensuring consistent application of policy and leveraging the expertise of regional office employees. Third, we added examples to our procedural instructions to illustrate the different ways an individual may be disadvantaged due to SSN misuse.

Recently, we published a policy clarification regarding child SSN misuse cases. We reminded our frontline employees that child cases can be different from adult cases. When SSN misuse has occurred with a child's number, the harm caused by the misuse—particularly credit damage—may go undetected by the child and parents for years. As a result, we instruct employees to carefully consider *all* evidence of disadvantage, and we remind them to coordinate closely with their regional offices. I want to thank the Subcommittee for alerting us to a specific case that demonstrated the need for a policy clarification in this area.

We encourage everyone to establish a *my* Social Security account. Doing so ensures that no one else can open an account with their SSN. We also educate individuals who suspect they may be victims of identity theft about how to block access to SSA electronic services. This block prevents all automated telephone and electronic access to Social Security records, as well as online claims. When we assign a new, different number, we automatically place a fraud indicator on the original number. This fraud indicator blocks the number from being used to establish a *my* Social Security account or get a replacement SSN card, or from verifying under our verification services for employers, driver's license-issuing entities, and others.

Going forward, we will continue to refine the role that our Special Assistant U.S. Attorneys (SAUSA) play in prosecuting SSN misuse. SAUSAs currently prosecute cases of alleged Social Security fraud that would not otherwise be prosecuted in Federal courts. We plan to maintain a corps of 35 SAUSAs in FYs 2018 and 2019. Their work is valuable in prosecuting current fraud and deterring potential future bad actors.

Moving Forward with New Solutions

We know the large challenges associated with fully addressing the dangers posed by identity theft. 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. At SSA, we take seriously the integrity of the SSN. We will continue to do what we can to prevent and mitigate the effects of SSN misuse and identity theft, and we will continue to evaluate new technologies and data to better secure the number. But just as we cannot control how other entities use the SSN for outside purposes, we alone cannot solve the problem overreliance on the SSN has caused.

Identity theft is a broader public policy issue. I applaud the Chairman and this Subcommittee for their efforts to protect the SSN. The "*Medicare Access and CHIP Reauthorization Act of 2015"* required the removal of the SSN from Medicare cards. We are pleased to support the Centers for Medicare and Medicaid Services (CMS) in its efforts to implement this bill, and I am happy to note the CMS has just begun issuing the new cards. The *Social Security Number Fraud Prevention Act of 2017* restricted the inclusion of SSNs on documents mailed by Federal Agencies. As we promised this Committee, we have continued our work to remove the SSN from notices where we can. Last month, we removed the SSN from benefit verifications, post-entitlement notices, and certain documents sent to appointed representatives. The Administration also encourages Congress to pass legislation with a requirement that employers use DHS's E-Verify system, such as the requirements in the *Legal Workforce Act*. Mandatory use of E-Verify by employers would help reduce the incidence of fraudulent use of SSNs. We would be happy to work with you as you contemplate that or similar legislation.

These bills are an important step. However, because identity theft is a pervasive issue, addressing it requires a unified effort that includes this Subcommittee and Congress, the Administration, and public and private experts throughout the country. Any solution must be a durable and comprehensive one in order to reduce and ultimately prevent identity theft throughout public and private industry.

Conclusion

As this Subcommittee—and Congress as a whole—considers how to address identity theft, I urge them to keep in mind that we designed the SSN to administer Social Security programs. We never intended the SSN to serve as the universal personal identifier it has come to be.

Thank you for the opportunity to discuss these very important issues. I will be happy to answer any questions you may have.