Hearing on Securing Americans' Identities: The Future of the Social Security Number

---

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

May 17, 2018

Serial No. 115-SS09

COMMITTEE ON WAYS AND MEANS KEVIN BRADY, Texas, *Chairman*	
SAM JOHNSON, Texas DEVIN NUNES, California DAVID G. REICHERT, Washington PETER J. ROSKAM, Illinois VERN BUCHANAN, Florida ADRIAN SMITH, Nebraska LYNN JENKINS, Kansas ERIK PAULSEN, Minnesota KENNY MARCHANT, Texas DIANE BLACK, Tennessee TOM REED, New York MIKE KELLY, Pennsylvania JIM RENACCI, Ohio KRISTI NOEM, South Dakota GEORGE HOLDING, North Carolina JASON SMITH, Missouri TOM RICE, South Carolina DAVID SCHWEIKERT, Arizona JACKIE WALORSKI, Indiana CARLOS CURBELO, Florida MIKE BISHOP, Michigan DARIN LAHOOD, Illinois BRAD R. WENSTRUP, Ohio	RICHARD E. NEAL, Massachusetts SANDER M. LEVIN, Michigan JOHN LEWIS, Georgia LLOYD DOGGETT, Texas MIKE THOMPSON, California JOHN B. LARSON, Connecticut EARL BLUMENAUER, Oregon RON KIND, Wisconsin BILL PASCRELL, JR., New Jersey JOSEPH CROWLEY, New York DANNY DAVIS, Illinois LINDA SÁNCHEZ, California BRIAN HIGGINS, New York TERRI SEWELL, Alabama SUZAN DELBENE, Washington JUDY CHU, California
GARY J. ANDRES, *Staff Director* BRANDON CASEY, *Minority Chief Counsel*	

SUBCOMMITTEE ON SOCIAL SECURITY SAM JOHNSON, Texas, *Chairman*	
MIKE BISHOP, Michigan VERN BUCHANAN, Florida MIKE KELLY, Pennsylvania TOM RICE, South Carolina DAVID SCHWEIKERT, Arizona DARIN LAHOOD, Illinois	JOHN B. LARSON, Connecticut BILL PASCRELL, JR., New Jersey JOSEPH CROWLEY, New York LINDA SANCHEZ, California

Hearing on Securing Americans' Identities:
The Future of the Social Security Number

U.S. House of Representatives,
Subcommittee on Human Resources,
Committee on Ways and Means,
Washington, D.C

WITNESSES

Nancy Berryhill
Acting Commissioner, Social Security Administration
Witness Statement

Elizabeth Curda
Director, Education, Workforce, and Income Security, Government Accountability Office
Witness Statement

Samuel Lester
Consumer Privacy Counsel, Electronic Privacy Information Center
Witness Statement

Paul Rosenzweig
Senior Fellow, R Street Institute
Witness Statement

Steve Grobman
Senior Vice President and Chief Technology Officer, McAfee, LLC
Witness Statement

Jeremy A. Grant
Coordinator, Better Identity Coalition
Witness Statement

James Lewis
Senior Vice President, Technology Policy Program, Center for Strategic and International Studies
Witness Statement

WAYS AND MEANS
CHAIRMAN KEVIN BRADY

Chairman Johnson Announces Hearing on Securing Americans' Identities: The Future of the Social Security Number

House Ways and Means Social Security Subcommittee Chairman Sam Johnson (R-TX) announced today that the Subcommittee will hold a hearing entitled "Securing Americans' Identities: The Future of the Social Security Number." The hearing will focus on the dangers of the use of the Social Security number (SSN) as both an identifier and authenticator, and examine policy considerations and possible solutions to mitigate the consequences of SSN loss or theft. **The hearing will take place on Thursday, May 17, 2018 in 1100 Longworth House Office Building, beginning at 10:00 AM.**

In view of the limited time to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit written comments for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, http://waysandmeans.house.gov, select "Hearings." Select the hearing for which you would like to make a submission, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word document, in compliance with the formatting requirements listed below, **by the close of business on Thursday, May 31, 2018**. For questions, or if you encounter technical problems, please call (202) 225-3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

All submissions and supplementary materials must be submitted in a single document via email, provided in Word format and must not exceed a total of 10 pages. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. The name, company, address, telephone, and fax numbers of each witness must be included in the body of the email. Please exclude any personal identifiable information in the attached submission.

Failure to follow the formatting requirements may result in the exclusion of a submission. All submissions for the record are final.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202-225-1721 or 202-226-3411 TTD/TTY in advance of the event (four business days' notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available at http://www.waysandmeans.house.gov/

SECURING AMERICANS' IDENTITIES: THE

FUTURE OF THE SOCIAL SECURITY NUMBER

Thursday, May 17, 2018

House of Representatives,

Subcommittee on Social Security,

Committee on Ways and Means,

Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:08 a.m., in Room 1100, Longworth House Office Building, Hon. Sam Johnson [Chairman of the Subcommittee] presiding.

*Chairman Johnson. Good morning and welcome to today's hearing on the future of Social Security and its number.

Good morning and welcome to today's hearing on the future of the Social Security number.

The Social Security card and the Social Security number were created in 1936, believe it or not, so the Social Security Administration could track earnings and correctly determine benefits. Today's use of Social Security numbers for everything -- you need one. So when you get a job, buy a house, or open a new credit card (sic).

Given all the ways we use it, it is no wonder Social Security numbers are a valuable target for identity thieves. For years, I have been dedicated to doing all I can to protect America -- Americans from identity theft by protecting the privacy of Social Security numbers. Military IDs no longer use Social Security numbers, and Medicare is now sending new cards without numbers, Social Security numbers, to seniors across the country. And last year Congress made all federal agencies stop mailing documents that contain Social Security numbers unless it is absolutely necessary.

For a long time keeping Social Security numbers secret meant keeping them safe. But after so many high-profile data breaches like Equifax, OPM, and Anthem, where hundreds of millions of Social Security numbers were stolen, it is clear they aren't a secret anymore. And it is time we stop pretending that they are.

Make no mistake, it is still important to limit the unnecessary use of Social Security numbers. But if we want to keep pace with identity thieves, we need to think beyond just keeping them.

As we will hear today, what makes these numbers so valuable to identity thieves is how we use them. Using Social Security numbers both to identify someone and to prove their identity doesn't make sense. But we have been doing it forever. We need to break the link between identification and authentication.

We will also hear from Social Security about what it takes get a new Social Security number when it has been stolen and why it is often harder to do than it should be. I recently learned of a case in Arizona where the mother of a child whose Social Security number had been stolen was told she needed to change her daughter's name and last name -- first, middle, and last name -- before her daughter could get a new Social Security number. Can you believe that? That is wrong.

But what is worse is that having to change your name isn't Social Security's policy. It was an extra hoop to jump through made up by a field office employee. While I am happy the little girl eventually got a new number without having to change her name, getting a new number shouldn't be so difficult. It shouldn't take a local news story or a call from a congressional office for Social Security to do right by those looking for help.

Identity theft is on the rise, and we must take a hard look at the future of Social Security numbers, both how it is used, and if Social Security needs to do things differently. We have a responsibility to do all we can to better protect Americans from identity theft.

I want to thank our witnesses for being here today and I look forward to hearing your testimony, all of you.

*Chairman Johnson. And I will now recognize Mr. Larson for his opening statement.

*Mr. Larson. Well, thank you, Mr. Chairman, and let me echo your sentiments and also acknowledge that you have been a leader in the United States Congress, both in protecting the integrity of the Social Security program from fraud and abuse, and certainly, in this case, of identity theft which threatens the entire system.

As you indicated, Mr. Chairman, the recent data breach at Equifax has left more than 145 million people wondering whether they will have their identity stolen or credit damaged. Their ability to get a mortgage, a small-business loan, or even a job is at the whim of criminals, who have stolen information to wreak havoc on their financial security.

It doesn't matter if you are in Plano, Texas or you are in East Hartford, Connecticut, or whether you are 6 weeks old or 96 years old. Cyber criminals don't care. Their only interest is in profiting from your identity in a way that makes them as much money as possible. Unfortunately, Equifax is just one in a long list of data breaches where personal

information about hard-working men and women has been compromised, including Social Security numbers, which is the subject of today's hearing.

The problem of identity theft is well known and it affects our entire economy. We need to come together in a bipartisan way to strengthen privacy protections and safeguard financial security. And I thank you, Mr. Chairman, for your continued efforts in reaching out along those lines, as well.

What is clear, that all users of Social Security numbers, both government and business, need to change their ways. The widespread use of Social Security numbers as a way to both identify and authenticate individuals poses an ongoing risk of identity theft. This practice assumes that only I have access to my Social Security Number.

But given the extensive data breaches, this is no longer a safe assumption, as I believe our witnesses will all agree. There is a role here both for government and for industry.

Unfortunately, there are steep headwinds in this fight. The pace of innovation in the technologies used by cyber criminals present a very difficult and foreboding challenge. At the same time, we must be sure that the solutions to better protect personal information are accessible to all Americans, even those of us who are less adept at the new technologies.

Finally, we must keep Americans' privacy concerns in mind about how data is collected about individuals, how it is used, and who controls it. Just as we must come together to protect Americans' personal identity information, we should also come together to protect the future of Social Security itself.

I know my dear friend and colleague shares my concern in this. I think we need to have a hearing on the future of Social Security itself. We have proposed bills and legislation. It is time that we expand the most successful program in the Nation's history, knowing that as we go forward it is important to protect it at its very heart to secure it from fraud and abuse, but also to understand that this is an insurance program that needs to be made actuarially sound, that was last touched in 1983, when Ronald Reagan was President and Tip O'Neill was Speaking of the House.

It is an actuarial problem that can and should be addressed to not only protect the future of Americans, but also, as disparity grows in this great country of ours, the one thing that every single person in this Nation can count on is that Social Security has never made a payment. We have an obligation on this committee, and as Members of Congress, to make sure that the integrity of the program and also its viability goes beyond the 75-year requirement that we are sworn to serve.

And with that, Mr. Chairman, I yield back and look forward to the questions and what we are -- look forward to asking questions, and look forward to hearing from our distinguished panel.

*Chairman Johnson. Well, thank you for your comments. As is customary, any member is welcome to submit a statement for the record.

And before we move on to testimony, I want to remind our witnesses to please limit your oral statements to five minutes. However, without objection, all of the written testimony will be made a part of the hearing record.

We have seven witnesses today. Seated at the table are Nancy Berryhill, acting commissioner of Social Security Administration; Elizabeth Curda, director, education, workforce, and income security for Government Accountability Office; Samuel Lester, consumer privacy counsel, Electronic Privacy Information Center; Paul Rosenzweig -- and that is not right -- Paul --

*Mr. Rosenzweig. It is Rosenzweig, sir, but --

*Mr. Johnson. Rosenzweig?

*Mr. Rosenzweig. Yes, sir.

*Mr. Johnson. Thank you. Senior fellow, R Street Institution. Steve Grobman, senior vice president and chief technology officer, McAfee; Jeremy Grant, coordinator, Better Identity Coalition; James Lewis, senior vice president, technology policy program, Center for Strategic and International Studies.

Acting Commissioner Berryhill, please begin your testimony.

STATEMENT OF NANCY BERRYHILL, ACTING COMMISSIONER, SOCIAL SECURITY ADMINISTRATION

*Ms. Berryhill. Chairman Johnson, Ranking Member Larson, and members of the subcommittee, thank you for inviting me to discuss identity theft and the future of the Social Security number. I am Nancy Berryhill, Social Security's acting commissioner.

The scope of our programs is enormous. We pay monthly benefits to over 62 million Social Security beneficiaries and 8 million supplemental security income recipients. During fiscal year 2017 we paid about 934 billion to Social Security

beneficiaries, and 55 billion to SSI recipients. In addition, we posted 279 million earning items to workers' records last year.

The SSN underpins the programs we administer. We designated this 9-digit number in 1936 to allow employers to accurately report earnings and determine eligibility for benefits. To date we have issued around 505 million unique numbers to eligible individuals.

Although we created the Social Security number for our programs, it has become a personal identifier used most broadly across government and the private sector. For example, in 1943 the executive order required federal agencies to use the SSN. Advances in computer technology and data processing in the 1960s further increased the use of the number within federal agencies.

For example, in 1961 the Federal Civil Service Commission began using the SSN as identification number for all federal employees. The next year the IRS began using the number as a taxpayer identification number. Beginning in the 1970s, Congress enacted legislation requiring the number for a variety of federal programs. Over the decades use of the SSN grew, not just in federal government, but throughout the state and local government, banks, credit bureaus, hospitals, and other parts of the private sector.

As use of the SSN has increased, so have the opportunities for misuse. We and Congress have made changes to try to protect the integrity of the number, including strengthening the security of the SSN card, and requiring additional proofs to issue them; establishing programs and ensure accurate and timely of the SSN (sic), such as enumeration at birth, program that assigns SSNs to newborns, and verifying SSNs for federally-funded programs, employment eligibility, and other programs.

Unfortunately, SSN misuse and identify theft continues to increase. We understand the distress and economic hardship victims of identity theft face. We advise suspected victims on how to contact the Federal Trade Commission and law enforcement, and we refer cases of misuse to our office of inspector general for investigation. In certain circumstances we assign a new number to a victim of SSN misuse who has been disadvantaged due to misuse of the number.

It is important to note that assigning a new number is often a last resort, because it can cause more problems than it solves. For example, the absence of a credit history under a new number makes it more difficult to obtain credit to buy a house or a car. Nevertheless, in recognition of devastating effects identify theft can have, we continue to refine our policies in this area. Our goal is to serve the needs of the victims.

Over the years we have added flexibilities to our policies where needed, and we encourage front-line employees to coordinate with experts in our regional offices. We will continue to do what we can to mitigate the effects of SSN misuse.

We -- but we cannot alone solve the problem of over-reliance of the SSN has caused (sic). As long as the SSN remains key to assessing things of value, particularly credit, the SSN itself will have commercial value, and it will continue to be targeted by fraudsters for misuse.

Identity theft is a broad public policy issue that must be addressed. I applaud the chairman and the subcommittee for their efforts to protect the SSN, including mandating the removal of the SSN from the Medicare cards and documents mailed by federal agencies. These bills are an important step.

However, addressing identity theft requires a unified effort that includes this subcommittee and Congress, the administration, public and private experts throughout the country.

Our chief information officer, who is sitting behind me, Rajive Mathur, is here with me today. He and I look forward to hearing the ideas raised during today's hearing.

Thank you, and I will be happy to answer any questions that you may have. Thank you.

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.

*Chairman Johnson. I appreciate your testimony.

Ms. Curda, welcome again. Please proceed.

STATEMENT OF ELIZABETH CURDA, DIRECTOR, EDUCATION, WORKFORCE, AND INCOME SECURITY, GOVERNMENT ACCOUNTABILITY OFFICE

*Ms. Curda. Chairman Johnson, Ranking Member Larson, and members of the subcommittee, thank you for inviting me here to discuss GAO's observations on the extent to which the paper Social Security card is currently used, and what it costs to produce.

SSA has issued about 500 million Social Security numbers and cards since the Social Security program began in 1935. Originally, the SSN was not intended to serve as a personal identifier outside of SSA's programs. But due to its universality and uniqueness, government agencies and private-sector entities increasingly use the SSN as a convenient means of identifying people.

However, as everyday transactions are increasingly conducted electronically, it raises questions about whether a paper card is still needed or desirable to communicate or verify a person's SSN.

Today I will first discuss whether there are any federal requirements to present a Social Security card. Second, I will discuss common situations in which other public or private-sector stakeholders may ask to see the card to conduct business. And finally, I will discuss stakeholder views about the potential implications of eliminating the cards, including potential cost savings.

Although there are many federal requirements to provide an SSN, we found no statutory requirements and only two regulatory requirements to show a card. Both requirements were to verify an individual's SSN under certain narrow circumstances such as for uniformed service members seeking to change their SSNs.

To identify requirements or customary uses of the cards outside of the Federal Government we spoke to a variety of associations representing human resource managers, the finance sector, higher education institutions, and state agencies. The stakeholders we spoke with described a variety of instances in which individuals may present a card among other acceptable forms of documentation in order to verify their identity or their SSN.

For employment, all U.S. employers must verify and document a newly-hired employee's employment eligibility. Although the Social Security card is the most commonly used document for this purpose, the card is one of several acceptable documents that employees may present to prove they are eligible to work in the United States. Other examples of acceptable documents include a U.S. passport or permanent residence card, among others.

A common reason employers may ask to see a card is to verify the accuracy of the employee's SSN because employers can be fined for submitting inaccurate W-2 forms, for example.

The card is also commonly used to apply for a driver's license under the Real ID Act of 2005. The card is one of several options for documents that an applicant must provide to verity their identity.

The card may also be used as documentation when setting up financial accounts or to resolve SSN discrepancies when processing educational loans. However, providing the card is not required.

SSA and the stakeholders we interviewed also provided their perspectives on the implications of eliminating the card. One advantage of showing the card is to ensure the accuracy of the SSN, instead of relying on someone's memory. A disadvantage stakeholders cited included that the card alone is not sufficient to ensure the identity of the card holder, so other forms of identification are usually needed.

However, most of the stakeholders we interviewed indicated that their processes would not change significantly if the card were eliminated. They would continue to collect SSNs, as required, but would use other documents for identification or verification purposes, or electronically verify the SSN with SSA.

SSA officials also provided their perspective that eliminating the card may result in limited cost savings, if any. In 2016, SSA estimated that the cost to produce a card ranged from $6 for a replacement card requested online to $34 for a card requested in person at a field office. These estimates include staff time, technology, paper, printing, postage, and overhead. If the card were eliminated, only some of these costs would be saved because of the labor and other costs still needed to generate new SSNs.

A conservative estimate of the savings based on the printing, paper, and mailing costs accounts for only $.60 of the cost of the card. SSA officials stated that the agency spent about $8 million in fiscal year 2016 on paper, printing, and delivery of the cards. However, implementing a new system to replace the card could offset these savings.

Other implications of a cardless electronic system, stakeholders cited, included security and control over personal information and potential barriers for people with limited access to technology.

This concludes my prepared statement, and I would be happy to answer the committee's questions.

United States Government Accountability Office

Testimony

Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives

For Release on Delivery
Expected at 10 a.m. EDT
Thursday, May 17, 2018

SOCIAL SECURITY ADMINISTRATION

Observations on Use and Costs of Social Security Cards

Statement of Elizabeth H. Curda, Director, Education, Workforce, and Income Security

May 17, 2018

SOCIAL SECURITY ADMINISTRATION

Observations on Use and Costs of Social Security Cards

GAO Highlights

Highlights of GAO-18-507T, a testimony before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

SSA has issued about 500 million SSNs and cards since the first design of the SSN and card in 1936. SSA provides a card to each individual when it issues an SSN, as required by law, and also issues replacement cards upon request. Concerns about costs and identity security in an increasingly paperless society have raised the question of whether a paper SSN card is still needed. GAO was asked to examine the use of the card.

This testimony focuses on (1) federal requirements for individuals to present an SSN card; 2) stakeholder views on the purposes for which the cards are used; and (3) potential implications of eliminating SSN cards and developing alternative approaches.

GAO reviewed federal laws and regulations; reviewed SSA fiscal year 2016 data on card costs (the most recent year available); conducted a literature search to identify paperless identification alternatives; and interviewed SSA officials, as well as federal, state, and private sector stakeholders that may need and are legally authorized to collect an SSN. Stakeholders included associations representing state agencies, financial institutions, and human resource managers.

What GAO Recommends

GAO is not making any recommendations. DHS and SSA provided technical comments, which we incorporated as appropriate.

View GAO-18-507T. For more information, contact Elizabeth Curda at (202) 512-7215 or curdae@gao.gov.

What GAO Found

GAO identified two federal requirements for individuals to show a Social Security card. Based on a search of federal statutes and regulations, GAO did not identify any federal statutory requirements for individuals to present their Social Security card. GAO identified two federal regulations that require individuals to present their card in order to verify their Social Security number (SSN) in certain circumstances, such as when updating a service member's or dependent's SSN information in certain Department of Defense records systems.

Stakeholders we interviewed identified certain situations where, even though not required, the card is commonly used to verify identity or an SSN. For example, officials from an association representing human resource managers said the card is one option on a list of acceptable documents that employees can present to prove they are eligible to work in the United States. Financial and education association officials told GAO that they may, in rare circumstances request the card if there is a discrepancy with the SSN provided by the individual. Representatives from an association of state human services agencies also told GAO that the card is not required when applying for certain public benefit programs, such as the Supplemental Nutrition Assistance Program, although applicants may use it as a form of identification.

Organizations who use SSNs said eliminating the paper card would not change their current processes. Social Security Administration (SSA) officials and stakeholders we interviewed cited some issues to consider for use of cards and for alternative approaches, including:

- **Identity verification:** According to stakeholders, the card can help ensure an SSN is recorded accurately. However, they also noted that it is not sufficient to verify identity, and stakeholders often require electronic verification of SSNs.
- **Cost:** SSA officials said eliminating the card may result in only limited cost savings, if any, and alternatives may create new costs. In fiscal year 2016, SSA estimated that the cost to produce a card ranged from $6 to $34, depending on the mode by which the card was requested, including staff time, technology, printing, and postage. Officials said that printing and mailing account for only 60 cents of that cost. In fiscal year 2016, SSA officials stated that the agency spent about $8 million on printing and delivery of the cards. SSA officials said they have not developed cost estimates for an alternative system because the law requires SSA to issue cards.
- **Other factors:** Stakeholders also said there are other issues to consider in developing electronic approaches, including privacy, cost, and the effect on vulnerable populations, such as individuals with limited access to computers.

Several government entities, including the Department of Homeland Security (DHS) and foreign governments, have begun to use electronic methods rather than cards to authenticate individual identities. For example, one electronic method allows users to print a copy of a document that contains identity information, if needed, although the document is maintained in an electronic system.

Chairman Johnson, Ranking Member Larson, Members of the Committee:

Thank you for the opportunity to discuss our work on the use of Social Security cards. The Social Security Administration (SSA) has issued about 500 million Social Security numbers (SSN) and cards since the first design of the SSN and card in 1936. SSA provides a counterfeit-resistant paper card to each individual when it issues an SSN, as required by law, and it also issues replacement cards upon request.[1] SSNs have become a central means for establishing and confirming identity, but also can be used to perpetrate identity theft. Aside from concerns about the use and security of the SSN itself, there is interest in the cost of producing a paper Social Security card and whether the card enhances SSN security or adds to its risk.

Issues regarding identity security and cost in an increasingly paperless society have raised the question of whether a paper Social Security card is still needed. My remarks today are based on work requested by this committee. For this statement, we examined (1) the federal requirements for individuals to present their Social Security card; (2) stakeholder views on the purposes for which the cards are generally used; and (3) the potential implications of eliminating the cards, and developing alternative approaches.

For the first objective, we reviewed federal laws and regulations to identify what requirements exist for an individual to present his or her Social Security card. For the second objective, we interviewed federal, state, and private sector stakeholders that may need, and are legally authorized, to collect an SSN, in order to learn when a paper Social Security card may be requested or required by policy or practice. Stakeholders included associations representing financial and higher education institutions, human resource managers, and state agencies, such as those that administer certain human services programs. For the third objective, we reviewed SSA data on actual costs for producing and mailing Social Security cards, as well as its estimates of the per-card cost for issuing Social Security cards in fiscal year 2016 (the most recent year available). We assessed the reliability of SSA's actual cost data and estimated per card cost data by reviewing existing information about the data and the systems that produced them, and interviewing agency

[1] See 42 U.S.C. § 405(c)(2)(G).

officials knowledgeable about them. We determined that these data were sufficiently reliability for the purposes of this testimony. We conducted a literature search to identify paperless identification alternatives in use or being developed by government, both in the United States and abroad. We interviewed SSA officials regarding the production and mailing of Social Security cards. We also asked SSA officials and stakeholders about possible effects of eliminating the card.

We conducted the work on which this statement is based from October 2017 to May 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Background

In 1936, following the enactment of the Social Security Act of 1935, the newly-created Social Security Board (which later became SSA) created the 9-digit SSN to uniquely identify and determine Social Security benefit entitlement levels for U.S. workers. SSA uses a process known as "enumeration" to create and assign unique SSNs for every eligible person as part of their work and retirement benefit record.

Originally, the SSN was never intended to serve as a personal identifier outside of SSA's programs, but, due to its universality and uniqueness, government agencies and private sector entities increasingly used the SSN as a convenient means of identifying people. The expansion of government use of the SSN began with Executive Order 9397, issued by President Franklin D. Roosevelt in 1943. This required all federal agencies to use the SSN exclusively to identify individuals in their systems.[2] Since Executive Order 9397 was issued, additional federal statutes have authorized or required the collection or use of SSNs for a

[2] In 2008, Executive Order 13478 amended Executive Order 9397 to rescind the requirement for federal agencies to use SSNs exclusively.

wide variety of government activities.[3] Appendix I lists examples of such statutes.

At the inception of the program, all SSNs and cards were issued based solely on information provided by the applicant. However, in the 1970s, SSA began requiring proof of age, identity, and citizenship. According to SSA, the agency has instituted numerous evidentiary requirements to further safeguard and preserve the integrity of the SSN and to ensure issuance of SSNs and cards only to eligible individuals.

SSA reported that 16.4 million Social Security cards were issued in fiscal year 2017. This total includes 5.8 million new cards issued when someone is enumerated—issued an SSN—either at birth, upon entering the United States, or becoming a permanent resident. SSA issued 10.6 million replacement cards, many through their Internet SSN replacement card (iSSNRC) system, which allows people to order replacement cards online. By law, SSA generally must limit the number of replacement cards an individual may receive to 3 per year and 10 in a lifetime, beginning with cards issued on or after December 17, 2005.[4]

SSA issues three types of Social Security cards:

- One shows a person's name and SSN, and lets someone work without restriction; it is issued to U.S. citizens and people lawfully admitted to the United States on a permanent basis.
- A second also shows a person's name and SSN, with a note saying "Valid for work only with DHS authorization." It is issued to people lawfully admitted into the United States on a temporary basis who have Department of Homeland Security (DHS) authorization to work.
- The third has a person's name and SSN, and the note "Not valid for employment." SSA issues it to people from other countries who are lawfully admitted to the United States without work authorization from DHS, but have a valid non-work reason for needing an SSN.

[3] In recent years, there have been efforts to reduce the use and display of SSNs in government programs. For example, in April 2018, the Centers for Medicare and Medicaid Services began issuing Medicare cards that use new unique numbers in place of cardholder SSNs.

[4] See Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7213(a), 118 Stat. 3638, 3831.

While the design of original and replacement cards has been the same since 1976, SSA changed the design many times in prior decades. Counterfeit protections were first put on the card in 1983, but older versions of the card remain in circulation and are valid. As a result of the Intelligence Reform and Terrorism Prevention Act of 2004, SSA reported that it implemented additional security features in 2007 based on recommendations by an interagency task force. In the past, Congress and SSA have considered enhanced cards that were more resistant to tampering and counterfeiting. Prior GAO work found several limitations regarding the security of the Social Security card.[5] First, expertise of counterfeiters and the wide availability of state-of-the-art technology make it increasingly difficult to develop and maintain a document that cannot be counterfeited. In addition, while the employment verification process relies on a variety of documents to establish identity, the role of the Social Security card in proving authorization to work has limitations, in part because SSA did not begin requiring identification documents from all persons until 1978. Prior work also found that improvements to state drivers' licenses and identification cards, as a result of the REAL ID Act of 2005,[6] may enhance the government's ability to identify individuals and establish better links to the Social Security card and employment eligibility determinations.

[5] GAO, *Social Security Administration: Improved Agency Coordination Needed for Social Security Card Enhancement* Efforts, GAO-06-303 (Washington, D.C., Mar. 29, 2006).

[6] See Pub. L. No. 109-13, Div. B, 119 Stat. 302. The REAL ID Act sets minimum security standards for driver's license issuance and production, including procedures for states to follow when verifying the identity of license applicants, and prohibits Federal agencies from accepting for certain purposes driver's licenses not meeting these minimum standards.

GAO Identified Two Federal Requirements for Individuals to Present Their Social Security Card, and These Requirements Involve Verifying an Individual's Social Security Number

We did not identify any federal statutory requirements for individuals to present their paper Social Security card. However, we identified two federal regulations that call for individuals to present their Social Security card in order to verify their SSN in certain circumstances (see table 1). We also spoke with officials at SSA, and they said they were unaware of any federal requirements to present the paper card.

Table 1: Federal Requirements for Presentation of a Paper Social Security Card

Federal Provision	Social Security Card Requirement
32 C.F.R. § 161.23(l)	Department of Defense regulations require members of the uniformed services and their dependents seeking to change their SSN in the Defense Enrollment Eligibility Reporting System (DEERS) to provide certain documentation, including Social Security cards establishing the individual's old and new SSN.
34 C.F.R. § 681.51(b)[a]	Department of Education regulations regarding the Health Education Assistance Loan (HEAL) Program require schools to verify the information provided by students in their HEAL application, including, but not limited to, the student's citizenship status and SSN. To comply with this requirement, the school may request the student provide documentation required by the school, including a paper Social Security card.

Source: GAO review of the U.S. Code and Code of Federal Regulations. | GAO-18-507T

Note: We used a legal database and appropriate search terms to conduct a search in the U.S. Code and the Code of Federal Regulations for provisions that require individuals to present their own paper Social Security card and provisions that authorize an entity to require individuals to present their paper Social Security card. Consistent with the purpose of our search, we excluded any provisions we identified that mention a Social Security card but do not require an individual to present his or her own card. See 42 U.S.C. § 675(5)(I) and 25 C.F.R. § 20.506(h). In addition, we determined that provisions that allow individuals to present their Social Security card to verify their identity or SSN, but do not require them to do so, were outside the scope of this objective, and therefore did not include them in this table. For example, we identified two provisions that require individuals to present their Social Security card if they have it available; however, these provisions do not describe the circumstances that would make a card unavailable, and they allow individuals to provide other documentation or take other steps instead of providing the card. See 6 C.F.R. § 37.11(e) and 26 C.F.R. § 31.6011(b)-2. We did not interview relevant agency officials about the agency requirements we identified, nor did we attempt to identify and review related agency guidance or other documentation.

[a]The making of new HEAL Program loans was discontinued on September 30, 1998. See 42 U.S.C. § 292a(a). However, the reporting, notification, and recordkeeping associated with refinancing HEAL loans, servicing outstanding loans, and administering and monitoring of the HEAL Program regulations continues. In 2014, the HEAL Program and the authority to administer it were transferred from the Department of Health and Human Services (HHS) to the Department of Education. See Pub. L. No. 113-76, § 525, 128 Stat. 5, 413. Regulations promulgated by HHS in 1992 contain the same language as the Department of Education regulations. See 42 C.F.R. § 60.51(b). However, according to the Department of Education, HHS intends to remove the HEAL Program regulations from its regulations. See 82 Fed. Reg. 53,374, 53,374 (Nov. 15, 2017).

Stakeholders Reported that the Social Security Card Is One of Several Documents that May Be Used to Verify SSNs

In addition to the two requirements described above, stakeholders described instances where individuals may present a Social Security card, among other acceptable forms of documentation, in order to verify identity or their SSN.

Employers

The Social Security card is the most commonly used document to verify employment eligibility, according to officials from an association that represents human resource managers we interviewed. The Immigration Reform and Control Act of 1986 amended the Immigration and Nationality Act to require all U.S. employers to complete an employment eligibility verification (Form I-9) process to verify a newly-hired employee's identity and employment eligibility.[7] The card is one of a list of acceptable documents that employees may present to prove that they are eligible to work in the United States. Other acceptable documents include a U.S. passport or permanent residence card. Employers are required by regulation to physically examine the documentation that the individual presents to verify that the document is genuine and relates to the individual.[8]

According to DHS officials, employers may also use E-Verify, an internet-based employment eligibility system administered by U.S. Citizenship and Immigration Services (USCIS), to verify identity and employment eligibility. While all U.S. employers must have all newly-hired employees

[7] See Pub.L. 99-603, § 101(a), 100 Stat. 3359, 3360-72 (codified as amended at 8 U.S.C. § 1324a).

[8] See 8 C.F.R. § 274a.2(b)(1)(ii)(A).

fill out an I-9 form, E-Verify is optional for most employers.[9] E-Verify electronically compares information the employer enters from the Form I-9 to SSA and DHS records. While use of E-Verify does not require a card, according to a USCIS official, about 77 percent of E-Verify cases in the last 5 years used SSNs collected from cards presented for the I-9.

According to an official from an association that represents human resource managers, employers are required to complete a wage and tax statement (W-2) for every employee and provide this information to the government, in order to transmit earnings records to the employee's Social Security record. IRS guidance states that employers should examine the paper card if presented to verify that the SSN is correctly recorded on the employee's W-2. Employees are not required to present the card to verify their SSN, but employers may ask for it because they can be penalized for providing incorrect information on the W-2. In addition, according to this official, new employees have to provide their SSN to their employer, such as by providing a card, for enrollment in employee health benefits. According to another official, the Patient Protection and Affordable Care Act includes a requirement for employers to report the number of employees receiving health care, and the SSN of each employee and dependent.[10]

Financial Institutions

Representatives of financial institution associations said that although applicants for new accounts are not required to present a Social Security card, presenting the card is one way individuals can prove their identity when setting up a new account. Financial institutions may use the paper card as one of multiple forms of identification to establish a customer's identity. In addition, pursuant to provisions in the USA PATRIOT Act[11] and

[9] E-Verify is a voluntary program. However, employers with federal contracts or subcontracts that contain the Federal Acquisition Regulation E-Verify clause are required to enroll in E-Verify as a condition of federal contracting. Employers may also be required to participate in E-Verify if their states have legislation mandating its use. According to USCIS, employers who wish to employ F-1 OPT foreign students with STEM extensions and agricultural employers who would like to immediately employ a new H-2A employee already working for another employer as an H-2A in the United States must be enrolled in E-Verify. Additionally, according to USCIS, all federal departments and agencies (OMB Memo M-07-21) and in the Legislative Branch, each Member of Congress, each officer of Congress and the head of each agency of the legislative branch that conducts hiring must enroll in E-Verify.

[10] See Pub. L. No. 111-148, 124 Stat. 119 (2010).

[11] See Pub. L. No. 107-56, § 326, 115 Stat. 272, 317-18 (2001) (codified at 31 U.S.C. § 5318).

the Bank Secrecy Act[12] financial institutions are generally required to verify certain information when customers open new accounts such as date of birth, address, and identification number.[13] According to officials we interviewed from a financial association, the goal of this requirement is to prevent money laundering, fraud, and misuse of the banking system. Financial institutions may also use other government-issued documents, or non-documentary methods (such as by contacting the customer), to verify identity. Officials said that a person could still open an account or apply for a loan if he or she does not have their card as long as they have photo identification and some other government-issued documentation, such as a passport.

Educational Institutions

According to officials representing post-secondary educational institutions, students are rarely asked to present a card or even an SSN to enroll. Officials told us that the only time a school might request a paper card is to resolve discrepancies in a student's personal information, such as when the student's name and SSN on a financial aid form do not match information on other databases.

State Departments of Motor Vehicles (DMVs)

According to an official representing motor vehicle administrators, the REAL ID Act of 2005 requires DMVs to collect and verify the SSN when issuing a driver's license. A person must provide proof of his SSN or proof that he is not eligible for an SSN.[14] A stakeholder told us the most common proof provided for REAL ID purposes is the card, although other documents, such as the W-2, can be used.

Federal benefits

According to officials from an association that represents state human services agencies, while the SSN is required for certain public benefit programs such as the Supplemental Nutrition Assistance Program and Temporary Assistance for Needy Families programs, states that administer these programs do not require the paper card to determine

[12] See Pub. L. No. 91-508, 84 Stat. 1114-24 (1970) (codified as amended at 31 U.S.C. § 5311 et seq.).

[13] An identification number could be an SSN if the person has been issued one, or a Taxpayer Identification Number, which is issued by the IRS in the administration of tax laws.

[14] According to USCIS officials, Form I-9 does not require that the driver's license be REAL ID compliant when completing Form I-9. Official uses are defined as accessing federal facilities, entering nuclear power plants, and boarding federally-regulated commercial aircraft. Therefore, according to USCIS, driver's licenses that are not REAL ID compliant are acceptable for Form I-9 and E-Verify.

eligibility. According to these officials, program applicants and recipients may provide the card as a source of identification, but the SSN is verified through electronic systems. A stakeholder representing state Medicaid agencies also told us that the card is not required for Medicaid services and requesting one would, in their opinion, be a very unusual practice.

Eliminating the Card Likely Would Have a Limited Effect on Stakeholders' Processes and SSA Cost Savings, While Paperless Alternatives Raise Issues to Consider

Most Stakeholders Indicated Eliminating Cards Would Not Affect Processes

Most of the federal, state, and private sector stakeholders we interviewed who have reason to collect SSNs said their current processes would not change if the card was eliminated. For example, officials from one association we spoke with stated that without the card, individuals could continue to use the SSN and verify their identity using other government-issued documents such as a passport or driver's license.

Several stakeholders mentioned that a card can help to verify the SSN rather than accepting a person's recollection, which may be incorrect, and helps those who may not have committed it to memory. This can help ensure the SSN is recorded accurately, which can help avoid fines or time-consuming efforts to determine whether an incorrect SSN was fraudulent or simply an error. One stakeholder said that in light of recent data breaches, it could be helpful to have a physical record to show that an SSN was originally linked to the person named on the card. Another stakeholder said it can also be helpful for those who may need access to accounts of deceased family members.

Stakeholders also raised disadvantages of continued use of the card, including that the card itself is not sufficient to authenticate someone's identity. SSA officials acknowledged that the card is not an identity document; it is merely a record of the SSN issued to the person whose name is shown on the card. Even when someone presents a card, it may be difficult to determine whether the card is valid, in part because people sometimes laminate the card, which invalidates certain card security features. Stakeholders we interviewed said they need electronic verification of SSNs even when a person presents a card. SSA services

allow employers and others to determine whether an SSN matches information in SSA's records.[15] These efforts help to link the SSN to the person presenting the documents. Finally, a card can be lost or stolen, which can contribute to disclosure of the SSN and identity theft.[16]

According to SSA Officials, Eliminating the Card May Not Result in Cost Savings

SSA officials said that eliminating the card may result in only limited cost savings, if any. According to SSA officials, the costs of printing and mailing the cards are small compared to other costs associated with producing the card, and an alternative approach likely would introduce new costs that would offset any savings. They said the total cost varies by the circumstances of the card request, which can happen by: (1) visiting an SSA field office; (2) birth of a newborn; (3) admittance of a lawful permanent resident; and (4) using SSA's internet application for replacement cards. In fiscal year 2016, SSA estimated that its cost for producing a card requested at a field office was about $34, while the cost for one requested online was about $6 (see table 2). According to SSA, the agency's costs vary because SSA field offices handle the SSN application, whereas for the other methods, the application information is provided by another entity outside SSA.

[15] The Social Security Number Verification Service allows registered employers to quickly verify whether a person's name and SSN match Social Security's records, without needing the Social Security card. This service is used for wage reporting purposes only. The Consent-Based SSN Verification Service is typically used by companies that provide banking and mortgage services, process credit checks, provide background checks, and satisfy licensing requirements. This service does not verify identity, citizenship, or employment eligibility. According to SSA, which administers both services, in fiscal year 2017, these two systems received over 2.1 billion queries to verify SSNs.

[16] SSA officials said that the agency has included language in certain SSA publications to promote safeguarding the Social Security card and keeping it in a secure place to prevent identity theft. See for example, SSA, *Understanding the Benefits*, Pub. No. 05-10024.

Table 2: SSA Fiscal Year 2016 Estimated Total Cost per Social Security Card

Card request method	Cost per card	Number of cards issued
SSA Field Office	$34[a]	12,212,643
Enumeration at Birth (EAB)	$10	4,001,936
Enumeration at Entry (EAE)	$6	326,767[b]
Internet Social Security Number Replacement Card (iSSNRC) Application	$6	98,967[c]

Source: SSA data. | GAO-18-507T

[a]According to SSA officials, approximately 75 percent of all Social Security cards are requested and issued through field offices. The majority of field office requests are for replacement cards. With respect to cards issued in response to field office requests, SSA is unable to distinguish between original and replacement Social Security cards in estimating its costs.

[b] The number of cards issued for the Enumeration at Entry program includes both original and replacement cards.

[c] According to SSA officials, in FY 2016, iSSNRC was available in 14 states and the District of Columbia. As of FY 2017 it has been rolled out to an additional 10 states.

SSA's cost estimate of producing a card includes staff time devoted to taking and processing the application for the card; information technology (IT) support associated with maintaining SSN records; and the actual cost of printing, paper, and delivery of the card.[17] Agency officials said that the main portion of the cost is the staff time to interview applicants and review their documentation. Of the $34-per-card estimate for a field office, approximately $28 was attributed to operational costs, such as front-line personnel who take applications and review documentation, and associated management costs. Costs associated with IT systems used for enumeration account for another $5 of this total. This amount also includes personnel costs for staff who produce cards at SSA facilities. Postage, printing and paper costs account for only about 60 cents per card. In fiscal year 2016, SSA officials stated that the agency spent about $8 million on printing and delivery of Social Security cards.

According to agency officials, SSA is required to create and deliver the card, and therefore has not developed a formal proposal or cost estimate for eliminating the card or any replacement delivery system. However, the agency pointed out that while eliminating the card could reduce some costs, such as printing and some personnel costs, it could also create

[17] SSA estimates operational and systems costs using the agency's cost allocation methodology, while postage, printing and paper costs are actual costs incurred.

costs, depending on what alternative replaced the cards. SSA officials noted that current agency systems do not support electronic or paperless delivery of SSNs; if this type of alternative was chosen, the officials said the agency would have to design, build, and maintain a new system to support it. Officials further stated that in addition to cost considerations, SSA would need time to develop new processes. Even if no alternative replaced the card, the agency would still have to inform people of their SSNs—for example, by mailing a letter with the SSN to each person—which could also create costs. Officials said that any change is likely to result in transition costs, such as increased traffic at the SSA field offices and phone calls to customer service because people would call with questions about the change in policy.

Federal Agencies and Others Already Use Some Paperless Alternatives to Verify Identity, and Stakeholders Raised Issues to Consider in Developing Alternatives

Several government entities, including federal agencies and foreign governments, have begun to use electronic methods, rather than cards, to identify and authenticate individuals (see table 3). Although these methods apply to systems that are very different in purpose and scale to SSNs, they could provide insight into some considerations to moving to a paperless system. For example, one of these methods allows users to print a copy of the document if needed, although the document is maintained in an electronic system. Others capture biometric data, such as a fingerprint, upon enrollment that is later used to authenticate identity.

Table 3: Examples of Government-Sponsored Paperless Identity Alternatives

Agency/government entity	Purpose of program	Description
Department of Homeland Security (DHS), Customs and Border Protection (CBP), I-94	Immigration/travel	CBP issues an I-94 number to certain people legally visiting the United States. Previously, the I-94 number was provided on a hard copy form that was attached to the person's passport. Now, for entries at air and sea ports, CBP creates an electronic record, and a paper copy can be downloaded from a website if needed as proof of legal-visitor status.
DHS, CBP, Global Entry	Travel	Participants submit an on-line application and complete enrollment with an in-person appointment, which includes a background check and fingerprinting. When arriving at the airport, participants present a passport or permanent resident card and place fingerprints on a scanner for verification.
DHS, Transportation Security Administration, Pre ✓™	Travel	Participants submit an on-line application and complete enrollment with an in-person appointment, which includes a background check and fingerprinting. Accepted applicants receive a Known Traveler Number; no card is issued.
State Departments of Motor Vehicles (DMV)	Mobile identification	Some state departments of motor vehicles are piloting a Mobile Driver's License concept where driving credentials are accessed via an application on a smartphone.

Agency/government entity	Purpose of program	Description
Austria, Citizen Card	Mobile identification	Despite its name, the Citizen Card is a virtual, technology-neutral concept that can be implemented on a smart phone, smart card or other device. The user authenticates his/her identity using their chosen device and a secure Personal Identification Number.
Estonia, Mobiil-ID	Mobile identification	Estonia has created a government-issued, digital identity that allows people to use a mobile phone as a form of secure digital ID, which can be used to access government services, bank accounts, voting and other secure services.
New Zealand, RealMe®	Mobile identification	Users sign up for a RealMe account online by providing personal information such as passport and birth information. A mobile phone is used in the verification process. After the user's identity has been verified by the government, the RealMe account can be used to access government services, including registering to vote, opening a bank account, and renewing a passport.

Source: GAO analysis of literature search results and stakeholder interviews. | GAO-18-507T

Note: We conducted a literature search to identify paperless identification alternatives in use or being developed by government, both in the United States and abroad. To describe the programs used abroad, we relied exclusively on secondary materials and did not do any independent legal research.

Stakeholders we spoke with provided general views on cardless systems that can electronically authenticate an individual's identity. They suggested a variety of issues that should be considered in developing any such electronic approach:

- Vulnerability of such a system to data breaches;
- Privacy considerations (i.e., control over personal information);
- The need for strong authentication systems;
- Acceptance by federal regulators (for example, related to oversight of financial institutions or federal financial aid);
- Costs of implementation for institutions and individuals; and
- Effect on vulnerable populations, such as those with limited access to electronic technology.

SSA officials also noted several issues that would need to be considered in developing an alternative to the current card. While SSA officials indicated that the agency continues to look for ways to reduce external reliance on cards, they noted that any alternative must be as secure as the current Social Security card and processes. In particular, an SSA official said that SSA and the U.S. Postal Service have protocols in place so that Social Security cards are delivered to the intended recipients, and

that they get returned if they cannot be delivered to a secure location.[18] Further, SSA officials stated they were unsure about potential effects on fraud and identity theft if paper cards were no longer used, and they stated that an electronic system would need to address concerns about personally identifiable information and security.

Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee, this concludes my prepared statement. I will be pleased to answer any questions that you or other members of the subcommittee may have.

GAO Contact and Staff Acknowledgments

For future contact regarding this testimony, please contact Elizabeth Curda at (202) 512-7215 or curdae@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Key contributors to this testimony were Mark Glickman (Assistant Director), Dana Hopings, and Vernette Shaw. In addition, key support was provided by John de Ferrari, Holly Dye, David Forgosh, Rebecca Gambler, Sarah Gilliland, Gina Hoover, Lawrence Malenich, Sheila McCoy, Almeta Spencer, and Adam Wendel.

[18] SSA Office of Inspector General (OIG) found in 2018 that about 360,000 undeliverable Social Security cards are returned to SSA each year, and that about 150,000 of these cards could have been delivered to the correct address had there been a process in place to validate the address. See SSA OIG, *Undeliverable Social Security Number Cards (Limited Distribution),* A-15-17-50279 (Baltimore, Md.: April 2, 2018).

Appendix I: Examples of Federal Statutes that Authorize or Require the Collection or Use of Social Security Numbers (SSNs)

Federal statute	Government entity and authorized or required use
7 U.S.C. § 2025(e)	Requires the Secretary of Agriculture and state agencies to require SSNs for participation in the Supplemental Nutrition Assistance Program.
20 U.S.C. § 1090(a)(12)	Authorizes the Secretary of Education to include the SSNs of parents of dependent students on certain financial assistance forms.
26 U.S.C. § 6109(d)	Authorizes the Commissioner of the Internal Revenue Service to require that taxpayers include their SSNs on tax returns.
42 U.S.C. § 405(c)(2)(C)(i)	Authorizes states to collect and use SSNs in administering any tax, general public assistance, driver's license, or motor vehicle registration law.
42 U.S.C. § 405(c)(2)(C)(ii)	Requires states to obtain parent's SSNs before issuing a birth certificate unless there is good cause for not requiring the number.
42 U.S.C. § 405(c)(2)(C)(iii)	Authorizes the Secretary of Agriculture to require the SSNs of officers or owners of retail and wholesale food concerns that accept and redeem food stamps.
42 U.S.C. § 405(c)(2)(D)(i)	Authorizes states and political subdivisions to require that blood donors provide their SSNs.
42 U.S.C. § 405(c)(2)(E)	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors.
42 U.S.C. § 666(a)(13)	Requires states to include SSNs on applications for driver's licenses and other licenses; on records relating to divorce decrees, child support orders, or paternity determinations; and on death records.
42 U.S.C. § 1320b-7(a) (1)	Requires that, as a condition of eligibility for certain program benefits, including Medicaid benefits, applicants for and recipients of these benefits furnish their SSNs to the state administering program.
42 U.S.C. § 3543(a)	Authorizes the Secretary of the Department of Housing and Urban Development to require program applicants and participants to submit their SSNs as a condition of eligibility for housing assistance.

Source: GAO-17-553 | GAO-18-507T

*Chairman Johnson. Thank you. I appreciate your testimony.

Mr. Lester, welcome. Please go ahead.

STATEMENT OF SAMUEL LESTER, CONSUMER PRIVACY COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER

*Mr. Lester. Chairman Johnson, Ranking Member Larson, members of the subcommittee, thank you for the opportunity to testify today. My name is Sam Lester. I am the consumer privacy counsel at the Electronic Privacy Information Center. EPIC is an independent, non-profit research organization here in Washington, D.C. established in 1994 to focus public attention on emerging privacy and civil liberties issues.

I appreciate your interest in this critical topic. I cannot overstate the urgency that we update our privacy laws. There is no other form of personal information that poses a greater threat to privacy than the Social Security number. The recent Equifax breach exposed the Social Security numbers of over half of the U.S. adult population.

The SSN was never meant to be an all-purpose identifier in the private sector. When it was first introduced in 1936 it was to be used only for the administration of Social Security taxes. The fact that it is now so pervasive as both an identifier and authenticator, a user name and a password, has undoubtedly contributed to the alarming rise in data breaches, identity theft, and financial fraud.

SSNs are the keys to the kingdom for identity thieves. A criminal in possession of your SSN can file fraudulent taxes in your name, open new accounts in your name, take out lines of credit, and many other forms of fraud.

If you are about to buy a home, for instance, you could experience your worst nightmare when a lender pulls your credit and sees that your FICA score is too low to qualify for a loan because someone has fraudulently run up debt in your name. For someone who has experienced new account fraud, it can take years to recover, financially.

In 2017 identity theft impacted almost 17 million consumers. More importantly, consumers cannot protect themselves from the misuse of the SSN. As others have stressed, the Social Security Administration will only replace your SSN in the most extreme circumstances.

And furthermore, the credit reporting industry makes it even more difficult for consumers. A credit freeze is burdensome and costly, and credit monitoring and fraud alert services do not adequately protect consumers. The CEO of LifeLock had his identity stolen 13 times after he displayed his real Social Security number in a commercial that was supposed to demonstrate how effective his product was at preventing identity theft.

There have been recent efforts to limit the use of the SSN, but much more needs to be done. For example, in 2017 Medicare finally announced it would remove SSNs from cards, the result of an effort led by Chairman Johnson and Representative Doggett of this committee.

Also, a number of states have taken steps in the right direction. For instance, Alaska now prohibits the use of SSNs by both private companies and the government without explicit legal authorization. This would be a good model for federal legislation, and also shows why federal law should not prevent states from enacting their own safeguards.

To limit the devastating financial harm caused by the misuse of the SSN, Congress should take the following measures.

First, the SSN should be prohibited in the private sector without explicit legal authorization, and companies should be prohibited from compelling consumers to disclose their SSN as a condition of sale or service unless authorized by law.

Second, Congress should promote the development of context-specific identifiers. For example, if you are going to do banking, you have a bank account number. If you are obtaining a driver's license, you have a driver's license number. The advantage of these context-specific identifiers is that if one number gets compromised, an identity thief does not have access to all your accounts.

Finally, Congress must not replace the SSN with a national biometric identifier. This would be a very bad idea. This approach would pose serious privacy and security risks. In the massive breach of the Office of Personnel Management in 2015, foreign hackers targeted digitized fingerprints stored in federal databases. These risks would only be compounded if the U.S. were to move towards a national biometric identifier.

Thank you for the opportunity to testify today, and I will be happy to answer your questions.

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Sam Lester, EPIC Consumer Privacy Counsel
Electronic Privacy Information Center

Hearing on "Securing Americans' Identities: The Future of the Social Security Number"

Before the

House Committee on Ways and Means
Subcommittee on Social Security

May 17, 2018
1100 Longworth House Office Building
Washington, DC, 20002

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today on securing Americans' identities: the future of the Social Security Number ("SSN"). My name is Sam Lester. I am the Consumer Privacy Counsel at the Electronic Privacy Information Center ("EPIC"). EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has urged Congress to establish privacy safeguards for the SSN for two decades.[1] EPIC has also participated in leading cases involving the privacy of the SSN and maintains an archive of information about the SSN online.[2]

It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of personal identification that poses a greater risk to privacy. The recent Equifax data breach exposed the SSNs of almost half of the U.S. population. The SSN was never meant to be an all-purpose identifier. The fact that the SSN is now so pervasive as both an identifier and an authenticator in both the public and private sector has undoubtedly contributed to the alarming rise in data breaches, identity theft, and financial fraud.

In my testimony today, I will outline the steps Congress can take to protect the privacy of the SSN. Congress should (1) prohibit the use of the SSN in the private sector without explicit legal authorization; (2) prohibit companies from compelling consumers to disclose their SSN as a condition of service or sale unless there is a statutory basis for the request; and (3) promote technological innovations that enable the development of context specific identifiers. Congress should *not*, however, replace the SSN with a national biometric identifier, which would raise serious privacy and security risks.

I. Original purpose of the SSN and the dangers of a national identification number

A. The SSN was never meant to be an all-purpose identifier or to be used in the private sector

Social Security Numbers are a classic example of "mission creep," where a program with a specific, limited purpose is transformed for additional, unintended purposes, often with disastrous results. When the SSN was first introduced in 1936, it was to be used only as a means

---

[1] *See*, *e.g.*, *Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough*: *Hearing Before the S. Special Comm. on Aging*, 114th Cong. (Oct. 7, 2015) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf; *Protecting the Privacy of the Social Security Number from Identity Theft*: *Hearing Before the H. Ways & Means Subcom. on Social Security*, 110th Cong. (Jun. 21, 2007) (statement of Marc Rotenberg), https://epic.org/privacy/ssn/idtheft_test_062107.pdf; *Social Security Numbers & Identity Theft*: *Joint Hearing Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001) (statement of Marc Rotenberg), http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; *Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves*: *Joint Hearing Before the H. Ways & Means Subcom. on Social Security & the H. Judiciary Subcom. on Immigration, Border Sec. & Claims*, 105th Cong. (Sept. 19, 2002) (statement of Chris Jay Hoofnagle, EPIC), http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[2] *See, e.g., Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994); EPIC, Social Security Numbers, https://epic.org/privacy/ssn/.

of tracking earnings to determine the amount of social security taxes to credit each worker's account. At the time, public concern over potential abuse of the SSN was so high that the Social Security board had to reassure Americans that it was for the exclusive use of the Social Security system. Over time, however, Congress allowed SSNs to be used for purposes unrelated to the administration of the Social Security system. In 1961, Congress authorized the IRS to use SSNs as taxpayer identification numbers.[3] In the 1980s, Congress passed a series of bills authorizing the SSN for purposes such as opening an interest-bearing account, cash transactions over $10,000, and applying for numerous types of federal benefits.[4]

Congress attempted to rein in the widespread use of the SSN with the Privacy Act of 1974. A landmark 1973 report on privacy prepared by Willis Ware and the Department of Health, Education and Welfare ("HEW") described how the increasing use of the SSN in the private sector was promoting invasive profiling, and recommended legislation "prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes."

The HEW report laid the groundwork for the Privacy Act.[5] Specifically, Section 7 of the Privacy Act provides:

> (a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number
>
> (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it. [6]

This provision is critical to keep in mind today, because consumers are so often compelled to disclose their SSN to obtain a product or service.

As originally conceived, the Privacy Act would have applied to both the public and private sector. However, negotiations with the White House led to the removal of provisions that

---

[3] Pub. L. No. 87-397, 75 Stat. 828 (codified as amended at 26 U.S.C. §§ 6113, 6676).
[4] *See*, Carolyn Puckett, *The Story of the Social Security Number*, Soc. Sec. Bulletin, Vol. 69, No. 2, Soc. Sec. Admin., (2009), https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.
[5] Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 125-35 (MIT 1973), *available at* http://www.epic.org/privacy/hew1973report/.
[6] Pub. L. No. 93-579, 7. This provision of the Privacy Act was never codified, but is instead set out as a historical note to 5 U.S.C.A § 552(a) (2016).

covered the private sector.[7] As a consequence, the SSN has been allowed to proliferate as an all-purpose identifier in the private sector.

B. EPIC has repeatedly urged Congress to restrict the use of the SSN in the private sector

In 2007, EPIC testified before this Committee on how the proliferation of the SSN in the private sector has exposed consumers to unprecedented risks. We said:

> [T]he reality is that today the SSN is the key to some of our most sensitive and personal information. The financial services sector, for instance, has created a system of files, keyed to individuals' SSNs, containing personal and financial information on nearly 90 percent of the American adult population. This information is sold and traded freely, with virtually no legal limitations. In addition, credit grantors rely upon the SSN to authenticate a credit applicant's identity.[8]

In October 2017, EPIC testified before the Senate Banking Committee following the Equifax breach. We again emphasized how "the unregulated use of the social security number in the private sector has contributed to record levels of identity theft and fraud" and again urged Congress to restrict its use.[9] Earlier this year, EPIC reinforced the urgency of legislation to limit the use of the SSN in testimony before the House Financial Services Committee, explaining, "the more the SSN is used, the more insecure it becomes."[10]

II. Consumers face an epidemic of data breach, identity theft and financial fraud as a result of the pervasive use of the SSN in the private sector

The ubiquity of the SSN in the private sector has created unprecedented risks for consumers. Incidents of data breach continue to rise in the United States, and the prevalence of the SSN in consumer databases undoubtedly contributes to this alarming epidemic. Last year was again the worst year ever for data breaches, as the number of breaches almost doubled from

---

[7] EPIC, *The Privacy Act of 1974*, https://epic.org/privacy/1974act/; Robert Ellis Smith, *Gerald Ford: Privacy's Godfather*, Forbes (Jan. 5, 2017), https://www.forbes.com/2007/01/04/privacy-protection-ford-oped-cx_res_0105privacy.html.

[8] *Id*.

[9] *Consumer Data Security and the Credit Bureaus*: *Hearing Before the S. Comm. on Baking, Housing, and Urban Affairs*, 115th Cong., (Oct. 17, 2017), (statement of Marc Rotenberg, EPIC), https://epic.org/privacy/testimony/EPIC-Testimony-SBC-10-17.pdf.

[10] *Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing Before the S. Comm. on Financial Services*, 115th Cong. (Feb. 14, 2018) (statement of Marc Rotenberg, EPIC), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf.

2016.[11] 73% of all U.S. companies have now been breached.[12] As a consequence, identity fraud reached an all-time high in 2017, with 16.7 million victims and a total of $16.8 billion stolen.[13]

A. SSNs are the most valuable piece of personal data for identity thieves

SSNs are the "keys to the kingdom" for identity thieves.[14] The SSN is so valuable because it can be used to open new accounts without any other identifying information. Many retailers and banks will extend offers of credit to individuals with an SSN attached to a good credit score, even if the names do not match.[15] Those whose SSNs have been breached are more than six times as likely to suffer new account fraud.[16]

This is particularly important in light of the Equifax breach, in which almost half of all Americans had their SSN stolen. In a recent SEC filing, Equifax provided the most detailed analysis to date of the information that was stolen.[17] Of the 146.6 million victims, 145.5 million had their SSN stolen.[18] Compare that with only 20.3 million who had their phone number stolen, 17.6 million who had their driver's license number stolen, and 1.8 million who had their email address stolen.[19]

Criminals in possession of SSNs can completely derail a person's financial future. The Bureau of Justice Statistics reported that "[v]ictims experiencing the opening of a new account or the misuse of personal information had greater [out-of-pocket] loss than those experiencing misuse of an existing credit card or bank account."[20] The IRS estimates that it paid out $3.1 billion in fraudulent tax refunds for the 2014 filing season.[21] A criminal in possession of your stolen SSN can:

---

[11] Online Trust Alliance, *Cyber Incident and Breach Trend Report*, (Jan. 25, 2018), https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.
[12] *Id*.
[13] Javelin, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study*, (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.
[14] Fed. Trade Comm'n., *Security in Numbers: SSNs and ID Theft* 2 (Dec. 2008), https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf.
[15] Bob Sullivan, *Your Social Security Number Isn't a Secret*, N.Y. Times (Sept. 13, 2017), https://www.nytimes.com/2017/09/13/opinion/your-social-security-number-isnt-a-secret.htm.
[16] Identity Theft Resource Center, *New Account Fraud—A Growing Trend in Identity Theft* at 3 (November 2016), https://www.idtheftcenter.org/images/page-docs/NewAccountFraud.pdf.
[17] Brian Fung, *145 Million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers*, Washington Post, (May 8, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/.
[18] *Id*.
[19] *Id*.
[20] Erika Harrell, *Victims of Identity Theft, 2014*, Bureau of Justice Statistics, (revised Nov. 14, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[21] U.S. Gov't Accountability Office, GAO-16-589T, *IRS Needs to Further Improve Controls Over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud* 1–2 (2016), https://www.gao.gov/assets/680/676493.pdf.

- File fraudulent tax returns in your name
- Open new accounts in your name
- Take out lines of credit in your name
- Receive unemployment, food stamps and Social Security benefits in your name
- Apply for student loans, obtain driver's licenses and passports in your name

For example, a retired certified public accountant in Colorado received a Form SSA-1099 for $19,236 in Social Security benefits earlier this year, even though he had never applied for benefits.[22] A home buyer can experience their worst nightmare when a lender pulls their credit to discover that their FICO score is too low to qualify for a loan because someone has fraudulently run up debt in their name.[23] It can take years for individuals who have experienced new account fraud to recover financially.[24]

SSNs are routinely bought and sold on the black market. These illicit marketplaces are "growing in size and complexity" and are now dominated by "financially driven, highly organized and sophisticated groups."[25] Complete dossiers of personal data that contain SSNs—referred to as "fullz"—are sold in bulk for as little as $15 per victim, demonstrating how inexpensive it can be to commit identity theft, yet how lucrative it can be for a hacker who has stolen data on millions of individuals.[26]

Children in particular are targets for identity theft and fraud using their SSN because they do not have a credit history. Among the notified breach victims in 2017, 39 percent of minors were victims of fraud compared with 19 percent of adults.[27] Earlier this year, employees at the cybersecurity firm Terbium Labs spotted a set of stolen data—titled "infant fullz"—that contained a baby's full name, SSN, date of birth and mother's maiden name. The listing price was $312—significantly more than the $5 requested for similar bundles of information for adults.[28]

---

[22] Susan Tompor, *Social Security Benefits Stolen By Hackers, Leaving Families With Bill*, Detroit Free Press (Feb. 28, 2018), https://www.freep.com/story/money/personal-finance/susan-tompor/2018/02/28/identity-theft-crooks-steal-social-security-benefits/354307002/.
[23] Kenneth R. Harney, *Theft of Equifax data could lead to years of grief for home buyers and mortgage applicants*, Washington Post, (Sept. 13, 2017), https://www.washingtonpost.com/realestate/theft-of-data-could-lead-to-years-of-grief-for-home-buyers-and-mortgage-applicants/2017/09/12/ed0f66fc-971a-11e7-82e4-f1076f6d6152_story.html.
[24] *Id*.
[25] Lillian Ablon, Martin C. Libicki, & Andrea A. Golayix, RAND Corp., *Markets for Cybercrime Tools and Stolen Data*, at ix (2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
[26] Dell SecureWorks, *Underground Hacker Markets* 14 (2016), https://www.secureworks.com/resources/rp-2016-underground-hacker-.
[27] Kelli B. Grant, *Identity theft isn't just an adult problem. Kids are victims, too*, CNBC, (Apr. 24, 2018), https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html.
[28] Bree Fowler, *Why Child Identity Theft Is a Growing Concern During Tax Season*, Consumer Reports, (Apr. 12, 2018), https://www.consumerreports.org/identity-theft/why-child-identity-theft-is-a-growing-concern-during-tax-season/.

B. Consumers cannot protect themselves from the misuse of their SSN

The SSN is so coveted by identity thieves because, unlike a credit card number, it is almost impossible to change. In 2014, the Social Security Administration replaced only 250 SSNs due to identity theft or misuse.[29] The SSA will only replace an individual's SSN in the most extreme circumstances, such as "harassment, abuse, or life endangerment."[30] Even then, the SSA will only assign you a new number if "you've done all you can to fix the problems resulting from misuse of your SSN, and someone is still using your number."[31]

The credit reporting industry also makes it difficult for consumers to protect themselves. Credit freezes are burdensome and costly. Consumers wishing to freeze their credit must contact all three credit bureaus and pay a fee to each company every time they freeze and unfreeze their credit. Credit monitoring and fraud alerts are far less effective, and do not prevent thieves from accessing credit files or opening new accounts. The CEO of LifeLock had his identity stolen 13 times after he displayed his real SSN in a commercial that was supposed to demonstrate how effective his product was at preventing identity theft.[32]

III. There have been recent efforts to limit the use of the SSN, but much more needs to be done

In 2015, we explained to the Senate Special Committee on Aging that identity theft disproportionately targets seniors.[33] In 2017, Medicare finally announced that it would remove SSNs from Medicare benefits cards, the result of an effort led by Senators Susan Collins and Claire McCaskill.[34] And the Social Security Number Fraud Prevention Act of 2017, sponsored by Representative David Valadao of this Committee, prohibits federal agencies from including anyone's SSN on any document sent by mail unless authorized by law.[35]

---

[29] Aarti Shahani, *Theft of Social Security Numbers is Broader Than You Might Think*, NPR, (Jun. 15, 2015), https://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think.

[30] Soc. Sec. Admin., *Can I Change My Social Security Number?* (Mar. 11, 2016), https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-.

[31] Soc. Sec. Admin., *Identity Theft and Your Social Security Number* 6 (Feb. 2016), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[32] Kim Zetter, *LifeLock CEO's Identity Stolen 13 Times*, Wired (May 18, 2010), https://www.wired.com/2010/05/lifelock-identity-theft/.

[33] *Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough*: *Hearing Before the S. Special Comm. on Aging*, 114th Cong. (Oct. 7, 2015) (statement of Marc Rotenberg, EPIC), https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf.

[34] EPIC, *Medicare to Remove SSN from ID Cards*, (Sep. 5, 2017), https://epic.org/2017/09/medicare-to-remove-ssn-from-id.html.

[35] Pub. L. No. 115-59, 131 Stat. 1152 (2017).

In addition, a number of state laws limit the use of the SSN in higher education,[36] by private businesses,[37] by state agencies,[38] and financial institutions.[39] For example, Arizona prohibits state universities and community colleges from using the SSN as an ID number.[40] Rhode Island prohibits businesses from requiring consumers to disclose all or part of their SSN to purchase most goods or services.[41] A number of states prohibit private insurers from printing SSNs on identification cards.

Many private organizations have also curtailed or eliminated the use of the SSN. Georgetown University prohibits use of the SSN "as the primary record key, or sort key, in any University database or other business system or operation."[42] In lieu of SSNs, Georgetown uses the "Georgetown University ID," a "nine digit number beginning with the numeral 8" listed on each person's GU identification card.[43] And nearly a decade ago, the Blue Cross Blue Shield Association mandated that its members replace SSNs with Subscriber ID numbers.[44]

IV. Solutions to prevent misuse of SSNs and protect consumers

There is widespread support for legislation limiting the use of the SSN. According to a Pew Research Report, 90% of adults said they were "very sensitive" about their SSN, the highest percentage for any form of personal data.[45] Pew Research Center also found that 91% of consumers say they have lost control over how their personal information is collected, and 64% support greater regulation over how companies handle their personal information.[46] Even leading CEOs now support stronger privacy protections in the United States. Congress should adopt the following measures to limit the use of the SSN and protect consumers from identity theft and financial fraud:

- **Prohibit the use of the SSN in the private sector without explicit legal authorization**. While an employer should be permitted to ask an employee for an SSN for tax-reporting purposes, a health club should not be permitted to ask a customer for an SSN as a condition of membership. Even if a service is not conditional on someone providing their

---

[36] *See e.g.* N.Y. Educ. Code sec. 2-b; W. Va. Code Ann. sec. 18-2-5f; Ariz. Rev. Stat. Sec. 15-1823.
[37] *See e.g.* R.I. Gen. Laws 6-13-17; Vt. Stat. Ann. tit. 9, § 2440; N.C. Gen. Stat. § 75-62.
[38] *See e.g.* Ala. Code sec. 41-13-6; Cal. Civ. Code sec. 1798.85.
[39] *See e.g.* Mass. Gen. Laws. Ann. ch. 167B, sec. 14.
[40] Ariz. Rev. Stat. Sec. 15-1823.
[41] R.I. Gen. Laws 6-13-17.
[42] Georgetown University Information Security Office, *Policy on the Use, Collection, and Retention of Social Security Numbers by Georgetown University*, https://security.georgetown.edu/it-policies-procedures/use-collection-retention-policy#.
[43] *Id*.
[44] *Empire Physician Sourcebook*, EMPIRE BLUE CROSS BLUE SHIELD, https://www11.empireblue.com/provider/noapplication/f4/s2/t0/.
[45] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 14, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.
[46] George Gao, Mary Madden, *Privacy and Cybersecurity: Key Findings From Pew Research*, Pew Research Center, (Jan. 16, 2015), http://www.pewresearch.org/fact-tank/2015/01/16/privacy/.

SSN, having that field on a form causes many people to provide it anyway, assuming it is required.

- **Prohibit companies from compelling consumers to disclose their SSN as a condition of service or sale unless there is a statutory basis for the request**. Representative Patrick McHenry has proposed the PROTECT Act of 2017, which would prohibit consumer reporting agencies from using a consumer's SSN as a method to identify the consumer.[47] Congress should go much further, however, and prohibit its use for all commercial transactions unless the use is explicitly authorized by statute.

- **Promote technological innovations that enable development of context-specific identifiers**. A system of decentralized identification reduces the risks associated with data breaches and the misuse of personal information. Such a decentralized approach is consistent with our commonsense understanding of identification. If you're going to do banking, you should have a bank account number. If you're going to the library, you should have a library card number. Utility bills, telephone bills, insurance, the list goes on. An example of this approach is the Medical Identification Number used in Canada. These context-dependent usernames and passwords enable authentication without the risks of a universal identification system. That way, if one number gets compromised, all your other numbers are not spoiled, and identity thieves cannot access all your accounts. All of your accounts become compartmentalized, enhancing their security.

- **Do not replace the SSN with a national biometric identifier**. There have been proposals recently to replace the SSN with a national biometric "identity framework," with fingerprints and facial recognition.[48] This is the wrong solution and would raise serious privacy and security risks. In passing the Privacy Act of 1974, Congress was specifically reacting to and rejecting calls for the creation of a single entity for the reference and storage of personal information. There are also significant problems that would arise with the breach of a biometric identifier. In fact, in the massive OPM data breach, foreign hackers targeted the digitized fingerprints stored in federal databases.[49] That risk would be compounded if the US were to move to a national biometric identification system.

Conclusion

There is little dispute that identity theft is one of the greatest concerns for consumers in the United States today. There are many factors that have contributed to this problem, but the

---

[47] H.R. 4028, 115th Cong. (2017).

[48] *See*, *e.g.*, *Protecting Consumers in the Era of Major Data Breaches*: *Hearing Before the S. Comm. on Commerce, Science and Transportation*, 115th Cong. (Nov. 8, 2017), (statement of Todd Wilkinson, President and CEO, Entrust Datacard), https://www.commerce.senate.gov/public/_cache/files/9348f11b-49a4-4c47-922e-f5cc98d61b54/469C33D81041FAB151DC6B1E6608A18B.11.08.2017---wilkinson-testimony.pdf.

[49] David E. Sanger, *Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says*, N.Y. Times, (Sept. 23, 2015), https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html.

widespread use of the SSN in the private sector and the failure to establish privacy safeguards are key parts of the problem. It is time that Congress passed strong and effective legislation that will limit the use of the SSN, encourage the development of more robust systems for identification that safeguard privacy and security, and not limit the ability of states to develop better safeguards. Congress must not, however, replace the SSN with a new national identification system.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

*Chairman Johnson. Thank you, sir. I appreciate your testimony, as well.

Mr. Rosenzweig?

*Mr. Rosenzweig. Thank you very much.

*Chairman Johnson. Is that the right pronunciation?

*Mr. Rosenzweig. Rosenzweig, but --

*Chairman Johnson. Weig, okay.

*Mr. Rosenzweig. Thank you very much.

*Chairman Johnson. Pardon me. Well, please proceed.

STATEMENT OF PAUL ROSENZWEIG, SENIOR FELLOW, R STREET INSTITUTE

*Mr. Rosenzweig. Thank you very much, Chairman Johnson, Ranking Member Larson, members of the subcommittee. I too am pleased to be able to speak with you today about the future of the Social Security number.

The Social Security number has a long history of utility as an identifier. I don't think that is the problem. The use of it as an identifier is no different than the use of my phone number as an identifier or the use of my name as an identifier. The problem is that the Social Security number has mutated in its use, so it is now also an authenticator of my identity.

Authenticators are classically only useful if they involve something that you know exclusively, something you have, or something you are, and they are kept confidential. Today Social Security numbers are so deeply compromised and so widely available in public -- albeit often through criminal means -- that they can no longer be used as an authenticator. This is because recent incidents like the Equifax breach that we have already spoken of, and whose anniversary occurs this week, have effectively disclosed the vast majority of previously confidential Social Security numbers. My own Social Security number, to my knowledge, has been breached at least three times in the past four years. So I feel this quite personally.

As a result, in my view, any enterprise that continues to use a Social Security number as an authenticator is engaging in borderline privacy and security malpractice. Yet some do. Just the other day I was shocked that a bar renewal membership used my -- the last four of my Social Security as a way of authenticating my identity. And this was a governmental use.

So what should we do about that? What should we do in response to the problem? In my judgement, Congress has three logical options.

The first is to, as Mr. Lester has just suggested, regulate or outlaw Social Security numbers. That is a plausible solution, but one that I respectfully think is not appropriate. That comes with all the usual disadvantages of government intervention: regulatory gridlock, administrative costs, enforcement mechanisms that are necessary, along with procedural safeguards, as well.

In short, I think a regulatory response will come with a great deal of expense and be a relatively slow result, perhaps even no quicker than the next solution, which is to do nothing.

In a lot of ways, the market is addressing this problem. The disutility of SSNs as an authenticator has become widely known and is increasingly on the decline (sic). Eventually, the market will take care of the problem. The problem with that answer, of course, is that before it does, a great number of Americans will suffer from data breach and identity theft. So I think that is a second-best solution.

The best solution, in my judgement -- and one of the joys of being in a think tank is your ability to think creatively about problems and think outside the box -- is to eliminate the utility of the Social Security number as an authenticator. Make it impossible, in practice, for anyone to continue to use it in this way.

One simple and quite elegant solution that I offer both as a thought experiment and also as a possible practical solution is to simply publish a phone book with every citizen's Social Security number in it. In other words, by publishing it publicly, we would make it impossible for any enterprise to continue to legitimately use it as an authenticator of identity. To continue to do so after that and after a suitable transition time would, in my judgement, be per se negligence of the sort that ought to involve liability for the enterprise.

One final point that I would make. Congress needs to look to its own house. Repeatedly in law we have mandated the collection of Social Security numbers as identifiers, and sometimes continued to use them as authenticators, as my colleague has already testified to. At a minimum, I think it is incumbent upon Congress to review government's use of the Social Security number and its processes, if only so that by cleaning up our own house we can speak to the private sector with authority.

I thank you for the opportunity to testify before you, and I look forward to the chance to answer questions.

STATEMENT

of

Paul Rosenzweig
Senior Fellow, R Street Institute
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Washington, D.C.

before the

Subcommittee on Social Security
Committee on Ways and Means
United States House of Representatives

May 17, 2018

The Future of the Social Security Number

Introduction

Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee, I thank you for your invitation to appear today and present testimony on the question of data security and the use of Social Security Numbers (SSNs). My name is Paul Rosenzweig and I am a Senior Fellow at the R Street Institute.[1] I am also the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice; a Senior Advisor to The Chertoff Group and a Professorial Lecturer in Law at George Washington University, where I teach a course on Cybersecurity Law and Policy and another on Artificial Intelligence Law and Policy. From 2005 to 2009, I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

[1] The R Street Institute is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work. Information about our funding is available at: http://www.rstreet.org/about-rstreet/funding-and-expenditures. My Truth in Testimony Disclosure accompanies this testimony.

Members of R Street testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for the R Street Institute or its board of trustees. I thank my colleagues at R Street for their research assistance and for helpful comments on an earlier draft of this testimony.

My testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients.

In my testimony today, I want to make a few points, which I can summarize as follows:

- The Social Security Number has a long history of utility as an identifier. Over time, however, the use case for SSNs has mutated so that now it is frequently used both as an identifier and as an authenticator.
- Authenticators of identity only have utility to the extent they rely on confidential, non-public information. This is classically defined as something you know, something you have or something you are. Initially SSNs appeared to be a suitable authenticator since they were non-public information that only a Social Security recipient would know.
- Today, however, SSNs are so deeply compromised and so widely available to the public (albeit, often through criminal settings) that they can no longer be used as an authenticator. This is because recent incidents, such as the Equifax breach (the anniversary of which occurs this week), have effectively disclosed the vast majority of previously confidential SSNs.
- As a result, any enterprise that continues to use an SSN as an authenticator is engaging in borderline cybersecurity malpractice. Yet, some do. Just the other day, for example, the last-four digits of my own SSN were used to verify my identity when I went to renew my Bar membership.
- In my view, Congress has the following three options for dealing with this problem. They range from worst to best.
    - Regulate or outlaw the use of SSNs. This is a plausible solution but one that comes with all of the usual disadvantages of government intervention: regulatory gridlock, administrative costs, and enforcement systems that necessitate procedural safeguards. In short, a regulatory response would come at great expense with a slow result, perhaps even no quicker than doing nothing.
    - Do nothing. The disutility of the SSN as an authenticator continues to become widely apparent. Eventually, the market will take care of the problem, but not before many more Americans suffer from data breach and identity theft.
    - Eliminate the utility of the SSN as an authenticator. Make it impossible, in practice, for anyone to continue to use it in this way. One simple, indeed quite elegant, solution (that I offer as both a thought experiment and as a possible practical answer) is to simply publish a phone book with the name and SSN of every citizen. In other words, make it clear that SSNs cannot be used as authenticators by making them radically publicly available.

A Short History of SSNs

Starting in 1936, most workers were required to participate in the Social Security program. As a result, the government needed a system to track all the participants. While the Social Security Act of 1935 did

not specifically call for a numbering system, it did require the federal government to create a tracking method for record purposes.[2]

Many ideas were considered, including the use of participants' names and addresses or a fingerprint system similar to what some federal agencies already had in place. Name identification proved unwieldy and ineffective.[3] And even though fingerprinting had a proven track record in the federal government, the public had an unfavorable view of the association between fingerprints and criminal activity. Fearing a backlash, the Social Security Administration (SSA) settled on the numbering system we use today.

SSNs were never designed for or intended to be national identification numbers (or cards) and were never supposed to be used to confirm a person's identity.[4] However, only a few years after the passing of the Social Security Act, President Roosevelt issued Executive Order 9397 that instructed federal agencies to use SSNs to identify individuals in any new system the agency was creating.[5] Few, if any, federal agencies complied with the new rule until 1961 when the Civil Service Commission adopted the practice. The Internal Revenue Service followed in 1962.[6] The trend only accelerated with the deployment of new electronic record keeping systems for which numerical identifiers were ideal, though the Privacy Act of 1974 did attempt to limit it somewhat.[7]

Once SSNs became universal identifiers, it was only a matter of time before they also became a universal authenticator.

Starting in the 1970's, Congress mandated the use of SSNs in any number of laws (for example, to combat welfare fraud and to stop undocumented workers from seeking employment). Over the next two decades, a series of laws required people to provide their SSNs to be verified with the government in order to receive benefits other than Social Security or to be hired. Today, SSNs are used in everything from banking to insurance to healthcare – often at the mandate of the federal government.

---

[2] Robert Pear, "The Nation; Not for Identification Purposes (Just Kidding)," *The New York Times*, July 26, 1998. https://www.nytimes.com/1998/07/26/weekinreview/the-nation-not-for-identification-purposes-just-kidding.html.

[3] This was the so-called "Fred Smith" problem: too many similar names existed for them to be used as a unique identifier. See Carolyn Puckett, "The Story of the Social Security Number," *Social Security Bulletin* 69:2 (2009). https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

[4] Indeed, from 1946 until 1972, Social Security cards explicitly disclaimed that they were for "Social Security purposes—not for identification." See Adrianne Jeffries, "Identity Crisis: how Social Security numbers became our insecure national ID," *The Verge*, Sep. 26, 2012. https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic.

[5] "Executive Order 9397 Numbering System for Federal Accounts Relating to Individual Persons," The White House, Nov. 22, 1943. https://www.ssa.gov/foia/html/EO9397.htm.

[6] Pear. https://www.nytimes.com/1998/07/26/weekinreview/the-nation-not-for-identification-purposes-just-kidding.html.

[7] A good summary is provided in Flavio L. Komuves, "We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers," *The John Marshall Journal of Information Technology and Privacy Law* 16:3 (1997-1998), pp. 529-574.

Meanwhile, Congress has allowed private companies to use Social Security Numbers as both identifiers and authenticators without any restrictions. However, the private marketplace is neither specifically authorized nor restricted in asking for a person's SSN for record keeping purposes or authentication.[8]

Data Breach and the Loss of Confidentiality

Recent history is replete with examples of data breaches and the harm they cause. Especially relevant to this subcommittee is the Equifax breach that resulted from poor data security practices and compromised the sensitive, personal data of over 140 million Americans. Moreover, some of these data—like SSNs—cannot be changed, which means that individuals may face a long period of frustration and vulnerability to identity theft. This event was largely preventable had Equifax implemented reasonable security measures, such as encrypting relevant data.

The federal government itself has not been immune to cyber-attacks. A few years ago, for example, a breach at the Office of Personnel Management compromised the records of over 20 million people that also contained sensitive information, such as SSNs and fingerprints. Although it was made public in 2015, the attack occurred more than a year earlier and went unnoticed by the OPM. I, personally, was a victim of both of these breaches.

These attacks are emblematic of the fact that U.S. companies and the U.S. government have been and remain vulnerable to attacks, many of which are by actors linked to nation-states that are adversaries of the United States. Nor are these isolated incidents. As the most recent annual Verizon Data Breach Investigations Report notes, 2017 (the last year for which data is available) saw more than 53,000 incidents and over 2,200 confirmed breaches.[9] So, make no mistake, cyber threats are real, and recent experience has shown that neither the private nor public sectors are fully equipped to cope with them.

Indeed, it does not matter if your personal data is held by a private business or the government, as both have lost millions of SSNs to hackers. Indeed, even before the Equifax breach, experts hypothesized that between 60 - 80% of all Americans have had their SSNS stolen.[10] After Equifax, that number is surely a low estimate.

Given the prevalence of data breaches, it is no surprise that SSNs are not expensive on the Dark Web. Indeed, the SSNs of newborns, which are highly coveted by bad actors because, in essence, they are

[8] "The Expansion of the SSN as an Identifier," U.S. Social Security Administration. https://www.ssa.gov/history/reports/ssnreportc2.html.

[9] "2018 Data Breach Investigations Report," Verizon, 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

[10] Aarti Shahani, "Theft of Social Security Numbers is Broader Than You Might Think," *NPR*, June 15, 2015. https://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think.

clean slates, only cost around $300.[11] By contrast, an adult's Social Security Number can sell for as little as $1 each.

In short, the modern rule of thumb is simple: assume your SSN is insecure.

The SSN Authenticator Nightmare

The idea of an SSN as an identifier is not terribly problematic. Everyone in America has a half dozen identifiers that are ways of uniquely denoting their identities to other people. I, for example, am Paul Samuel Rosenzweig. That's my primary identifier.

But I am also a number of other identities. For example, I am my email address: prosenzweig@rstreet.org. That identifier changes more often than my name, but it is, nonetheless, a unique way of pointing to me. A much more permanent identifier that most Americans have today is their mobile phone number. Ever since Congress made sure that we could transfer our number when we changed mobile carriers (thank you!), it has become a commonplace for people to keep their cell phone number, even if they move across country. I took my (202) number with me when I went on sabbatical to Chicago, and most people today anticipate never giving up the number they started with. That unique ten-digit string of numbers is me and only me.

In much the same way, my 9-digit SSN is also a unique string of numbers that is tied inextricably to me, and only to me. The problem is not, however, that the SSN identifies me. I need an identifier for the purposes of accessing my government social security account and, in this way, the SSN is really no different than my account number at the bank where I keep my checking account. It is merely a number linked to my name. But that numerical symbol is as much me as my name or my SSN is.

Nor is the problem that, 20 years ago, some enterprises started to use the SSN as an authenticator. After all, at the time they did so, the SSN was a confidential number known only to the issuer (the federal government) and to the beneficiary. If I, as the beneficiary, shared that SSN with an enterprise to use as my password for an account, I did decrease its confidentiality. But as an approximation of a confidential random password, the SSN was accurate. More importantly, at least at the outset it was efficient. Almost everyone has an SSN and almost everyone could remember it, which created a ready-made password authentication system.

The problem is that our initial assumptions about the confidentiality of the SSN (and thus about its utility as an authenticator) have, over time, proven not to be robust. As the SSN became more and more widely used for authentication, it became more and more widely known. Indeed, the concern about widespread use of a password/authenticator is why one of the cardinal rules today in password management is to try to avoid reusing the same password in multiple settings. This is, of course, because, when compromised, reused password/authenticators become a ready pathway to widespread access.

[11] Emma Z., "Excuse Me, Are You Using That Child Tax Credit?," *Terbium Labs*, January 18, 2018. https://terbiumlabs.com/2018/01/18/excuse-me-are-you-using-that-child-tax-credit.html.

And, with widespread use comes widespread vulnerability. A reused password is only as secure as the least-secure place that it is stored. As we have already discussed, it turns out that almost no storage location is secure enough – and even those like Equifax in whom we might repose greater confidence prove quite vulnerable.

Despite this, for reasons that surpass comprehension, some enterprises still use the SSN to authenticate my identity and prove that I am who I say I am. In fact, every Member of this subcommittee has, I am certain, been asked to provide the last-four digits of his or her SSN not to denote an identity but rather to prove it conclusively.

But, in a post-Equifax world, SSNs are so widely known and so readily available on the Deep Web or Black Market that they effectively provide no security at all. It would almost be as if my User Name for a login were my email address and the website allowed me to use the last-four letters of my last name as my password. That would be ludicrous, but the last-four digits of my SSN are as widely known and as readily available publicly as the last-four letters of my last name.

Ending the Nightmare

So, what then, should be done? If SSNs are valueless as authenticators, why do we continue to use them this way? The answer seems relatively clear – momentum or, if you prefer, legacy costs. Having built systems that rely on the SSN, too many users have sunk costs in their security architecture. Changing how identities are verified is costly. It may require significant expenditures of time and money. New systems may not be backward compatible with older ones, which necessitates wholesale re-architecture. In short, it is sometimes easier to do nothing than to change.

Of course, that is not the whole story. Increasingly, companies in America are beginning to bear the costs of their security failures. Data-breach insurance is now becoming commonplace and it comes at a real cost to those who purchase it. As time passes, we can anticipate that insurers will come to more closely grade the security of the enterprises to whom they issue insurance and charge differential rates based on that assessment.

Thus, over time, the market will come to value greater security against identity theft through insurance pricing. One perfectly plausible solution, then, to the SSN problem is simply to do nothing and over time, the insecurity of SSNs as authenticators will come to be so great a cost that enterprises will migrate away from them. Though I have not seen any data on the subject, it does seem anecdotally that this is already happening. Fewer enterprises today are using SSNs than were doing so ten years ago. And that is a good thing.

But waiting for the market to fix the problem has a cost. As I have already noted, the market is “sticky.” With sunk costs and barriers to change, many enterprises will be slow to modify their practices. The question then, is whether or not Congress has a role in moving this process forward more rapidly in the interest of avoiding continued harm to social security registrants.

To this end, one can envision two possible ways forward.

The first, more typical one would be for Congress to directly regulate the matter in the form of a law that directs companies to stop using the SSN as an authenticator. Such legislation would necessarily come with all of the regulatory baggage that attends all such laws. For example, there would be notice-and-comment rulemaking, followed by some form of audit and ultimately regulatory enforcement. If the task were given to the Social Security Administration (a natural choice since they "own" the SSNs), this would become an administrative requirement that would likely distract the SSA from its current duties. The SSA is not set up to handle most issues outside their core mission of helping seniors and disabled Americans. Indeed, while the Social Security Trust Fund is funded by dedicated taxes, administration money is appropriated. Any additional regulatory requirement would flounder unless Congress were to accompany it with additional funding; a problematic thought in these times of deficit spending.

Thus, I offer you a second possibility derived from the groundbreaking work of Nobel prize winning economist Richard Thaler:[12] Simply publish the Social Security Numbers. In other words, instead of continuing to treat them as confidential numbers that are "secret" when they manifestly no longer are, instead change the paradigm. Make them public numbers that are identifiers in the same way that my telephone number is an identifier published in the phone book. Doing so would demonstrate, in a definitive way, that SSNs are not suitable for identify verification or authentication (any more than my phone number is).

Admittedly, this idea may seem a bit outside the box at first. However, if the goal is to move the markets to more quickly discontinue use of the SSN as an authenticator, we need to make its disutility even more clear than it is now. This would raise the costs of maintaining it to a point where the incentive to stop using it is greater. Such a method simply helps to push the markets in the wiser policy direction without being overly directive in a regulatory way.

Of course, some individuals might object. I suppose we could add an opt-out provision that came with personal liability for identity theft. But my preference would be to see the publication of SSNs as a public good—much like vaccination—that the government could undertake on its own initiative.

I feel confident in predicting that within three to five years of publication in a public SSN log, their use as an identity authenticator would be a thing of the past. And that would be a good thing.

One final thought: As the brief history we recounted at the beginning of this testimony reflects, Congress itself bears much of the blame for the use of SSNs as identifiers and authenticators. We have legislated uses for SSNs that range from welfare fraud and bank identification to certifications of healthcare insurance compliance. In many ways, then, Congressional concern over SSN usage has an air of unreality given this history – and so another first step or nudge would be to systematically reduce and ultimately eliminate all use of SSNs as authenticators within government programs. As in the case of most federal programs, U.S. government leadership could also drive private sector change.

[12] These are summarized for popular consumption in Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Penguin Books, 2009).

Conclusion

In any event, the bottom line is simple. SSNs should no longer be used as a method of authenticating identity. The sooner we get to a place where this is universally true, the more secure our systems will be. While I have offered one creative way forward, others can also be imagined. The singular key is for Congress to take the initiative and lead the charge. Exactly how we get there in the end matters far less than the fact that we start down the road.

*Chairman Johnson. Thank you, sir. I appreciate your testimony.

Mr. Grobman, you are recognized.

STATEMENT OF STEVE GROBMAN, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, MCAFEE, LLC

*Mr. Grobman. All right, good morning, Chairman Johnson, Ranking Member Larson, and members of the subcommittee. It is a proud honor to testify today. And Chairman Johnson, it is an honor to work in your district. McAfee actually has its largest U.S. location in Plano, Texas. So it is an honor to testify today.

As McAfee's senior vice president and CTO I set our technical strategy to protect connected computing worldwide for both consumers and business architectures. I have worked in the field of cyber security for 2 decades, and have 24 U.S. and international patents in the fields of security, software, and computer architecture.

McAfee is one of the world's leading independent cyber security companies providing solutions for both business and consumers.

The nine-digit Social Security number first appeared as an identifier in 1936, but has since become the de facto national identifier and federal credential, uses for which it was never intended. Simply knowing a Social Security number has become accepted as a mechanism to impersonate an individual, and the Social Security number has become the premier target for cyber criminals.

Social Security numbers are sold in bulk in the black market for as little as $1 each. And once stolen, a Social Security number cannot easily be reissued or replaced. Last year's Equifax breach resulting in 145 million U.S.-based users having their personal information compromised reminds us that the U.S. needs to modernize its national identification standard.

There are three elements that need to be discussed when we transition to a next-generation personal identifier: identity, authentication, and authorization. In our current model Social Security numbers play a role in all three. Identity is an identifier that can be public. It is like an individual's Twitter handle; it identifies an individual, but simply knowing the handle doesn't enable someone to impersonate the account holder.

Whereas, authentication is the process of proving that you are a specific identity, and generally relies on one of three types of factors: either something you know, like a password; something you have, like a smart card; or something you are, such as a biometric. An authorization is granting a specific capability or benefit to a specific entity. All three parts need to be in scope for a next generation system.

We have all the technology pieces to move towards a high-quality, high-security, well-thought-out, next-generation identity management system based on strong authentication. What is more difficult is understanding the requirements that will be acceptable for both government and the citizens.

We need to ask questions such as is this a solution exclusively for government-related services? How can a system be inclusive to all citizens, regardless of wealth or access to advanced technologies? Does a government biometrics database create unacceptable privacy issues? How will recovery mechanisms work when technology assets are lost or stolen? What are the cost constraints, funding options, and timelines for implementing and maintaining a solution into the next generation, and how long does the underlying cryptography need to last?

This last question is interesting, in that we are on the verge of quantum computing becoming a viable reality. Quantum computing is well suited to break the underlying cryptography that protects the world's data. Specifically, RSA, but public key algorithm which is the heart of most protection and identity solutions. A next-generation architecture must comprehend the quantum computing world we will likely face in the next few decades.

We need to look at what technology options are available, and I have been asked whether things such as blockchain could be useful. I do not recommend it. While a powerful technology providing properties such as decentralized trust, blockchain also brings scalability, complexity, and its own security challenges. In the case of our next-generation system, we do have a trusted central authority: the U.S. Government. We need to focus on the problem that we are trying to solve, and the one thing that we must do is not use the current system that we have.

A few quick recommendations: We need an identity management executive order that outlaws the use of Social Security numbers as authenticators; We need to push federal agencies to act as validators of identity and mandate all federal e-government service require the use of strong authentication; We need to let innovation flourish. NIST and the private sector can work together on this. And we need to move faster in implementing quantum-safe algorithms to protect both data protection and identity solutions.

It is an honor to testify to this subcommittee. I appreciate your interest in considering my recommendations, and look forward to answering your questions.

STATEMENT FOR THE RECORD OF
STEVEN GROBMAN, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, MCAFEE, LLC
BEFORE THE WAYS AND MEANS SUBCOMMITTEE ON SOCIAL SECURITY
May 17, 2018, 10:00 AM

Good morning, Chairman Johnson, Ranking Member Larson and members of the subcommittee. Thank you for the opportunity to testify today. McAfee has over 1,000 employees based in Plano Texas, in Chairman Johnson's congressional district. We have found the district, with its strong base of IT professionals, to be a very friendly business environment. We also appreciate Chairman Johnson's long dedication to the district and our country, and I know he will be missed when he retires from Congress at the end of the year.

I am pleased to address the subcommittee on modernizing the identity and authentication system for citizens of the United States. This will have a profound impact on our citizens, our security and our economy. The Committee's focus on holding a "big think" hearing makes a great deal of sense. Before developing policy and operational solutions to solving our nation's identity management challenge, we need to make sure we're asking the right questions so the right identity management system requirements can be defined and the right roles and responsibilities for both the public and private sectors can be delineated.

First, I would like to provide some background on my experience and McAfee's commitment to cybersecurity. As McAfee's Senior Vice President and Chief Technology Officer (CTO), I set our technical strategy, ensuring that we create technologies that protect smart, connected computing devices and infrastructure worldwide. A large part of my role as CTO is driving innovation at McAfee, and my team includes: McAfee Labs, R&D, threat research and McAfee's internal CISO organization.

Prior to joining McAfee, I spent over two decades in senior technical leadership positions at Intel Corporation related to the field of cybersecurity, resulting in being named an Intel Fellow and worldwide McAfee CTO in 2014. I have 24 U.S. and international patents in the fields of security, software and computer architecture. I earned my bachelor's degree in computer science from North Carolina State University.

MCAFEE'S COMMITMENT TO CYBERSECURITY AND IDENTITY MANAGEMENT

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions from device to cloud that make the world a safer place. By building solutions that work with other industry products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices and in the cloud, we secure their digital lifestyle at home and while on the go. By working with

other security players, we are leading the effort to unite against state-sponsored actors, cybercriminals, hacktivists and other disruptors for the benefit of all. McAfee is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide.

McAfee has also made a commitment to helping our customers address their identity management challenges. McAfee's Identity Theft Protection allows users to take a proactive approach to protecting their identities with personal monitoring, financial monitoring and recovery tools needed to keep identities personal and secured. Key features include:

- Cyber Monitoring – Scans the online black market and the Dark Web and alerts users when their personal information is at risk.
- Social Security Number Trace – Delivers reports of known aliases and addresses tied to a users' Social Security Number so they can review for potentially fake identities.
- Credit Monitoring – Sends reports based on lending and credit history, and alerts users to changes to their creditworthiness.
- 24/7 Dedicated Agent Support – Allows users access to agents who can answer questions and provide guidance on topics from using credit responsibly to handling identity theft.
- Identify – Provides complete visibility into data, context and user behavior across all cloud services, users and devices.

In addition, we've done a lot of thinking about identity management and what problems we as a nation need to solve. Here are some of our thoughts.

THE SOCIAL SECURITY NUMBER CAN NO LONGER BE USED AS AN EFFECTIVE AUTHENTICATOR

The once venerable nine-digit Social Security number first appeared as an identifier in 1936. It has become the de facto national identifier and a federal credential that people use for a range of both governmental and commercial purposes – uses for which it was never designed. Simply knowing an SSN has become accepted as a mechanism in many cases to impersonate an individual; it's also become a premier target for cybercriminals. SSNs are sold in bulk on the cybercrime black market for as little as one dollar. Once stolen, the SSN cannot easily be reissued or replaced, making it a weak foundation upon which to build identity.

The steady stream of major breaches where consumers' SSNs have been stolen creates a compelling opportunity for change. Last year's Equifax breach resulted in 145 million US-based users having their personal information compromised. Attackers reportedly exploited a vulnerability on the company's website to steal names, Social Security numbers, birthdates, addresses and, in some cases, driver's license numbers and passport numbers. Breaches like this remind us that the United States needs to modernize the national identification standard for its citizens. It is unrealistic for a Social

Security number (SSN) to be shared and distributed to many parties and stay confidential for the better part of a century.

Policymakers need to modernize the systems and methods that identify citizens as well as enable citizens to prove their identity with minimal risk of impersonation and without overtly compromising privacy. A good start is to determine what digital technologies offer strong security to create renewed confidence in the modernized credential system that must replace our current paradigm of using the current SSN across public and private ecosystems.

The growing cyber threat makes finding a solution even more urgent. McAfee Labs logged 63.4 million new samples of malware – an all-time high – in the fourth quarter of 2017. We found that cyber criminals are increasingly targeting the healthcare sector, where information, including personal identifiers, is non-perishable. The sale of personal information, including Social Security numbers, has become a lucrative business in underground markets.

NOT A NEW PROBLEM

While we're hearing more about it now because of recent breaches, the matter of using the SSN as a personal identifier is not a new problem. Twenty-five years ago, computer scientists voiced concerns about sharing a single piece of permanent information as a means of proving a person's identity. Simply having this piece of information was sufficient for an individual to prove his or her identity. Part of the problem is that there hasn't been an incentive, or forcing function, to change the way identity transactions work.

Ironically, we have not taken steps to develop better standards for protecting personal identity, yet we've taken these steps in other areas, such as credit card security. For many years, individuals' credit card numbers, the card expiration date and CID (card identification) number were all that was necessary to prove individuals could charge against an account. The massive retail breaches forced a reconsideration of this practice. The financial services industry recognized that this model needed to be changed and transitioned to chip-based technology or smart card–based credit card capabilities.

In Europe and much of the rest of the world, the transition was to a system known as chip and PIN, where the card not only has a computer chip, but the individual also must enter a unique PIN that is stored on the card. In the United States, the transition has been first to a partial improvement where a chip in a credit card can be used to prove physical possession of the card by having the smart card respond to a cryptographic challenge that it uniquely can respond to. This system can be enhanced in the future with the full adoption of "chip and PIN," which will have the chip only respond if the correct PIN is entered as well.

With chip and PIN, there is never any disclosure of the secret information to parties with whom individuals are transacting. It is simply a matter of using math -- cryptography algorithms – to prove that individuals are who they say they are, as opposed to giving the parties something that would let them impersonate the individual. The simplest technical

requirement truly boils down to that. The question we need to ask as U.S. citizens is, why would we move forward to a more secure system for financial instruments such as credit cards but lag in our progress toward a more secure system for proving our identities as individuals?

DEFINING REQUIREMENTS

We must recognize that there are three elements that need to be discussed: identity, authentication and authorization. In our current SSN system, the simple number plays a role in all three, while in the field of computer science, we recognize the criticality of looking at these independently. Identity is the identifier that should be public and not pose a risk to the individual if many parties know it. The President of the United States' @POTUS Twitter handle is an identity. It identifies the President; however, knowing the Twitter handle does not let you impersonate the president.

Authentication is the process of proving you really are a specific identity. Authentication typically relies on something you know (a password), something you have (for example, a smart card) or something you are (such as a biometric). The strongest form of authentication requires multiple forms of authentication, such as a PIN (something you know) combined with a smart chip card (something you have). Authorization is granting a capability to a specific identity – for example, allowing a user to receive benefits or have access to specific information such as private medical data. All three – identity, authentication and authorization – must be part of a new personal identification system.

We have all the technology pieces to begin the journey to a high-quality, high-security and well-thought-out identity solution for U.S. citizens. We understand the cryptography, biometrics, how to build hardware devices and how to deploy them to scale to millions of people. We can apply the lessons we have learned, using proven technologies, from mechanisms such as our financial instruments, as well as looking at what has and has not worked in countries that have moved to more modern identity systems.

There are several ways to do this, from simply implementing proven credit card technologies such as "chip and PIN" for personal IDs, to employing technologies that are directly based on who someone is, such as biometrics (which makes it more difficult for a thief to use a stolen card or token). Chip and PIN technologies could allow individuals to electronically authenticate with a higher level of security than if they simply asserted a number (such as our existing SSNs).

What's going to be more challenging, however, is coming up with a solution that strikes the right balance between security and privacy, and deciding what the scope of this should be. Is this a solution for individuals to prove their identity for government-related services and transactions, Social Security and other government benefits? Or is this the solution for individuals to prove who they claim they are for other types of transactions? States currently provide identity solutions such as driver's licenses or ID cards. Does the new standard complement that? Does it replace elements of that?

These are some of the difficult questions that need to be debated: What is the intent? How do we want to protect privacy? What is a reasonable requirement to ensure that all citizens of the United States can prove their identity regardless of wealth or access to advanced technologies? Is it a reasonable requirement to have the federal government maintain a biometrics database for citizens such as fingerprints, iris scans or facial features? How will citizens who are disabled or require someone to legally act on their behalf utilize a next-generation authentication system? How will recovery mechanisms work when technology assets are lost, stolen or socially engineered? As a technologist in the field of cybersecurity, I have many building blocks at my disposal that can be used to define a next generation system; however, answering these questions is critical to choosing an appropriate solution.

We also must understand the pragmatic requirements of a next generation system. What are the cost constraints and funding options? How quickly must we move to this new system, and what does that migration plan look like? How many years does the underlying cryptography need to be secure?

This last question is interesting in that we are on the verge of quantum computing becoming a viable reality, likely within the next two decades. Quantum computing relies on the principles of quantum physics to solve specialized classes of mathematical problems that are not practical to solve on traditional computers. Quantum computers use quantum bits (qubits), unlike digital computers, which are based on transistors and require data to be encoded into binary digits (bits). These qubits can exist in multiple states simultaneously, offering the potential to compute a large number of calculations in parallel, speeding time to resolution. One of the key workloads that quantum computing is well suited for is to break the underlying cryptography that protects the world's data – specifically, the RSA public key algorithm, which is at the heart of most protection and identity solutions. RSA public key is at a high risk of compromise when quantum computing becomes a reality.

While we applauded the work by NIST to start the process to look for quantum-safe algorithms, we must understand that adversaries can place data on the shelf now (especially if it has long- term value such as national secrets) and attack it later when quantum computing becomes viable. Similarly, a next generation identification system should last 100 years or more, such that the next generations can prosper from the systems we invest in today. Careful consideration needs to be made about whether this new capability needs to be quantum safe – or at a minimum, have an architecture that allows the replacement of algorithms as quantum safe capabilities become available, even if we start with well-understood and tested components of today.

MOVING TOWARD A SOLUTION

I've been asked if blockchain technology could help put us on a path toward a secure identifier. I do not recommend this approach. Blockchains are a powerful technology that solves some very specific problems. They enable a trust model for an immutable ledger when a trusted party does not exist. In the case of cryptocurrency, this is exactly the problem you are trying to solve: you want to ensure that you can create transactions

without reliance on any trusted agency or government. Part of what drives the viability of cryptocurrency is incentives for individuals to run the distributed infrastructure that powers the blockchain. We find, however, that blockchain has performance, scalability and privacy challenges that are not easily overcome.

During the cryptographers' panel at this year's RSA conference, Ron Rivest, a well-known cryptographic expert whose name accounts for the "R" in "RSA," discussed some of the failings of blockchains for certain security applications. He noted that they "fail miserably in terms of scalability, throughput and latency…[and] in certain applications [such as] voting they are a very poor fit.…[I]n many applications they are a bad database choice…. [T]hey have limited security properties that may or may not fit your need."

In the case of our next generation ID system, we have a trusted central authority (the US Government) and require significant scale for the infrastructure that would not be served well by a blockchain distributed system and architecture. Instead, we should focus on well understood tools and principles that our knowledge of cryptography, authentication and identity technologies provide, as opposed to falling victim to the "blockchain" hype.

We need to focus on what problems we are trying to solve. If a key requirement is that an individual's identity is not transferable, or that an individual can't have multiple IDs, then biometrics may be worth considering. India has moved to a national biometric identity program, allowing 1.3 billion citizens to prove their identities through fingerprints, facial recognition and eye iris scans. The country faced an even more difficult problem than compromised SSNs because there was no single starting database of citizens. Because benefits came with being a citizen, there were concerns that an individual might attempt to register in one town under one name and then register in another town under another name. The Indian government addressed this issue by creating a biometrics database to register its population. If your biometrics were already in the database, the government would know that you were a duplicate person. It also provided a mechanism that let you walk into any government office and reprove that you were you.

In the U.S., we need to move to a system in which an individual can prove their identity to someone, but not make it such that when proving their identity, they're giving the other party the ability to impersonate them. If we continue to rely on private pieces of information to prove our identity, we will continue to have those pieces of information stolen and misused—which will impact millions of individuals in the United States.

Yet there will certainly be an interim period during the transition that will require SSNs to play a role. There is a difference between using a number as an identifier and having that identifier be considered sensitive information. Given that lots of data already exists in all sorts of databases, and SSNs are used as a part of those datasets, it would be unrealistic to ban their use overnight. But they should be used strictly as an identifier, so they cannot be used to prove that imposters are the genuine individuals.

It is reasonable that the IRS uses an SSN as a part of its tax accounting solution, at least for the near term. But if somebody calls the IRS and simply gives their SSN and date of birth, that in and of itself should no longer be sufficient for the IRS to believe that the

individual is definitively who they claim to be. It is the difference between using something as a reference to an individual as opposed to being an authenticator – an instrument that proves an individual identity.

We need to debate if keeping the SSN as an identifier is acceptable as long as it is not used for authentication or direct authorization. As mentioned earlier, a piece of data that is only an identifier does not pose a security risk even if it is widely known. The most critical focus should be on eliminating the SSN for authentication. We do need to recognize that we are running out of SSNs. The number of permutations in a 9-digit number is 1 billion. There are now about 325 million citizens in the United States, which could exhaust the pool of SSNs within a few generations. Is this acceptable? If we determine it is OK to re-use SSNs, we have some headway, but if we are re-architecting the system, it may be a good time to consider a larger namespace that eliminates the need for re-use in the long run.

Change will require a good partnership between the private sector and federal, state and local governments, given that identity is something that is used where citizens interact with many forms of government. Even within the private sector, we will need partnerships to determine what is appropriate for different types of private transactions.

We need to move quickly, however. Every day that we do not solve this problem sets up the opportunity for criminals to use compromised consumer data for the impersonation of individuals whose data has been breached. Granted, the world needs to operate during the transition, and we need to have a high level of pragmatism to work through this. At the same time, we should not indefinitely kick the can down the road and ignore the problem, forcing ourselves to default to systems that are inherently insecure.

The mega retail breaches of a few years ago changed financial institutions' perspectives and pushed U.S. merchants to move to chip-based credit cards. That series of events was the catalyst that made major industries take a step forward in using available technology. The Equifax event is very similar; it is a catalyst that should make us say, "Let's talk about this."

Now I'd like to make some policy recommendations.

POLICY RECOMMENDATIONS

Issue an Identity Management Executive Order – The Administration's executive orders on IT modernization and cybersecurity focused attention on modernizing our federal IT and cybersecurity capabilities. While these orders touched on identity management, the state-of-affairs in identity management is at such a critical stage that the President should issue an up-to-date executive order on this topic. An executive order on identity management would be a powerful call to action to all federal departments to leverage existing authorities to drive real change. Such an order would reinforce the Office of Management and Budget's (OMB) recent identity management guidance, "Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management".

Examples of initiatives should include:

- Developing model legislation to ban the simple knowledge of a Social Security number as an accepted form of authentication throughout our economy.
- Doubling down on privacy – what works in some countries will not work in the United States, given our long-held aversion to the type of system India has developed.
- Reinvigorating the National Strategy for Trusted Identities in Cyberspace, NSTIC, by funding and staffing it properly to continue progress between the public and private sectors on identity management standards.
- Encouraging and enabling federal agencies to act as validators of identity, given the many credentials over which the federal government has authority, including passports.
- Mandating all federal e-government services provided directly to citizens require the use of strong authentication to enhance trust in government services.

The latter action would improve citizen trust and satisfaction in government services and set an example the private sector is likely to replicate, given the power of the government to influence adjacent markets. But achieving success will require federal agencies, particularly the Social Security Administration, to double down on their IT and cybersecurity modernization efforts. Agencies should leverage IT modernization innovation funds to ensure their authentication systems are both modern and secure. Care needs to be taken to ensure cloud services that help enable citizen authentication are secure end-to-end, given the risk of assuming that just because personal identifying information (PII) is in the cloud, it is secure.

Let Innovation in the Private Sector Flourish – The private sector has not stood still. The FIDO (Fast IDentity Online) Alliance has made progress toward addressing the lack of interoperability among strong authentication devices and solving the problems users face creating and remembering multiple usernames and passwords. The Organization for the Advancement of Structured Information Standards (OASIS) has developed the Security Assertion Markup Language, an open standard for exchanging authentication and authorization data between identity providers and service providers. A standard called OAuth has also been developed – an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.

Yet more needs to be done. To date, the private sector has not solved the authentication challenges needed to build a truly modern identity management system. More private sector collaboration is needed to construct all the technical components – all the truly open and interoperable standards needed to give American citizens the high-quality identity management environment they deserve. If more progress is made in creating interoperable standards based on collaboration, a single, more proprietary, de-facto identity management system could develop.

While there are examples of de-facto standards, in the PC industry for instance, the risk of de-facto standards, particularly in an area as vital to the national interest as identity management, is that vendor lock-in could slow down innovation and progress. The government, led by NIST, should collaborate with FIDO and the other private sector identity management alliances and working groups, to share best practices and encourage the development and deployment of truly open standards and technologies. An identity management ecosystem based on open architecture solutions will promote innovation and increase the freedom of citizens to choose the identity management approach that meets their own needs.

Invest in Research and Development – The government has a fine track record of supporting basic research and development managed by universities and other centers of learning such as think tanks. These investments have enabled the United States to lead the world in semiconductors, software and bio-medicine. Investments in identity management research and development can produce similar results, particularly in a world where such stair-step innovations as quantum computing have the potential to disrupt our current and future identity management models.

Move Faster in Driving Quantum-Safe Algorithms and Integrating into Identity and Crypto Solutions – The government needs to incentivize and fund aggressive research into quantum computing. The private sector has already put a good deal of effort behind developing a quantum computer, with companies like Intel and Microsoft making good progress. Other nations realize that the country that develops the first quantum computer will have a significant advantage over others. The U.S. should take note of this and – at a minimum – make sure quantum-safe algorithms are integrated into network protocols and data protection algorithms as well as identity solutions. It is a matter of when, not if, quantum computing will be available to break current quantum-unsafe algorithms. A new identity architecture should at least allow the replacement of algorithms as quantum-safe capabilities become available.

CONCLUSION

It is an honor to testify before this subcommittee. We face identity management and cybersecurity challenges that merit immediate and sustained attention and investment. The fact that this committee, with its Social Security oversight and policy authority, is focused on solving the identity management challenge is truly encouraging. I appreciate your interest in considering my recommendations and look forward to answering your questions.

*Chairman Johnson. Thank you for coming all the way from Plano.

*Mr. Grobman. You bet.

*Chairman Johnson. Mr. Grant, welcome. Please go ahead.

STATEMENT OF JEREMY A. GRANT, COORDINATOR, BETTER IDENTITY COALITION

*Mr. Grant. Thank you. Good morning, Chairman Johnson, Ranking Member Larson, members of the committee. Thank you for the opportunity to discuss the future of the Social Security number with you today.

I am here on behalf of the Better Identity Coalition, an organization launched earlier this year focused on bringing together leading firms from different sectors to develop a set of consensus, cross-sector policy recommendations that promote the adoption of better solutions for identification and authentication.

The Coalition's founding members include recognized leaders from diverse sectors of the economy, including financial services, health care and technology, telecommunications, fin tech, payments, and security. Our members are united by a common recognition that the way we handle identity today in the U.S. is broken, and by a common desire to see both the public and private sectors each take steps to make identity work better.

As background I have worked for more than 20 years at the intersection of identity and cyber security. In 2011 I was selected to lead the National Strategy for Trusted Identities in Cyber Space, which was a White House initiative focused on improving security, privacy, choice, and innovation through better approaches to digital identity. In that role I also led the identity team up at NIST.

I left government three years ago, and now lead the technology business strategy practice at Venable, a law firm here in town with the country's leading privacy and cyber security practice. And in that role I serve as the coordinator of the Better Identity Coalition.

Let me say I am grateful to the committee for calling this hearing today. The SSN is a key component of our identity infrastructure, and the future of this number impacts every American. Up front, I would submit that many of our challenges here are linked to more

than 80 years of contradictions in policy around how this number should be managed and used.

Among the biggest contradictions, the SSN is simultaneously presumed to be both secret and public: secret, because we tell individuals to guard their SSN closely; public, because we have multiple laws that require individuals to give it out to facilitate all sorts of interactions with industry and government; secret, because we then tell those entities to ensure that, if they store it, which the law often requires them to do, that it be protected; and public, because that has proven quite hard to do, to the point that the majority of Americans' SSNs have been compromised multiple times over the last several years, amidst a wave of data breaches.

Now, these contradictions are not the result of anything malicious. On the contrary, they reflect years of trying to balance several important roles played by the SSN and the Social Security Administration. What is most important now is that the government, one, recognizes these contradictions and, two, takes steps to put policies in place that are more consistent, and that put us on a path towards a system that enhances security, privacy, and convenience for Americans.

I believe there are five areas where change is needed.

First, when talking about the future of the SSN and whether it needs to be replaced, it is essential, as Chairman Johnson noted and many members of the panel have noted, to understand the difference between the number's role as an identifier, which is a number used to sort out which Jeremy Grant I am among the hundreds in the U.S., and its use as an authenticator, which is something that can prove I am actually this Jeremy Grant.

SSNs should no longer be used as authenticators. That means, as a country, we stop pretending this number is a secret, or that knowledge of an SSN can be used to prove that someone is who they claim to be.

Second, just because SSNs should no longer be used as authenticators does not mean that we need to replace them with some sort of new SSA-issued identifier. I have yet to see any proposal here that does not involve spending billions of dollars and confusing hundreds of millions of Americans with very little security benefit.

Rather than create a new identifier, our focus ought to be on crafting better authentication solutions that are not dependent on the Social Security number and are resilient against modern vectors of attack.

Third, on the authentication topic, there is good news. Multi-stakeholder efforts like the FIDO Alliance and the World Wide Web Consortium have developed standards for next-generation authentication that are now being embedded in most devices, operating

systems, and browsers in a way that enhances security privacy and the user experience. The government can play a role in accelerating the pace of adoption.

Fourth, even if we assume the SSN is publicly known, that does not mean it needs to be used everywhere. Many of the members of the Better Identity Coalition would love to reduce where they use the SSN, due to the risks that it presents to them, relative to other identifiers. However, they are running up against laws and regulations that require them to collect and retain the SSN.

Finally, we need to focus not just on the SSN, but also the future of the Social Security Administration. The issue here goes beyond the future use of a nine-digit number to encompass a broader topic: What role should the government play in the future of the identity ecosystem?

Now, while identity may not be a part of the SSA's mission statement, there is no question that in 2018 the SSA is in the identity business. It is time to acknowledge that fact and then take a step back to contemplate what that means.

Having agencies like SSA accept their role here may be the most impactful thing that the government can do to help solve our identity challenges. Specifically, like allowing consumers to start asking agencies that have their personal information to vouch for them to parties they seek to do business with.

The SSA and state departments of motor vehicles have the most to offer here, and this concept was embraced in the 2016 report from the Bipartisan Commission on Enhancing National Cyber Security. The federal government should work to, one, develop a framework of standards and rules to make sure this is done in a secure, privacy-protecting way; and second, fund work to get it started.

I appreciate the opportunity to testify today and look forward to answering your questions.

Jeremy Grant
Coordinator, The Better Identity Coalition
and
Managing Director, Technology Business Strategy, Venable LLP

U.S. House Committee on Ways & Means
Subcommittee on Social Security

""Securing Americans' Identities: The Future of the Social Security Number"

May 17, 2018

Chairman Johnson, Ranking Member Larson and members of the committee, thank you for the opportunity to discuss the future of the Social Security Number (SSN) with you today.

I am here today on behalf of the Better Identity Coalition[1] – a new organization launched earlier this year focused on bringing together leading firms from different sectors to develop a set of consensus, cross-sector policy recommendations that promote the adoption of better solutions for identity verification and authentication. The Coalition's founding members include recognized leaders from diverse sectors of the economy, including financial services, health care, technology, telecommunications, FinTech, payments, and security.

As our name would suggest, the Better Identity Coalition is not seeking to push the interests of any one technology or industry. Instead, our members are united by a common recognition that the way we handle identity today in the U.S. is broken – and by a common desire to see both the public and private sectors each take steps to make identity systems work better.

As background, I've worked for more than 20 years at the intersection of identity and cybersecurity. Over the course of my career, I've been a Senate staffer, led a business unit at a technology company architecting and building digital identity systems, and done stints at two investment banks helping investors understand the identity market – cutting through what works and what doesn't, and where they should put capital. In 2011, I was selected to lead the National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative focused on improving security, privacy, choice and innovation online through better approaches to digital identity. In that role I worked with industry and government to tackle major challenges in identity, built out what is now the Trusted Identities Group at the National Institute of Standards and Technology (NIST), and also served as NIST's Senior Executive Advisor for Identity

[1] More on the Better Identity Coalition can be found at https://www.betteridentity.org

Management. I left government in 2015 and now lead the Technology Business Strategy practice at Venable, a law firm with the country's leading privacy and cybersecurity practice. In that role at Venable I serve as the Coordinator of the Better Identity Coalition.

Setting the stage

Let me say up front that I am grateful to the Committee for calling this hearing today. The SSN is a key component of America's identity infrastructure, and the sometimes conflicting roles that the SSN plays – which I will outline today – are a topic that impacts every American. At a high level, the way we handle identity in America impacts our security, our privacy, and our liberty. And from an economic standpoint, particularly as we move high-value transactions into the digital world, identity can be the great enabler – providing a foundation for digital transactions and online experiences that are more secure, more enjoyable for the user, and ideally, more respectful of their privacy.

But when we don't get identity right, we enable a set of great attack points for criminals and other adversaries looking to execute attacks in cyberspace. And unfortunately, we have not been doing well here. Last year, a whopping 81% of hacking attacks were executed by taking advantage of weak or stolen passwords, according to Verizon's annual Data Breach Investigation Report. 81% is an enormous number – it means that it's an anomaly when a breach happens and identity does not provide the attack vector.

And outside of passwords, we've seen private and state-sponsored adversaries seek to steal massive data-sets of Americans, including their SSNs. With these stores of data, they have an easier time compromising the questions used in "identity verification" tools like Knowledge-Based Authentication or Verification solutions (KBA/KBV). We've seen an uptick in breaches that exploit these tools as a result.

A key takeaway for this Committee to understand today is that attackers have caught up with many of the "first-generation tools" we have used to protect and verify identity – and one's knowledge of his or her SSN has been a key component of these tools. The recent Equifax breach may have driven this point home, but the reality is that these tools have been vulnerable for quite some time. There are many reasons for this – and certainly blame to allocate – but the most important question is: "<u>What should government and industry do about it now?</u>"

I believe we are at a juncture where the government will need to step up and play a bigger role to help address critical vulnerabilities in our "digital identity fabric." To that end, it is important to talk not only about the future of the SSN, but also the role of the Social Security Administration (SSA).

The role of the SSA – and the future of the SSN

Up front, I would submit that many of our woes in identity are linked to the rather bizarre way the United States has treated the Social Security Number over the last 80 years. I expect the history of the SSN is well known to this Committee, but I do think it's worth briefly pointing out some of the contradictions in policy around how it should be managed and used.

1. First, the SSN is simultaneously presumed to be both secret and public. Secret because we tell individuals to guard their SSN closely. Public, because we also tell individuals to give it out to facilitate all sorts of interactions with industry and government. Secret because we tell those entities in both government and the private sector to ensure that if they store it – which the law often requires them to do – that it be protected. And public, because that's proven quite hard to do: to the point that the majority of Americans' SSNs have been compromised multiple times over the last several years amidst a wave of data breaches.

2. Second the SSN is commonly used as both an identifier and an authenticator. As I will discuss today, years of breaches mean the SSN is of little value for authentication – but it is still quite valuable in the role it was first created for, as a unique identifier. Understanding this difference is key to crafting a solid strategy for the SSN's future.

3. Third, the SSN system is managed by an agency not formally tasked with providing an essential element of the country's identity infrastructure. Yet the SSA finds itself in that role by default – and is increasingly being asked to do more.

These policy contradictions are not the result of anything malicious; on the contrary, they reflect years of trying to balance several important roles played by the SSN and the SSA. What's most important now is that the government 1) recognizes these contradictions, and 2) takes steps to put policies in place that are more consistent, and that put us on a path toward a system that enhances security, privacy and convenience for Americans.

That process starts by changing how we view the SSN and how we use it.

I believe there are five areas where change is needed – and where this change can contribute to material improvements in the confidentiality, reliability and integrity of America's identity ecosystem, while also improving privacy and eliminating barriers to digital commerce.

1. Up front, government should acknowledge that there is not a need to "replace" the Social Security Number (SSN) – at least not in the way that some have suggested in recent months. Rather, government should take steps to change how we use it.

There's been a ton of discussion on this topic over the last few months as some industry and government leaders, along with security and privacy experts, have called for the country to come up with "something to replace the SSN."

Unfortunately, the debate has been muddled by people failing to differentiate between whether the SSN is an identifier or an authenticator. Part of the confusion is that SSN has been used as both identifier and authenticator in recent years.

At its core, the SSN was created as an identifier. It is a 9-digit code, issued by the Social Security Administration at birth, that is used to help the government know "which Jeremy Grant" they should associate wage and tax data with, and to help administer the delivery of Social Security benefits. Over time, use of the SSN has expanded beyond the purposes for which it was intended, with thousands of private sector entities collecting the SSN as part of the account opening experience — and by credit reporting firms, data brokers, and other private firms, who have used the SSN as one way to aggregate and match data about a person.

These expanded uses of the SSN are all as an identifier. But where things have really changed is the practice of using the SSN as an authenticator. Every time a party asks for the last four digits of that number, for example, the premise is that the SSN is a secret — and thus possession of the SSN could be used to authenticate a person.

There was a time when SSN as authenticator made sense: someone's SSN was not widely known or publicly available, so it was safe to presume that it was a secret. But in 2018 — after several years of massive data breaches where millions of SSNs have been stolen — the notion that SSNs are a secret is a fallacy. The Equifax breach may have woken people up to this fact, but for several years now, SSNs have been widely available on the dark web for just a dollar or two.

The message is clear: data breaches have gotten bad enough that we should assume an attacker can get someone's SSN with only minimal effort. The attackers have caught up to authentication systems that use SSN as a factor — it's time to move on to something better.

With this, we need to move beyond using the SSN as an authenticator. Beyond delivering immediate improvements to security, such a move would also lessen the value of SSNs to criminals and other adversaries.

2. Just because SSNs should no longer be used as authenticators does not mean that we need to replace them as identifiers. When architecting a system for security, identifiers don't have to be a secret – and many times it is desirable that they be known. Given that -

rather than replace the SSN as an identifier, instead, let's start treating SSNs like the widely-available numbers that they are.

Doing this is the single best way to reduce the risks associated with use of the SSN as an identifier. If we shift everybody's mindset to one where everybody understands that SSNs are widely known – and design security systems that don't allow someone with just an SSN to use it to gain access to data or services – it effectively devalues the SSN as an attack point.

There have been a number of proposals suggesting that America should instead scrap the SSN and invest in creating a new, revocable identifier administered by the SSA.

I've yet to see any proposal that does not involve spending tens of billions of dollars and confusing hundreds of millions of Americans – with very little security benefit. The reality is that both government and industry would simply map that new identifier back to the SSN and other data in their systems. Because the new and old identifiers would be connected, the security benefits would be close to nil.

Moreover, the possibility of chaos due to errors in mapping and matching these additional identifiers would be quite high, given that many government and commercial systems deliver less than 100 percent accuracy today; think about what might happen when a system fails to associate a new identifier with the right person.

Winston Churchill once said: *"Democracy is the worst form of Government except for all those other forms that have been tried."* So it is with the SSN – it's not a perfect identifier, but keeping it beats the alternatives.

Rather than create a new identifier, the focus ought to be on crafting better authentication solutions that are not dependent on the SSN, and are resilient against modern vectors of attack.

3. On the authentication topic – we need to recognize that the problems with using SSNs as an authenticator extend to using any "shared secret" for authentication. It doesn't matter if the so-called "secret" is the SSN or passwords – they both are terrible.

   As I mentioned earlier, 81% of 2016 breaches were enabled by compromised passwords, which is about as clear a sign as you can ask for that things need to change. There is no such thing as a "strong" password or "secret" SSN in 2018 and we should stop trying to pretend otherwise. We need to move the country to stronger forms of authentication, based on multiple factors that are not vulnerable to these common attacks.

   There is good news in this regard: parts of government and industry have recognized the problems with old authenticators like passwords and SSNs – as well as other forms of

authentication using "shared secrets" – and worked together these past few years to make strong authentication more secure and easier to use. Multi-stakeholder groups like the Fast Identity Online (FIDO) Alliance and the World Wide Web Consortium (W3C) have developed standards for unphishable, next-generation multi-factor authentication (MFA) that are now being embedded in most devices, operating systems and browsers, in a way that enhances security, privacy and user experience. Government should recognize the significance of this market development that is enabling authentication to move beyond the password, and embrace it.

What makes this possible is the fact that the devices we use each day have evolved. Just a few years ago, MFA generally required people to carry some sort of stand-alone security device with them. This added costs and often degraded the user experience. Moreover, these devices were generally not interoperable across different applications.

Today, however, most devices – be they desktops, laptops or mobile devices – are shipping from the factory with a number of elements embedded in them that can deliver strong, multi-factor authentication that is both more secure than legacy MFA technology and also much easier to use.

What are these elements?

1) Multiple biometric sensors – most every device these days comes with fingerprint sensors, cameras that can capture face and sometimes iris, and microphones for voice.

2) Special tamper-resistant chips in the device that serve as a hardware based root of trust – such as the Trusted Execution Environment (TEE) in Android devices, the Secure Enclave (SE) in Apple devices, and the Trusted Platform Module (TPM) in Windows devices. These elements are isolated from the rest of the device to protect it from malware, and can be used to 1) locally match biometrics on the device, which then 2) unlocks a private cryptographic key which can be used for authentication.

Together, these two elements enable the ability to deliver authentication that is materially more secure than older authentication technologies, and also easier to use. Because rather than require the consumer to carry something separate to authenticate, these solutions are simply baked into their devices, requiring them to do nothing more than place a finger on a sensor or take a selfie.

The rest of the authentication (the other factors) automatically happens "behind the scenes" – meaning that the consumer doesn't have to do the work. A biometric matched on the device then unlocks a second factor – an asymmetric, private cryptographic key,

that can then be used to securely log the consumer in, without a password or any other shared secret.

While the actual composition of these two elements – both biometric sensors and security chips – varies across manufacturers, most of the companies involved in making these devices and elements have been working together to create the FIDO and related W3C Web Authentication standards. The power of these standards is that they enable all of these elements all to be used – interoperably – in a common digital ecosystem, regardless of device, operating system or browser. Which means that it's become really easy for banks, retailers, governments and other organizations to take advantage of these technologies to deliver better authentication to customers. Firms such as Aetna, PayPal, Google, Microsoft, Cigna, Intel, T-Mobile, Samsung, and several major banks are among those enabling consumers to lock down their login with FIDO authentication; the Department of Veterans Affairs recently enabled Veterans logging into the Vets.gov website to protect their accounts with FIDO as well.

Government can play a role in accelerating the pace of adoption of strong authentication through two key actions:

1) First, agencies should look to make use of the FIDO and W3C Web Authentication standards in more of its own online applications. This will set an example for the private sector to follow – and ensure that citizen-facing applications are more secure and convenient to use. The SSA should be among the first here, given the importance of its MySSA online portal.

2) Second, through the regulatory process, government should ensure that regulated industries are keeping up with the latest threats to first-generation authentication – and implementing the latest standards and technologies to address these threats.

4. Back on the topic of identifiers: even if we assume that the SSN is publicly known, that doesn't mean that it needs to be used everywhere. Many of the members of the Better Identity Coalition would love to reduce where they use the SSN, due to the risks that collecting and retaining SSN may create relative to other identifiers. However, in some cases, they are running up against laws and regulations that require companies to collect and retain the SSN.

   Among the legal requirements here:

   - The Federal government requires employers to collect SSN each time they hire someone

- The Federal government requires financial institutions to collect the SSN as part of account opening or applying for a mortgage – and requires them to retain it for up to five years after the account is closed

- The Federal government requires college students to provide their SSN when applying for student loans

- The Federal government requires state governments to collect the SSN when Americans apply for a driver's licenses

- Health insurers are required by the government to collect the SSN of each person they insure

- Many states require blood donation services to collect and retain the SSN of blood donors

- The Coast Guard requires SSN to be collected as part of its Vessel Identification System

Much of industry's ability to reduce their reliance on the SSN will be dependent on the government changing its requirements for them to collect it.

Moreover, this list also demonstrates just how embedded the SSN is as an identifier in so many of our identity processes – and helps to frame the complexity and cost associated with any effort to replace it.

5. Finally, any discussion of the future of the SSN also ought to include a discussion on the future of the SSA. The issue here goes beyond the future use of a 9-digit number to encompass a broader topic: what role should the government play in the future of the identity ecosystem?

   While identity may not be a part of the SSA's mission statement, there is no question that SSA is in the identity business. It's time to acknowledge that fact – and then take a step back to contemplate what that means.

   One of the biggest challenges the U.S. faces when it comes to digital identity is that the country has a number of authoritative government identity systems – the SSN included – which consumers, agencies and businesses have been able to leverage for <u>in-person</u> transactions. However, these systems are largely rooted in the physical world – based on cards and paper – at a time when commerce is moving to the online world.

   Industry has tried to fill the gap with tools like so-called Knowledge-Based Verification (KBV) systems that attempt to verify identity online by asking an applicant several

questions that, in theory, only he or she should be able to answer. But as I noted earlier, adversaries have caught up with these systems, and other first-generation tools that America has used for remote identity proofing and verification.

Against this backdrop, governments at both the Federal and State level should look to modernize their legacy identity systems around a privacy-protecting, consumer-centric model that allows consumers to ask the government agency that issued a credential to stand behind it in the online world – by validating the information from the credential.

The Social Security Administration (SSA) and state governments – the latter in their role as issuers of driver's licenses and identity cards – are the best positioned entities to offer these services to consumers.

To that end, the recent action by this Committee – and the full House – to advance H.R. 5192, the Protecting Children from Identity Theft Act, was a welcome development. The legislation would allow consumers to electronically request that the SSA validate whether SSA has a name, SSN and date of birth on file that matches the one they provide to a financial institution for certain kinds of account openings covered under the Fair Credit Reporting Act (FCRA).

The lack of such a service makes it much easier today for criminals to set up fraudulent accounts with "synthetic identities" using a fake name and a real SSN – often the SSN of a child.

Note that this new bill is not targeting SSN's use as an authenticator, only as an identifier; the goal is to enable consumers to request that SSA verify to a financial institution that a particular person with their name, date of birth and SSN actually exists. Enabling SSA to validate this information will lower the cost of digital transactions and close off a loophole that is commonly exploited by criminals to steal identities and fund illicit activities.

The bill is a great start, and I hope to see it become law this year. That said, it does not go far enough:

1) First, because as a consumer, I'd like to be able to ask SSA to help prove I am really me for a variety of different purposes online, not just opening a bank account.

2) Second, because it limits SSA to only validating three core attributes – Name, date of birth and SSN – when SSA also may have the ability to assist consumers by validating other attributes in SSA's systems.

Note that this concept was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity[2], who, in response to the wave of attacks leveraging compromised identities, stated "The government should serve as a source to validate identity attributes to address online identity challenges." Per the report:

> *"The next Administration should create an interagency task force directed to find secure, user-friendly, privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market. This action would enable government agencies and the private sector to drive significant risk out of new account openings and other high-risk, high-value online services, and it would help all citizens more easily and securely engage in transactions online.*
>
> *"As part of this effort, the interagency task force should be directed to incentivize states to participate. States—by issuing drivers' licenses, birth certificates, and other identity documents—are already playing a vital role in the identity ecosystem; notably, they provide the most widely used source of identity proofing for individuals. Collaboration is key. Industry and government each have much to gain from strengthened online identity proofing. The federal government should support and augment existing private-sector efforts by working with industry to set out rules of the road, identify sources of attributes controlled by industry, and establish parameters and trust models for validating and using those industry attributes."*

Government should act on this recommendation, with a particular focus on having the Federal government 1) identify how SSA and other agencies can offer these services; 2) lead development of a framework of standards and operating rules to make sure this is done in a secure, privacy-enhancing way, and; 3) fund work to get it started.

As part of that effort, the SSA should be directed to outline what other attributes they may be in a position to validate.

In closing, while our current use of the SSN poses some challenges, they are not insurmountable. On the contrary, we have before us a series of ideas on the future of the SSN that can be used to address these challenges – and that are actionable today. I am grateful for the Committee's invitation to offer recommendations on how government can improve the SSN – and SSA's role in the identity ecosystem – for the future, and look forward to your questions.

[2] https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

*Chairman Johnson. Thank you, sir.

Mr. Lewis, welcome. Thank you for being here. Please proceed.

STATEMENT OF JAMES LEWIS, SENIOR VICE PRESIDENT, TECHNOLOGY POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

*Mr. Lewis. Thank you, Mr. Chairman and Ranking Member Larson. I thank the committee for the opportunity to testify.

One of the leading scientists of the 20th century said that an expert is a individual who has made all possible errors in a particular field. And I think that qualifies me as a expert in this issue, since I have been involved in programs like this since 1992, none of which have worked.

So let's give it a try.

We have all heard how the SSN is the key identifier. It is unique to each individual. It is issued by a trusted source. And most importantly, it links to different databases. So your SSN can link to your bank, your tax account, your driver's license. It is irreplaceable.

It is invaluable for business. But as we have heard, it is also invaluable for crime. One estimate is that somewhere between 60 and 80 percent of all Social Security numbers have been stolen. Another estimate puts the cost of stolen Social Security numbers at $16 billion annually. I think the committee is on the right track here by looking at ways to modernize and strengthen the SSN, the Social Security number, because this will provide real benefits and reduce crime.

Our goal should be to provide the same level of service and security that citizens expect from the private sector, or that citizens enjoy in other developed economies.

There are several options for modernizing the SSN. These include federated authentication of identity, public encryption, blockchain, and smart cards. Some of these have been tried in the past, but they faced problems of complexity, cost, and they raise privacy concerns.

Simply publishing the SSN, as you heard, is a -- is the least expensive option, but it doesn't fix all the problems we face.

An easy first step would be to replace the Social Security card with a smart card, a plastic card with an embedded chip, like the credit cards that most of us carry. Millions of commercial transactions are carried out with these cards every day. Most people are familiar with them, which would ease the burden of both acceptance and transition.

A smart card provides a foundation for a security Social Security number. When your credit card is stolen, your financial institution cancels the old one and issues you a new one, issues you a new number. You are still linked to your account, you are still responsible for any legitimate charges, but you are not linked to the old number. And a similar approach might help us in thinking about how to streamline, modernize, and make the Social Security number more secure.

Social Security Administration could use a similar approach. It could administer a smart card approach, or it could contract it out to the private sector, a solution that other countries have used. Further debate is required, and I think we all recognize that, to decide which modernization option is best and, equally important, how we will pay for it, because there is no free replacement for the SSN.

Blockchain technology may offer an option for a modernized SSN, but it is not ready, as you have heard. It is not yet mature.

The best argument for smart cards is that we already use them on a massive scale. Companies and citizens are familiar with them. Implementation, of course, would be difficult. Any change for so venerable an institution is going to be difficult. But we have the advantage of knowing the technology and processes already work because of our experience with credit cards and banks.

Thank you for the opportunity to testify. I look forward to your questions.

Statement Before the

House Ways and Means

Subcommittee on Social Security

"Securing Americans' Identities: The Future of the Social Security Number"

A Testimony by:

James A. Lewis

Senior Vice President

Center for Strategic and International Studies

May 17, 2018

1100 Longworth House Office Building

Mr. Chairman and Mr. Ranking Member, I thank you and the Committee for the opportunity to testify. The Social Security Number (SSN) is the key identifier for the United States. In many ways, it is also out of date. The SSN is widely used for commercial purposes. The prime reason for this is that the SSN is a free credential that is unique to each individual, issued by a trusted source, and links records held in different private and government databases back to the same person. In reality, this makes the SSN indispensable.

The SSN is invaluable for businesses, but it is also invaluable for criminals. One estimate is that 60% to 80% of all SSNs have been stolen. SSN's can be bought in bulk in the cybercrime black market, along with other personal information. Since they are used not only to identify an individual, but to authorize online transactions, stolen SSNs or fake SSNs are a potent source of fraud and identity theft.

SSNs were never designed for online commerce. They were created in 1936, and originally intended only to link citizens to federal benefits. Over time, its use has expanded in both government and private transactions and it has been adopted for online use. SSNs still come on a paper card that is not intended to be either a credential or an identifier. Once stolen, the SSN is very difficult to be replaced. This makes the current SSN system ineffective for electronic commerce. While there have been good steps to let people verify SSNs, fraud is still possible. Modernizing the SSN is a good goal for action and there are several options for replacement.

What I will not discuss is a national ID system, however. I encourage the Committee to avoid going down this rabbit hole. The U.S. has made several efforts over the last twenty years to create a secure digital identifier, but each of these efforts has run into problems of complexity, cost, and privacy concerns. The authentication of identity online is an intricate process. Many smaller countries have solved the problem by creating national identity systems that lets people securely identify themselves online. These are often based on a National Identity card, but the U.S. is not ready for such a bold step.

The committee should avoid a discussion of authentication of identity online and instead focus on modernizing and strengthening the SSN, a more achievable goal that will in itself provide real benefits and reduce the risk of online fraud. Modernizing the SSN could be a first step toward better digital authentication in the U.S The goal should be to provide citizens with the same level of service they would expect from a credit card company or a major online retailer.

In thinking about how to do this, we need to consider how to manage continuity, cost, and complexity in any new system. The most important aspect of this is that any modernization should not break the SSNs critical role as a unique national identifier. A modernized SSN would require decisions on several elements.

There are basically two approaches to reducing the risk of using the SSN as an identifier. The first is to strengthen the SSN to make it harder to steal or use fraudulently. The second is to reduce or eliminate its value as a credential. Moving to a more secure and modern SSN will be a difficult and complex transition. The central goals are to take advantage of the growth in internet connectivity that has occurred in the last decade and to model a modernized SSN on existing online systems and their safeguards. There are several decisions required on what course to take and what options to select. We can sketch out one path (among several) for SSN modernization.

The first step is to replace the paper SSN card with a "smart card," a plastic card with an embedded integrated circuit (a "chip"), like the credit cards most of us carry. This is the solution adopted by credit card companies some time ago as a way to reduce fraud. Most people are familiar with this kind of card, which would ease the burden of both acceptance and transition for SSN holders.

Even if nothing else was changed, a smart card would be an improvement over the current paper card. A smart card provides the foundation - for use now or for later - to build a more secure system. If the Congress decided to take advantage of a smart cards additional capabilities, it could model a modernized SSN on the credit card system and its safeguards. When your card is stolen, your financial institution cancels the old one and issues you a new card number. You are still linked to your account, but not to the old credit card number.

SSA could use a similar approach. SSA should have some way to replace an SSN when it is compromised, since compromise is unavoidable. The added complexity is that a replacement SSN must preserve the ability to link multiple records to the same individual. There are ways to do this but they involve additional cost and responsibility for the SSA.

The SSN itself would not be used in commercial transactions. It would instead be used to generate a number associated with the SSN account. If this number was compromised, a new number could be generated using the SSN "root." The SSN itself could be kept secret, encrypted, and the generation of the replacement number could be controlled by the SSA.

For example, the new smart card SSN could use a proxy number, a replaceable number linked to your SSN account. You would still be issued an SSN at birth, but it would not be made public. Instead, you would get a proxy number, stored on the new smart card and linked to your SSA account number. People are already familiar with this from credit card or debit card use. Your credit card has a number used to authorize transactions. It is linked to an account at a financial institution that has its own account number. This account number is linked to your SSN, for tax and verification purposes. When your credit card is stolen or compromised, you notify the card company, which generates a new credit card with a new number for you, linked to your account, whose number does not change.

For the SSN, this means the number on your SSA-issued smart card will not be your SSN. Instead, it will be a "proxy" number that links to your SSN. The proxy number could use a different format than the nine-digit SSN to avoid confusion, and the SSN itself would not be used for commercial purposes - this might require legislation to require companies to transition to the new system and to replace the SSN in their account with the new proxy number.

For this to work, merchants, banks and others who now use the SSN will need some way to verify that the proxy number links to a real SSN account. This means SSA will need some sort of verification process similar to that used by credit card companies. When you present your credit card, the number is automatically checked to see if the card has been reported stolen or if there are indications of fraud. An SSN verification system could build off existing verification systems already in use by SSA, where an employer submits an SSN to see if it is a real number, except now these systems would need to be expanded to confirm that the proxy number is linked to a real account. At some point in the future, SSA could even develop a mobile "app" for the verification process.

SSA currently operates two verification services that confirm the social security number and name for wage reporting purposes. If it was to move to a system similar to that used by credit card, it would need to first use the SSN issued at birth to generate another number (a "pseudo-SSN") that could be used for identification purposes (and which could be replaced if compromised), and then adapt the existing verification system to allow people to check if the pseudo-SSN was still valid. SSA could develop additional measures (similar to those used by financial institutions) to identify possible fraudulent use. SSA would also need some system for citizens to report when their number has been compromised and needs to be replaced.

Exchanging a compromised proxy number would require a citizen going to SSA and requesting a replacement. Before issuing a replacement, SSA would need to verify that the request was legitimate. This requires some kind of process for the authentication of identity. The system that banks and online merchants use is multifactor authentication. This uses a "shared secret," usually a password, and then some other some other secret to verify identity. Again, the transition burden would be reduced as may citizens are already familiar with these systems.

To replace an SSN, a citizen could call or log onto the SSA website. There are several different approaches to multi-factor authentication that could be used to ensure that the replacement request was legitimate. SSA could issue a PIN number with the smart card, and the PIN would need to be entered to request a new number. SSA could use the mobile texting system many banks and online service provider use, where you enter a request and then are sent a code to verify identity, such as with Gmail or Office 365.

SSA would need to assign a password to each account, and then take additional steps depending on what authentication method Congress choses, whether it is a PIN, additional shared secret (like

asking user to identify the color of their first home) or to generate an authorization code. SSA would need the ability to receive a request, verify the password, and have on file an email address or phone number to which an authorizing code could be sent.

This sounds complicated, but hundreds of millions of commercial transactions are carried out every day using these systems. Congress needs to move the social security system into the 21st century. There are costs, however. Non-recurring costs include replacing paper cards with plastic smart cards, building an online account verification system at SSA, and the cost to firms and agencies to change their number used in existing accounts from the real SSN to the proxy. Recurring costs would include providing the verification service and the cost of regenerating a new proxy number.

Given the complexity of these systems, and the immense experience of the private sector in implementing them, Congress could choose to rely on private sector service provides to supply the smart card and the proxy number. Commercial venders already have the "backroom" processes needed for this smart card approach. Private sector suppliers would still rely on SSA to create and hold the "real" SSN. This would reduce the burden on SSA, but raises the question of who pays for all this? Does SSA subcontract the issuance process to the private sector, should there be user fees (something almost certain to be unpopular, although we charge for passports and driver's licenses), or should a new system be subsidized from general revenues.

The options are to have SSA do this, to contract to the private sector, or to piggy-back on the existing driver's license issuance process (where states could either charge customers or be subsidized). States have not yet moved to smart cards, however, and an effort to mandate this would almost certainly run into opposition. Further debate is required to decide which might be bets, but no modern system comes without cost.

One consideration to bear in mind is that in the past, interoperability has been the principal flaw in private credential systems. Countries with smaller populations face a lesser burden as they have fewer companies involved (often only three or four), but the UK, with a population of 65 million, found it difficult to implement a "federated," private sector authentication system, as did the U.S. in the mid-2000s. A bad outcome would be a world where each individual required multiple credentials - this is one of the advantages of the SSN and a replacement system would have to duplicate this.

If the Congress chooses to let private sector entities issue an SSN-based credential, it will need to create incentives for companies to offer this service. Incentivizing consumers might require some kind of appropriate liability limitation, mirroring that used in the Fair Credit Billing Act. Congress will also need to develop privacy rules that restrict the ability of a private sector provider to "harvest" user data for commercial purposes.

Congress would need to set a transition period for the move to a smart-card based system, and it would have to create negative incentives for companies and individuals to move from the SSN to the proxy number, perhaps by forbidding SSN use perhaps by publishing SSNs, which would lower their value as an identifier. Publication would force companies to find an alternative solution and, judging from the Swedish and Norwegian experiences, could incentivize a market for private credentials. Private credential issuers could be required to meet identification standards such as HSPD-12 or NIST's SP 800-63 *Digital Identity Guidelines.*

The security risks of publishing SSN could be reduced after publication, by replacing SSNs with a proxy number and its more robust identity verification system. For citizens, the would receive a new smart card in the mail with a new proxy number, perhaps followed by separate mailings with the PIN needed to access their account. There are ways to automate the replacement process that could be developed to ease the transition burden. This smart card approach would permit the adoption of blockchain technology should blockchain ever mature to the point where large scale deployments are possible.

Simple publication of SSNs is the least expensive option for the Federal government and for the private sector and would create incentives to use something other than the SSN as an identifier (it would still need to work as an identifier for tax and benefits purposes). While creating a searchable database has associated costs for SSA, it would be cheaper than the annual cost of fraud and identity theft (an estimate in the economist pegs this at $16 billion).[1]

The effect would be to make the SSN more secret. If a consumer was notified of a data breach that compromised their proxy SSN, they could go to an SSA website and generate a new number. To request a new number, SSA would need to move to some kind of multifactor authentication such as that now use by many banks, so that a consumer requesting a replacement would need a password, a PIN, and an access number sent to their cellphone or email (this would have to be the cellphone of a parent or guardian for minors).

This approach would retain the SSNs critical function as a unique identifier of an individual while providing some way to replace an SSN when it has been compromised - and compromise is unavoidable. The goal, as many have said is to separate the SSN as an identifier from its use as an authorizer.

I have not discussed a public key infrastructure or federated identity system. Having been deeply involved in earlier federal effort to create PKI or federated identity systems, I believe they are too complex and costly to be successfully implemented. Perhaps the best argument for this smart card approach is that we already use it on a massive scale, for credit or debit cards or for online accounts.

[1] https://www.economist.com/news/leaders/21739961-gdprs-premise-consumers-should-be-charge-their-own-personal-data-right

Companies and citizens are familiar with it. Implementation by SSA would be difficult, but we have the advantage of knowing that the technology and processes already work.

Thank you for the opportunity to testify on this subject and I look forward to your questions.

*Chairman Johnson. Thank you, sir. I appreciate that. We will now look to questions.

As is customary, for each round of questions I will limit my time to five minutes, and I ask my colleagues to also limit their questioning time to five minutes, as well.

Acting Commissioner Berryhill, the alarming story about the child in Arizona raises many questions about how Social Security treats identity theft victims. Are you taking a close look at how you handle requests for new Social Security numbers?

*Ms. Berryhill. Mr. Chairman, I am very aware of the case that you are referencing in Arizona, and thank you for bringing that to our attention. We have worked very hard with our staff to issue clarification policies to all of our front-line employees. We have also held national calls with all managers, area directors, and we also decided that we would have regional experts available to the front-line employees at the time, when the time comes, where they have a complex case. In this situation, we would consider that a complex case.

So having those regional experts that are well-trained on enumeration, on replacement cards, on new -- issuing new SSNs I think will help. So we took that immediate action, and all those actions have been accomplished.

*Chairman Johnson. Well, with more than 1,200 field offices, what are you doing to make sure that your policies are being followed?

*Ms. Berryhill. That is why we held national calls with all of our managers and our area directors that have oversight to our managers, and we will continue to do checks and balances to make sure that those policies are followed.

I really believe having a regional expert there so the front line employees can consult if they have questions is really going to be a key change for SSA.

*Chairman Johnson. You know, I was shocked to learn that Social Security employees' voicemails tell callers to record their Social Security number with their name and phone number to get a return call. How is that a good practice, given all the concerns with identity theft and phone scams?

*Ms. Berryhill. I certainly understand that, and I am aware of that situations that we have (sic).

We do use the Social Security number to look up our records. Certainly, if an individual is not comfortable leaving their Social Security number, they should not do that. However, it does expedite the transaction when they call us back. We can certainly,

in the front line, pull up someone's record, have that available so when we return that call we can quickly go through the process with them and answer any questions.

But again, if someone is uncomfortable, they should not leave their Social Security number.

*Chairman Johnson. Okay. Well, maybe we ought to take another look at that.

Mr. Grobman, this panel has talked about some big ideas today. What do you think?

*Mr. Grobman. I think the --

*Chairman Johnson. Is now the time to take action?

*Mr. Grobman. Absolutely. I think the one thing that we heard universally across this panel is using Social Security numbers as authenticators is something that needs to be addressed as the most time-critical element of the issue.

There are clearly other issues on the fringe of Social Security number as an identifier. But from a magnitude perspective, looking to remove Social Security knowledge as an authenticator is something that we must act on immediately, and invest whatever it takes in order to make that a practical reality.

*Chairman Johnson. Yes, we have been trying to do that for 20 years.

Mr. Larson, you are recognized.

*Mr. Larson. Thank you, Mr. Chairman. I want to thank the panelists. It is -- we have an awful lot of hearings, but it is always refreshing when you actually have panelists who give you some solutions, as well.

Acting Secretary Berryhill, first of all, let me commend you for your service.

Let me also acknowledge that there is no one who has been working harder to make sure that we have a permanent chair of -- the Secretary of Social Security than the chairman himself. And we have -- support him in those efforts, and hope that the administration will act soon, but want to thank you for your service.

I think there is unanimity on the committee with respect to authentification (sic). How would you go about implementing that? And what is the cost of that?

*Ms. Berryhill. So certainly, any ideas -- I think there has been some great ideas listed by the panel members today -- we will take all of them and review them and cost

them out. Certainly not something I could address today. Lots of ideas are good, but then you have to look at the price tag that is attached to them.

So again, we will go back and take a look at any ideas that the committee would like us to look at.

*Mr. Larson. Any idea on that price, Mr. Grobman?

*Mr. Grobman. I think one thing that we need to recognize when we look at the price is the price of not taking action.

So if you look at the cost related to fraud or misuse of Social Security numbers as authenticators, my opinion is that is a staggering figure that needs to be comprehended when looked at the cost of implementing a new plan.

*Mr. Larson. Mr. Lester, you had the -- a number of solutions. But one of the things that you emphasized is that you -- we make sure that we steer clear of any biometric solution. Would you explain why?

*Mr. Lester. When Congress passed the Privacy Act in 1974, they were explicitly responding to and rejecting calls for a national identification system. There are national identification systems that rely on biometrics in other countries that raise really grave civil liberties and privacy concerns.

For example, in India their new biometric system -- AADHAR, I think -- was recently breached, compromising the biometric data on its 1.2 billion citizens. I think that any problems with a biometric system are demonstrated by the recent breach of the OPM.

*Mr. Larson. Would all the panelists agree that that is a reasonable concern?

*Mr. Grobman. I think it very much depends on the problem that you are trying to solve. In India, part of what they were trying to solve was there was no starting point, and they needed to ensure that an individual only registered a single time for benefits. So, by using biometrics, it prevented an individual from registering in one town and then walking down the road to another town and registering again.

So, in that case, biometrics was a practical technology in order to solve that specific problem. I don't believe we have that problem at scale in the U.S. And therefore, I think the points are well taken that we should look for other, less privacy-intrusive mechanisms as a first step. And as Mr. Lewis mentioned, things such as smart cards can be a much more rapid practical option that could be distributed without requiring every citizen to have biometrics --

*Mr. Larson. Is there consensus amongst the panel with respect to smart cards?

Mr. Rosenzweig?

*Mr. Rosenzweig. I -- Rosenzweig. I think it is a good interim solution. But to be honest, you know, the smart card security system is not itself terribly robust. We have all experienced credit card fraud, as well, that is a result of a lot of that.

On the issue of biometrics, I think it really is the difference between a centralized database and a distributed database. Biometrics, as a localized identifier, is actually something that the -- President Obama's White House supported as a substitute for passwords because they are more readily usable by most citizens than the password system.

So I wouldn't write with such a broad brush --

*Mr. Larson. You also objected to one of Mr. Lester's solutions. Could you explain why? And hopefully Mr. Lester will get a chance to reply.

*Mr. Rosenzweig. Well, I don't so much object. Regulation is clearly one of the normal tools in our toolkit here in Washington, alongside taxation --

*Mr. Larson. Is it regulation or the efficiency of the ability to regulate?

*Mr. Rosenzweig. Well, we all live in Washington. I am not a fan of our efficiency in the regulatory system. To take just -- to be brief about it, we have already acknowledged that it would have to exclude legal uses --

*Mr. Larson. City of northern charm and southern efficiency?

*Mr. Rosenzweig. Indeed.

*Mr. Larson. No disrespect to anyone from the South, but --

*Mr. Rosenzweig. I think it would cost us quite a bit and take far too long.

*Chairman Johnson. The gentleman's time has expired.

Mr. Kelly, you are recognized.

*Mr. Kelly. I thank you, Chairman, and thank you all for being here today.

Mr. Rosenzweig, I had a coach in high school had the same name, we just called him Rosie. So maybe the rest of the panel can do that.

[Laughter.]

*Mr. Kelly. First of all, thank you all for being here. But, you know, Ms. Berryhill, I am -- I think when we look at the size and scope of the program, and the number of beneficiaries, is there anybody in the private sector that even comes close to facing these types of problems, as far as making sure we are sending the right money to the right people, and the fact that there is so much fraud in the system already?

Is there any approach out there that people are looking at that would make sense?

*Ms. Berryhill. So, you know, first of all, we need to protect our records. And our focus for the Social Security number has been collecting wage information and paying benefits.

We have a robust, anti-fraud process that we put in place, so we review claims ahead of time, we will flag certain high-risk claims. But as far as comparing that to the private sector, we have to make sure that, in government, that our beneficiaries, our recipients are protected, and their data is protected.

*Mr. Kelly. Well, it just seems to me the very nature of the way we do things today -- we have a safe that we put things into that we cannot lock. There is somebody finding a way to get into this data all the time, and yet we keep thinking, well, you know what? This is just the way we do things today. We are going to just have to keep going down that path. I just -- I am really fascinated.

Mr. Grobman, you said something I have written down here. Is there any information that indicates the cost of not finding a remedy to this? I think those numbers would be so staggering that most of us would not even want to discuss it.

Is there any idea of what the cost of not fixing this is -- because it seems to me -- there is an old saying. You keep doing the same thing over and over again, expecting a different result -- I don't see how we fix this the way we are going right now. So that cost of not fixing it, any ideas?

*Mr. Grobman. I don't have a quantitative number.

*Mr. Kelly. Yes. Nobody does.

The chairman is right; it is the definition of insanity, but --

*Mr. Grobman. There is one estimate, and it was from The Economist, and it was $16 billion a year.

*Mr. Kelly. Sixteen?

*Mr. Grobman. Billion.

*Mr. Kelly. Billion, with a B. That is -- down here. One, six, and with a B, billion. So -- okay.

Mr. Grant, some companies have recognized problems with the Social Security number and have shifted their business models in response. Can you share some examples in the private sector of how people are addressing this?

*Mr. Grant. Sure. So one of the founding members of our coalition is Aetna, who -- their chief security officer, Jim Routh, and the team there led an effort I think they launched in 2014 focused on reducing the instances of the Social Security number within their systems.

Talking about costs, this is a 6-year, roughly $60 million investment that the company is voluntarily undertaking because they think that they can reduce their risk profile by reducing the instances of the SSN across their enterprise. And I think to date they have eliminated about 10 billion instances, which -- not that they have 10 billion beneficiaries, but it shows you, if I am one of theirs, that I probably had my SSN in a dozen different systems.

So, you know, companies are willing to do this today, and I think you are starting to see, you know, particularly Fortune 500 companies who are holding on to SSN are looking at it as a liability. But the cost is significant. It can't happen overnight.

They are also hindered in that, as a health insurer, they are required by the government to leverage the SSN for pretty much all of their government business, as well as any beneficiary who they have to report to the government had health insurance.

So, you know, I highlighted this a little in my opening testimony. There is a lot of government requirements that are out there that state that private industry has to collect the SSN. As long as we have those out there, it is going to be quite hard to eliminate it entirely.

*Mr. Kelly. As we keep going forward, then, I -- and we all look at this program and we refer to it as an entitlement, and some people say that is a negative term. No, entitlement means you are entitled to this benefit because you have paid into it your whole life.

I think there is total agreement on this committee and throughout the whole Congress that we have to protect this program because it is so vital to our folks.

Listen, I really appreciate you all being here today, but could you please continue weighing in and give us other examples and other solutions to what it is we are trying to fix? It is just this is so massive right now, I think it is one of those things you sit back and say it is too big for us to work with.

But I like Mr. Grobman -- it is only going to get bigger and bigger and more expensive if we don't do it.

*Mr. Grobman. Absolutely. And I think, following up on that comment, one of the things we need to look at is the opportunity cost of continuing to try to protect Social Security numbers from becoming public, when we know that they are already public in so many cases.

So, although there are a number of interesting efforts put forward in the last few years to reduce the disclosure of Social Security numbers, what I would ask is what if we re-purposed all of those efforts into building a modern authentication system so that we just simply use Social Security number as an identity, not an authenticator.

*Mr. Kelly. Very good. Thank you.

*Chairman Johnson. The gentleman's time has expired.

Mr. Pascrell, you are --

*Mr. Pascrell. Thank you, Mr. Chairman. A great panel.

I want to start by -- Mr. Lester, would you respond to Mr. Larson's question that you didn't get a chance to respond to before?

*Mr. Lester. Sure. So I think you are talking about the cost --

*Mr. Pascrell. You got 30 seconds.

*Mr. Lester. I think you are talking about the costs of regulation, right? So Mr. Rosenzweig talked about the cost of regulating this, and I would just like to mention a cost which is 16.7 billion, to be precise. That is the amount that was stolen as a result of identity theft in 2017. The cost of not regulating is in the billions.

And furthermore, what we are talking about is restoring the Social Security number to its original purpose, which is to be used only by the Social Security Administration. That is what it was intended for. Congress has many times looked at this. When they passed the Privacy Act in 1974, that is originally what it was intended to do. So --

*Mr. Pascrell. Thank you.

*Mr. Lester. Yes.

*Mr. Pascrell. Thank you.

Last month, Mr. Grant, the Ways and Means Committee marked up a bill to protect children and consumers from identity theft -- it was H.R. 5192 -- by helping reduce the prevalence of synthetic identity fraud. The bill would do this by facilitating the validation of identifying information provided by lenders, and upon the consent of the customer -- consumer, rather, I am sorry -- through a database maintained by the Social Security Administration. The bill is considered an important step that Congress took to help prevent identity theft.

But I wanted to get your view very quickly about what the extent this validation system will solve the problem or not. What is your thoughts?

*Mr. Grant. So I actually talked about this a bit in my written testimony, but didn't get to it in my opening statement. I think it is a great first step.

The idea actually goes to a key point that I flagged in my opening statement, which is can we shift the model a little bit when it comes to identity verification services, so that government agencies like the SSA that are the authoritative roots of trust when it comes to my data -- they have got the truth, in terms of what my name and my SSN are -- why can't I ask them when I am opening an account to let my bank check to see if there really is a Jeremy Grant with my SSN and date of birth in their system?

And so this new bill, if it passes -- and I think it is also in the Senate reg reform package for banking that is currently in front of the House -- will be a good first step.

But two things I would add to that. It is only limited to account openings covered under the Fair Credit Reporting Act. I can't imagine, as a consumer, why I wouldn't want to ask SSA to validate that for everybody. And then I think the other question that has come up is if we are worried about synthetic identity fraud, this will take care of new account openings going forward. But there is probably, you know, thousands, if not millions of synthetic accounts that are out there today.

And so, one question has been should financial institutions have an opportunity to have a one-time window where they could retroactively put existing accounts out there to make sure that things match?

*Mr. Pascrell. Thanks, Mr. Grant, I appreciate that. Look, there is widespread data breaches at the Office of the Personnel Management, Home Depot, J.P. Morgan, Target, U.S. Postal Service, and, of course, Equifax. And they highlight the need to focus our attention on how better to authenticate identities.

From a consumer protection standpoint, this is outrageous. Hackers assessed -- accessed personally-identifiable information from millions of customer accounts. In the wrong hands, access to Social Security numbers, birth data, address, driver's license number could turn someone's life upside down. We must do everything possible to

establish privacy safeguards Social Security (sic). Protecting the individual's personal information to ensure their identities are protected must be one of our top priorities.

Should the burden be on the government to create a unique identifier to identify individuals, or should it be on the private corporations to establish unique identifiers with their clients? Anybody?

Mr. Lester?

*Mr. Lester. Right. So I think that is where the importance of context-specific identifiers comes into play. So if you are transacting with a company you have a unique identifier for that company. That way, if an identity thief steals that identifier, they do not have access to all your accounts, and they cannot open new accounts in your name and destroy your financial life.

*Mr. Lewis. Congressman, if I could just add, in the many attempts we have had to come up with a national identifier, we have learned that there is only one trusted source, and that is the government. And that is why SSA is the default identifier. People don't trust other sources.

*Mr. Pascrell. Mr. Chairman -- thank you, but I must add this point to you. Are we really serious about doing this? Are we really serious about changing the culture, which is a different thing? And why haven't we done more? We need to ask ourselves that question.

*Chairman Johnson. You are right. Thank you for your questions.

Mr. Rice, you are recognized.

*Mr. Rice. You know, this is a incredibly complicated problem, but it is not new. This is not new. Identity theft has existed since people had identities, right?

Our -- thinking back to law school and commercial paper, and in order to allow for the free flow of commerce, we had laws to protect consumers with commercial paper. So a bank had a duty to know your signature, right? So if somebody forged your check, that wasn't your problem, it was the bank's problem. And that kind of applies here, too, doesn't it?

I mean if somebody negligently releases your personal information, don't they have a liability for that?

Mr. Lester?

*Mr. Lester. Absolutely. The burden is on the companies that collect this information. It is important to stress that Equifax chose to collect the information on consumers. Consumers did not provide that information to Equifax. And in fact, when Equifax is breached, they are the ones that put the cost on the consumer by charging them for credit freezes and fraud monitoring. And I think it is also important to stress that there needs to be --

*Mr. Rice. Did Equifax --

*Mr. Lester. -- a private right of action --

*Mr. Rice. Did Equifax have liability for that?

*Mr. Lester. Absolutely, which is why I need to stress that there needs to be, in any privacy law, private right of action for consumers to get redress.

*Mr. Rice. So you are advocating for specific identifiers for everything.

And I think I heard Mr. Grant say he didn't have a problem with Social Security as a national identifier. I think you said the same thing, Mr. Grobman, and you did, too, Mr. Rosenzweig. And I kind of agree with you.

I mean everybody has got an identifier, right? It is their name, at the very least. But the name is not unique. I mean there is a lot of Tom Rices out there.

So you need some type of a national identifier, I would think, to make commerce work. And I don't know why Social Security couldn't be that. But it can't be an authenticator, because it is not private any more. Right?

Mr. Rosenzweig?

*Mr. Rosenzweig. Using my Social Security number as an authenticator is as stupid as using the last four letters of my last name as my authenticator. It -- or the last four digits of my phone number, which is another -- mobile phone numbers, now that they are mobile, everybody has one and it is probably one you are going to keep for the rest of your life, even if you move to Washington.

*Mr. Rice. And I just think that -- I mean, personally, just as a matter of common sense, I think completely -- the idea that you would completely identify -- I mean eliminate any sort of unique identifier is just not practical. I mean we have got to have some kind of unique identifier, and I don't know why it couldn't be your Social Security number.

So I would think that the way to attack this problem -- because this -- I don't care what we do, I don't care if we come up with the most, you know, beautiful and complex system that would do away with any hacking today, tomorrow the hacker is going to figure out something different. This is not new, it has been going on since the beginning of time, and it is going to keep on going on.

So I would think that the way to attack this is kind of like they did with commercial paper, and that we should put liability on people who negligently release your information.

Mr. Rosenzweig?

*Mr. Rosenzweig. Well, there has been at least one proposal by a colleague of mine who was in the last administration to make people strictly liable for that.

For myself, I would probably prefer a negligence standard over strict liability, but I do think that what you are onto is exactly the right economic answer, which is putting the obligations on the least cost avoider. One of the reasons that I kind of like my fanciful proposal of publication is that it makes it impossible for anyone to maintain the idea of security for the Social Security number as an authenticator. Liability would be another opportunity.

*Mr. Rice. What do you think about that, Mr. Grobman?

*Mr. Grobman. Oh, cyber crime is a market-driven enterprise. Cyber criminals are looking to steal things of value. And the reason that cyber criminals are looking to steal Social Security numbers is in today's world they have value because they can be used as an authenticator.

One of the most practical ways to stop the theft is to de-value what they are going after. And that is, in general, a much more practical mechanism at scale than trying to have the world --

*Mr. Rice. Okay, I got to stop because I only have 10 seconds. If you all would respond to this by raising your hand, do any of you -- who of you have a problem with using Social Security numbers as an identifier, but not an authenticator? One. One out of eight. Thank you.

*Chairman Johnson. The time has expired.

Ms. Sanchez, you are recognized.

*Ms. Sanchez. Thank you, Mr. Chairman, and thank you to all of our witnesses.

Social Security numbers were originally created as a way to track earnings, and were never meant to be used as an identifier in the private sector. The Social Security number has since morphed into a tool used to identify and authenticate individuals in a number of different situations, greatly expanding the universe of people and companies who have access to this incredibly valuable information.

The ubiquity and widespread use of Social Security numbers has left consumers vulnerable to identity theft helpless to stop it.

As we all know, Social Security numbers are incredibly valuable for identity thieves, and can be used to open new accounts and credit cards, or even take out mortgages, often leading to financial ruin for unsuspecting and innocent consumers.

And as technology continues to advance at alarming rates, our unique Social Security numbers are increasingly vulnerable to cyber theft and fraudulent use. Recent data breaches demonstrate the urgent need to secure this information and just how valuable Social Security numbers and other personal data are.

The Equifax hack alone comprised over 145 million American -- pardon me, compromised over 145 million Americans' personal data, including their Social Security numbers. That is almost half of the U.S. population who are now at risk for identity theft or financial fraud.

Social Security numbers have become the default identifier because they are truly unique, standardized, and can be verified. But as more and more of our personal information is available on the dark web for cheap, we need to start thinking about the best ways to identify and verify individuals.

Mr. Lester, I would like to begin by asking you. Americans, consumers, don't have a full picture of what information is being collected about them. What kind of data is being collected about Americans? And are companies required to protect it?

*Mr. Lester. Thank you. So first I would just like to clarify raising my hand to Representative Rice's poll question, because it wasn't a yes or no answer. I don't have a problem with the Social Security number being used as an identifier for Social Security.

To answer your question, companies are now collecting vast amounts of data on consumers, and the problem is that consumers do not have control over this data.

When Equifax collects data from consumers it is getting it from other commercial sources, and consumers are not providing it to Equifax. And so, in addition to limiting the use of the Social Security number in the private sector, consumers need to have control over their personal information.

There needs to be a default credit freeze so that companies like Equifax can only disclose your information when consumers have affirmatively opted in. This would solve the problem of identity thieves opening up new accounts in your name, if Equifax could only pull your credit when you, as the consumer, have affirmatively given them permission to do so.

*Ms. Sanchez. Great. And -- but I want to get at a -- sort of a larger question that folks wonder from time to time: Are companies required to protect that information?

*Mr. Lester. There is no federal standard right now for data security. The Federal Trade Commission does enforce data security when companies -- you know, they have authority over unfair and deceptive practices. So if a company is representing they have good data security, like in the case with Uber, they represented over and over again our data security is great, when in fact it was non-existent.

But no, there needs to be national standards that set a baseline, because states need to have the freedom to regulate upward in this area, because it is a dynamic and evolving field. So there needs to be a federal standard that sets a floor for data security.

*Ms. Sanchez. I would agree with that, and I would just say that I believe most consumers believe that companies are required to protect their information.

Mr. Lester, could you talk a little more about how context-specific identifiers work, and the medical identification number that they use in Canada?

*Mr. Lester. Oh. Oh, yes. So the medical identification number in Canada, as I understand it, it is a unique context-specific identifier. I am not super familiar with it. So I can certainly get back to you with more information on that.

*Ms. Sanchez. I would appreciate it, because I would be interested in knowing how that specifically works, because it might be instructive in terms of setting policy for how we begin to reign in the ubiquitous use of the Social Security number.

*Mr. Lester. And there is many other examples of context-specific identifiers. In my statement I mention, like, the university identifier that is a recent innovation by universities like Georgetown, my school, where they give you a nine-digit ID number in lieu of using your Social Security number.

*Ms. Sanchez. Thank you, and I yield back.

*Chairman Johnson. Thank you.

Dr. Wenstrup, you are recognized.

*Mr. Wenstrup. Thank you, Mr. Chairman. I appreciate it. Thank you all for being here.

Mr. Rosenzweig, I don't have a question for you, I just wanted a shot at saying your name, and I hope I got it right.

[Laughter.]

*Mr. Rosenzweig. Perfect.

*Mr. Wenstrup. Thank you. My question is for Ms. Berryhill. But listening to Mr. Johnson's story earlier, I am reminded of a song called "Secret Agent Man," you know, and it says we are giving you a number and taking away your name. And that is a concern, obviously.

But I want to ask you about getting a new Social Security number. You know, when you lose your credit card, or it gets stolen, I tell you what. That bank wants to get you a new one right away: one, because they want you to use it again; and two, they want to make sure that no more money comes out of their account, because it personally affects them, as well.

And I don't see the same for the Social Security Administration in that environment because, if you think about it, when somebody's Social Security number is taken, the fraud is either at the bank, or through the IRS, a taxpayer. Maybe, if somebody is getting your Social Security check, it may affect you. I don't know. I am kind of asking about that.

But why do we make it so difficult to get a new number when that really is the problem? Because I don't know that there is the same amount of concern on the Social Security Administration like there is at the bank when your credit card gets taken. And I know somebody mentioned it might be, like, $34 to get a new card. Well, that may be a lot on your end, but it is pretty small on the other end, where the fraud is taking place.

So why is it so difficult to get a new number?

*Ms. Berryhill. So usually it is a last resort to issue a Social Security -- new card, a new number, because it doesn't always solve the problem. Many times banks, other companies, will cross-reference the old number to the new number. So you haven't really solved the problem in many situations.

We do look at misused -- are people disadvantaged? Are they not getting a loan for their house? Are their IRS tax returns and so forth -- but again, I hope that our recent change in looking at our instructions to our front line will help that.

But our number, again, is really designed to collect wage information and to pay benefits. As you can see, many of the examples are really about credit card fraud, banking fraud, not about our programs.

*Mr. Wenstrup. But let me get back --

*Ms. Berryhill. Our --

*Mr. Wenstrup. Let me get back to my question. There is no harm, monetarily or otherwise, to the Social Security Administration's budget. It is usually affecting someone else. So you don't have the vested interest that the bank does in this situation. And the cross-referencing, that doesn't need to happen. They get rid of the old number. They don't need to keep that data. So I don't find that as a very good answer as to that being a problem.

So I really think you need to take a look at what can be done to get somebody a new number, because that is exactly what a business is going to do. If your identifier is stolen, they have a motive to get you a new one to protect themselves. But I don't find that you are at risk when somebody's Social Security number is taken away in any way. So there is not this desire to solve this problem.

But $34, if that is what it actually costs to give somebody a new card, new number, whatever the case may be, that is a pittance to the hundreds or thousands of dollars that are going out on the other end. I just want to -- I want to clarify that, because there is really no detriment to the Social Security Administration, is that right?

*Ms. Berryhill. Well, I don't know if I would agree with that. Certainly, if we open up the flood gates and said everybody that wants a number come on and get one, we probably --

*Mr. Wenstrup. No, no, no, you would have to have a reason, not just say I don't like the number, it ends in an odd number and I want an even number. That -- let's be realistic here. We are talking about people that have been victimized, not just anyone who wants a new number.

*Ms. Berryhill. And again, we believe that we want to do due diligence, we want to know what has happened with that number, we want to make sure that it is appropriate to assign them a new number.

*Mr. Wenstrup. I get that. But why is it so hard? Why is somebody told they have to change their name?

*Ms. Berryhill. That was not an appropriate answer to say you change your name.

*Mr. Wenstrup. Well, thank you. I think we need to look into that further.

I yield back, thank you.

*Chairman Johnson. Thank you. Is Mr. Schweikert here?

*Mr. Schweikert. Mr. Chairman, I apologize. We also have the -- running at the same time, so --

*Chairman Johnson. You are recognized if you care to make some questions.

*Mr. Schweikert. And I actually had a couple -- have you ever actually started to write down a couple questions and -- where some of us have brutal disagreements on the utilization of node networks and -- but it is also a threat to certain companies.

So I want to go -- I want to take one gigantic step backwards, because I have missed a number of the questions here. If I came to all of you, either as policy, technology experts and said how do we design almost a single portal in our society that, whether -- have a combination of multi -- I am a big fan of certain token tradeoffs with the biometric and a password.

So you could go on there and see your last 10 years of your IRS tax returns, or of your Social Security benefits, your veterans discharge, your -- you know, where all these things that we, as government -- all of us, as government -- hold on you, and create a single portal so you could see them, but in a way that would be safe, robust, elegant.

And we have actually been sketching out a concept of sort of a, you know, pass code biometric to a token back -- if I was to run down the line, A, is that just techno-Utopian; but B, would it actually not only solve our issue here on the misuse of Social Security numbers, but also some of the other policy decisions we as Congress and the bureaucracy have made of starting to blind documents for our Medicare population, and those things, and now having to get unique identifiers, and the re-issuing of such things, and the confusion and cascade of chaos I expect to come from that?

And could -- run down. Let's start. If I came to you and said I don't want a simple, incremental solution, I want a disruption of more -- of a unified portal, can it be done?

*Ms. Berryhill. So my first concern was if that unified portal was breached, does that mean all of my information is then out there from all different --

*Mr. Schweikert. It wouldn't if we designed permissions. So -- and we will probably get to that, but there is a way to -- so let's right now, for theoretically, just say it is -- we were able to level -- produce levels of security.

*Ms. Berryhill. I would certainly be willing to work with you on any ideas that you have. But again, my concern that if one portal -- everything was breached, we would be in a worse situation today.

*Mr. Schweikert. Okay.

*Ms. Curda. It sounds like a nice, aspirational idea. And the federal government, in terms of designing such complex systems, does not have a great track record. And it is extremely costly, so --

*Mr. Schweikert. We were thinking we would go to McAfee and --

*Ms. Curda. Very difficult to do.

*Mr. Lester. So, moving towards centralized database is exactly the wrong approach. I would use the example of container ships. They are compartmentalized, so that if there is a rocky wave, all the oil is not in one container to capsize the ship. It is the same with identity. As --

*Mr. Schweikert. So why do countries like Estonia and others have incredible success because you create levels of permission that require -- that -- it is a unified portal, but different levels of permission and pass and security?

*Mr. Lester. Is that for me?

*Mr. Schweikert. Yes.

*Mr. Lester. I don't know about the case of Estonia. As I understand, it is a much smaller --

*Mr. Schweikert. Yes, what is your coding background?

*Mr. Lester. I am sorry?

*Mr. Schweikert. Your coding --

*Mr. Lester. My coding background? I don't have a coding background.

*Mr. Schweikert. Okay, sorry. And I am sorry, I was trying to go more technical than that. I am not being mean.

*Mr. Rosenzweig. I would say that Estonia is a good case study. My concerns would mostly be about scalability issues.

*Mr. Schweikert. Yes, that is actually fair.

*Mr. Rosenzweig. It is much smaller. I think that such a system is at least feasible within the context of design.

I do share some people's concerns that U.S. Government large-scale procurement programs like this never seem to actually get there. So even if we could idealize it, the government sector might --

*Mr. Schweikert. Oh, yes.

*Mr. Rosenzweig. -- not quite get it --

*Mr. Schweikert. And let's be brutally honest. There will be a knife fight because --

*Mr. Rosenzweig. Yes.

*Mr. Schweikert. -- you are interrupting a lot of bureaucracies, layers of power and authority.

*Mr. Grobman. It can absolutely be done. I think if you look at the large-scale systems that exist today for authentication, whether it is financial services, whether it is some of the models that -- there is numerous capabilities. The private sector has built a set of protocols that enable one entity to do authentication, and then allow that authentication to be honored by others. Things like SAML and OATH.

Really, the discussion needs to be about getting the right balance between privacy and security --

*Mr. Schweikert. Well, you hit one thing I fixate on, and that is -- we hit quantum. I will absolutely have to have a token, because I think -- because an algorithmic is under threat (sic).

*Mr. Grobman. So one of the key points I made in my written testimony is although we haven't settled on exactly what quantum-safe algorithms to use, in the design of a new system we can design it such that we have the ability to swap algorithms out as we --

*Mr. Schweikert. Well, you don't think a token system would be more robust?

*Mr. Grobman. I think that it is part of the solution, but I think that the underlying cryptography that needs to be used in the solution does need to eventually be --

*Mr. Schweikert. I need to learn more. If you have something I can read --

*Chairman Johnson. The time of the gentleman has expired.

*Mr. Schweikert. Oh, all right. I will talk after. But thank you for tolerating me. I need to disclose I have had a lot of caffeine.

[Laughter.]

*Chairman Johnson. Thank you.

To keep pace with the identity thieves we need to start thinking beyond just protecting Social Security numbers, and start thinking about how to make the numbers less valuable to criminals in the first place.

You know, it is time to take a hard look, I think, at the future of Social Security numbers, and to decide what needs to change to better protect Americans from identity theft. This hearing has given us a good starting point, and I look forward to working with my colleagues in the future to figure out the next steps forward.

Americans are counting on us to get this right. They want, need, and deserve nothing else.

Thank you to all our witnesses for your testimony today, and I thank you to our members for being here.

With that, the -- you want to?

*Mr. Larson. Yes.

*Chairman Johnson. I recognize Mr. Larson --

*Mr. Larson. I want to thank --

*Chairman Johnson. -- for a comment.

*Mr. Larson. I want to thank the chairman. This is indeed one of the more interesting panels that we have. And as you can tell, a number of our members still have a lot of questions.

What we would like to ask of you is that if you could submit to us in writing -- because it was very valuable to get your input -- we don't -- and the chairman has already indicated that we, as a committee, will meet internally to digest what you send us in writing, in terms of your solution and also the urgency that you all attach with this, especially, as the chairman has already outlined, under authentification (sic), and how we

might proceed. Because there is a -- this was a very fertile and productive meeting. I thank the chairman.

*Chairman Johnson. Thank you.

*Mr. Larson. And I appreciate the opportunity to respond.

*Chairman Johnson. Thank you. And thank you all for being here. We appreciate your presence.

With that, the subcommittee stands adjourned.

[Whereupon, at 11:36 a.m., the Subcommittee was adjourned.]

MEMBER QUESTIONS FOR THE RECORD

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515

June 7, 2018

Elizabeth Curda
Director of Education, Workforce, and Income Security
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Curda,

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security at the May 18, 2018 hearing on "Securing Americans' Identities: The Future of the Social Security Number." In order to complete our hearing record, we would appreciate your responses to the following question:

1. The Government Accountability Office found that the current paper cards can cost up to $34 per card. How would this cost change if the Social Security Administration switched to a biometric or smart card?

We would appreciate your responses to these questions by June 21, 2018. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson

Sam Johnson
Chairman
Subcommittee on Social Security

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

June 20, 2018

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Thank you for the opportunity to testify before the Subcommittee on May 17, 2018 during the hearing on "Securing Americans' Identities: The Future of the Social Security Number." The attached enclosure is GAO's response to the question for the record you submitted. If you have any questions, please contact me at curdae@gao.gov or (202) 512-7215.

Sincerely yours,

Elizabeth H. Curda
Director
Education, Workforce
and Income Security

Enclosure

Post-Hearing Questions for the Record
Submitted to Elizabeth Curda
Director, Education, Workforce, and Income Security Team
U.S. Government Accountability Office

From Rep. Sam Johnson
"Securing Americans' Identities: The Future of the Social Security Number"
May 17, 2018

1. The Government Accountability Office found that the current paper cards can cost up to $34 per card. How would this cost change if the Social Security Administration switched to a biometric or smart card?

Response:

Our review focused on costs of the current paper card and implications of eliminating the card. We did not specifically look at the cost of producing biometric or smart cards. SSA officials reported that of the $34-per-card estimate, the largest component ($28) is the cost of an in-person field office visit. Information technology and systems support is about $5 and paper, printing, and postage is about 60 cents. However, some cards are less expensive for SSA to produce. For example, replacement cards requested online cost an estimated $6 per card.

Based on our prior work[1], a biometric card would likely be more expensive than a paper card. We previously reviewed options to enhance the Social Security card, such as adding machine-readable features such as a magnetic stripe or bar code, and adding biometric features such as photographs and fingerprints, to eliminating the card entirely. We reported that including additional features on the card would increase the cost of the card. For example, adding machine-readable or biometric features to the card would also require additional equipment in SSA's approximately 1,230 field offices, and employers and other users would also need equipment if they were expected to read features on the card. Further, biometric features would likely require cardholders to have their biometric information updated at periodic intervals—greatly affecting the number of cards cardholders would receive in their lifetime and long-term card issuance costs.

Also, given the current state of technology, a biometric card may not be necessary. As described in our report, current technology used by the U.S. Customs and Border Protection Global Entry program confirms identity using a fingerprint scan, along with a passport or permanent resident card.

[1] GAO, *Social Security Administration: Improved Agency Coordination Needed for Social Security Card Enhancement Efforts*, GAO-06-303 (Washington, D.C.: March 29, 2006).

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515

June 7, 2018

Jeremy A. Grant
Managing Director
Venable LLP
600 Massachusetts Ave NW
Washington, DC 20001

Dear Mr. Grant,

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security at the May 18, 2018 hearing on "Securing Americans' Identities: The Future of the Social Security Number." In order to complete our hearing record, we would appreciate your responses to the following questions:

1. Understanding that the current nine-digit Social Security number (SSN) format has a limited number of combinations, and that its design was limited by the technology available in 1936, what considerations need to be taken into account for a future version of the SSN?

2. In your testimony, you discussed how some companies have shifted their business practices in recognition of the risk of using SSNs, however some government requirements hinder additional private sector efforts. What are these specific requirements and what steps can Congress take to remove these barriers to private sector action?

We would appreciate your responses to these questions by June 21, 2018. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson

Sam Johnson
Chairman
Subcommittee on Social Security

Additional Questions for the Record

Jeremy Grant
Coordinator, Better Identity Coalition
and
Managing Director, Technology Business Strategy, Venable LLP

U.S. House Committee on Ways and Means
Subcommittee on Social Security

"Securing Americans' Identities: The Future of the Social Security Number"

1. Understanding that the current nine-digit Social Security number (SSN) format has a limited number of combinations, and that its design was limited by the technology available in 1936, what considerations need to be taken into account for a future version of the SSN?

While it is true that the current nine-digit SSN has a limited number of combinations, my understanding is that the SSA is not anywhere close to being in danger of running out of potential numbers. According to SSA, as of 2008, they had issued just over 450 million SSNs[1] - and they issue about 5 million new SSNs each year. That means we are somewhere around the halfway point in terms of possible combinations, and that – even with population growth – it will likely be more than 70 years before some action needs to be taken.

Assuming that the SSN is only used going forward as an identifier, there may not need to be any changes to the format during this time. One potential enhancement would be the addition of a "check sum" number – a 10th digit at the end of the SSN that would be derived from the other nine numbers, and could help systems detect whether there might be errors in the data. Check sum numbers can help, for example, to detect whether someone mis-keyed a SSN when typing it into a system, or whether a number submitted was made up on the fly by someone looking to avoid providing a legitimate SSN.

[1] See https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html

2. In your testimony, you discussed how some companies have shifted their business practices in recognition of the risk of using SSNs, however some government requirements hinder additional private sector efforts. What are these specific requirements and what steps can Congress take to remove these barriers to private sector action?

As I noted in my testimony, there are a number of legal and regulatory requirements in place that require the SSN to be collected and retained by different organizations. Much of industry's ability to reduce their reliance on the SSN will be dependent on the government changing its requirements for them to collect it.

I have attached two inventories of policies that cover use of the SSN: one focused on requirements pertaining to the financial services industry that was compiled by the Financial Services Roundtable (FSR) – they have given us permission to share this here – and a second compiled by the Better Identity Coalition that focuses on requirements for firms outside of the financial sector.

These lists are not intended to be an exhaustive inventory of the policies in place requiring use of the SSN, but they do serve to highlight how embedded the SSN is as an identifier in so many of our identity processes – and helps to frame the complexity and cost associated with any effort to replace it.

While some of these requirements may be able to be repealed without much impact, repeal of others could make it quite difficult for government or industry to achieve certain outcomes or execute core parts of their mission. This is because identifiers are important – many government and industry entities require an identifier to deliver a service or fulfill key policy objectives. Thus, we would not advocate for a wholesale repeal of these requirements.

It could be helpful, however, for the government to review all of the places where the SSN is required to be collected today and consider if alternative approaches may allow government to ensure better outcomes.

Federal Laws and Regulations Related to Financial Institutions' Obtaining Social Security Numbers

Statute & Regulation	Social Security Number Requirement	Retention/Disposal Provisions
A. BSA/AML		
Customer Identification Program *31 C.F.R. § 1020.220*	**Prior to opening an account**, the bank/thrift/credit union must, at a minimum, obtain the customer's name, date of birth, address (residential or business), and an **identification number** (can be taxpayer identification number).	The bank must retain identifying information for **five years after the account is closed**.
Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks *31 C.F.R. § 1010.415*	**No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for $3,000 or more in currency unless it maintains records of the following information,** which must be obtained for each issuance or sale of one or more of these instruments to any individual purchaser which involves currency in amounts of $3,000-$10,000 inclusive: **If the purchaser does not have a deposit account with the financial institution:** (A) The name and address of the purchaser; (B) The **social security number** of the purchaser, or if the purchaser is an alien and does not have a social security number, the alien identification number; (C) The date of birth of the purchaser; (D) The date of purchase; (E) The type(s) of instrument(s) purchased; (F) The serial number(s) of the instrument(s) purchased; and (G) The amount in dollars of each of the instrument(s) purchased.	Records required to be kept shall be retained by the financial institution for a period of **five years** and shall be made available to the Secretary upon request at any time.
Beneficial Ownership *31 C.F.R. § 1010.230 (effective May 11, 2018)*	Financial institutions are required to obtain, verify, and record the identities of the beneficial owners of legal entity customers. As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and **social security number** or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.	A financial institution must retain the records for five years after the date the account is closed.
B. Consumer Financial Products and Services		
Application for a residential mortgage loan (Truth in Lending Act) *12 C.F.R. §§ 1026.3(a)(3)(ii); 1026.25*	For residential mortgage transactions, an application consists of the submission of the consumer's name, the consumer's income, the consumer's **social security number** to obtain a credit report, the property address, an estimate of the value of the property, and the mortgage loan amount sought.	A creditor shall retain evidence of compliance for **two years** after the date disclosures are required to be made or action is required to be taken.

Electronic Fund Transfer Act – Error Notice *12 C.F.R. §§ 1005.11 and 1005.13*	A financial institution shall comply with the requirements of this section with respect to any oral or written notice of error from the consumer that: (i) Is received by the institution no later than 60 days after the institution sends the periodic statement or provides the passbook documentation, on which the alleged error is first reflected; (ii) Enables the institution to identify the consumer's name and account number; and(iii) Indicates why the consumer believes an error exists and includes to the extent possible the type, date, and amount of the error, except for requests described in paragraph (a)(1)(vii) of this section. ***Content of error notice.*** The notice of error is effective even if it does not contain the consumer's account number, so long as the financial institution is able to identify the account in question. For example, the consumer could provide a Social Security number or other unique means of identification.	Any person subject to the Act and this part shall retain evidence of compliance with the requirements imposed by the Act and this part for a period of not less than **two years** from the date disclosures are required to be made or action is required to be taken.
C. Privacy/Information Security		
Privacy of Financial Information *12 C.F.R. pt. 332*	**Nonpublic personally identifiable information includes any information a** consumer provides to you to obtain a financial product or service from you. The regulation: (1) Requires a financial institution to provide notice to customers about its privacy policies and practices; (2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and (3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to exceptions.	No specific recordkeeping requirement.
Interagency Guidelines Establishing Information Security Standards *12 C.F.R. pt. 364, App. B (and corresponding regs)*	An institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to **sensitive customer information, which includes SSN,** because this type of information is most likely to be misused, as in the commission of identity theft. **Notice to Regulator:** The institution's response program must include procedures for notifying its primary federal regulatory as soon as possible when the institution becomes aware of an incident involving unauthorized access to or uses of **sensitive customer information.**	An institution's information security program must ensure the proper disposal of customer information and consumer information.

	Notice to Consumer: When a financial institution becomes aware of an incident of unauthorized access to **sensitive customer information**, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.	
D. Identity Theft/Consumer Reports		
Red Flags Rule *12 C.F.R. pt. 334, App. J (and corresponding regs)*	Requires financial institutions and creditors to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts: Suspicious personal identifying information includes: • Social security number has not been issued or is listed on the Social Security Administration's Death Master File • Lack of correlation between the SSN range and date of birth • The SSN provided is the same as that submitted by other persons opening an account or other customers.	
Duties of Consumer Reporting Agencies Regarding Identity Theft *12 C.F.R. § 1022.123*	**Consumer reporting agencies shall develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity** where the consumer asserts a good-faith belief that have been a victim of identity fraud or a related crime. **Examples of information** that might constitute reasonable information requirements for proof of identity are provided for illustrative purposes only: *Consumer file match.* The identification information of the consumer including his or her full name (first, middle initial, last, suffix), any other or previously used names, current and/or recent full address (street number and name, apt. no., city, state, and zip code), full nine digits of **Social Security number**, and/or date of birth.	

Disclosure by CRA of Consumer File to Consumer; Free Annual Report; *15 U.S.C. §§ 1681g, 1681h, 1681j(a); 12 C.F.R. pt. 1022, subpart N.*	Every consumer reporting agency shall, upon request, clearly and accurately disclose to the consumer **all information in the consumer's file** at the time of the request, except that if the consumer to whom the file relates requests that the first five digits of the SSN not be included, and the reporting agency has adequate proof of the identity of the requester, the reporting agency shall so truncate the disclosure. A CRA shall require, as a condition of making that disclosure, that the consumer furnish **proper identification**. Free Annual Reports: There is a centralized source for requesting annual file disclosures from nationwide CRAs which collects only as much **personally identifiable information** as is reasonably necessary to properly identify the consumer and to process the transaction requested by the consumer. Any **personally identifiable information** collected from consumers as a result of a request for annual file disclosure, or other disclosure required by the FCRA, made through the centralized source, may be used or disclosed by the centralized source or a nationwide consumer reporting agency only: (1) To provide the annual file disclosure or other disclosure required under the FCRA requested by the consumer; (2) To process a transaction requested by the consumer at the same time as a request for annual file disclosure or other disclosure; (3) To comply with applicable legal requirements, including those imposed by the FCRA and this part; and (4) To update personally identifiable information already maintained by the nationwide consumer reporting agency for the purpose of providing consumer reports, provided that the nationwide consumer reporting agency uses and discloses the updated personally identifiable information subject to the same restrictions that would apply, under any applicable provision of law or regulation, to the information updated or replaced.	

Federal Laws and Regulations Related to Obtaining and Maintaining Social Security Numbers

Statute & Regulation, Including Enacting Legislation and Citation	Social Security Number Requirement
A. Employment	
Income Tax Collected at Source *Enacting legislation does not have a specific name. Public Law 96-601 is titled "An Act" "to simply certain provisions of the Internal Revenue Code of 1954, and for other purposes." *26 U.S.C. § 3402*	A request that an annuity or any sick pay be subject to withholding under this chapter…shall be made by the payee in writing to the person making the payments and shall contain the **social security number** of the payee.
Verification of Identity and Employment Authorization *8 C.F.R. § 274a.2*	A person or entity that hires or recruits or refers for a fee an individual for employment must ensure that the individual properly completes section 1 - "Employee Information and Verification" - on the Form I-9 at the time of hire. Section 1 of Form I-9 includes a field for **social security numbers**.
B. Education	
Returns Relating to Higher Education Tuition and Related Expenses Taxpayer Relief Act of 1997 *26 U.S.C. § 6050S*	Any person: (1) which is an eligible educational institution which enrolls any individual for any academic period; (2) which is engaged in a trade or business of making payments to any individual under an insurance arrangement as reimbursements or refunds (or similar amounts) of qualified tuition and related expenses; or (3) except as provided in regulations, which is engaged in a trade or business and, in the course of which, receives from any individual interest aggregating $600 or more for any calendar year on one or more qualified education loans, **shall make the return** described in subsection (b) with respect to the individual at such time as the Secretary may by regulations prescribe. **A return** is described in this subsection if such return: (1) is in such form as the Secretary may prescribe, and (2) contains: (A) the name, address, and **TIN** of any individual (i) who is or has been enrolled at the institution and with respect to whom transactions described in subparagraph (B) are made during the calendar year…
Social Security Number *34 C.F.R. § 668.36*	[T]he Secretary attempts to confirm the **social security number** a student provides on the Free Application for Federal Student Aid (FAFSA) under a data match with the Social Security Administration. If the Social Security Administration confirms that number, the Secretary notifies the institution and the student of that confirmation.

	An institution may not disburse any title IV, HEA program funds to a student until the institution is satisfied that the student's reported **social security number** is accurate.
C. Healthcare	
Reporting of Health Insurance Coverage The Patient Protection and Affordable Care Act *26 U.S.C. § 6055*	Every person who provides minimum essential coverage to an individual during a calendar year shall, at such time as the Secretary may prescribe, make a **return** described in subsection (b). A **return** is described in this subsection if such return: (A) is in such form as the Secretary may prescribe, and (B) contains (i) the name, address and **TIN** of the primary insured and the name and **TIN** of each other individual obtaining coverage under the policy…
Eligibility Determinations The Patient Protection and Affordable Care Act *42 U.S.C. § 18081*	An applicant for enrollment in a qualified health plan offered through an Exchange in the individual market shall provide: (A) the name, address, and date of birth of each individual who is to be covered by the plan (in this subsection referred to as an "enrollee"); and (B) the information required by any of the following paragraphs that is applicable to an enrollee. The following information shall be provided with respect to every enrollee: (A) In the case of an enrollee whose eligibility is based on an attestation of citizenship of the enrollee, the enrollee's **social security number**; (B) In the case of an individual whose eligibility is based on an attestation of the enrollee's immigration status, the enrollee's **social security number** (if applicable) and such identifying information with respect to the enrollee's immigration status as the Secretary, after consultation with the Secretary of Homeland Security, determines appropriate.
Eligibility Process *45 C.F.R. § 155.310*	The Exchange must require an applicant who has a **Social Security number** to provide such number to the Exchange.
D. Driver's License	
Minimum Issuance Standards REAL ID Act *49 U.S.C. § 30301 note*	To meet the requirements of this section, a State shall require, at a minimum, presentation and verification of the following information before issuing a driver's license or identification card to a person: (A) A photo identity document, except that a non-photo identity document is acceptable if it includes both the person's full legal name and date of birth; (B) Documentation showing the person's date of birth; (C**) Proof of the person's social security account number or verification that the person is not eligible for a social security account number**; (D) Documentation showing the person's name and address of principal residence.

Application and Documents the Applicant Must Provide *6 C.F.R. § 37.11*	(1) Except as provided in paragraph (e)(3) of this section, individuals presenting the identity documents listed in § 37.11(c)(1) and (2) must present his or her **Social Security Administration account number card**; or, if a Social Security Administration account card is not available, the person may present any of the following documents bearing the applicant's **SSN**: (i) A W-2 form; (ii) A SSA-1099 form; (iii) A non-SSA-1099 form; or (iv) A pay stub with the applicant's name and SSN on it. (2) The State DMV must verify the **SSN** pursuant to § 37.13(b)(2) of this subpart. (3) Individuals presenting the identity document listed in § 37.11(c)(1)(vi) must present an SSN or demonstrate non-work authorized status.
Requirement of Statutorily Prescribed Procedures to Improve Effectiveness of Child Support Enforcement Personal Responsibility and Work Opportunity Reconciliation Act of 1996 *42 U.S.C. § 666*	Each State must have in effect laws requiring the use of the following procedures…: Procedures requiring that the **social security number** of— (A) any applicant for a professional license, **driver's license**, occupational license, recreational license, or marriage license be recorded on the application. For purposes of subparagraph (A) (cited above), if a State allows the use of a number other than the social security number to be used on the face of the document while the social security number is kept on file at the agency, the State shall so advise any applicants.
E. Miscellaneous	
Blood Donor Locator Service Technical and Miscellaneous Revenue Act of 1988 *42 U.S.C. § 1320b-11c*	A request for address information under this section shall be filed in such manner and form as the Commissioner of Social Security shall by regulation prescribe, shall include the blood donor's **social security account number**, and shall be accompanied or supported by such documents as the Commissioner of Social Security may determine to be necessary.
Establishment of a Vessel Identification System Coast Guard Authorization Act of 1989 *46 U.S.C. § 12501*	The vessel identification system shall include information prescribed by the Secretary including: (1) identifying a vessel; (2) identifying the owner of the vessel, including— (A) the owner's **social security number** or, if that number is not available, other means of identification acceptable to the Secretary; or (B) for an owner other than an individual— (i) the owner's taxpayer identification number; or

	(ii) if the owner does not have a taxpayer identification number, the **social security number** of an individual who is a corporate officer, general partner, or individual trustee of the owner and who signed the application for documentation or numbering for the vessel;

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515

June 7, 2018

Steve Grobman
Senior Vice President and Chief Technology Officer
McAfee, LLC
5000 Headquarters Drive
Plano, TX 75024

Dear Mr. Grobman,

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security at the May 18, 2018 hearing on "Securing Americans' Identities: The Future of the Social Security Number." In order to complete our hearing record, we would appreciate your responses to the following question:

1. Understanding that the current nine-digit Social Security number (SSN) format has a limited number of combinations, and that its design was limited by the technology available in 1936, what considerations need to be taken into account for a future version of the SSN?

We would appreciate your responses to these questions by June 21, 2018. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson

Sam Johnson
Chairman
Subcommittee on Social Security

Social Security Subcommittee Hearing on "Securing American Identities: The Future of the Social Security Number"

Question for Steve Grobman:

- Understanding that the current nine-digital Social Security Number (SSN) format has a limited number of combinations, and that its design was limited by the technology available in 1936, what considerations need to be taken into account for the future version of the SSN?

Answer:

The number of permutations in a 9-digit number, the number of digits on each Social Security number, is 1 billion. There are now about 325 million citizens in the United States, which could exhaust the pool of SSNs within a few generations. From a security point of view, this is not acceptable given the constant innovation of both hardware and software that makes cracking 1 billion combinations a relatively easy task. Over time, innovations in Quantum computing will enable hackers to crack virtually all known methods of encryption. The federal government should design a larger namespace that eliminates the need for re-use in the long run, while also rethinking its approach to securing the Social Security number, including taking into consideration such capabilities as two factor authentication to help protect the integrity of the SSN.

There are three work flows in an identity management system: identity, authentication, and authorization. In our current SSN system, the SSN plays a role in all three, while in the field of computer science, we recognize the criticality of segregating these processes to ensure a high level of security. The use of the SSN should be limited as an identifier that should be public, much like a citizen's email address. At the same time, both the public and the private sectors need to develop new models of authentication and authorization that can be used in conjunction with the SSN to give Americans the modern identity management system they deserve. To enable this type of innovation, policy makers should ban the simple knowledge of a Social Security number as an accepted form of authentication throughout our economy, enable federal agencies to act as validators of identity, given the many

credentials over which the federal government has authority, including passports, and mandate all federal e-government services provided directly to citizens require the use of strong authentication to enhance trust in government services.

A truly robust, modern identity management system needs to have the ability to do the following things: Assure the new means to identify an individual can be reissued in the event it is compromised to help guarantee the system and the individual better long-term security. Look at ways to provide authentication and authorization without having to store all privacy related information of each US citizen in one single place. Require the least amount of information needed to accurately authenticate the individual. Leverage multi-factor authentication mechanisms as a part of the solution; what you have, what you know, and who you are. Consider the benefits of biometrics, with user consent, and if, and only if, there is broad public support for such a solution. Many new phones and laptops support limited use of biometrics today. Broad-based acceptance of biometrics may well increase over time. Look at what has worked in financial services industry and other countries for feasible ideas and deployment techniques. Invest in research and development to overcome identity management challenges of the future such as Innovations in Quantum computing that have the potential to make current methods of encryption obsolete. Don't try to solve all the identification, authorization and authentication challenges for the entire US digital economy out of the gate. Initially, focus on improving the SSN to providing US Federal services and benefits to US citizens. Use a phased approach to produce broad based, long term success.

Finally, Subcommittee Members should consider the cost of failing to take-action. Identity theft and fraud cost consumers more than $16 billion per year according to report from Javelin Strategy & Research, Feb 1, 2017. The other concern is the deteriorating trust the American population has in the fundamental components targeted by identity theft and fraud. The Subcommittee should ask the U.S. Government Accountability Office (GAO) to conduct a study, using dynamic scoring, that compares the cost to consumers and our overall economy of identity theft and fraud to the costs and benefits of architecting a modern, identity management system. A well-done study

could overcome the objections of policy makers who say that it is too hard or too expensive. We owe it to our citizens to take legislative and budgetary action now.

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515

June 7, 2018

Paul Rosenzweig
Senior Fellow
R Street Institute
1212 New York Ave NW
Suite 900
Washington, DC 20005

Dear Mr. Rosenzweig,

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security at the May 18, 2018 hearing on "Securing Americans' Identities: The Future of the Social Security Number." In order to complete our hearing record, we would appreciate your responses to the following question:

1. In your testimony, you suggested that publication of a "phonebook" with every Social Security number (SSN) would make it clear that the use of SSNs as authenticators was no longer a reasonable option. Would this approach work if only the SSNs were published, or would additional associated data elements such as names have to accompany the SSNs?

We would appreciate your responses to these questions by June 21, 2018. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson
Chairman
Subcommittee on Social Security

R Street

e. rstreet@rstreet.org
o. 202.525.5717
f. 1.877.793.4920
rstreet.org

15 June 2018

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Johnson:

Thank you for your question regarding the May 18, 2018 Committee on Ways and Means Subcommittee on Social Security hearing on "Securing Americans' Identities: The Future of the Social Security Number."

Question

"In your testimony, you suggested that publication of a 'phonebook' with every Social Security number (SSN) would make it clear that the use of SSNs as authenticators was no longer a reasonable option. Would this approach work if only the SSNs were published, or would additional associated data elements such as names have to accompany the SSNs?"

Response

My proposal to publish SSNs is intended to eliminate their utility as an authenticator – that is, it is intended to prevent any security system from using a social security number to authenticate the name of a person for purposes of providing access to a system. As such, simply publishing the SSNs alone without names would not achieve the objectives of the proposal. The virtue of the proposal lies in providing a public link between a name and a social security number thereby draining the SSN of any patina of secrecy of confidentiality that it might still retain.

Sincerely,

Paul Rosenzweig
Senior Fellow
R Street Institute

PUBLIC SUBMISSIONS FOR THE RECORD

napbs
National Association of Professional Background Screeners
The Voice of Screening Professionals

May 17, 2018

Honorable Sam Johnson
Chairman, House Ways and Means
Subcommittee on Social Security
2304 Rayburn House Office Building
Washington, DC 20515

Honorable John Larson
Ranking Member, House Ways and Means
Subcommittee on Social Security
1501 Longworth House Office Building
Washington, DC 20515

RE: Preserving Access to Social Security Numbers in Key Federal Databases to Protect Americans' Health and Safety

Dear Chairman Johnson and Ranking Member Larson:

The National Association of Professional Background Screeners (NAPBS) applauds the Subcommittee for convening today's hearing on the future of the Social Security Number. Our 800 members work to promote the safety and security of our communities and workplaces, and in order to meet that objective access to and usage of identifiers such as the Social Security Number (SSN) is vitally important. Indeed, the use of SSNs is a critical tool for our members to meet the federal statutory obligation imposed on our members by the Fair Credit Reporting Act for "maximum possible accuracy." While the SSN was not designed to serve as a broadly-used identifier when it was created in the 1930s, it nevertheless serves that function in many facets of the American economy and modern society. Curtailing its use in that regard would be highly disruptive and costly, and would just lead to a search for similarly broad identifiers to use in its place.

NAPBS understands and shares the concerns expressed by Members of the Subcommittee and other stakeholders about the potential misuse of SSNs to perpetuate identity theft or other fraud. We recognize that in light of the breaches of consumer data extending back many years have likely exposed most consumers' SSN and other personal identifiable information to risk of misuse. Accordingly, the Subcommittee is appropriately concerned about the future use of SSNs and we welcome the opportunity to share some high-level recommendations:

(1) The use of SSNs as an *identifier* should be preserved.

(2) The use of SSNs as an *authenticator* should be constrained.

(3) Market-based technological solutions for authentication will provide appropriate solutions for consumer authentication

(4) The federal government can establish a leadership role, by eliminating the use of SSNs for authentication purposes when used with data held by the federal government.

The difference between using SSN as an identifier and using it as an authenticator is a key difference – but is frequently overlooked. An identifier is a piece of information used to tag other information as belonging to an individual. An authenticator is a piece of information that tends to confirm that the person you are interacting with is the person that they claim to be.

SSN is an ideal *identifier*. Almost all adult Americans have one, and the number is unique to that individual. That means that a simple 10-digit number can be used as a common index to find data. Employers, schools, banks, health care providers, government agencies, and millions of others can quickly identify their records about an individual using SSN. This has enormous value to both organizations and the individual.

But SSN is a terrible *authenticator*. An ideal authenticator is a piece of information that only the person being authenticated and the person authenticating know, and that is difficult to guess. The very fact that SSN is so useful as an identifier – its common format, its widespread use – make it a terrible authenticator because it is not a secret at all. It is likely that, for most Americans, hundreds of organizations have records of their SSN, and at least thousands of individuals have access to those records.

As technology has evolved, credit card companies, phone companies, and others began using SSNs as *authenticators*, to verify that people are who they claim to be. In effectively treating SSNs as secret information, these institutions have increased the danger of identity theft by both augmenting the power of SSNs, and by sharing the data with their employees. The Federal Trade Commission has acknowledged this issue, noting in a 2008 report that "the SSN may not be well-suited as an authenticator itself, but can be and is used effectively to detect potential fraud by permitting access to other authentication-related information."

With the foregoing in mind, it is important to underscore the critical aspect of SSNs as an *identifier*. Redacting important identifying information such as SSNs from public records greatly impacts the ability of background screeners – which are hired by employers to obtain the critical information needed to make accurate and timely hiring decisions. Having an individual's full DOB and at least the last four digits of his/her social security number are critical identifiers for public records as they help ensure the correct data is matched to an individual. This is particularly important when dealing with common names, as search results can potentially yield hundreds of results. Preserving access to SSNs, therefore, will help ensure the greatest possible accuracy when running background checks for individuals serving in sensitive positions.

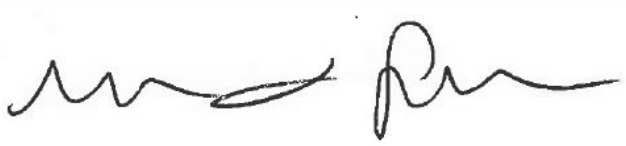
The ultimate solution to authentication will be market-based and technology-focused. But some of the best authentication technology in existence today relies on information that is *identified* using SSN without *authenticating* with the SSN. For example, each of the major credit bureaus uses information from their files about individuals – typically indexed using SSN as a major element – to generate "out of wallet" quizzes to confirm the identity of individuals who request their credit reports. These quizzes ask individuals multiple choice questions regarding matters that the credit files show (such as prior addresses, or the amounts of car or house payments) and

napbs®
National Association of
Professional Background Screeners
The Voice of Screening Professionals

that would be unlikely for another person to know. These questions *authenticate* the person, but the information that leads to the question is *identified* by the SSN.

While the ultimate solution to SSN utilization will be market based and technology focused, the federal government can and should take the lead by restricting agencies' use of SSN as authenticator. Accordingly, NAPBS would like to encourage Congress and Federal agencies to preserve the collection of, use and access to SSNs where appropriate for public safety. Thank you for your time and consideration of these comments.

Sincerely,



Melissa L. Sorenson
Executive Director
National Association of Professional Background Screeners