HEARING ON THE SOCIAL SECURITY ADMINISTRATION'S ROLE IN COMBATTING IDENTITY FRAUD

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MAY 24, 2023

Serial No. 118–SS02

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PUBLISHING OFFICE
54–359 WASHINGTON : 2024

COMMITTEE ON WAYS AND MEANS

JASON SMITH, Missouri, *Chairman*

VERN BUCHANAN, Florida
ADRIAN SMITH, Nebraska
MIKE KELLY, Pennsylvania
DAVID SCHWEIKERT, Arizona
DARIN LAHOOD, Illinois
BRAD WENSTRUP, Ohio
JODEY ARRINGTON, Texas
DREW FERGUSON, Georgia
RON ESTES, Kansas
LLOYD SMUCKER, Pennsylvania
KEVIN HERN, Oklahoma
CAROL MILLER, West Virginia
GREG MURPHY, North Carolina
DAVID KUSTOFF, Tennessee
BRIAN FITZPATRICK, Pennsylvania
GREG STEUBE, Florida
CLAUDIA TENNEY, New York
MICHELLE FISCHBACH, Minnesota
BLAKE MOORE, Utah
MICHELLE STEEL, California
BETH VAN DUYNE, Texas
RANDY FEENSTRA, Iowa
NICOLE MALLIOTAKIS, New York
MIKE CAREY, Ohio

RICHARD E. NEAL, Massachusetts
LLOYD DOGGETT, Texas
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
EARL BLUMENAUER, Oregon
BILL PASCRELL, JR., New Jersey
DANNY DAVIS, Illinois
LINDA SÁNCHEZ, California
BRIAN HIGGINS, New York
TERRI SEWELL, Alabama
SUZAN DELBENE, Washington
JUDY CHU, California
GWEN MOORE, Wisconsin
DAN KILDEE, Michigan
DON BEYER, Virginia
DWIGHT EVANS, Pennsylvania
BRAD SCHNEIDER, Illinois
JIMMY PANETTA, California

MARK ROMAN, *Staff Director*
BRANDON CASEY, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

DREW FERGUSON, Georgia, *Chairman*

MIKE CAREY, Ohio
DAVID SCHWEIKERT, Arizona
RON ESTES, Kansas
BLAKE MOORE, Utah
RANDY FEENSTRA, Iowa
GREG STEUBE, Florida
DAVID KUSTOFF, Tennessee

JOHN LARSON, Connecticut
BILL PASCRELL, New Jersey
LINDA SÁNCHEZ, California
BRIAN HIGGINS, New York
DAN KILDEE, Michigan

C O N T E N T S

OPENING STATEMENTS

WITNESSES

MEMBER QUESTIONS FOR THE RECORD

PUBLIC SUBMISSIONS FOR THE RECORD

United States House Committee on
Ways & Means
CHAIRMAN JASON SMITH

FOR IMMEDIATE RELEASE
May 17, 2023
No. SS-02

CONTACT: 202-225-3625

Chairman Smith and Social Security Subcommittee Chairman Ferguson Announce Subcommittee Hearing on the Social Security Administration's Role in Combatting Identity Fraud

House Committee on Ways and Means Chairman Jason Smith (MO-08) and Social Security Subcommittee Chairman Drew Ferguson (GA-03) announced today that the Subcommittee on Social Security will hold a hearing to discuss the Social Security Administration's unique role in combatting Social Security number-related identity fraud. The hearing will take place on **Wednesday, May 24, 2023, at 2:00PM in the Sam Johnson Room, 2020 Rayburn House Office Building**.

Members of the public may view the hearing via live webcast available at https://waysandmeans.house.gov. The webcast will not be available until the hearing starts.

In view of the limited time available to hear the witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance 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 can do so here: WMSubmission@mail.house.gov.

Please ATTACH your submission as a Microsoft Word document in compliance with the formatting requirements listed below, **by the close of business on Wednesday, June 7, 2023**. 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 reserves the right to format it according to 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. Please indicate the title of the hearing as the subject line in your submission. 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.

ACCOMMODATIONS:

The Committee seeks to make its facilities accessible to persons with disabilities. If you require accommodations, please call 202-225-3625 or request via email to WMSubmission@mail.house.gov in advance of the event (four business days' notice is requested). Questions regarding 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 on the Committee website at http://www.waysandmeans.house.gov/.

###

SOCIAL SECURITY'S UNIQUE ROLE IN COMBATING SOCIAL SECURITY NUMBER-RELATED IDENTITY FRAUD

WEDNESDAY, MAY 24, 2023

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON SOCIAL SECURITY,
COMMITTEE ON WAYS AND MEANS,
Washington, DC.

The subcommittee met, pursuant to call, at 2:01 p.m. in Room 2020, Rayburn House Office Building, Hon. Drew Ferguson [chairman of the subcommittee] presiding.

Chairman FERGUSON. We will call the subcommittee to order.

Welcome today to today's hearing on Social Security Administration's role in combating identity fraud.

When the Social Security Administration began issuing Social Security numbers in 1936, they were simply used to track workers' earnings and administer the Social Security program. Times have changed dramatically since then, and now the Social Security number, or SSN, is the linchpin of American identity. SSNs are used for a number of reasons, some required by law, others not. If you want a job, you must—or if you want to buy a home, if you want to open a credit card, you need a Social Security number.

But after countless data breaches, it is clear that Social Security numbers are far from safe and far from a secret. In 2022 alone, there were more than 1,100 data breaches that included Social Security numbers. So it should come as no surprise that the Social Security number is still an attractive target for criminals and fraudsters, and that identity theft is real—is a real threat to millions of Americans, and that includes our children and our seniors.

In 2021, roughly 1.25 million children were the victims of identity fraud, which cost American families real time, real money, and real worry to resolve this crime. The last thing that somebody needs when they are trying to protect themselves or a loved one from identity fraud is red tape. But unfortunately, resolving an issue related to a stolen Social Security number can be a long and complex ordeal, placing additional burdens on victims, and it extends time for criminals and fraudsters to misuse the Social Security number.

As the creator and issuer of Social Security numbers, the Social Security Administration is uniquely positioned to not only combat Social Security number fraud, but also protect people whose Social Security numbers have been compromised from harm due to identity fraud. But Social Security's policies don't always make things

easy. Today we will have an opportunity to hear firsthand about how difficult it is to resolve issues related to lost Social Security numbers or stolen Social Security numbers and discuss some ways that the Social Security Administration can make it easier for Americans to protect themselves from harm before it occurs.

If a burglar breaks into your house, you call the police. They don't tell you to wait a few weeks and hope that your situation improves. Instead, they send an officer to respond. It is not always how victims of identity theft are treated, and that is a problem. The American people deserve a similar response from government services when they are victims of identity theft. That is why I have partnered with Ranking Member Larson to reintroduce the Improving Social Security Service to Victims of Identity Theft Act that would require the Social Security Administration to provide a single point of contact for individuals whose numbers have been misused, and to help resolve cases as quickly as possible.

We have also had a chance to hear from both—we will also have a chance to hear from both Social Security Administration and its Office of Inspector General about ongoing efforts at the agency to combat identity fraud and the ways these can be improved. The agency's records are valuable anti-fraud tools because they associate the numbers, Social Security numbers, with other verified identity data such as the name, date of birth, and date of death. In limited cases, these records have been leveraged to help combat fraud by sharing death data with other Federal and state agencies, and by partnering with the private sector to establish Electronic Consent-Based Social Security Verification number, or the ECBSV.

But as we will hear today, there is more that the SSA and Congress can do to improve the effectiveness of these efforts. Identity theft is a serious issue, and we all have a responsibility to do a better job of protecting Americans from this threat and to restore the public trust.

I want to thank our witnesses for joining us today, and we look forward to your testimony.

Chairman FERGUSON. I am pleased to recognize the ranking member from Connecticut, Mr. Larson, for his opening statement.

Sir, you are recognized.

Mr. LARSON. Thank you, Mr. Chairman, and I am honored to join with you in terms of putting forward this legislation.

As you have indicated in your remarks, identity theft is vitally important to the American people, as is Social Security itself, the nation's number-one insurance plan, the nation's number-one program with respect to making sure that our elderly stay off of poverty and our children stay off of poverty. And more veterans, of course, rely on Social Security disability than they do the VA. Yet important as identity theft is—and it is, and we must take it serious—it is also important that we fund Social Security appropriately.

And the Social Security Administration is the most effective and efficient agency we have in the Federal Government. In insurance parlance, they operate at what is called a 99 percent loss ratio. I come from an insurance capital. That means that they are able to operate their agency and serve the more than 66 million Americans with under 1 percent administrative costs. They don't need to be

cut, they need to be enhanced, and especially in this area of identity fraud, as well.

And so I think it is incumbent upon us not only to strengthen the Social Security Administration so they are capable of doing their job, especially after the devastation we have seen from the pandemic and what that has done all across the country and the nation, and specifically with a agency—there is no other Federal agency, none, that operates and administers what it has to do with under one percent. That is incredible. We should be striving to make a model of what Social Security does and how effective they have been in terms of getting—because they certainly, as we all would agree, having talked to our constituents, can do better.

So, Mr. Chairman, I as well wanted to do this, as well as at the start. I have a card for everybody. You even have your picture on it there, Mr. Chairman. But I am going to have them pass it out for both Democrats and Republicans. I intend to give these to everyone in the Congress. And I hope that we can join together, because I think the most important thing that we can do with regard to identity theft and with regard to Social Security is enhance the program. And Social Security has not been enhanced since Richard Nixon was the President of the United States in 1971. There have been no improvements.

So, when you get your card—and Mr. Chairman, I took the liberty—you know, I blew up your card and my card, but everyone is going to get these. And on it, it will tell you just how many Social Security recipients you have in your district, and then it will break it down to those children in your district that are getting Social Security, to those veterans that are getting that Social Security. But most importantly, and something we don't talk enough about as well, is how this is an engine for economic recovery.

Mr. Chairman, you have 161,374 Social Security recipients in Georgia's 3rd, and monthly your district gets $270 million comes into the district. That is incredible. I have 147,662 Social Security recipients who get $270 million monthly. We have not improved or enhanced that in 52 years. A gallon of milk cost $0.72 in 1971. Obviously, everybody on this committee knows what has happened in terms of prices.

And when you add that to what we are living in now, in terms of what political scientists and historians are calling a poly-crisis, when you look at what is happening globally, just in the area of, let's say, the pandemic, the supply chain issues, the ensuing global inflation, and then add to that a global war—that is, in essence, what the Ukraine war amounts to—and you look at the pressure, who is the group that that impacts the most? Seniors. How so?

Everybody knows this, but we don't talk about it enough. Of the more than slightly over 1.2 million people who have perished in this pandemic, 855,000 were over the age of 65. Of the people that are impacted the most on inflation, those are people on fixed incomes. Those are the 66 million people on Social Security. They need our help, and they need it now, not only in terms of protecting identity theft, but most importantly, the theft of not having their Congress do what it should do. Five million of our fellow Americans get below-poverty-level checks, having worked all their lives, and paid into a system that only Congress can change.

Chairman FERGUSON. Mr. Larson, you are about a minute over here, and we all appreciate and share——

Mr. LARSON. My passion. I'm sorry that I went over time.

Chairman FERGUSON. Quite all right. This is an important topic, an important program. And in the coming months——

Mr. LARSON. I apologize, Mr. Chairman, and I yield back. [Laughter.]

Chairman FERGUSON. Thank you. And while all of the points that you made are worthy of intense debate and discussion, today we do not want to miss an opportunity to focus on a very important topic, which is identity fraud, and so now I will introduce our witnesses.

Mr. Sean Brune is the deputy commissioner for systems and chief information officer at the Social Security Administration.

Ms. Katie Wechsler is the co-executive director at Consumer First Coalition.

Ms. Margaret Hayward is a private citizen and a mother of three who has been invited to share her personal experience trying to resolve an issue related to her daughter's lost Social Security number.

I would also like to take a point of privilege to recognize your husband and children who are here. Thank you for joining us, as well. We are glad to have you here and look forward to the commentary from the back row back there. [Laughter.]

Chairman FERGUSON. Mr. Robert Roach—good to see you again—as President of the Alliance for Retired Americans.

And Mr. Jeffrey Brown is the deputy assistant inspector general at the Office of Audits for the Office of Inspector General at the Social Security Administration.

Welcome to you all and thank you for your time today.

Mr. Brune, your written statement has been made part of the record, and you are now recognized for five minutes, sir.

STATEMENT OF SEAN BRUNE, DEPUTY COMMISSIONER FOR SYSTEMS AND CHIEF INFORMATION OFFICER, SOCIAL SECURITY ADMINISTRATION

Mr. BRUNE. Thank you, Mr. Chairman, Ranking Member Larson, and members of the subcommittee. Thank you for inviting me to discuss Social Security Administration's role in combating identity theft. I am Sean Brune, the Deputy Commissioner for Systems and Chief Information Officer for SSA.

Today I will talk about our efforts to mitigate the harm resulting from criminals who try to misuse SSNs for their own gain. All of us play a role in finding the solutions to this misuse, and I greatly appreciate the subcommittee's many years of work on this important issue.

The Social Security Act of 1935 did not mandate the use of SSNs, but it did authorize the creation of a record-keeping system for accurate wage reporting. We designed the SSN to allow employers to uniquely identify and properly report individual earnings, and to help us track earnings, determine eligibility for benefits, and pay the correct amount. Today, almost 90 years later, the SSN remains at the core of our record-keeping, and is essential to carrying out our mission.

Over many decades, use of the SSN for non-programmed purposes has spread. Businesses now use the SSN to track, identify, and exchange information about individuals. Data aggregators amass and sell large volumes of personal information, including SSNs, collected by businesses. As SSN use has expanded, so have incentives to obtain fraudulent SSNs.

At one time it may have been helpful to use the SSN as secret information, something that would only be known by the person to whom the SSN was assigned. That is no longer the case and has not been the case for many decades. The SSN was never and will never be evidence of someone's identity. It is simply a number associated with specific individual—with a specific individual in our records.

Over time, SSN misuse and identity theft, including synthetic identity theft, have continued to persist. Identity thieves have learned to target children because of their credit history are clean, and their records may be used for years before anyone realizes someone has stolen their identities or misused their SSN. None of this is acceptable.

We understand the frustration, distress, and economic hardship SSN misuse and identity theft causes victims. As a matter of practice, online and in our field offices we provide individuals who suspect their identities have been stolen with up-to-date information about steps they can take to minimize the damage caused by the criminals. We also help to prevent identity theft by continuing to work with government agencies and external groups to raise awareness of the problem. And we support our Office of Inspector General Office of Investigation in their law enforcement efforts to stop identity theft.

Awareness, however, is only part of the answer. Even though we advise people to keep their SSN confidential, public and private data leaks have greatly reduced the likelihood that SSNs are secret. This is why SSA's lawfully authorized electronic SSN verifications have become so important. Annually, we perform over 2 billion automated SSN verifications through more than 3,500 data exchanges. Using electronic systems such as our Social Security Number Verification Service and the Electronic Consent-Based Verification Service, we are making it harder for identity thieves to operate.

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

We understand the significant challenges associated with identity theft, with both—within both government and private sector. As long as the SSN remains key to accessing things of value, the SSN itself will have commercial value, and it will continue to be targeted for misuse. SSA will continue to do what we can to prevent and mitigate the effects of SSN use, misuse, and identity theft. We stand ready to work with you and with other government and private industry partners as you consider ways to protect Americans' personal information.

Thank you, and I would be happy to answer any questions.
[The statement of Mr. Brune follows:]

HOUSE WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

UNITED STATES HOUSE OF REPRESENTATIVES

MAY 24, 2023

STATEMENT FOR THE RECORD

SEAN BRUNE

DEPUTY COMMISSIONER FOR SYSTEMS and CHIEF INFORMATION OFFICER

SOCIAL SECURITY ADMINISTRATION

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

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

The SSN and Our Programs

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

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

Expansion of SSN Use for Other Purposes

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

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

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

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

Use of the SSN by the Private Sector

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

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

Responding to the External Use of the SSN

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

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

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

Identity Theft and the SSN

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

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

Public Education

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

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

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

SSN Verifications

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

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

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

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

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

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

Keeping the SSN Secure

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

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

Planning for the Future

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

Chairman FERGUSON. Thank you, Mr. Brune.

Ms. Wechsler, you are now recognized for five minutes.

STATEMENT OF KATIE WECHSLER, CO-EXECUTIVE DIRECTOR, CONSUMER FIRST COALITION

Ms. WECHSLER. Chairman Ferguson, Ranking Member Larson, and members of the subcommittee, thank you for the opportunity to testify on SSA's role in combating identity fraud.

I am here to discuss a top priority of the Consumer First Coalition: preventing synthetic identity fraud through the use of SSA's Electronic Consent-Based SSN Verification, or ECBSV service, a service that, on a bipartisan basis, Congress directed SSA to establish.

A criminal creates a synthetic identity by combining real information such as a person's SSN with fabricated information, using that to apply for credit, and having a credit report created at the credit bureaus. With some patience, the criminal will spend time building up the credit profile of the synthetic identity. Later, the criminal obtains a large credit limit, maxes it out, and vanishes. The victims are the owners of the stolen Social Security numbers, many of whom are children.

Over one million children a year are victims of identity theft. The fraud may only be uncovered years later, when an 18-year-old applies for a student loan or credit card. Undoing synthetic identity fraud is a huge burden on that individual and his parents. This fraud costs the credit industry billions in losses every year, making credit more costly for all.

Recognizing this fraud problem in the mid-2000s, SSA used its existing legal authority to create a paper-based service, enabling users, for a fee, to verify whether a name, date of birth, and SSN matched SSA's records, with written consent from the SSN holder. That paper-based process is too slow for our increasingly digital credit system.

In 2018 Congress mandated that SSA create an electronic, real-time version of the paper-based system. Thus, ECBSV became part of SSA's mission. This committee was essential to that enactment, as it unanimously passed the legislation that ultimately became the law.

The ECBSV system allows financial institutions, with a consumer's electronic consent, to verify whether a name, date of birth, and SSN combination match SSA's records. The response is either a match or no-match result. Twenty-two entities use the system, many of whom are service providers submitting on behalf of multiple financial institutions.

Our coalition has worked closely with SSA since the 2018 law was passed. I want to focus on the execution of this congressional mandate.

Improvements are necessary for the viability of the program. I do not say this lightly. The ECBSV system is at risk of collapse if changes are not made.

First, SSA must extend the timeframe for recovering the cost of the system. The law mandates that users fully reimburse SSA, and we wholly accept that obligation. However, SSA is attempting to re-

cover $38 million in the next 3 years, a deadline not in the enacting statute, by substantially increasing user fees.

There was a price increase last April and another one takes effect in July. Some users will be expected to pay more than 22 times what they originally paid for the exact same system. If this continues, it is highly likely that current and potential users will be deterred. Some users may stop altogether, and some may submit transactions only for high-risk scenarios. That means fewer transactions, which could cause SSA to increase the fees again for the remaining users. That is not viable.

We ask Congress and SSA to work with us to extend the cost recovery timeframe to 10 years.

Second, SSA should explore ways to provide further detail on a no-match result. It is impossible to determine, based on that result alone, if there is synthetic identity fraud. Data shows that roughly 40 percent of the no-match results are fraud, while the rest are typos or another benign issue. Enhancements to the technology of the system and additional granularity, all while protecting consumers' privacy and data, are worth exploring. This could significantly improve the usefulness of the system and attract more users.

Finally, SSA should consider how else ECBSV could be used. Other entities in both the public and private sector may find this system worthwhile. We have a vested interest in ensuring ECBSV is a success, as it could be a model of good government and public-private collaboration. If it fails, the only people that benefit are criminals.

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

[The statement of Ms. Wechsler follows:]

House Committee on Ways and Means
Subcommittee on Social Security Hearing:
"Social Security Administration's Role in Combatting Identity Fraud"
May 24, 2023

Testimony of Katie Wechsler
Consumer First Coalition

Chairman Ferguson, Ranking Member Larson, and members of the Subcommittee: thank you for the opportunity to testify today on the Social Security Administration's (SSA) Role in Combatting Identity Fraud. My name is Katie Wechsler, and I am co-executive director of the Consumer First Coalition (Coalition). Formed in 2018, the Coalition is a group of financial services companies committed to combatting new forms of fraud, protecting identities, and upholding the privacy protections of consumers.

My testimony today is focused on the main priority of the Coalition — combatting synthetic identity fraud through the implementation of SSA's Electronic Consent Based SSN Verification (eCBSV) service. Congress authorized the creation of eCBSV in 2018 to address synthetic identity fraud.

What is Synthetic Identity Fraud?

Before I discuss SSA's eCBSV system, it's necessary to define synthetic identity fraud and understand why it is a considerable threat to consumers. As defined by the Federal Reserve as part of its FedPayments Improvement initiative,

> *Synthetic identity fraud is the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.*[1]

Personally identifiable information that may be used to create a synthetic identity includes information that is unique to an individual (e.g., name, date of birth, Social Security number, and other government-issued identifiers). It may also include supplemental information that can help

[1] "Synthetic Identity Fraud Defined," The Federal Reserve FedPayments Improvement, https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/synthetic-identity-fraud-defined/.

substantiate or enhance the validity of an identity, but cannot establish an identity by itself (e.g., a mailing or billing address, phone number, email address or digital footprint).

Common uses of synthetic identities include:

- Credit repair scams. This involves individuals' efforts to hide negative credit history or bad debt in order to appear creditworthy.
- Fraud for living. This is the use of false identity information to apply for employment or services (e.g., utilities, housing, bank accounts).
- Payment default schemes. These are schemes to use a false identity to obtain goods, cash, or services with no intent to repay over a period of time.[2]

Criminals create a synthetic identity by combining SSNs, names, and birthdates of multiple people, or by combining real information about a single person with fabricated information. A criminal will use this identity to apply for some type of credit, often a credit card. When financial institutions receive an application for new credit, they typically submit an inquiry to one or more of the credit bureaus. If an applicant has fabricated an identity, the credit bureaus will report that the identity does not have a credit history. As a result, the financial institution will reject the application.

This is, however, just the start of the synthetic fraud. Even though the credit is denied, the initial inquiry creates a credit file for the synthetic identity. The criminal will continue with similar attempts to obtain credit, and at some point, likely will be successful in obtaining a loan or credit card, albeit for a small amount. The criminal will use this new line of credit to establish a timely repayment history, often with the addition of "authorized user" tradelines. This repayment history can then be leveraged to obtain higher credit limits and additional accounts. It's a long game, but at the end, the criminal has successfully created a seemingly strong credit profile for a synthetic identity, which they use to obtain a large amount of credit, with zero intent to repay.

[2] FedPayments Improvement, "Synthetic Identity Fraud Defined."

Synthetic identity fraud is reported to be the fastest growing type of financial crime.[3] Synthetic fraud is estimated to cost several billion dollars in losses each year. Basic "Know Your Customer" checks often miss this type of fraud. One analysis found that credit card accounts associated with synthetic identities charge off 50 times more frequently than a typical consumer, for an average of $13,000.[4]

As one example, last year a Georgia man was sentenced to more than seven years in prison for a synthetic identities scheme that defrauded banks out of nearly $2 million.[5] In 2020, federal prosecutors charged two Florida residents with bank fraud conspiracy for allegedly using synthetic identities to commit crimes, including defrauding banks and stealing more than $3 million from COVID-19 relief programs.[6]

While the financial loss is often borne by financial institutions, the true victims are the actual owners of the stolen SSNs. Even worse, a frequent target of this fraud is children. One study found that in one year alone, one million children were victims of identity fraud.[7] Most parents are not checking their child's credit reports, and the child's SSN is rarely used. For fraudsters, this is ideal — an SSN that is not yet in the financial services and credit ecosystem. If a child is a victim of synthetic identity fraud, it could be many years before that fraud is uncovered. It may not be discovered until the child turns 18 and is applying for a student loan or their first credit card. At that point, they have a daunting and painstaking task ahead of them: undoing years of synthetic identity fraud and ensuring it is only their own name that is associated with their SSN.

---

[3] "The Need to Define Synthetic Identity Fraud," The Federal Reserve FedPayments Improvement, p. 3. https://fedpaymentsimprovement.org/wp-content/uploads/synthetic-identity-fraud-definition-overview.pdf
[4] Maxwell Blumenfeld, "Updated customer identification rules are long overdue," *American Banker*, April 22, 2022, https://insight.sentilink.com/hubfs/Bank%20Think%20Article%20American%20Banker%202022.pdf.
[5] "Georgia Man Sentenced to Over 7½ Years in Prison for Synthetic Identities Scheme That Defrauded Banks Out of Nearly $2 Million," United States Attorney's Office, Central District of California, https://www.justice.gov/usao-cdca/pr/georgia-man-sentenced-over-7-years-prison-synthetic-identities-scheme-defrauded-banks.
[6] "Two Men Who Allegedly Used Synthetic Identities, Existing Shell Companies, and Prior Fraud Experience to Exploit Covid-19 Relief Programs Charged in Miami Federal Court," United States Attorney's Office, Southern District of Florida, https://www.justice.gov/usao-sdfl/pr/two-men-who-allegedly-used-synthetic-identities-existing-shell-companies-and-prior-0.
[7] Al Pascual and Kyle Marchini, "2018 Child Identity Fraud Study," Javelin, https://javelinstrategy.com/research/2018-child-identity-fraud-study.

SSA holds the Solution to Stopping Synthetic Identity Fraud

Synthetic identity fraud is more prevalent in the U.S. than in other countries due in part to a strong reliance on SSNs as identifiers.[8] Thus, SSA is key to combatting this type of fraud. SSNs were originally created by SSA for a specific purpose: tracking earnings histories of individuals to determine Social Security benefits. "Over time, the use of SSNs has expanded substantially to become an almost de facto universal identifier in the United States."[9] When an SSN is compromised, it can easily be used by a fraudster to take over an identity or create a synthetic identity. SSA is the one true source of the information needed to determine whether an identity is real or fraudulent.

SSA recognized the problematic SSN-related identity fraud more than fifteen years ago. In 2008, the Agency created a written Consent Based Social Security Number Verification (CBSV) service.[10] This service, which remains in operation, enables paid subscribers to verify a name, date of birth, and SSN match against the SSA's records with written consent from the SSN holder. The CBSV service, however, is a paper-based process that requires a physical or "wet" signature from the SSN holder. This process takes time, and as more of the financial ecosystem went digital, it became impossible for most application channels to use the antiquated, paper-based system.

The Digital Solution: eCBSV

Responding to the need for a more efficient real-time solution, as part of a larger banking bill in 2018, Congress directed SSA to establish an electronic consent-based verification system.[11] The law required SSA to create a system that compares a name, date of birth, and SSN combination provided in an inquiry by a financial institution (as defined by Gramm-Leach-Bliley) or its service provider (together with financial institutions, so-called permitted entities) to confirm or not confirm the validity of the information provided. The system must be scalable and provide real-time machine-to-machine accurate responses. A financial institution may submit such a request to

[8] "Allure of a Synthetic to a Fraudster: Ease of Creation," The Federal Reserve FedPayments Improvement, https://fedpaymentsimprovement.org/wp-content/uploads/allure-of-a-synthetic-to-a-fraudster.pdf.
[9] FedPayments Improvement, "Allure of a Synthetic."
[10] In 2002, SSA had a pilot program, "Social Security Number Verification Pilot for Private Businesses," which was replaced in 2005 with the "Interim Verification Process." The CBSV program replaced that process in November 2008.
[11] Economic Growth, Regulatory Relief, and Consumer Protection Act, Pub. L. No. 115-174, § 215 (2018).

the system only if it has obtained a written, including electronic, consent from the individual who is the subject of the request. Additionally, the purpose of such a request must be for a credit transaction or for another permissible purpose as set forth in the Fair Credit Reporting Act.[12]

To use the system, a company must certify that it: (1) meets the statutory definition of a "permitted entity"; (2) is in compliance with the enabling statute; and (3) is in compliance with its privacy and data security requirements under the Gramm-Leach-Bliley Act, with respect to information the entity receives from SSA's system. The law gives SSA the authority to audit and monitor to ensure proper use by permitted entities of the system and deter fraud and misuses by permitted entities with respect to the system.

The Coalition worked closely with SSA as it developed eCBSV. We appreciate SSA's open and constructive dialogue as the agency worked to develop all aspects of the system, from the technical side of the API to the consent language and user agreement.

In 2020, SSA launched the pilot of eCBSV with 10 permitted entities. By 2021, SSA expanded enrollment to other permitted entities that initially expressed interest when the pilot was announced. In 2022, SSA opened enrollment again, permitting any entity that qualified to enroll as an eCBSV user, subject to agreeing to the user agreement. There are now 22 direct permitted entities, and several of those are service providers (e.g., credit bureaus), that are submitting verification requests on behalf of multiple financial institutions.

To be clear, SSA is not sharing its data with the users of the system. It provides a match/no match response or death indicator based on how the information provided by the permitted entity compares to SSA's data. This simple match/no match answer can stop synthetic identity fraud in its tracks. It also can help with financial inclusion. A match from eCBSV is a strong signal that the individual is who they purport to be, but are simply new to the credit system. Increasingly, eCBSV is being used to help validate thin-file consumers, which is promising for financial inclusion purposes.

[12] Fair Credit Reporting Act, 15 U.S.C. 1681b (2003).

We understand that roughly eight in 100 submissions come back as a "no match" response. Some analysis shows that of the eight that come back as a no match, three of those are fraudulent attempts and the other five are generally legitimate consumers and the mismatch was simply the result of a typo or a nickname being used.[13]

Costs of eCBSV

The law dictates that SSA's costs to build and operate the system shall be fully recovered from the users of the system. SSA establishes the amount to be paid by the users and shall periodically adjust those amounts to ensure that amounts collected are sufficient to fully offset the cost of the administration of the system.

Prior to the initial launch and as mandated by the law, SSA collected 50 percent of the start-up costs — $9.2 million.[14] The initial fee schedule ranged based on annual transaction volumes, with five tiers and annual fees ranging from $400 (for annual volume of up to 1,000) to $860,000 (for transaction volumes between 50,000,001 and up to 2 billion).[15] In November 2020, SSA stated that the total cost for developing the service is $45 million and SSA will recover the cost over a five-year period, assuming projected enrollments and transaction volumes materialize.[16]

In January 2022, SSA announced substantial changes to its eCBSV tier fee schedule. The revised tier fee schedule was based on 45 participating permitted entities in FY 2022 submitting an anticipated volume of 280 million transactions. The total cost for developing the service is $50 million through FY 2021, and SSA will recover the cost over a three-year period, assuming

[13] "The Electronic Consent Based SSN Verification Service," SentiLink, https://blog.sentilink.com/electronic-consent-based-ssn-verification-service.
[14] "Agency Information Collection Activities: Proposed Request," *Federal Register*, December 5, 2019, https://www.federalregister.gov/documents/2019/12/05/2019-26259/agency-information-collection-activities-proposed-request; "Agency Information Collection Activities: Proposed Request," *Federal Register*, March 10, 2020, https://www.federalregister.gov/documents/2020/03/10/2020-04807/agency-information-collection-activities-comment-request.
[15] *Federal Register,* December 5, 2019; *Federal Register*, March 10, 2020.
[16] "Agency Information Collection Activities: Proposed Request," *Federal Register*, November 30, 2020, https://www.federalregister.gov/documents/2020/11/30/2020-26292/agency-information-collection-activities-proposed-request.

projected enrollments and transaction volumes meet SSA's projections.[17] SSA moved from a five-tier schedule to a seven-tier schedule, with annual fees ranging from $400 (for annual volume of 1-1,000) to $7,500,000 (for annual volume over 50 million).

After that new fee schedule was announced, the Coalition expressed some concerns with SSA. We noted that the new fee schedule may inadvertently frustrate the purpose of eCBSV and interfere with SSA's goals to increase usage and participation. We also noted that the new tiers are structured in such a way that the marginal cost of a single additional transaction is significant, which will disincentivize greater use of eCBSV. We asked SSA to work closely with users on future adjustments to this schedule, particularly to incentivize greater use of eCBSV while also allowing SSA to recover its costs. We also asked for more information on the time period for recovering costs, and noted that a longer time frame may be needed to recover the costs.

Earlier this month, SSA announced another increase to the tier fee schedule. The new schedule is based on 20 participating permitted entities in FY 2023 submitting an anticipated volume of 65 million transactions. The total cost for developing and operating the service is $53 million through FY 2022. Of this amount, $38 million remains unrecovered/unreimbursed. The new subscription tier schedule is intended to recover these costs over a three-year period, assuming enrollments and transaction volumes meet these projections.[18] The new tier schedule is effective July 10, 2023. This new schedule has 10 tiers with annual fees ranging from $7,000 for annual transaction volume between 1-10,000 up to $8.25 million for annual transaction volume of 25,000,001 – 75 million.

These fee increases are significant. For example, in the first two years of the system, a user with an annual volume of 200,000 transactions paid an annual fee of $14,300. Last year that increased to $40,000, and beginning in July, for the same user, that annual fee will be $130,000. That is a nine-fold increase in fees for the same system. For a user with an annual volume of 20

[17] "Notice of Open Enrollment and Fee Increase for Our Electronic Consent Based Social Security Number Verification Service," *Federal Register*, January 14, 2022, https://www.federalregister.gov/documents/2022/01/14/2022-00638/notice-of-open-enrollment-and-fee-increase-for-our-electronic-consent-based-social-security-number.
[18] "Notice of Fee Increase for Our Electronic Consent Based Social Security Number Verification Service," *Federal Register*, May 9, 2023, https://www.federalregister.gov/documents/2023/05/09/2023-09753/notice-of-fee-increase-for-our-electronic-consent-based-social-security-number-verification-service.

million transactions, the initial annual fee was $276,500. In 2022, that increased to $1.5 million, and in July, that user's annual fee will be $6.25 million. That user will be expected to pay more than 22 times its original amount for the same service.

In developing this new tier schedule, SSA engaged in a constructive dialogue with the industry. In the new tier structure, SSA adopted two key suggestions from the industry: (1) the agency added more tiers between 1 million and 50 million transactions to incent greater use of eCBSV and (2) incenting permitted entities to submit higher volumes by discounting pricing as permitted entities use or commit to higher volumes. However, the new tier structure does not address two issues that must be resolved for the long-term success of the system: (1) the short timeframe SSA has set to recover the remaining costs of the initial system development and (2) the estimated annual operational costs. Accordingly, the industry sent a letter to SSA expressing concerns about further increasing the fee schedule. That letter is attached to my testimony.

Improving eCBSV

SSA's eCBSV is critical to preventing synthetic identity fraud. It is hard to envision a resource more suited for this task. While the ramp-up in usage of the system has taken some time, SSA is seeing steady transaction volume. That alone shows the need for this system.

The success of eCBSV is in the best interest of consumers, the financial services industry, and the government. If eCBSV is not efficient and effective, the only people who benefit are criminals. To ensure the long-term success of eCSBV, the Coalition offers the following:

First, as noted previously, the industry has serious concerns regarding the recently announced increase in the fee tier structure. To be clear, we fully understand and accept the industry's responsibility to reimburse SSA for the costs of eCBSV. That is not a point we dispute. What we do have concerns about is the short time frame in which SSA is trying to recover these costs. Total cost for developing and operating the service is $53 million through FY 2022. Of this amount, $38 million remains unreimbursed, and SSA has said it plans to recover that amount within three years. To do so, it has substantially increased the prices to use the system. If SSA continues on this path, we are very concerned that current and potential users will be deterred. We understand that SSA wants to attract new users and increase usage and participation, and we

believe these price increases will have the opposite effect. If that deterrence occurs, it will be impossible for SSA to recover the costs in the three-year timeframe. SSA has relayed to us that they are constrained due to the operations of appropriations law and the length of time they have to recover the initial build costs. We want to work with SSA and Congress on possible solutions, such as extending the recovery time period to 10 years.

Second, existing SSA policy makes it very difficult to determine the impact of the system on combatting fraud. A permitted entity receives only a binary match/no match response, with no indication of which data field caused the mismatch. The lack of insight restricts financial institutions from determining whether it was a potential entry error, such as a misspelled name or abbreviated first name, or an actual synthetic identity. We ask SSA to explore ways to share additional information about the reasons for mismatches, so that users can better understand the root cause of a mismatch. This may be in enhancements to or more transparency into SSA's "fuzzy logic." Such insights would significantly improve the usefulness of the system and allow calculations regarding its value in combatting fraud.

Finally, we believe it is worth exploring other ways eCBSV can be used. The system was established to assist financial institutions and their service providers with credit decisions. However, it may be possible for this system to be used by other entities with legitimate purposes, such as landlords for tenant screenings or employers for hiring purposes. SSA has used a substantial amount of resources to build this system, and it is worth exploring what other entities, both government and private, could use this system.

Thank you for holding this hearing today and for the opportunity to testify on synthetic identity fraud. SSA and eCBSV are critical to combat synthetic identity fraud. The Consumer First Coalition stands ready to work with SSA and Congress to extend the time frame to recover costs and enhance the effectiveness of the system. We want eCBSV to be an effective tool to thwarting synthetic identity fraud and protecting some of the most vulnerable consumers. If eCBSV fails, the only winners are the criminals.

Appendix

March 1, 2023

Acting Commissioner Kilolo Kijakazi
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235

Re: eCBSV Tier Fee Schedule

Dear Acting Commissioner Kijakazi:

The undersigned associations have appreciated the opportunity to partner with the Social Security Administration ("SSA") to make the SSA's electronic Consent Based Social Security Number Verification ("eCBSV") Service as effective and efficient as possible. We, along with our members, have worked closely with SSA in developing and implementing the system mandated by Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 (the "Banking Bill").

It is our understanding that SSA is considering changes to the eCBSV tier fee schedule, including significantly increasing the fees for many users. We urge you **not** to move forward with these changes to the tier fee schedule. We are very concerned that these potential increases will force some current users to withdraw from participation in the eCBSV program and deter potential new users from enrolling. At a time when SSA is hoping to attract new users and increase usage and participation, these changes would move the program in the opposite direction. If prices continue to increase, we have grave concerns on the viability of eCBSV in the long term.

We recognize that SSA must recover the costs associated with eCBSV, and we stand ready to work with SSA and other policymakers, including Congress and OMB, on the best approach to do so. However, we believe it is not feasible for SSA to fully recover the development costs by FY 2025. It is our understanding that as of August 2022, SSA has only recovered $12.4 million of the total development costs of roughly $50 million, resulting in $39 million in unreimbursed costs. We recognize that SSA may have constraints on the timing of recovering these costs, and we commit to working with policymakers to ease these constraints to the extent possible. Additionally, we ask SSA to reevaluate the annual operating costs of the system, as we are concerned that is not sustainable.

One underlying issue that seems to be contributing to the high number of unreimbursed costs is the original transaction and usage estimates used by SSA in building the system varied significantly from those estimates provided by industry and have continued to shift significantly year after year. In 2019, the industry relayed to SSA that a reasonable estimate based on industry surveys and Federal Reserve data would be to expect 300-400 million inquiries each year with an upper bound of 500 million, but noted that if permitted entities could reuse results (which they effectively can – by noting in their internal systems that data associated with an identity on file had matched data at SSA) that the volume would be much lower. SSA, however, moved forward with building a system that could support over 1 billion annual inquiries – or more than double the high-end of what industry suggested would be the likely volume if there was no way to reuse results.

Appendix

In December 2019, SSA based its cost estimates for the eCBSV pilot phase on **10 participating entities** in FY 2020 submitting an anticipated volume of **307,000,000 transactions**; actual transactions in FY 2020 were much lower. Despite that lower number, in November 2020, SSA based cost estimates on **123 participating entities** in FY 2021 submitting an anticipated volume of **1,100,000,000 transactions**; again, actual numbers were much lower. In January 2022, SSA based its revised tier structure on **45 participating entities** in FY 2022 submitting an anticipated volume of **280,000,000 transactions**. At that time, SSA also stated that it anticipated recovering the development costs over a three-year period, assuming projected enrollments and transaction volumes meet SSA's projections.

We flag this history to note that SSA's projected transaction volume substantially diverged from the estimates that the industry provided in 2019, with the result being that the program incurred much greater costs in the eCBSV development than was necessary to address industry demand for the eCBSV system. As SSA moves to recover those dollars, it is important that the economics of the program also incent industry to use eCBSV. As noted earlier, we are concerned that another round of material price increases will instead force some current users to withdraw from participation in the eCBSV program and deter potential new users from enrolling – which will, in turn, make it much harder for SSA to recover the funds currently expended.

Additionally, existing SSA policy makes it very difficult to determine the impact of the program on combatting fraud. The average mismatch rate that SSA reports for submitted queries generally hovers around 8%. Unfortunately, a permitted entity only receives a binary match / no match response with no indication which data field caused the mismatch, whether it was name, date of birth, or wrong SSN. This lack of insight restricts financial institutions from determining whether it was a potential entry error such as a misspelled name, abbreviated first name e.g. Katy for Katherine, or an actual synthetic identity. We would ask SSA to reconsider this decision and explore ways that additional information could be shared about the reasons for mismatches to allow financial institutions to better understand the root cause of mismatch, which would significantly improve the usefulness of the system and allow calculations regarding its value in combatting fraud.

We want to continue to work with SSA to make eCBSV an effective tool in preventing synthetic identity fraud. We ask SSA to not move forward with the proposed increases to the tier fee schedule and work with the industry on developing a sustainable path forward.

We appreciate your attention to the issues we have raised. If you would like to discuss these issues, please contact Paul Benda, American Bankers Association, pbenda@aba.com, Jeremy Grant, Better Identity Coalition, jeremy.grant@venable.com, and Katie Wechsler, Consumer First Coalition, kwechsler@snwlawfirm.com.

Sincerely,

American Bankers Association Better Identity Coalition Consumer First Coalition

Chairman FERGUSON. Thank you, Ms. Wechsler.

Ms. Hayward, we now look forward to hearing from you. You are recognized for five minutes.

STATEMENT OF MARGARET HAYWARD, PRIVATE CITIZEN AND MOTHER OF THREE

Ms. HAYWARD. Chairman Ferguson, Ranking Member Larson, and members of the subcommittee, thank you for the opportunity to share our family's story with you.

Through no fault of her own, our infant daughter's identity was put at risk when she was just a few weeks old. This experience has been stressful for our family during an already vulnerable time and is something that I hope other families won't ever experience.

At the beginning of August last year, my husband and I welcomed our third child shortly after relocating to Pennsylvania. When she was seven weeks old, I realized we had never received her Social Security card. I checked the Social Security Administration's website, and saw it was taking about three weeks to issue them. Being well beyond that window, I immediately called the 1–800 SSA telephone number.

When I reached an SSA representative, he listened to my concerns, encouraged me to be patient, and give it a few more weeks. He told me it didn't matter if she had been assigned a number or not, because either way I could just complete the form requesting a new card. I told him from an identity standpoint, it did matter. It mattered significantly. If she had already been issued a card, her identity could be at risk because someone else could have it. According to that representative, our only option was to request a new card. I could not receive her social security number over the phone so we could begin the process of protecting her identity. Marcy and I would have to visit a field office, and the only way to be assured her identity was protected—assigning a new number—was not an option.

Going anywhere with a newborn, much less waiting at a government office, is no small feat. For us, this requirement became extra challenging. I planned to go to the Social Security office right away. However, just hours after I called, our daughter became acutely ill and was admitted to the hospital for RSV. Three weeks later our child was finally healthy and durable enough to visit our local Social Security office in person.

Off we finally went to the SSA field office to complete our online request for a new card and find out our daughter's Social Security number. The visit followed the same pattern. It was once again suggested I be patient and give it more time. And contrary to what the telephone representative told me, they also would not provide me with our daughter's assigned number. All we could do was finalize the request of a replacement card and wait.

When it comes to protecting your child, waiting, and hoping is not an acceptable course of action.

When Marcy was three months old, the replacement card arrived, and we finally learned our daughter's Social Security number. It was only then that we were able to begin the laborious process of monitoring and protecting her credit through each of the

non-government credit bureaus. Her original card remains unaccounted for and could be in anyone's hands.

The Social Security Administration personnel made what was already a stressful time even more difficult with inconsistent and inaccurate information. On top of the frustration, we had to weigh the risks of bringing a medically fragile baby to a field office to move the process of protecting her forward. Each interaction went the same way: repeating our situation and pushing to be connected to the right resources.

Many parents don't have the education, time, or experience navigating complex systems that I do, and until this is fixed, it is their children who stand to lose the most.

Before she was even a month old, a vital piece of our daughter's identity was compromised. And she has no choice but to use that number for life. As long as we are successful at protecting her, Marcy won't meet the SSA's threshold to receive a new number. At best, she will be inconvenienced with a locked credit forever.

A singular, knowledgeable point of contact within the SSA who was familiar with our case and could help us navigate this process would have been immensely helpful. A new Social Security number for our daughter would prevent us and someday her from a lifetime of credit and identity monitoring, saving hours of time and years of stress and attention.

Prior to our daughter's birth, I worked as a family nurse practitioner. And when it comes to one's health, prevention is so much more valuable than treatment. I would like to see the SSA apply the same philosophy to identity protection. Even the threat of identity compromise is time consuming and exhausting.

I am heartened by the subcommittee's focus on this important issue and implore you to continue your work to ultimately pass legislation that will give my family and so many others readily attainable peace of mind. Thank you so much for allowing me to share our family's story with you today.

[The statement of Ms. Hayward follows:]

Statement of Margaret Hayward, MSN, RN, FNP-BC
House Ways and Means Subcommittee on Social Security
Hearing on Social Security Administration's Role in Combatting Identity Fraud
May 24, 2023

Chairman Ferguson, Ranking Member Larson, and Members of the Subcommittee, thank you so much for the opportunity to share our family's story with you. Through no fault of her own, our infant daughter's identity was put at risk when she was just a few weeks old. This experience has been stressful for our family during an already vulnerable time and is something that I hope other families won't have to experience.

At the beginning of August 2022, my husband and I welcomed our third child shortly after relocating to Pennsylvania. Like we had for our first two children, we submitted the paperwork for a birth certificate and Social Security card while we were still in the hospital after her birth. I breathed a sigh of relief as I always do when the birth certificate arrived. It wasn't until she was seven weeks old that I realized we had never received her Social Security card. I checked the Social Security Administration's (SSA) website and saw that it was taking about three weeks to issue them and became concerned.

First I assumed we must have received it and overlooked filing it – life with a brand new baby and two other young children is chaotic. I reviewed every piece of mail we had received since our daughter was born. I went back and reviewed our daily USPS informed delivery emails several times as well. Each time, I saw only the birth certificate's arrival.

I immediately called the SSA 1-800 number listed on the website. When I reached an SSA representative, he listened to my concerns and then encouraged me to be patient and give it a few more weeks to arrive. I pressed for more help, reiterating my concerns about the safety of her identity. He then searched for how long it should take us to receive the card in the mail. He informed me what I already knew, that for Pennsylvanians it was taking about three weeks. I reminded him that our child was seven weeks old, so it should have arrived a month ago. I told him that I first needed to know if the form had been lost in transit to the SSA, or if our request had been received and a card had been issued but not made it to us. He told me it didn't matter if she had been assigned a number or not, because either way I could just complete the form requesting a new card. I told him from an identity standpoint it did matter; if she had been issued a card already, her identity could be at risk because someone else could have her card.

The SSA representative then agreed to see if she had a record and had been assigned a number, so I provided our daughter's information to him. He confirmed that the card had been created and was mailed to us approximately a month prior. At that point, he admitted that it probably should have arrived already and told me if I didn't want to continue to wait, I could go online and submit the form for the request of a new Social Security card. I asked if she could be assigned a fresh Social Security number for her

protection since we had obviously not used it yet, and was informed that that was not possible.

Without the opportunity to get a new number, I asked if I could be told her Social Security number so that I could take immediate steps to secure her identity since someone could have intercepted her card and already be using the number. Without knowing the number, we were powerless to do anything to protect her like set up fraud alerts or freeze her credit. He informed me that he could not provide me with that information, but I could go in person to a Social Security office and they would tell me. He also informed me that we would need to go to the local SSA office to show documents as part of the online application for the replacement Social Security card. I asked somewhat desperately what I could and should do to protect her identity in the meantime, and he referred me back to the SSA website, told me I could contact the Social Security Inspector General and provided me their number, and referred me to the FTC if I suspected her identity had been compromised- though without knowing her Social Security number, none of these resources were actually available to us.

Every parent can appreciate that going to an in-person appointment with an infant can be difficult, but for us it turned out to be extra challenging. I intended to go to the Social Security office right away, however just hours after I telephoned the SSA, our daughter became acutely ill and was admitted to the hospital the next day with RSV. Upon her discharge from the hospital, it took more than a week for her to recover, and another couple weeks for us to be willing to bring a fragile infant to an indoor space to wait around other people. So, approximately three weeks later, our child was healthy and durable enough to visit our local Social Security office in person. I had hoped that once we visited our local office, we would then have all the information we needed to expeditiously put this experience behind us.

Prior to our in-person visit, I completed the online portion of the application for a new card as advised by the representative over the phone. Armed with everything the telephone representative and the SSA application instructed me to bring, we went to our local SSA office. When our number was called, I explained our situation and told the woman at the desk that we were there to provide verification documents and complete the in-person interview for my daughter's new Social Security card application. The SSA employee looked at me, glanced at my baby, and suggested that I be patient and give it more time for her card to arrive.

This employee then looked up the issuance timeline provided online and verified it was three weeks, then looked up our daughter and again confirmed to me that a card was mailed out close to 2 months prior and admitted I probably should have gotten it by then. She then asked me each of the questions I had already submitted as part of the online application, seemingly never pulling up the application I had submitted prior to coming in. I asked her if we could be assigned a new number and she said no one can get a new number unless they have years of proof their identity was stolen.

After verifying my identity, she then asked to see my supporting documentation for our child which I provided. She immediately handed back some of the documents I

provided- all of which I'd been told over the phone or online I would need to bring- stating that she didn't know why everyone brought those because they weren't needed. She did not like that the medical records for our daughter were printed from our home but that was all I had because her pediatrician uses an online patient portal. I showed her hospital wristbands, but everything from her birth did not have her name on them as she was "Baby Girl Hayward" for her birth hospitalization. The only reason I had medical records with her legal name to provide was because of her subsequent hospitalization, which most children are lucky enough not to have had at 11 weeks old.

After we completed the new request for a card, I asked if I could please be informed of my child's Social Security number as I needed to take immediate steps to protect her identity. The SSA employee told me that would not be possible. I told her that I had been informed over the phone by someone at SSA that I would be able to find out the number our daughter had been assigned when I arrived in person and verified our identities. The employee told me that was incorrect, they do not do that at SSA offices and that's never possible. I pleaded with her to help me promptly protect my child's identity and she told me I'd have to wait for the new card. I expressed concern that the entity that failed to deliver our first card (USPS) would deliver a second one in a timely manner. She suggested that I "contact my postmaster" or "go to the post office" to ask them to help me, and that maybe they could locate the lost mail for me.

I was not willing to wait another three weeks to take steps to protect our daughter's identity. I contacted our Senator and asked for case management help. They were sympathetic but they too were unable to connect me with a prompt resource to learn the number our daughter had been assigned outside of facilitating the request of a new card which I had already done.

When our child's Social Security card finally arrived, I verified that it was the new one we requested, as the issue date is printed on the card. At the time of this testimony, our daughter is nine months old and her original card never arrived and could be in anyone's hands.

For those who have not done it, the process of monitoring a minor child's credit, setting up fraud alerts, and freezing their credit is incredibly time consuming. Not only does it involve putting trust in third party credit agencies- which have historically had security breaches- it is a nauseating experience to provide every kind of invasive identity-supporting documentation for one parent and the minor child to a non-government entity. Previously, we've balked at freezing the credit of our first two children because it required providing so much of the very information we wish to protect to a company that could also be subject to a breach. Further, the information also has to be sent by mail, the same system that's original failure started this ordeal.

A vital piece of our daughter's identity, ***that she has no choice but to use for her whole life,*** was compromised before she was a month old. It's taken hours of effort over months for us to protect her from identity theft and the threat will ***never*** completely go away unless she's assigned a new Social Security number. This would be a

quick, logical, and permanent fix from a lifetime of vulnerability and yet it is not an option.

As it currently stands, I'm told she's unable to be issued a new number until she's both incurred harm and there is substantial proof of this harm. As a medical professional, I have a hard time grasping an approach that completely eschews prevention. As a mother, I have an immediate uphill battle to proactively protect my daughter and, ironically, if successful she won't meet the SSA's threshold for a new number. Our daughter had the good fortune to be born to parents who understand the importance of identity privacy and protection and were applying for a passport for her. Otherwise, this process of protecting her would have been further delayed and likely proceeded very differently. I shudder to think what families not in our situation will continue to experience without a change in policy.

What's more, the Social Security Administration made what was already an unfortunate and stressful circumstance even more difficult. Every step of the way I was encouraged by SSA to be patient and allow more time for her identity to be potentially compromised. I had to remind every person I spoke with at the SSA of my concerns of identity theft, and push to be connected to resources to help. It was frustrating and confusing to receive inconsistent information when I was on the phone and on the SSA website versus when I was at the field office. I've been able to act quickly because of luck and privilege, and that will not be the case for many families that find themselves in this situation.

I have the benefit of extensive education and significant experience navigating complex systems. I was also home with our young children and wasn't balancing the expectations of a working mother like I was with our first two children. Simply not being a first-time parent was a significant advantage in our situation. I knew when to generally expect to receive my daughter's Social Security card and knew early in the process there was a problem. I was able to take the time and make the effort to advocate for our child and to find out what I needed despite the obstructions provided by the SSA, an amount of time so many parents do not have.

I was never told the steps I should take once I learned our daughter's Social Security number or given any indication that identity fraud is something that I should reasonably be concerned about. If it hadn't already been on my radar, I wouldn't have known there was a potential risk for our child. May our child be so lucky to have the worst effects of this be to have to unfreeze her credit whenever she needs to open an account, and not learn of a wrecked credit history due to identity fraud when she reaches adulthood.

It would have been so helpful for us to have a singular, knowledgeable point of contact within the SSA who was familiar with our case and could help us navigate this difficult process. A new Social Security number for our daughter would prevent us -and someday her -from spending a lifetime monitoring her credit and identity, saving hours of time and years of stress and attention.

Identity theft is not abating. Our children will face constant attacks on their privacy, much more than we did when we were growing up. It is unacceptable that our current system can put their privacy – and potentially, future economic well-being – at risk long before they take their first steps. I do not pretend to be a policy expert on such matters, but I know the current system is insufficient to meet modern and future challenges.

Prior to our daughter's birth, for years I worked as a family nurse practitioner and when it comes to one's health, prevention is so much more valuable than treatment. I'd like to see the SSA apply the same philosophy to identity protection. Even the threat of identity compromise is time consuming and exhausting for multiple individuals. I am heartened by the Subcommittee's focus on this important issue and implore you to continue your work to ultimately pass legislation that will give my family and many others readily attainable peace of mind.

Thank you so much for allowing me to share our family's story with you today.

Chairman FERGUSON. Thank you, Ms. Hayward.
Mr. Roach, you are now recognized for five minutes.

STATEMENT OF ROBERT ROACH, PRESIDENT, ALLIANCE FOR RETIRED AMERICANS

Mr. ROACH. Good afternoon. I am Robert Roach, president of the Alliance for Retired Americans. I would like to thank Subcommittee Chairman Ferguson and Ranking Member Larson, my good friend, and members of this committee for this opportunity to testify and participate in this hearing.

Founded in 2001, the Alliance is a grassroots organization with 4.1 million members in 38 states working to strengthen retirement security for all. Nearly 66 million Americans, 1 out of every 5 households, rely on Social Security's lifetime guaranteed benefits. These benefits are essential to all who rely on them, including seniors, people with disabilities, and their families of deceased workers [sic].

All Americans are rightly concerned about identity theft. Last week, as part of our Older Americans Month celebration, the Alliance held a retiree town hall with the Social Security Administration commissioner. During that event she specifically addressed the issues of fraud and identity theft and the efforts that SSA is making to combat them. We applaud SSA's efforts to increase public awareness of fraud and identity theft.

If the already short-staffed Social Security Administration was forced to cut the budget by 22 percent as prescribed in House Bill 2811, the agency's work to protect Americans from identity theft would be hampered. In fact, the drastic funding cuts in the bill would dramatically reduce the services beneficiaries depend on. Less staff and fewer field offices will mean much longer waits for people who need information about their Social Security and Medicare benefits. People applying for Social Security and disability benefits will have to wait two months longer than they do now.

Instead of shrinking the Social Security Administration's budget, Congress needs to strengthen the program, including providing adequate funding to administrate it. Administrative expenses come from Social Security trust fund paid for by workers and employers. The Social Security Administration's funding must be predictable year over year, especially at a time when 10,000 Americans turn 65 each year.

Another way to strengthen Social Security is by passing legislation such as the Ranking Member's—Larson's soon-to-be-reintroduced Social Security 2100 Act. Among the most critical items, it increases Social Security benefits, extends solvency of Social Security—of the Social Security Trust Fund. It repeals the windfall elimination provision and the government provision offset.

The practical way to strengthen Social Security is by lifting the cap on Social Security payroll taxes above the current $160,200; require the wealthy of us to pay their fair share into the system.

This is more about—this is much more about the numbers and how we pay for something. This is about people. Firsthand, I have seen people standing in line, senior citizens at my supermarket and other supermarkets, who are leaving food at the cashier because they are unable to pay for food, food that they normally and cus-

tomarily buy. Coming from Pentagon City, where we spent $800 billion a year to protect the nation from foreign adversaries, less than a mile away people are making decisions whether to buy food or medicine on a daily basis. In the world's most powerful, richest country in the world, this is just unacceptable.

This is now a family issue because now—and everybody has a story. This is a family issue because, as people grow older and because of the dwindling income that they have, because of the decimation of pension plans and Social Security has not kept pace with inflation, everybody has a story about how they are taking care of parents and grandparents. Some of us have resources and others don't.

In this—at this committee in 2019 you heard the story of Katrina Brown, who was on her way to being a doctor, full scholarship to Ivy League colleges. And because her mother got sick, all that got put aside. Those are a few examples underlying our country's desperate need to expand Social Security benefits.

Social Security importance cannot be overstated because the decline in traditional pension plans, decades of stagnant wages that have made it harder for individuals to save for retirement. It is sapping our human resources because the youth are now taking care of grandma and grandpa.

The U.S. Labor Department representatives for pensions and retirement say that almost two-thirds of beneficiaries receive 50 percent or more of their total income from monthly Social Security checks. And one-third of elderly beneficiaries count on Social Security to provide 90 percent or more of their income.

Moreover, Social Security benefits are insufficient, evidenced by the average monthly Social Security benefit for a retired worker, which is a modest $1,833 a month.

Our members are frustrated. Instead of acting—we want common-sense changes enacted, and we want it done on a bipartisan basis. This is not a White problem. This is not a Black problem. This is not a Hispanic problem or an Asian problem. This is an American problem. And we anticipate, we hope that the united Congress will pass a bill, 2100 Act or something similar, and work together to fix this problem for all Americans and all their families. We are in desperate times, and we put our faith and our hope in the good people that we send to Congress to help us fix our problems.

[The statement of Mr. Roach follows:]

TESTIMONY
ROBERT ROACH, JR.
PRESIDENT OF THE ALLIANCE FOR RETIRED AMERICANS
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON WAYS AND MEANS SUBCOMMITTEE ON SOCIAL SECURITY

HEARING TOPIC: THE SOCIAL SECURITY ADMINISTRATION'S ROLE IN COMBATING IDENTITY FRAUD

May 24, 2023

ALLIANCE FOR RETIRED AMERICANS
815 16TH STREET, NW
WASHINGTON, DC 20006
www.retiredamericans.org

Good afternoon. I am Robert Roach, President of the Alliance for Retired Americans. On behalf of the Alliance, I would like to thank Subcommittee Chairman Ferguson and Ranking Member Larson and the distinguished members of this committee for the opportunity to testify and participate in today's important hearing on the topic of the Social Security Administration's role in preventing identity theft.

Founded in 2001, the Alliance is a grassroots organization representing more than 4.4 million retirees and seniors nationwide. The Alliance and its 39 state chapters work to advance public policy that strengthens the health and retirement security of older Americans.

For decades, Social Security has delivered guaranteed benefits on time and without interruption to millions of Americans. Americans work hard to earn their Social Security benefits, and they contribute to the system with every paycheck. These benefits are essential to all who rely on them, including seniors, people with disabilities and families of deceased workers.

Today nearly 66 million Americans – one out of every five households – relies on Social Security's lifetime, guaranteed benefits. The Alliance strongly believes that to continue to provide retirement security for current and future generations, it is necessary to strengthen and expand Social Security to augment the program's solvency and increase its benefits. Poll after poll clearly demonstrates that 8 in 10 Americans overwhelmingly not only want Social Security's solvency preserved but want program benefits enhanced.

Members of the Alliance and Americans nationwide are concerned about the threat of identity theft. As part of celebrating May as Older Americans Month, the Alliance held a Retiree Town Hall with SSA Acting Commissioner Kilolo Kijakazi last week. During the event, she specifically addressed the issues of fraud and identity theft and the efforts SSA is making to combat them.

In response to an Alliance member's question regarding identity theft and what the SSA is doing to prevent and address it, she replied that "on the Social Security website there is a link prominently displayed right at the top of the site which describes in detailed fashion how to avoid being the victim of a scam and how to avoid a scam." We applaud SSA's efforts to increase public awareness of fraud and identity theft. And certainly, SSA is not exclusively responsible for protecting Americans from identity theft. Although it plays an important role, many other federal agencies as well as the private sector can do much to educate and protect Americans from fraud and identity theft, especially older Americans

If the Social Security Administration, however, which is already short staffed, was forced to cut its budget by 22%, as prescribed in the Republican passed debt ceiling bill, H.R. 2811, the "Limit, Save, Grow Act," the Agency's work to protect Americans from Social Security number

identity theft and other fraud would be hampered. Moreover, the drastic funding cuts in the bill, which would lead to agency staff cuts in its wake, would also:

- Force the Social Security Administration to close or reduce field office hours and reduce access to in-person services;
- Force seniors to endure longer wait times when they call for assistance for both Social Security and Medicare because of Social Security field office closures and the reduced hours they are open to the public;
- Further increase the wait time by an additional two months for people applying for Social Security disability benefits.

From the Alliance's perspective, we believe that instead of shrinking the Social Security Administration's critical funding, Congress needs to strengthen the Social Security system. One way is to secure necessary funding to administer the program. After all, administrative expenses come from the Social Security Trust Fund, paid for by workers and employers. There needs to be a mechanism in place so that SSA's administrative funding is predictable year over year, especially at the time when 10,000 Americans turn 65 each year.

Further, Congress needs to strengthen the Social Security system by passing legislation, such as Ranking Member Larson's soon to be introduced Social Security 2100 Act, that, among other critical items:

- Increases Social Security benefits;
- Extends the solvency of the Social Security Trust Fund;
- Provides assistance to caregivers;
- Repeals the Windfall Elimination Provision (WEP) and the Government Pension Offset (GPO).

We believe the practical and fair way to accomplish this is to lift the cap on Social Security payroll taxes above the current $160,200 and require wealthy Americans to pay their fair share of taxes into the system. Certainly, a person earning a middle class income in America ends up paying a much higher percentage of their income into the system than a wealthy person does. That said, we believe it is evident that lifting the payroll cap would also return increased fairness to the program itself.

I have seen examples for myself firsthand of the need to increase Social Security's benefits. I have observed on many occasions seniors at the supermarket checkout who had to leave food at the checkout line because the grocery bill was more than they had. This has become a family issue because children are increasingly helping their parents because their parents are not financially secure or self sustaining.

Seniors are having to make decisions between food and medicine on a daily basis. These are just a few of the many examples that clearly underline our country's desperate need to expand Social Security benefits.

I think everyone here would agree that the importance of Social Security cannot be overstated. The decline of traditional pension plans and decades of stagnant or declining real wages have made it harder for individuals to save for retirement. Social Security has become a larger part of Americans' retirement income. The U.S. Labor Department's Representative for Pensions and Retirement says that almost two-thirds of retiree beneficiaries' receive 50% or more of their total income from monthly Social Security checks, and one-third of elderly beneficiaries count on Social Security to provide 90% or more of their income.

Moreover, Social Security benefits are insufficient, as evidenced by the average monthly Social Security benefit for a retired worker, which is a modest $1,833. One primary reason for this is because the Social Security cost-of-living adjustment is inadequate and not representative of the true measure of inflation that seniors pay for what they buy. To correct this, the Alliance supports adopting the Consumer Price Index for the Elderly (CPI-E) so that COLAs more accurately measure the spending patterns of seniors.

Another item of critical importance to the Alliance is that of the Windfall Elimination Provision (WEP) and the Government Pension Offset (GPO), which we believe need to be repealed. The WEP affects nearly two million public sector retirees with public pensions, while the GPO reduces by two-thirds the spousal or survivor benefits of nearly 800,000 retirees who collect a public pension. These are outdated provisions that deprive educators and other public employees of the benefits that they have earned and the secure retirement they deserve. Additionally, eliminating the WEP and GPO would also serve as a tremendous financial boost not only to seniors but for the United States' economy overall, given that spending by seniors supports tens of millions of jobs and contributes trillions of dollars annually to the nation's economy.

Social Security is also extraordinarily important to the financial security of women. Women, who on average live longer than men, also incur increased financial risk that they may outlive their savings. Moreover, women are slightly less likely to have an employer-provided pension than men, and even those who do have pensions, oftentimes receive smaller amounts than those received by men. Beyond a doubt, women benefit enormously from Social Security's life long benefits and yearly adjustments for increases in inflation.

The program is also integral for Americans with disabilities. The Old-Age, Survivors, and Disability Insurance Trust Fund (OASDI) provides assistance to nearly 9 million disabled workers and their family members. Disability Insurance (DI) provided through Social Security is

the largest government sponsored income support program for Americans who are disabled, as it provides monthly cash benefits to workers who sustain severe, long-term disabilities. Disability Insurance benefits serve as the main or sole source of income for about 80% of program beneficiaries, while approximately one in three does not have any other source of income.

A majority of African American retirees rely on Social Security benefits for 90% or more of their income. Because African Americans oftentimes have lower earnings and less pension coverage than Whites, Social Security benefits become an integral part of their retirement income. The importance of Social Security to African Americans is even more salient given the higher poverty rates for Black Americans, as the program prevents Black Americans from falling into poverty after retirement.

.

Similarly, for the Hispanic population, whose workers are often concentrated in lower-wage jobs that frequently lack pension coverage, Social Security benefits are of critical importance. Statistically, the Hispanic population often experiences high rates of poverty and underemployment, and consequently has less of an ability to save and invest for their retirement, leading many to depend almost exclusively on Social Security for their retirement income.

Alliance members are frustrated that instead of enacting common sense changes that will help older Americans, many members of Congress are pushing drastic changes that threaten Social Security and the benefits that Americans of all ages have earned. These include raising the full retirement age, partially or fully privatizing the program, or creating special commissions or panels to make decisions that adversely affect Social Security and its beneficiaries without the benefit of public input. The Alliance for Retired Americans strongly opposes any and all attempts to reduce Social Security benefits or enact proposals that will lead to the reduction of Social Security benefits. A number of examples of proposals currently under consideration include:

Raising the Retirement Age

One frequently discussed change to Social Security is increasing the age at which beneficiaries can claim the “full” retirement benefits they have earned. The last change was made in 1983 when the 98th Congress voted to raise the full retirement age from 65 to the current age of 67 for people born in 1960 or later. This increase in age has happened over time.

Another increase in the full retirement age to 70 will result in a lifetime benefit cut for all Americans. Proponents of a higher retirement age assert that this is needed because “Americans are living longer.” However, the demographic facts are otherwise. The Centers for Disease Control reported last August that life expectancy in the U.S. declined in both 2020 and 2021. Americans with lower-incomes do not live as long as those with high incomes; in fact, a 2020

Harvard study found that men in the top 10% in household income could expect to live to 88 years old, while those in the bottom 10% could expect to live to just 76.

Moreover, people who work in physically demanding jobs are less able to work until they are 70. Clearly, increasing the full retirement age unfairly reduces lifetime Social Security benefits for those who may need to rely on them the most.

Lastly, there is an unfair racial component inherent in the proposal of raising the retirement age. This is because on average White Americans live longer (an average of 76.4 years in 2021) than Black Americans (70.8 years), largely because of sizable health disparities and historical economic and social racial biases.

Privatizing Social Security

Privatization of the Social Security program would most likely lead to the ownership of large retirement accounts for the wealthy and more profits for Wall Street. Those advocating for privatization justify this idea by claiming that the Social Security program has sunk into a financial crisis that cannot be resolved without entirely dismantling the program and converting it into a system of market based, individual investments. For individual Social Security beneficiaries, private investment accounts would dramatically decrease their financial security in retirement. Unlike defined pension benefits which are guaranteed, investment accounts such as 401(k) accounts and others depend on the stock market and, as we have seen in recent years, can quickly lose value.

Privatization will not provide a financial boost to the Social Security system, but instead destroy the current system by failing to buttress the fundamental solvency of the program. Because private accounts would be financed by taking money out of Social Security, privatization plans would severely harm the financial stability of the Social Security Trust Fund.

Commissions to "Study" Social Security

Commissions to study Social Security have been thinly veiled attempts to create political justifications for fundamental changes and cuts to Social Security's earned benefits.

One concrete legislative proposal for a committee to "study" Social Security's finances which has surfaced in the last few Congresses is the TRUST Act. This proposal would form a committee with the ability to conduct meetings behind closed doors and fast track recommendations to the House and Senate floors. This anti-democratic scheme in all likelihood would lead to substantive benefit cuts.

The Alliance strongly rejects this approach and believes that any changes to Social Security must start from the premise that the benefits the American people have earned are a sacred promise between workers and the government that must be kept intact and expanded for future generations.

Moving Social Security Off-Budget

Another proposal from the Republican Study Committee suggests removing Social Security's "off-budget" status, which protects it from cuts designed to balance the rest of the federal budget. Similar ideas have been raised by Senators Rick Scott and Ron Johnson.

Social Security is a sacred trust between the American people and its government. In exchange for contributions made to the system with every paycheck, Americans are promised guaranteed benefits that will not change as they age.

To treat Social Security like any other government program with unstable levels of funding from year to year would undermine the retirement security for millions.

Adopting a Chained CPI

The 2022 House Republican Blueprint for Americans also called for a so-called Chained CPI, which would be devastating for older Americans who rely on Social Security. It would significantly decrease Social Security benefits for both current and future beneficiaries and inadequately reflect the items older Americans must purchase every month. As previously stated, instead of using a formula such as Chained CPI that would adversely affect Social Security recipients benefits, a CPI-E formula for the elderly should be used.

Legislative Proposals to Enhance and Expand Social Security

In addition to Ranking Member Larson's Social Security expansion bill, there are a number of additional legislative proposals that would not only enhance benefits but also extend the solvency of Social Security. These proposals, which the Alliance has endorsed, expand Social Security benefits for all beneficiaries, require that wealthy Americans pay their fair share, and assist caregivers. These include:

- **The Social Security Expansion Act** (S. 393, H.R. 1046), introduced by Sen. Bernie Sanders (I-VT) and Rep. Jan Schakowsky (D-IL), increases benefits and extends the solvency of Social Security by 75 years by lifting the cap and subjecting all income above $250,000 to the Social Security payroll tax;

- **The Social Security Enhancement and Protection Act** (H.R. 671), introduced by Rep. Gwen Moore (D-WI), augments Social Security's ability to protect vulnerable Americans living in poverty;
- **The Social Security Fairness Act** (H.R. 82, S. 597), introduced by Rep. Garret Graves (R-LA) and Sen. Sherrod Brown (D-OH), repeals the WEP and GPO;
- **The Protect Social Security and Medicare Act** (H.R. 814), by Rep. Mark Pocan (D-WI), raises the vote threshold to pass any legislation that reduces Social Security or Medicare benefits;
- **The Medicare Social Security and Fair Share Act** (S. 1174) by Sen. Sheldon Whitehouse (D-RI), extends the solvency of Social Security and Medicare by 20 years while increasing fairness in the tax system by increasing the share that wealthy taxpayers contribute; and
- **The Social Security Caregivers Act** (S. 1211), introduced by Sen. Chris Murphy (D-CT) and Rep. Brad Schneider (D-IL), allows caregivers to receive a Social Security credit, while providing retirement compensation in the form of credits to individuals who left the workforce to care for loved ones.

The time to strengthen and expand Social Security is now.

I want to once again thank this committee for inviting the Alliance for Retired Americans to participate in today's important hearing and I am available to answer any questions you may have.

Mr. ROACH. These proposals——

Chairman FERGUSON. Mr. Roach, thank you for your testimony. Your time has expired. I look forward to continuing the conversation.

Mr. Brown, you are now recognized for five minutes.

STATEMENT OF JEFFREY BROWN, DEPUTY ASSISTANT INSPECTOR GENERAL, OFFICE OF AUDITS, OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Mr. BROWN. Thank you and good afternoon, Chairman Ferguson, Ranking Member Larson, and members of the subcommittee.

I commend you for holding this important hearing today on the Social Security Administration's role in combating identity fraud.

Social Security touches the lives of every American. About 175 million people work and pay Social Security taxes, and nearly 67 million receive a Social Security benefit each month.

As we heard in earlier testimony, the SSN was originally intended to track earnings, but it has become the de facto national identifier. This has given rise to individuals using other people's SSNs for illegal purposes. And as the chairman said in his opening remarks, the SSN has become the linchpin to identity theft, one of the fastest growing crimes in America, affecting millions each year.

The Office of the Inspector General, or OIG, plays a vital role in combating SSN misuse and identity theft. And throughout our history, SSN misuse has been a priority in our oversight efforts. OIG has established a multi-disciplinary team of professionals that develop and implement innovative approaches to combat identity theft and scams. This is done through audits, criminal investigations, and prosecution, civil enforcement, and public outreach and education. I would like to briefly touch on these approaches.

The OIG's Office of Audit identifies vulnerabilities in SSA's programs and operations that may result in identity theft. Our audits found, among other things, instances where fraudsters improperly used the SSN of older adults and deceased children.

Our audit work also examined potential vulnerabilities in the Internet services that SSA offers. Since the COVID–19 pandemic, users rely heavily on e-services, increasing the need for our oversight. We found that bad actors exploited some of NSA's public-facing systems to potentially commit identity fraud. These instances underscore the need for SSA to thoroughly evaluate its systems to—for potential vulnerabilities to ensure users are who they claim to be, and that systems aren't misused.

Many of the cases our Office of Investigations has successfully conducted involve SSN misuse, including synthetic identity theft. As we heard earlier, synthetic identity theft is a unique form of fraud that combines the SSNs of real people with fraudulent information, such as false names and dates of birth, to create new identities. It is one of the most difficult forms of fraud to detect because fraudsters build good credit over time using a fake profile before making fraudulent charges and abandoning the identity.

For example, in one of our joint investigations individuals were charged with using approximately 700 synthetic identities between January 2017 and August 2020 to open bank accounts and credit

cards and to create shell companies. They are alleged to have fraudulently obtained over $20 million from the Payroll Protection Program. The pandemic resulted in criminals finding ways, such as the case I just mentioned, to fraudulently take advantage of the infusion of trillions of dollars in Federal funding.

Identity theft is a common thread running through many investigations related to the misuse of pandemic relief funds. Since the start of the pandemic, OIG has engaged with other law enforcement agencies, and we have been involved in over 150 investigations related to pandemic relief programs, funds, and scams.

For over a decade, the American public has been plagued by scammers impersonating government agencies with the goal of stealing money or personal information, including SSNs. Safeguarding the public from financial fraud and scams is a top priority for the OIG. We hold a National Slam the Scam Day each year. This campaign amplifies our outreach efforts and encourages the public to hang up or ignore suspicious calls or messages. In other words, to slam the scam.

We thank the Members of Congress for helping to educate your constituents to protect themselves from Social Security-related and other government imposter scams.

In conclusion, I want to thank the subcommittee for inviting me here today to highlight OIG's oversight and outreach efforts in combating and preventing misuse of SSNs.

I will be pleased to answer any questions you have.

[The statement of Mr. Brown follows:]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chairman FERGUSON. Thank you, Mr. Brown. We are now pleased to recognize the chairman of the full committee, our colleague from Missouri, Jason Smith.

Mr. Smith, you are now recognized for five minutes for an opening statement. Thank you for joining us today.

Chairman SMITH. Thank you, Chairman Ferguson, Ranking Member Larson. Thank you all for the opportunity to share a few remarks on an important topic that affects every American.

We all know someone who has had to go through the ordeal of identity theft. One of the reasons I wanted to hold this hearing was after learning about, about everything our former colleague, Governor Kristi Noem, had to deal with after Congress publicly disclosed the Social Security numbers of her, her husband, all of her children, and her son-in-law. I asked the governor to share with this committee about her experience, the difficulties since her family's numbers were made available to the public, and what reforms we should consider through our jurisdiction to help families who find themselves in a similar unfortunate circumstance.

I have with me a statement from Governor Noem expressing her appreciation for and interest in the committee holding today's hearing. Governor Noem writes in part, "It is troublesome enough that identity thieves and fraudsters can try to steal our personal information right out from under us. But the government should not be doing fraudsters favors by improperly disclosing these important numbers that provide intimate access to one's identity. Furthermore, government should also be a help and not a hindrance for those whose Social Security numbers have been compromised."

"While disclosing your Social Security number for a legitimate purpose causes millions to take a pause, it is even more alarming when a citizen can't trust their own government to keep their personally identifying information secure. Unfortunately, that is exactly what happened to me and my family when Congress exposed the Social Security numbers of me, as well as that of my husband, my three children, and son-in-law to the entire world."

Governor Noem goes on to describe how the disclosure occurred, and how she found out. "In December of 2020 my family and I provided our Social Security numbers to the White House as part of an official visit in my capacity as governor of South Dakota. However, these records went unredacted to the National Archives, and were provided to the United States Congress. They were then needlessly and carelessly published, again without redaction, for all those on the Internet."

"Unbelievable as that is, of equal concern I learned of the public disclosure of our private information through reports in the media. That is outrageous. It wasn't a call from the Social Security Administration or from any of the governmental bodies who published our personal information for millions to see. Failing at each turn to safeguard the personal information entrusted to it, instead, I learned from the media and reporters who reached out about the disclosure."

In her statement Governor Noem also highlights the financial fallout from this experience that has already occurred, and the burden on her family going forward. She writes, "My family has already had to spend time and money to protect ourselves from the

government's careless disclosure of our personal information. And already, bad actors have tried to use that information to their advantage. It may be years before we experience the full impact of this disclosure. But for the foreseeable future, we must closely monitor every financial transaction we see, realizing there may be ones out there we never see."

"Congress needs to take steps to not only better protect the Social Security numbers of American citizens, but for those who do have their numbers compromised, at a minimum, make sure they are made aware of such a disclosure."

"Additionally, we must cut the bureaucracy and red tape one must go through when trying to navigate the cumbersome and difficult situation of replacing their own or their child's Social Security number, once it is compromised."

I ask unanimous consent to insert the governor's entire statement into the record.

Chairman FERGUSON. Without objection, so ordered.

[The information follows:]

Governor Kristi Noem
State of South Dakota
May 24, 2023

Statement on Social Security Identity Theft

I appreciate the Committee on Ways and Means holding a hearing on the need for the Social Security Administration and Congress to do more to protect Americans from the harm of identity fraud as a result of the improper use or disclosure of the Social Security numbers of American citizens. It is troublesome enough that identity thieves and fraudsters can try to steal our personal information right out from under us, but the government should not be doing fraudsters favors by improperly disclosing these important numbers that provide intimate access to one's identity. Furthermore, government should also be a help and not a hindrance for those whose Social Security numbers have been compromised.

While disclosing your Social Security number for legitimate purpose causes millions to take a pause, it is even more alarming when a citizen can't trust their own government to keep their personally identifying information secure. Unfortunately, that is exactly what happened to me and my family when Congress exposed the Social Security numbers of me, as well as that of my husband, my three children, and son-in-law to the entire world. That is simply unconscionable. We must hold the government responsible to prevent such irresponsible disclosures from occurring, and to reduce the harm to those whose information has been compromised when it fails to meet that trust.

In January of 2023, I learned, along with approximately 2,000 other individuals, that the Social Security numbers of my family had been disclosed in a report produced by the U.S. House of Representatives. In December of 2020, my family and I provided our Social Security numbers to the White House as part of an official visit in my capacity as Governor. Somehow, these records went unredacted to the National Archives and were provided to the United States Congress. They were then needlessly and carelessly published, again without redaction, for all to see on the internet.

Unbelievable as that is, of equal concern, I learned of the public disclosure of our private information through reports in the media. That is outrageous. It wasn't a call from the Social Security Administration or from any of the governmental bodies who published our personal information for millions to see, failing at each turn to safeguard the personal information entrusted to it. Instead, I learned from the media and reporters who reached out about the disclosure. Is nobody in the federal government responsible to inform American citizens when the actions of their own government make them more vulnerable to identity theft and fraud?

My family has already had to spend time and money to protect ourselves from the government's careless disclosure of our personal information, and already bad actors have tried to use that information to their advantage. It may be years before we experience the full impact of this disclosure, but for the foreseeable future, we must closely monitor every financial transaction we see, realizing there may be ones out there we never see. Congress needs to take steps to not only better protect the Social Security numbers of American citizens, but for those who do have their numbers compromised, at a minimum, make sure they are made aware of such a disclosure. Additionally, we must cut the bureaucracy and red tape one must go through when trying to navigate the cumbersome and difficult situation of replacing their own or their child's Social Security number once it is compromised.

Americans are right to be wary of their government. Time and again federal agencies have failed their stated mission or failed to protect those they are meant to serve. I look forward to working with the Committee to try and restore that trust and faith which has been lost.

Chairman SMITH. Thank you, Mr. Chairman. And I yield back.

Chairman FERGUSON. Thank you. Thank you again to the witnesses for your testimony. We will now begin with the question-and-answer session, and I will begin.

Ms. Hayward, thank you again for being here today, and thank you for sharing your story. You touched in your testimony about the difficulties that you experienced in trying to solve this problem. Tell us a little bit how a single point of contact would have been—would have made this easier for you.

Ms. HAYWARD. A single point of contact would allow a certain amount of consistency, obviously. That would have been so helpful. I wouldn't have been jockeying around and starting from scratch every time I was interacting with a representative or a person, an employee in the office. And having one person who could follow up with me and make sure that I was doing what I should be doing, make sure that, you know, there wasn't anything that could be done to, you know, move things more quickly. Because as we have learned through the testimony today, you know, it sounds like the time that you don't know your number is time that you can't be protecting your child, in my case.

Chairman FERGUSON. Okay, thank you. This is a follow-up question. You have obviously spent a lot of time on this. Personal resources that you and your family have had to expend on this. What do you think that cost is?

Ms. HAYWARD. It is impossible to quantify the amount of time that we have spent, the worry, freezing her credit, trying to navigate all of the different elements between the Social Security Administration, FTC resources, the three non-government credit bureaus. And that is to say nothing of our actual experience just trying to acquire her replacement card. We have had to squeeze this in between school pickups, doctor's appointments, hospitalizations, and woken up in the middle of the night occasionally worrying about this.

And this isn't going to go away either after this hearing. It will continue to be with us unless our daughter is able to get a new Social Security number.

Chairman FERGUSON. Thank you.

Mr. Brune, if—when someone like Ms. Hayward has a problem like this, what do you think the cost of that is to the agency in terms of a dollar amount to help solve this problem? I mean, what kind of resources does it take?

Mr. BRUNE. Chairman Ferguson, in our field offices and on our 800 number, we strive to provide courteous and empathetic professional service to each person who visits or calls. Each contact is handled with great care, according to our policy——

Chairman FERGUSON. I understand. I am looking for a number here. Does it cost—do you think it costs $1,000, $10,000, $20,000——

Mr. BRUNE. I——

Chairman FERGUSON [continuing]. In agency resources to address the problem?

Mr. BRUNE. Well, you know, I am an IT guy, not the CFO.

Chairman FERGUSON. All right. Well, I will tell you what, why don't we go to Mr. Brown?

Do you have a rough idea of the costs associated with resolving—an average cost of resolving a particular case?

Mr. BROWN. Mr. Chairman, I don't have that information.

The agency does have costs associated with its——

[Audio malfunction.]

Chairman FERGUSON. Okay, thank you.

Ms. Wechsler, the Social Security Administration, as you noted in your testimony, it will be updating its fee structure on the ECBSV service. I think you mentioned that you have got concerns about how this would, you know, would impact usage. Can you dive into that just a little further, and tell us what you anticipate?

Ms. WECHSLER. Thank you for the question. I would be happy to.

We do think this new tier structure is going to discourage use from both the current users and possible users that aren't quite using the system. I want to give one example to help quantify this.

So, one user that initially was expected to pay $276,500 is about to be expected to pay $6.25 million for the same service. That is 22-fold increase over just 2 years. That discourages use. There is no way about that it does not discourage use. That is like Netflix saying your $15 a month subscription is going up to $330. So, our concerns is this tight timeframe for them to recover their cost is creating a vicious cycle. It would be less users, and then the cost would have to increase again.

So, we want to work with SSA and Congress to make sure that does not happen because that is in no one's interest.

Chairman FERGUSON. Mr. Brune, it is my understanding that the Administration did not conduct an analysis of how increasing the fees on the system would affect utilization. So how did you determine the initial fee structure, and what considerations have been made for the subsequent fee structures?

Mr. BRUNE. Thank you for the question, Chairman Ferguson.

The fee structure is based on input from the coalition and industry partners who use the service, and their expected volume of verifications, as well as guided by the statute that authorized the program, ECBSV, and appropriations law, which requires us to collect our costs for building and operating the system within a specific period of time.

Chairman FERGUSON. It seems like Ms. Wechsler has an excellent point, that if you increase fees so rapidly, that it is going to discourage use. Was that not taken into account when this new fee structure was put in place?

Mr. BRUNE. We have had extensive conversations and ongoing discussion with the coalition Ms. Wechsler represents. And our intent is to incentivize usage, thereby increasing the, you know, number of verifications and generating more fees.

Chairman FERGUSON. Well, I——

Mr. BRUNE. We are open to further discussion with you about ways to resolve this challenge, and we do want to make it an efficient and effective service.

Chairman FERGUSON. Okay. Thank you.

Mr. Brown, obviously, Social Security number fraud and theft is a real problem, and it has been done for, basically, the same way for a number of years now. A real threat on the horizon is artificial

intelligence. Have you been able—has your office been able to look at criminal activity around artificial intelligence?

And also, do you think that your office and the Administration is prepared to address theft via artificial intelligence in the future?

Mr. BROWN. Thank you, Mr. Chairman. That is absolutely a rapidly evolving technology that I think we are all trying to keep up with. And I think it is important for the agency and for the OIG to monitor this very closely.

Artificial intelligence has, I think, the opportunity for tremendous benefit to the agency in helping to process claims and handle its workloads. But there is also considerable risk if it gets in the hands of bad actors, risks that we can't even contemplate at this point.

There has been an incident a few years ago where it did appear that artificial intelligence was calling the Social Security Administration to try to process direct deposit changes on behalf of Social Security beneficiaries. And we worked with the agency to alert its employees of this scam.

But like I said, it is a rapidly evolving technology, and we need to keep tabs on this very closely.

Chairman FERGUSON. Thank you. I now recognize the ranking member, Mr. Larson.

You are recognized for five minutes.

Mr. LARSON. Well, thank you, Mr. Chairman, and I want to thank all of our witnesses also. And I am sorry the chairman had to leave, but I completely concur with him that there is—that is a travesty, what happened to Governor Noem, and we should be doing everything to make sure that sensitive data like that is always redacted. And that is a shame.

I also want to thank the witnesses, especially Ms. Hayward.

You are a model for what an American citizen should be in terms of impacting your family directly, and then seeking a resolution, and then making sure that you are speaking out for the, as you indicated, the many mothers who perhaps aren't in the same situation like you and have taken the time and care—or have that time and care to do that.

Mr. Brune, how is it that her situation cannot be resolved more timely, and given the individual the security and the notion that this is being looked into?

Mr. BRUNE. Congressman Larson, we regret the stress and confusion that was caused to Ms. Hayward. We do strive to provide timely answers. We are glad that the replacement for the SSN card was, in fact, issued after her field office visit, and we would be happy to work with Ms. Hayward to identify if there are any other ways that we might improve our service.

Mr. LARSON. Well, it seems to me like—and I know that there is difficulty in getting a new card, but her testimony seemed to indicate that she is not going to feel secure until they have been issued a new card. How long should that take?

Mr. BRUNE. In the state of Pennsylvania, where Ms. Hayward lives, I believe three weeks for the issuance of the card is still the case. Once it processes through our——

Mr. LARSON. Well, could we charge you to be personally responsible to make sure that this matter gets looked into?

And listen, as I said in my opening statement—and everybody should know this, as well, and I think Mr. Brown brought it up when you asked him the question, Mr. Chairman—there are costs associated with all this, aren't there?

And has the Social Security Administration been funded appropriately?

Mr. BROWN. We have not done audit work to look at whether SSA has been funded appropriately.

Mr. LARSON. And to make this technological—and the chairman is completely right, too, about artificial intelligence. After all the hearings that we have had on this and the capability that exists out there, we better get prepared really quick to deal with this. And that is not going to be something that we say we can reshuffle the agency and they are going to be able to do this on their own. That is simply isn't going to happen.

And most importantly, when we are talking about all of this—and Ms. Wechsler, you brought it up, and I am empathetic to your concerns, but you too said—what is the cost, $38 million I think you referenced?

You know, again, the agency has got to be able, again, to deal with the—Mr. Roach pointed out—the 10,000 Baby Boomers a day become eligible for Social Security—a day. That is 3,650,000 a year. So, it will be over 70,000 Social Security recipients within a couple of years. So, we are going to need to have to fund Social Security. We are not going to be able to solve this problem by cutting Social Security, and cutting benefits, and cutting the agencies so that they can deal with this problem.

And in fact, Mr. Chairman, I think we should look into, especially as it relates to artificial intelligence, what we have to do, because we may have to take that as a whole separate entity. But noting that this is the number-one insurance program for the country, and along with Medicare and the military budget account for 70 percent of our overall budget, this is an area where I believe that we can work in a bipartisan manner to solve this problem so no mother—and, hopefully, because of your efforts, Ms. Hayward—that no other mother has to go through this process.

But we have to make sure that we are providing the funding that is needed, and further investigate technologically, along with the humanization of our agencies as to how we can best operate.

Chairman FERGUSON. Thank you, Mr. Larson, and I do look forward to bipartisan conversations related to this. Next we will call on Mr. Carey.

You are recognized for five minutes.

Mr. CAREY. Thank you, Mr. Chairman. I want to thank all the witnesses for participating in this very important conversation regarding the role of Social Security Administration in combating identity fraud.

As many of our panelists have mentioned, Social Security numbers have become a common identifier for a range of purposes beyond what was intended to—to tracking income and Social Security benefits. Unfortunately, the frequent use of the Social Security numbers has exposed Americans to fraud, identity theft, which in turn causes unsuspecting Americans to become victims of fraud each year.

While the financial loss is often borne by the financial institution, the owners of those stolen Social Security numbers are true victims. There was a study done—and we were talking about—Ms. Hayward mentioned unmeasurable and how—in terms of how much it costs you. On average, we have seen an estimate that 1 in 50 children were victims of identity fraud. The average cost to the family trying to resolve that issue is $372 in expenses. So, I just thought I would throw those numbers out.

Recently, a constituent of mine back in my district had her bank account hacked and her identity stolen. The constituent's Social Security benefits were also stolen. And now the fraudster, believe this or not, has continually contacted SSA to try to get additional information. Now, my team back in the district is working hard to potentially get the constituent back their stolen benefits. However, we need to prevent this from ever occurring again.

As my dear friend from Georgia brought up in his opening testimony, in 2021 an estimated 1.25 million children were victims of that identity fraud. As the users of Social Security numbers, the SSA is in a unique position to help combat theft and the misuse of the Social Security numbers.

As Ms. Wechsler mentioned in her testimony, to combat identity theft Congress directed the SSA to establish an Electronic Consent-Based Verification System so no financial institution can match a consenting—so no financial institution can match a consenting consumer's information with the Social Security numbers to verify their identity.

Quickly, I am running short on time, Mr. Brune, why is the SSN adhering so closely to a short timeframe to recoup the costs of implementing the ECBSV?

Mr. BRUNE. The appropriations law requires us to recoup all our costs and sets a designated timeframe for doing so.

Mr. CAREY. Okay, so what plan does the SSA have in place to mitigate the risks of loss to the trust funds if the SSA fails to recoup the development and the operational costs of the ECBSV?

Mr. BRUNE. Congressman Carey, as I mentioned in my prior response, we are committed to making sure ECBSV continues to be an efficient and effective operating tool to combat identity theft.

We have ongoing conversations with the coalition Ms. Wechsler represents to understand impediments to usage, and to try to address them, with your assistance.

Mr. CAREY. Okay, so how many data exchange agreements does the SFA—or SSA have with other Federal and state agencies?

Mr. BRUNE. In total, as I stated in my statement, we have approximately 3,500 agreements and verifications where we verify SSN numbers and data associated with the SSN.

Mr. CAREY. Okay. I got a lot of remarks, but let me just ask a simple question. If Ms. Hayward was worried—and she says she has to worry about it, and I believe it, I have got a 17-month-old, so I get it—is it possible that that card was lost in the mail, right? Is it possible—I mean, your daughter is how old?

Ms. HAYWARD. Nine months.

Mr. CAREY. Nine months. Is it impossible to get a new Social Security number, instead of just a card, so we don't have to worry

about—she doesn't have to do the monitoring like I have to do because my military records were breached?

I mean, is that something that we can do?

Mr. BRUNE. Our policy does allow for that. And we would—you know, according to our policy, we would look at what options were available to, in this case, the young Miss Hayward.

And it is not a panacea to issue a new number. Right as soon as they are issued——

Mr. CAREY. But, I mean, if the kid is nine months old, I mean, wouldn't it be better to do that than all of a sudden, 12 years from now, all of a sudden, we have got to go back and we found out they have got a yacht booked off of—or booked in Boca Raton someplace?

Mr. BRUNE. We would be happy to look into that for Ms. Hayward.

Mr. CAREY. All right. Thank you, Mr. Chairman. I yield back.

Chairman FERGUSON. Thank you.

The gentleman from New Jersey, Mr. Pascrell, you are now recognized for five minutes, sir.

Mr. PASCRELL. Thank you, Mr. Chairman. Mr. Chairman, every member of this committee that I have listened to for a few years, and new folks, support efforts by the Social Security Administration. I have heard nothing different; I don't know, maybe you have to secure Social Security numbers and combat misuse and scammers. I have never heard somebody stand up and support that. You haven't, either.

But I want to highlight how Social Security is America's greatest achievement. We cannot let this hearing distract us. Some folks on your side have manufactured the crisis that threatens to blow up America's entire economy. If we breached the debt limit, we will not be talking about one or two or three or thousands of frauds. Over and over, there are those in the Congress threatening to gut Social Security. I didn't read that incorrectly, and I didn't hear that incorrectly, nor did you.

Some House members want to force Americans to retire later, work through illness, and make financial stability harder. As significant as this hearing is, you know it. You know this stuff already. We should be doing everything we can day in and day out to preserve Social Security.

I mean, you talk about making public names. Look what they did to that poor woman 14 years ago, 14 years ago. What are we talking about it now for? Well, because it is either got to be for everybody or nobody. And the Lerner investigation, 14 Democrats made to be axe murderers. And then no movements were made against them. They were innocent people. All—may be funny to you, but it is not funny to me. I just want you to know that. Fourteen of us were investigated by the same folks you want to investigate. And you are right in doing it. But what is good for one should be good for all.

So, I want to ask Mr. Roach a question, if I may. My staff recently met with the AFGE, the union representing frontline workers at Social Security. They shared the anguish and stress of being unable to help callers quickly with the existing staffing levels, just like we heard from the IRS. House Members' default on America

act would double down by slashing customer service funding. The Republicans' plan would cut customer service staff, clear and simple.

How would further cuts to Social Security Administration, Mr. Roach——

Mr. ROACH. Well——

Mr. PASCRELL [continuing]. Have a budget impact, because you have been here a little while, you know what is going on.

Mr. ROACH. Yes, the services that have been drastically cut already—further services would be cut. People trying to get disability would have to—a much longer waiting period. And, you know, offices have been closed, and people were unable to get in touch with the Social Security office to get things done. It would be dramatic. It would be drastic for further cuts in the Social Security Administration.

Mr. PASCRELL. By the way, Mr. Roach, if we have a default—and God forbid we have one—will—the members that exist in your department, will they be able to assist beneficiaries in the event of a default?

Mr. ROACH. I don't think there would be any place to hide. But I think that if there is a default, retirees will take the first brunt of it.

Mr. PASCRELL. Mr. Roach, the study committee from the other side, God bless them, their budget plan lengthens the Medicare waiting period from two years to five years. This denies severely disabled Americans. There are a lot of those folks out there, Mr. Roach, I don't have to tell you. You could tell me better. But for three years. What the heck is that going to mean for those people waiting for Medicare okays?

Mr. ROACH. It means that no one with disabilities severe enough to qualify for Social Security Disability Insurance should be without health insurance, period. It shouldn't happen. Two years is already two years too long to wait. So clearly, adding three more years for anyone waiting for urgently-needed health benefits is cruel, unacceptable in a country as wealthy as ours.

Mr. PASCRELL. And there is a two-year wait for getting disability benefits, correct?

Chairman FERGUSON. The gentleman's time——

Mr. PASCRELL. I am in the middle of the question. Can I finish it, please?

Chairman FERGUSON. Very quickly, my friend. Very quickly.

Mr. PASCRELL. I finished the question.

Chairman FERGUSON. Okay.

Mr. PASCRELL. The question. What does those three years' weight mean?

Mr. ROACH. It means that people will be—it means—three additional years for anyone waiting for urgently-needed health benefits, that would mean that would be cruel and unacceptable in the country, as other people would be out of their benefits for five years.

Mr. PASCRELL. Thank you, Mr. Roach.

Mr. Chairman, I want to thank you for putting this together today on this critical issue. We are all against fraud, though.

Chairman FERGUSON. Absolutely.

Mr. PASCRELL. Thank you.

Chairman FERGUSON. And the good news is we are all against it, and we are all here to help solve the problem. With that, the gentleman from Utah, Mr. Moore, is recognized for five minutes.

Mr. MOORE of Utah. Thank you, Mr. Chairman, and to all of our witnesses today, thank you for being here to discuss this really important opportunity to help protect our communities from fraud and theft. And we want to focus on this. These are important aspects of this subcommittee to be able to address this. And if we can, you know, talk about these issues, we can help avoid more tough things like the Hayward family had to go through. So, again, thank you for your testimonies.

Ms. Wechsler, the Social Security Administration is hoping to recover the costs of the ECBSV within just three years by raising rates on users. You know, there is always externalities to this type of stuff and other intended consequences—unintended consequences. For the users who do continue to use the system, how will these costs be passed along to consumers?

Ms. WECHSLER. Congressman, thank you for the question. I agree, as far as the cost of fraud is felt by everyone that uses financial products or services. And that is why we are here today, is to try to solve that problem and make those costs not be as significant as they are. And the best way we can do that is to extend the timeframe for ECBSV to recover that—or for SSA to recover the costs, and to make it as efficient and effective as possible and talk about, you know, other ways that ECBSV could be used, and then—and, you know, really bringing some predictability and sanity to the fee structure.

Mr. MOORE of Utah. Awesome. And continuing on with that, if more entities were permitted to use ECBSV and the base of users contributing user fees were broadened, this would alleviate some of the financing issues that we are seeing with the program.

However, the question is whether it is appropriate to expand the number of entities permitted to use ECBSV. Do you think there are legitimate uses for entities in different industries—telecommunications, health care, you name it—to use this program?

Ms. WECHSLER. I am so glad you are raising this point, Congressman. Yes, absolutely.

Our world is increasingly digital, and most sectors of the economy beyond financial services, they have a need to verify that a consumer is providing accurate identity information and is not trying to run a scam. So I think telecom providers is a great example of potential users of this system. Utility companies, residential landlords, others in the private sector. And maybe there is other ways for state and Federal Government agencies to be using the system. ECBSV put in a lot of resources for the system, and we think there is really strong reasons for expanding the use.

Mr. MOORE of Utah. Thank you.

Ms. Hayward, I have an 18–month-old at home too, and so I can only imagine having—with all the other you have to deal with, dealing with what you have done. It is an incredible story, and I am glad you are working through it, and I appreciate you being here today.

Identity theft is one of the fastest-growing crimes in America. Shockingly, one million kids are victims of identity theft every

year. Following our difficult experience—your difficult experience addressing the issue for your child, in your opinion, what is one change that could be made to the Social Security Administration to improve customer service for individuals, you know, trying to address identity theft?

You have talked a little bit about having a point person and things like that. And candidly, I ask the question because, like, this is something that we need to make sure we are doing across the board in our government agencies. And we talk a lot about the IRS, our congressional offices are working closely with our constituents to help them to liaise on this. We have been a big—you know, Republicans and Democrats have been a supporter of increasing the technology that they need to sort of get into the 21st century in a lot of cases. Is there things like that that you are thinking of that you wanted to add to your testimony about ways to improve?

Ms. HAYWARD. For us, the best way to improve would be to have a new Social Security number for our daughter. The ability to do that would really alleviate a lot of our time and effort in this area. And from that, you know, the singular point of contact, someone who could knowledgeably provide us with the most up-to-date information as things change over time, would be immensely calming and helpful for a family in our situation.

Mr. MOORE of Utah. Awesome. Thank you.

Mr. Brown, final question. You mentioned that Social Security Administration's OIG is working to find ways to defend against identity theft empowered by AI. Can you expand on the threats that are growing as a result of this?

Mr. BROWN. Congressman, as I mentioned briefly earlier, there was an incident a few years ago that alarmed, I think, the agency and the OIG of what appeared to be AI making automated phone calls to the 800 number to redirect beneficiaries' direct deposits. Since then, we are seeing this technology evolve very rapidly, including just in the last few months, as we have seen in the media. We are playing catch-up here. I think a lot of organizations are.

So, as I said earlier, it is something that we need to really get in front of as best we can.

Mr. MOORE of Utah. Awesome, thank you.

Thank you, Chairman.

Chairman FERGUSON. Before I recognize the next member, the ranking member has requested a point of personal privilege.

You are recognized.

Mr. LARSON. Thank you, Mr. Chairman. As I looked out into the audience, I was pleased to see a dear person who I think, in the minds of many of us up here, will get a direct shot to heaven at some point. But we have been joined today by Elsie Pascrell, as well, who is Bill Pascrell's beloved wife, and someone we admire and deeply respect.

Thank you for joining us, Elsie.

Chairman FERGUSON. Welcome, and thank you for being here.

Next, we will recognize the gentleman from Florida, Mr. Steube.

Mr. STEUBE. Thank you, Mr. Chairman.

The employer correction request notices, or the no-match letters, are letters that were sent from the Social Security Administration to notify employers when their employees' Social Security numbers

did not match government records. It was established during the Clinton Administration, and in the first few years approximately 1.7 million workers responded to no-match letters and had their missing wages reinstated, which is a good thing.

No-match letters were ended by the Obama Administration one week after the DACA program begun, which initially required applicants to disclose any Social Security numbers they would have used, essentially admitting to a felony in writing. The Trump Administration resumed the practice, sending out 1.6 million letters. Though there was a pause during the early part of the pandemic, these letters included a new attachment on instructions on how to register for and use business services online to view Social Security number mismatches.

The Biden Administration discontinued the practice again in April of 2021. Not every no-match letter means that there is fraud. When a woman changes her maiden name, for example, and doesn't notify the Social Security Administration is an example. If someone is unaware of a mismatch and has no opportunity to correct the errors, they would receive no Social Security benefits on account of the reported wages. Again, the Biden Administration discontinued this practice, but appears to be relying on the business services online.

The website says, "We have discontinued mailing EDCOR letters effective April 2021. We will continue to modernize our systems to make it easier for you to do business with us."

Mr. Brune, the website says "continue to modernize." What gaps are still in the business service online system, and how accurate is this new system in detecting both fraud and accidental errors?

Mr. BRUNE. Congressman, thank you for your question. The accurate collection of wage reports from employers is vital to our program. We work closely with the employer community, as well as payroll providers to continuously improve our electronic wage reporting.

Our free business services online system includes multiple tools for employers to reduce instances of no-matches before, during, and after they submit wage reports. So instead of a letter after the fact in real time, we are communicating with them after they have registered and, you know, authenticated properly. We are sharing with them as quickly as possible where they have inaccuracies that need to be corrected.

Mr. STEUBE. Would you be able to provide the committee with statistics on the effectiveness of the program?

Mr. BRUNE. We would be happy to get back to you for the record, yes.

Mr. STEUBE. Okay. And what impact has this specifically had on illegal immigration employment?

Mr. BRUNE. Well, wage reporting is one of the mechanisms, but that is pretty much after the fact.

We also support the Department of Homeland Security on E–Verify, and that allows a verification up front at the time of request for employment.

Mr. STEUBE. So, with the no-match letters—with the end of no-match letters, is the Social Security Administration being proactive in contacting American citizens when there are no-matches? Or is

the expectation that the citizens must be proactive in reaching out to you?

Mr. BRUNE. Well, as I said, we work closely with the employer and the payroll provider community, and they are responsible for communicating with their employee when a no-match occurs, if that is appropriate.

Mr. STEUBE. Okay. Is there any value in continuing the use of the no-match letters in addition to the business services online, especially for senior citizens who don't rely on technology?

Mr. BRUNE. We think the tools available in the business services online, which are largely used by the business and employer community, are effective because of their timeliness, how quickly they provide a match or a no-match, and that allows more immediate action to address the situation.

Mr. STEUBE. So, in the minute that I have left, how can we improve the Social Security Administration's collaboration with state authorities to ensure that they have the necessary technology to protect against data breaches?

Mr. BRUNE. We have many data exchanges with state authorities, and continually work to provide verifications that support accuracy of federally administered programs.

Mr. STEUBE. So what tools are lacking, in your opinion, from SSA currently to protect American citizens?

Is there things that Congress can do to ensure the protection of identity fraud and their Social Security number being fraudulently used that we—that currently isn't available?

Mr. BRUNE. Well, Congressman, as you noted in your questions—and Mr. Brown has indicated—technology evolves rapidly. Responding to those evolutions in technology requires continued focus on updating of our system and policies and procedures. Those updates, you know, obviously, require funding to be implemented.

I think that our verifications are robust. They cover not only Federal use of the SSN, but we have extensive partnerships with state and local entities as well as the business community that—and the payroll provider community.

Mr. STEUBE. My time is expired. Thank you, Mr. Chairman.

Chairman FERGUSON. Thank you. Next the gentlelady from California, Ms. Sanchez.

You are now recognized for five minutes.

Ms. SANCHEZ. Thank you, Mr. Chairman and Ranking Member Larson.

Today's hearing revolves around the Social Security Administration's role in combating identity theft and what fixes can be implemented to protect people from identity theft, which is a serious and an important topic. And I don't think anybody on this subcommittee will disagree with how serious this issue is, or how seriously we take our role as Members of Congress in finding a bipartisan solution to combat identity theft. And the witnesses today have provided some helpful suggestions on the steps that we could potentially take in order to combat this.

But I will note for the record that not one witness has suggested that we cut funding to the Social Security Administration or to the recipients who receive Social Security as a solution to combating

identity theft. I just want to point that out, because we are at risk of seeing massive cuts to the system that would be devastating.

I want to turn my attention a little bit to an issue that is very high on the priority list of seniors in my district. I interact with seniors quite frequently, as often as I can. And while identity theft is an important issue, the issue that they most often raise for me is improving the cost-of-living adjustment formula to better reflect inflation so that they can actually make ends meet.

Sadly, many of my Republican colleagues don't want to do that. Instead, the Republican Study Committee's most recent budget plan would cut the annual cost of living adjustments by using the Chained Consumer Price Index, which would result in a lower annual cost of living adjustment and less money for seniors to live off of.

Mr. Roach, what would be the impact of a lower cost of living adjustment on retirees who rely on their Social Security?

Mr. ROACH. Well, Social Security, as Ranking Member Larson indicated, hasn't had any improvement in 52 years, and the cost of living adjustment over that period of time has fell way behind the normal cost of living that it takes us to live. So, to slow that and not increase it would be devastating on seniors and, again, seniors and their families who are trying to take care of these seniors. It would be a terrible thing to do. And again, it would be devastating on all our seniors.

Ms. SANCHEZ. Thank you. And Mr. Roach, that same report calls for the privatization of Social Security, diverting worker and employee contributions directly into the stock market. How would privatizing Social Security affect benefits for recipients?

Mr. ROACH. Another terrible idea. It would just enhance, you know, investment bankers and those type of people. Today the stock market is drastically down, and seniors would be hurting. And you can't depend on the stock market to feed your family and to feed yourself. As a result, this organization, the Alliance for Retired Americans, was born out of fighting privatization of Social Security. It is money that is paid into the system, and we expect to get—we demand that we get the money back that we put into the system, and we don't want to put that money at risk.

Ms. SANCHEZ. And if we were to follow the Republican Study Group's guide to privatize Social Security and the government were to default, what would that do to the stock market and to retirees' savings that they are depending on to live off of?

Mr. ROACH. Well, I think that—I think if you look at the data, when I sat down here it was already—because some remarks were made that we may not get there by a public official, and it is already cratering. So, it would be devastating.

Ms. SANCHEZ. Okay.

Mr. ROACH. The stock market, you know, was down. Unless it got up, you know, a little while ago, it was—yesterday and today have been pretty much an example of what would happen if we default. We would—we could just—you know, basically, if we default—let me get real—we could just put up the Chinese flag and, you know, be a third-world country. That is what would happen.

Ms. SANCHEZ. I thank you for your honest and frank opinion.

We know that Social Security is a popular program because Americans know that they can count on it. It is a guaranteed benefit, which you have said, you know, they have earned after a lifetime of hard work and paying into the system. Along with many of my colleagues on this committee, we believe that the program needs to be strengthened for future generations. What are some fixes that Congress could make to the program to address the—to extend the life of the Social Security Trust Fund and increase benefits for recipients?

Mr. ROACH. I think the CPI that we talked about could be more advanced and up to date for the current cost of living. We could increase benefits; we could increase benefits and we can make the program solvent so people aren't worried about it every day. We could fix the many public sector employees that don't have access to Social Security. There is a whole number of things, and I believe the 2100 addresses all those concerns. And I think that is what we could do.

And if you lift the cap of the 160,000, which is the maximum that people pay in, lift that and garner some of the wealthiest people in the country, we would have sufficient funds for Social Security to be self-sufficient. So basically, we are not asking for Congress to appropriate funds that they have to borrow, we are saying we want the funds we—if you lift the cap, use the numbers, it will—the system will pay for itself.

Chairman FERGUSON. Mr. Roach, thank——

Ms. SANCHEZ. Excellent, thank you so much for your testimony, and I yield back.

Chairman FERGUSON. Thank you. Next, I recognize the gentleman from Tennessee, Mr. Kustoff.

Mr. KUSTOFF. Thank you, Mr. Chairman, for calling today's hearing, and thank you to the witnesses for appearing.

Ms. Wechsler, to you, for—as a means of prevention, would you recommend to somebody that they have their credit reports frozen in order to prevent Social Security theft?

Ms. WECHSLER. Well, you know, speaking personally, that is something that we do in my household. And after hearing my fellow panelist's story, I am going to take the process to do it for my young children, as well.

Mr. KUSTOFF. Yes, I—so I want to follow up on that.

Ms. Hayward, after what happened to you, to your daughter, you personally—you had you and your husband's credit reports frozen, right?

Ms. HAYWARD. At this time, we have been focusing our attention on our daughter and our children, and learning more about what we need to do to protect ourselves.

Mr. KUSTOFF. Yes.

Ms. HAYWARD. As you can understand, it is—can be difficult for an independent citizen to know exactly what the best practice would be. And it has ramifications when opening a line of credit or taking out a loan or buying a house. So at this time, you know, we are still trying to figure out what the best course of action would be, and are hoping that we can be provided with the best information to follow.

Mr. KUSTOFF. Fair enough. Thank you.

Ms. Wechsler, back to you. Is there—there is a difference in the process between freezing the credit of an adult versus a minor child, isn't there?

Ms. WECHSLER. That is my understanding, yes.

Mr. KUSTOFF. Okay. And it is more complicated, maybe substantially more complicated, to freeze the credit of a minor child versus an adult.

Ms. WECHSLER. Right. I can tell you, just because I have done a little research on what that looks like. Yes, there is a lot of documents we have to provide, as the parents of the children.

Mr. KUSTOFF. Good, thank you.

If I can, Mr. Brown, as it relates to you and to OIG, can you talk about the scammers who target, I guess, individuals versus groups?

Because there are both, right? There are some that are individuals, there are some that are professional groups.

Mr. BROWN. The scammers are, yes, individuals or groups.

Mr. KUSTOFF. Okay. Can you talk about the different types of groups that conduct the scamming?

Mr. BROWN. I think I can refer to—drawing on that example from a few years ago. The artificial intelligence that was likely backed up by unknown individuals, not likely one individual. And it was difficult to track the perpetrators down because this is all being done electronically through voice-over Internet telephone systems, calls that are being originated from outside the United States.

So, my point here is it is very difficult to identify the perpetrators, whether they are individuals or groups.

Mr. KUSTOFF. And the ones that are coming from outside the U.S., do you know or do you have an opinion where they are coming from?

Mr. BROWN. I will have to get back to you on that. I think our investigative work has tracked some of that down, but I don't have the information readily available.

Mr. KUSTOFF. Thank you. Do you coordinate with different law enforcement agencies?

Mr. BROWN. We do.

Mr. KUSTOFF. Primarily the FBI?

Mr. BROWN. Correct.

Mr. KUSTOFF. Can you think of any prosecutions in the last five years of these scammers?

Mr. BROWN. Unfortunately, my background is in the Office of Audit. The investigative side is not sort of in my portfolio. So, I would be happy to get some more information for you for the record.

Mr. KUSTOFF. Yes, I would appreciate that, if you could, if you could let me know if there have been any prosecutions, because it would seem like—I am a former Federal prosecutor, former U.S. attorney—that, you know, when you have one or X number of successful prosecutions, that it sends a strong deterrence effect to those who think about trying to perpetrate the same or similar crime.

Now, a lot of times they will adapt, and sometimes after the expansion of time they seem to go away. But the more those investigations and the more those prosecutions and the notoriety that

they receive, that—there is no doubt that there is a deterrence effect. So, if you could follow back up with me, I would appreciate it.

Mr. BROWN. Yes, sir.

Mr. KUSTOFF. Thank you, Mr. Chairman, as my time is expiring, I yield back my 10 seconds.

Chairman FERGUSON. Thank you.

Before we go to the next member, the ranking member and I have both commented several times on the artificial intelligence piece. And Mr. Brown or Mr. Brune—Mr. Brown, specifically—you keep going back to the one incident that you have been made aware of, which was a program that was calling in. Are you all doing anything right now to kind of survey where you may be in this process?

I mean, you are aware of one thing, but how much—is there a way to track penetration from AI into the system? I think we are just both kind of, you know, concerned about this. So, you know, it is—are you all doing anything to monitor that, or is it hard to do because you don't know what it is yet?

Mr. BROWN. Hard to do because we don't know what it is yet. Also, hard to track where it is coming from.

So, we are looking at data to try to decipher where this—these potentially fraudulent calls are coming from. But fraudsters have found ways to spoof legitimate phone numbers, redirect calls, so it looks like they are coming from within the United States when they are not. So, they are always, you know, sort of one step ahead of us, and we are trying to catch up here.

Chairman FERGUSON. Okay, thank you. Next, a gentleman from Arizona is recognized for five minutes.

Mr. SCHWEIKERT. Thank you, Mr. Chairman. And to my—I will call him my friend, Ranking Member, he and I both have a fixation on stability and survival of Social Security, though I think we see the actual financing mechanisms very different.

We did some of the math last night on the floor and showed that if you were to stabilize U.S. sovereign debt at 95 to 97 percent—because the real problem is actually more in the Medicare—I need a 24 percent payroll tax tomorrow and a 20 percent VAT tax tomorrow to stabilize U.S. sovereign debt to 97 percent of debt to GDP. That is the CBO math. And so, you can go—if you want to argue, go argue with CBO.

Mr. Chairman, back——

Mr. LARSON. Mr. Chairman——

Mr. SCHWEIKERT. My time—back about two years ago, we actually had a hearing in this room, maybe even three or four years ago—actually, I think you may have been in the chair—and there was part—one of the discussions was is there a way to actually sort of have a revolution on how we both have a—more—as we are using a Social Security number or a national ID number functioning—is what it becomes—for Medicare, Medicaid, Social Security, so many other items, to have a rotating encryption on it.

We actually, I think, at that time had a technology expert come speak to us saying, okay, just like, you know, here is the number, but underneath it is always a token that is rotating, or some sort of ability to—like this. Because my fear is, if I am reading the ma-

terials or even—and I am sorry, I ran back to the office to see if I could find the binder. I couldn't find it from a couple of years ago that had some of the material in it.

Has there been any type of research project, whether it be the Social Security level, you know, the IG, someone saying as technology gets better, as the AI gets better, as the data mining gets better, the fraudsters are going to get better. Is there a way we could build a much more bulletproof token that is also that tax ID?

And you seem to have the most expertise on this. I mean, what would you do?

Ms. WECHSLER. I appreciate the question, Congressman. I am not a technology expert, but I work with them, and we are happy to have these discussions.

I do agree, as far as the strong reliance that our country has on Social Security numbers, and that makes it such an attractive target for fraudsters. And that is, you know, why we have so much focus on the ECBSV program. But we are happy to have more discussions about that.

Mr. SCHWEIKERT. But within that, I think, actually, we had had some testimony in the back that—the amount of fraud that is in our Medicare system, even our Medicaid systems, often using—walking into an emergency room and using someone else's Social Security number and these things. So, this is a much greater scale than I fear we completely have our heads around. And maybe the goal here should be not only identifying the problem, because we seem to do this every couple of years, but are we ready to bring in some true experts?

Is there a way—you know, if I can carry around my bank accounts on this thing, and they are substantially bulletproof, is there a way we could provide that type of protection to the American taxpayers?

And just everyone, because, you know, we all have to live with this number.

And the other thing, how old is the little girl?

Ms. HAYWARD. Our daughter is nine months old.

Mr. SCHWEIKERT. So cute. The insane thing, I have a 10-month-old little boy we just adopted. And so, you are—hearing your story, and I am all of a sudden going, oh, God, we need to check. So, you see what you caused?

But to everyone on the panel—and then I will yield back, Mr. Chairman—if you come across any literature, a discussion of what we could do to actually fix this, you know, I would love us to actually be working on a fix instead of planning for next year's hearing again to do the same thing over.

So with that, I yield back.

Chairman FERGUSON. Thank you. The gentleman from New York, Mr. Higgins, is recognized.

Mr. HIGGINS. Thank you, Mr. Chairman.

You know, it has long been known and long ignored that Social Security has a customer service problem. You know, benefits are not cut, but when the administration is cut, it makes services for our individual constituents, every congressional district, very, very difficult.

Next Friday $25 billion in Social Security benefits are scheduled to be paid out but will not if the nation defaults on its debt.

You know, if there is a problem with fraud and abuse, whether it is an internal source or an external force, you know, the logical extension is that resources, that money is needed to fix that. President Biden proposed budget increases to improve Social Security services, including cutting fraud and theft by nearly $2 billion for a total of $15 billion; 224 million was to protect the program's integrity.

Part of the program's integrity is to ensure that it fulfills its mission in a way that is effective and efficient, because every single week $25 billion in Social Security benefits are paid out. That is $100 billion every single month. These are people that primarily depend on those resources to survive.

Additionally, they are net contributors to the American economy. These people do not save their Social Security payments. They spent a whole life contributing to it so that they could experience a life of dignity.

You know, there is a lot of talk about, you know, debt and deficit, and both parties are responsible, and that is true. What is not talked about as much is that American debt in the form of Treasury bonds, bills, and securities is the greatest, safest investment in the world. When there is a global recession or a national recession, it is called a flight to safety. That is what world markets buy because 60 percent of the world's economy is dependent on the American dollar. The full faith and credit of the United States shall never be questioned. That is the gold standard by which people invest in American debt.

Yes, the debt is a problem, but the way that you deal with that is through economic growth. And anybody that questions whether or not growth can do that, look back to the 1990s, 1992 to the year 2000. Sustained economic growth of four percent every single year for eight years. We did not have budgetary deficits. We had budgetary surpluses of $300 billion. We paid $400 billion down on the national debt. That kind of growth was only made possible by the investment that this Congress made in the American people and the growth of the American economy. And somebody says, well, you have four percent growth, you have an inflation problem. No, you didn't. Inflation was at 2.25 percent for that 8 years.

You know, you can't continue to hold the American people hostage because of a debt situation that you helped create. Seventy percent of American debt is owed to Americans. That is what the Chinese would love. They would love for us to default on our debt. Do you want to know why? Because they want to be the world's lead currency in the end.

The other issue which I still don't understand, but our friends on the other side in the House Ways and Means Committee prioritize who would get paid if we defaulted on our debt, and China was first. Not the American people, not the Social Security program, not the Medicare program.

So, I just simply want to say—and I have heard very clearly your your testimony, it has been very valuable to me in terms of learning a little bit more about this extraordinary program that, by the way, lifted 50 percent of American seniors out of poverty when it

was enacted in 1935. We have a demographics problem. People are living longer. We should be celebrating that. And that is why John Larson's Social Security 2100 Act is so visionary, is so valuable, not only to the American people, but to the American spirit.

I see my time is expired. I will yield back.

Chairman FERGUSON. Thank you, Mr. Higgins. And we all agree that raising the debt ceiling is something that should be done. We cannot default on the debt. And House Republicans have been the only ones in Washington, D.C. to vote to raise the debt limit so far in this discussion.

With that, I will yield to my colleague from Iowa, Mr. Feenstra.

Mr. FEENSTRA. Thank you, Chairman Ferguson. And I also want to thank Ranking Member Larson. Thank you for having this hearing, and it is really important and, you know, collaboratively, all right, I don't care about politics. I care about solutions, how we can work together.

You came here, each one of you came here to give testimony. You came here to discuss this critical issue that we have in front of us. And we need to find a solution together, and I thank you for that.

In Iowa our state has already received more official complaints of identity theft this year than all of 2022, and we are not even 6 months into the year yet. So this is a real concern. And so, Ms. Wechsler, I am just curious. Do you have any idea why we are seeing such an onslaught of identity theft starting already this year, compared to years past?

And by the way, is this nationally or is it more Midwest-driven?

Ms. WECHSLER. Thank you for the question, and I am sympathetic that so many of your constituents are already victims of identity theft this year. We are seeing that nationally in, you know, identity theft, but also specifically synthetic identity theft and fraud. It is the fastest-growing type of financial crime in the U.S., and it is the—and synthetic identity fraud is the largest type of identity theft.

And, you know, it is not just in the credit industry, but it is in other sectors of—you know, with government benefits and unemployment benefits. And we have heard from some of my fellow panelists on that. And that is why, you know, again, it is—ECBSV is such a critical tool for combating synthetic identity fraud. And we have to maximize the use and the effectiveness of this system.

Mr. FEENSTRA. Yes, so I agree. Thank you for those comments. I want to extrapolate on that just a little bit.

So, with AI, what is happening in AI, do you think—I mean, I get worried when you see things doubling so quickly. Do you think AI is the biggest producer of what is happening, you know, phishing attacks and all this other stuff?

I mean, is this something that oh, wow, I mean, we have got problems ahead of us? What is your thoughts?

Ms. WECHSLER. I know data breaches are more and more common.

Mr. FEENSTRA. Yes.

Ms. WECHSLER. And that is certainly an opportunity for Social Security numbers to become vulnerable and then be taken over.

Mr. FEENSTRA. Yes.

Ms. WECHSLER. So, is there other technology that is making that possible? That is very likely.

Mr. FEENSTRA. Yes, yes. So, I sat on the Science, Space, and Technology Committee last year, and I was the ranking member of the Research and Technology Committee. We talked a lot about artificial intelligence and, you know, obviously, it is a safety issue.

Are you working with other agencies—I am just thinking out loud here—like NIST, NSF, DoE, or is there any way that you guys can work collaboratively?

I mean, it just seems like—and I am hoping it is not the case that we are all in little silos trying to do our little—our work. I mean, is there ways that we can work together with some of these that we are all trying to somewhat combat this situation?

Any thoughts there, Ms. Wechsler or anybody else?

Ms. WECHSLER. We are certainly open to collaboration across the public and private sector. That is certainly what we are trying to achieve with ECBSV. And on a larger scale, absolutely.

Mr. FEENSTRA. Yes. And anyone else that you see, hey, I have done—we are doing X, Y, and Z with this different organization?

Mr. BRUNE. Congressman, at the Social Security Administration we are very collaborative with our Federal partners and with the technology community who not only provisions technology to the government, but to—you know, to the nation.

In recent, you know, discussions we have coordinated with multiple executive branch agencies to both learn more about the, you know, emerging technologies and identify positive use cases that help the government mission.

Mr. FEENSTRA. Awesome, glad to hear that. So, we are Congress. I am asking you questions I want to ask you, what can we do? All right? What do you see that Congress can do, Mr. Brune and Ms. Wechsler, all right? If you could say, hey, if you guys could do this, if you men and women could do X, what would that be?

Mr. BRUNE. Well, Congressman, I would say that as technology advances and as threats, as you have identified, change, adequate, sustained funding is an important measure to continue to advance the government's defenses.

Mr. FEENSTRA. Yes, thank you.

Ms. Wechsler——

Ms. WECHSLER. Just the important role you have played in making sure ECBSV was created to begin with, and then ensuring its efficiency and effectiveness.

Mr. FEENSTRA. Perfect. Thank you so much for your testimony, and I yield back.

Chairman FERGUSON. Thank you.

Our dear friend and colleague from Michigan, glad to have you back, sir, and healthy. You are now recognized for five minutes.

Mr. KILDEE. Thank you so much, Mr. Chairman. It is good to be back, I will say, and I have mentioned this a couple of times, I am not 100 percent yet. It still hurts for me to talk, which makes this a completely shared experience. [Laughter.]

Mr. KILDEE. I do want to thank the witnesses for being here, and I do agree with my colleagues, and I am glad this conversation is taking place. The notion that Americans, like Ms. Hayward and others, have to deal with the frightening reality of identity theft is

something that we have to take very seriously, and we have to deploy whatever capacity, whatever technology, whatever policies we can to try to address that. And I am pleased to hear that there are some ideas that we might need to invest in. We need to hold these bad actors accountable.

But we do also have to recognize that everything we do here has some impact on the capacity of the agency to address that. So, I am concerned, as some of my colleagues have expressed, that any steps that we might take that would potentially limit the resources available to the Social Security Administration or any other body of government could have the exact opposite effect of what we are trying to address during this hearing.

According to the acting Social Security commissioner, some of the cuts that could be proposed, for example, in the so-called Limit Save and Grow Act—at least this is according to the acting commissioner—could force the agency to close field offices and lay off, quite literally, thousands of people who go to work every day trying to make the agency's mission more achievable.

You know, I think about this—about, you know, in terms of how it affects the people I represent. Back home in Michigan, two million seniors rely on Social Security. And as Mr. Larson, who has supplied us regularly with data, my particular district is one that has a fairly high number of Social Security recipients, both seniors but also other beneficiaries of Social Security. And I am very concerned that we not talk about steps to address identity fraud and at the same time weaken the ability of the agency itself or the Administration to address this.

So if I could start with Mr. Roach, ask if you might just comment on how the proposed—and I know this is not something that is necessarily shared by all members on the other side of the aisle, but a majority of our Republican colleagues are a member of the Republican Study Committee that put forward these proposals—how this will impact the loss, for example, of field offices, the loss of employees who go to work every day trying to make the Social Security Administration more responsive to those Americans who have paid in?

What will be the impact on our ability not just to deal with this issue of identity fraud, but of all the challenges that come with running a large organization that provides benefits that, for many of the people who are the beneficiaries, is their principal, if not their sole source of income? Mr. Roach, could you just comment on that?

Mr. ROACH. Yes. Well, I know firsthand I had a problem with Social Security. Not—you know, I needed assistance. They had closed my office in Arlington, Virginia. I would have to travel many miles away. The phones weren't being answered in a timely fashion. They would call you back. It would be devastating. Many seniors are confined. They have to communicate and try to get information on various issues that come through. And every year there is a different issue.

So it would be a devastating thing to continue to close—I mean, to continue to do what is already happening. And that, you know, expand those offices and expand the ability to communicate directly with Social Security. As you said, you know, communicating is very

tough. And we cut staff. Nobody is answering the phone. And so, it would be—worsen—exacerbating a bad situation.

Mr. KILDEE. Well, I appreciate that. And I would just add to that by saying that I also think we ought to be careful. And I know, again, this often comes up where some would criticize the people who work in the Social Security Administration or any other agency of government as being bureaucrats and subject to all sorts of, I think, really unfair characterization.

These are people—these are Americans who go to work every day to serve their fellow American citizens. We ought to hold them up. We ought to support them, and especially when we are trying to deal with this really significant threat of identity fraud. Let's not on one hand say that we want to stop that, and on the other hand make it more difficult for the people who go to work every day trying to address these problems, to get their work done.

With that, again, Mr. Chairman, thanks for holding this hearing. I really appreciate it very much, and I appreciate your nice comments at the outset. Thank you.

Chairman FERGUSON. And you will appreciate the fact that I agree that that was not entirely too painful for either of us.

So, with that, the gentleman from Ohio, Dr. Wenstrup, is recognized for five minutes.

Mr. WENSTRUP. Well, I do want to welcome my friend back.

I am glad you are doing well.

And I want to thank you, Chairman Ferguson, Ranking Member Larson, for having this committee and for all of you being here today.

The fraud is a great concern of mine. Child identity theft is a serious problem in our country. I am concerned that maybe the Social Security Administration isn't doing enough to protect our children and grandchildren from having their identity stolen. That is one thing.

But maybe there is more we can do to protect these children, and that is that is where I want to go. Children's identities are valuable to criminals. It is a bonanza for them when they get it. They can go undiscovered for years, until that child is old enough to work, drive, or try to establish credit, and then it comes forward. And when children's Social Security numbers fall in the hands of the wrong person, it sets a stage for a future of financial hardships and problems before a child is even old enough to walk.

I do want to talk about the Social Security Child Protection Act. You know, as made clear by Ms. Hayward's testimony, the Social Security Administration's current policies make it extremely difficult for families who are trying to obtain a new Social Security number after being a victim of a comprised [sic] Social Security number.

I can tell you firsthand, when you adopt not immediately at birth, but say maybe months later, the advice you are given as parents of that child, new parents to that child, is "Get a new Social Security number," because of this very reason. Fortunately, we were given that advice and did just that.

It is just shocking to hear that such a vital piece of a child's identity was compromised before he—before she was only one month old. And fortunately, the story is not unique, apparently, and that

is why we were given the warning. So, I want to make sure that people can address this and have the ability to protect their children from having their identity stolen, and deserve the opportunity to open bank accounts, et cetera.

So that is why last Congress I worked with my colleague, Representative Blumenauer, to introduce the Social Security Child Protection Act. This common-sense bill would allow Social Security Administration to issue a new Social Security number to children aged 14 and under if their Social Security number has been compromised by theft of their Social Security number. So, we are planning on reintroducing this act this week, and I invite all the members here to join in this effort to protect our children and assist their families when their lives have been upended by child identity theft.

The Social Security Administration has a responsibility to provide protection for our children, to prevent what happened to Ms. Hayward and her family from ever happening again. I think we can make a big dent in that if we work together on this.

Ms. Hayward, can you discuss how things may have been different for you and your family if the Social Security Administration would have had the ability to issue your daughter a new Social Security number when you realized it had been compromised?

Ms. HAYWARD. Thank you. Yes. You know, from my understanding, from what I have been told is that we have to wait until there has been some harm incurred. We have to have substantial proof of that harm, which can take months, years, maybe even decades to even learn about.

And so if we had been able to have a new Social Security number given to us, even though we didn't have proof of harm yet, thank goodness, then it would save us and buy us more time to do what we needed to do—apply for a passport, you know, open a 529, that sort of thing—and give us a peace of mind that at least she is working with a clean slate.

Mr. WENSTRUP. Thank you very much.

I yield back, and I hope we can get this act passed. It is bipartisan. Let's work on that and help others out. Thank you, I yield back.

Chairman FERGUSON. Okay. Thank you for reintroducing that. I look forward to working with you to get that across the finish line.

Next, the gentleman from Illinois.

Mr. Davis, you are now recognized for five minutes, sir.

Mr. DAVIS. Thank you, Mr. Chairman, and let me thank you for giving me the opportunity to waive onto this hearing. I am not a member of the Social Security Subcommittee, but I have such a vital interest, and Social Security is so important to the district that I represent that I wanted to make sure that I heard what I could hear, and that I contributed whatever it is that I could contribute.

I am very interested in fraud and in Social Security. But I am really more interested in Social Security than I am in fraud. Both are very important, and we want to eliminate as much of it as we possibly can, not only in terms of individuals attempting to what

we call in the community where I live "pimping the system," and we certainly don't want to see the Social Security system pimped.

But we also want to be careful that we don't eliminate and leave out—I recall how Social Security sort of came into being, and people who were left out. And I am sure that the designers and promoters did not intend, but I grew up in rural America, and many of the people that I grew up with were farmers, they were sharecroppers. And so, they went many years without paying into Social Security. They were not allowed to pay in.

Therefore, as they reached retirement age, or even as they reached the age where they could contribute—and my father was one of those individuals, so I know exactly when they were able to contribute, and I also know exactly what his Social Security check was after he retired. He lived with me, and he was 92 years old.

His check was $536 a month, and he was a very proud individual. And often times, if we went to dinner or whatever, he would attempt to pay. He said, "Oh, let me pay for this.' " He would reach up, and pull out his money and he would always say to my wife, "Vera, I am paying for your dinner. Now, your husband can, you know, do the best he could." [Laughter.]

Mr. DAVIS. But I thought if he only had $536—fortunately, he was okay, he had children that he could live with and all of that, and so he didn't have to worry. So, I think we have to be very careful.

And I am hearing, you know, people wanting to raise, raise, and raise the retirement age. Well, I think we need to be very careful about that, as well. I think one of the reasons that Social Security has been so popular is that people know that they can depend on it. Social Security benefits for many people, of course, is about $20,000 a year. Many of the individuals in my districts about half of that. It is about $20,000. It is about $10,000 for them, and that is what many of them get.

So, I want to make sure that we protect Social Security as much as we can. And I hear this thought, this idea about privatization and privatizing. Well, you know, I think, to me, that is kind of like a gamble. And you never know what the outcome is going to be.

So, Mr. Roach, let me ask you. The idea of privatizing Social Security, how do your members—how do you react to that?

Mr. ROACH. You know, our members will not be satisfied with that. My organization, the Alliance of Retired Americans, was born out of the initial talks to privatize Social Security and put our money at risk. We put the money in and trust to the government Social Security. And we depend on that money coming out. And to put it at risk in stock markets and other financial institution instruments would be devastating mentally and physically to our members and Social Security recipients as a whole.

Mr. DAVIS. And the idea of more of a guarantee because we have been fortunate. We have never missed a payment yet, and people have been able to reap the benefits and have the security of—just about knowing, and they wait for the first of the month.

Mr. ROACH. Absolutely. The guarantee of the Federal Government means it is very comforting to all of our Social Security recipients, the fact that they are not looking at—they have to look at the stock market go up and down.

And, you know, people who are—have money outside of Social Security, they are more vulnerable to fraud and theft because the numbers are all over the place. And it is very difficult to keep track of these things. We are doing some work in that arena. But no, privatization and lack of a guarantee would be devastating to Social Security recipients and potential future Social——

Chairman FERGUSON. Thank you for your comments, Mr. Roach. The gentleman's time has expired.

I would like to thank each of our witnesses for coming today. Your testimony has been helpful. It has caused us to want to explore this area even more, and really be a partner in helping solve this very serious problem for our fellow Americans.

Please be advised that the members have two weeks to submit written questions to be answered later in writing. Those questions and your answers will be made part of the formal hearing record.

With that, this subcommittee stands adjourned.

[Whereupon, at 4:03 p.m., the subcommittee was adjourned.]

MEMBER QUESTIONS FOR THE RECORD

Questions for the Record
Submitted to Sean Brune
Deputy Commissioner for Systems and Chief Information Officer
Social Security Administration

House Committee on Ways and Means, Social Security Subcommittee
"Social Security's Role in Combatting Identity Fraud"
May 24, 2023

Representative Feenstra

1. **Customers of eCBSV have been clear that, given the increased tier-fee schedule, we will likely see lower use of the eCBSV system to prevent fraud. In some cases, the new pricing for industry users published earlier this month will represent a 29x fee increase for customers.**

   Does SSA have the authority to extend the 3-year period to, say, 10 years, which would mitigate the immediate fee increases, and also avoid reducing industry use of the eCBSV program? Or would Congress have to act to authorize this?

   We initially funded the electronic Consent Based Social Security Number Verification (eCBSV) expenses incurred to date from our primary annual account for administrating our programs, the Limitation on Administrative Expenses (LAE) account. Our LAE account is an annual account, meaning it provides one fiscal year to incur obligations. While we cannot incur new obligations beyond that first year, we are allowed to make payments and adjustments to existing obligations for the next five years. 31 U.S.C. § 1553(a). After these 6 years (first year plus 5 additional years), the account must be closed. 31 U.S.C. § 1552(a). Pursuant to section 215(h)(1)(A) of the *Economic Growth, Regulatory Relief, and Consumer Protection Act* (P.L. 115-174, referred to as the "Banking Bill"), when we recover funds from eCBSV users, we can retain those funds without fiscal year limitation and use those funds to relieve obligations against annual LAE accounts that have not closed. However, we cannot use those funds to relieve obligations against closed annual LAE accounts.

   Therefore, once the FY 2020 annual LAE account closes in FY 2025, we will be unable to reimburse the eCBSV obligations charged to the FY 2020 LAE account. If we do not reimburse the LAE, then those LAE funds would have been used for non-mission work. In addition, we would be out of compliance with the Banking Bill's requirement to fully recover all costs for eCBSV.

   Our May 2023 eCBSV Federal Register Notice[1] announced a revised fee structure to recover the remaining costs incurred through FY 2022 over a three-year period (i.e., FYs 2023-25). We implemented this three-year recovery period to stay within the appropriations law limits

[1] SSA, Notice of Fee Increase for Our Electronic Consent Based Social Security Number Verification Service, 88 Fed. Reg. 29959 (May 2023): https://www.federalregister.gov/documents/2023/05/09/2023-09753/notice-of-fee-increase-for-our-electronic-consent-based-social-security-number-verification-service.

discussed above while limiting the amount of time during which LAE funds are used for non-mission work. This timeframe allows for timely reimbursement for the development and initial administration of eCBSV, consistent with the Banking Bill, and helps ensure we have the resources we need to administer our programs.

2. **Your customers of eCBSV have been clear that many of them are seeing limited value from eCBSV in large part because roughly 60% of responses that come back as a "no match" are believed to be legitimate customers who might have entered a nickname instead of their given name, or accidentally transposed two numbers in their date of birth or SSN. We know they have asked that SSA share more details on the "fuzzy logic" it uses to resolve nickname errors, as well as create additional "reason codes" to indicate more about why a submission may have a no- match response (i.e., "name and DOB match, check SSN") which would then help a bank go back to their customer to double check the SSN. To date SSA has not been willing to do either of these things.**

   Is SSA refusing these requests because SSA does not believe it has the authority to do so? Would Congress have to act to authorize this? Or is there some other reason driving these decisions?

   In eCBSV, as in all of our data exchanges, there is a fundamental need to strike a balance between the usability of the system, the accuracy of the match, and the privacy and security of the sensitive public information we hold. We have decades of experience successfully balancing these concerns and are committed to finding opportunities to improve the Social Security Number (SSN) verification services that we offer.

   To that end, all of our data exchanges and verifications – including eCBSV – build in matching tolerances (i.e., "fuzzy logic") to adjust for common issues such as typographical errors. However, we cannot disclose the specifics of these tolerances to any entity, whether private or Federal, because doing so would allow potential wrongdoers to commit fraudulent acts related to identity theft, phishing, and the overall manipulation of the system to obtain information about individuals' sensitive information. Further, because these or similar tolerances are used for many purposes beyond eCBSV, disclosing them for any one system may put others at risk.

   After we apply tolerances, the eCBSV match rate exceeds 90 percent, which is consistent with our other real-time verification services. While we cannot confirm the feedback regarding 60 percent of no-match responses being legitimate customers, we can confirm that some legitimate individuals will not verify because their records are no longer up-to-date because, for example, of an unreported name change due to marriage or divorce. We understand that inaccurate non-matches can create issues for members of the public, and we are committed to working with industry users of eCBSV to better understand the causes of inaccurate non-matches and to identify further areas of improvement in our services.

   Regarding disclosing a "reason code," eCBSV provides only a "match" or "no-match" ("Y" or "N") response consistent with our longstanding disclosure policy and data exchange

practices. Individuals consenting to eCBSV authorize us to release only this match/no-match response. Across our data exchanges, we do not provide additional information for non-program purposes (i.e., work unrelated to administering the Social Security and Supplemental Security Income programs) except to other government agencies in very limited circumstances, and expanding the information we disclose in eCBSV would increase the risk of improper disclosure of the public's sensitive information. Due to the sensitivity of the information we collect, we follow a policy of strict confidentiality of our records, which conforms to applicable laws and regulations.

3. **Industry has been clear in communications with SSA and Congress that one of the best ways to increase use of the eCBSV system – and in driving more volume, reduce the average cost of a transaction – would be to allow the eCBSV system to be used for additional use cases beyond those tied to new credit applications. For example, applications for checking accounts, or other areas where SSN validation is helpful such as background checks. Given that everything in eCBSV is tied to consent of the individual, it seems like there should be nothing that prevents an American from asking SSA to "vouch" for them by validating whether their data matches what is in SSA records for any use case where they need to prove who they are online. However, SSA has not expanded the use of eCBSV to these other applications.**

   Is anything legally precluding SSA from doing this? Would Congress have to act to authorize this? Could SSA find ways to offer these services under existing authorities?

   To handle our mission—delivering Social Security benefits and services to millions of Americans—we have focused our eCBSV work and resources on satisfying the requirements of the law. The current eCBSV system fulfills the requirements of the Banking Bill. Under section 215(b)(4) of the Banking Bill, the customers of eCBSV (i.e., Permitted Entities that have signed an eCBSV user agreement) are financial institutions, as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809), or service providers, subsidiaries, affiliates, agents, subcontractors, or assignees of a financial institution.

   The Banking Bill does not require us to allow other eCBSV users beyond financial institutions and their service providers who are seeking an SSN verification in connection with a credit transaction. We have not explored expanding the eCBSV customer base. Expanding the customer base would increase a non-mission workload, and raise issues related to security and privacy risks and the proper method for reimbursement.

   We have longstanding processes that allow an entity to obtain an SSN verification based on the number holder's written consent with a pen and ink (wet) signature. Each year we perform over 2 billion automated SSN verifications through more than 3,500 data exchanges with Federal and State agencies, among others, under various legal authorities.

4. **While preventing fraud in financial services has driven much of the discussion behind the eCBSV system, fraud also hurts many government programs and the taxpayers directly. There are documented examples of criminals using synthetic identity fraud to claim undue government benefits, like unemployment assistance. Federal and state agencies have been interested in accessing eCBSV to prevent synthetic ID fraud in government benefit programs.**

   Does the SSA allow use of eCBSV to additional governmental agencies to help prevent entitlements fraud or does the SSA have that ability to under existing authority? Would Congress have to act to authorize this?

   Government agencies do not use eCBSV; however, we provide similar SSN verification services through other forms of electronic exchanges with them. We perform over 2 billion SSN verifications annually for State and Federal agencies, among others. For example, we provide data, including SSN verifications, to Federal and State agencies for the administration of health and income maintenance programs in accordance with law (e.g., 5 U.S.C. § 552a(b)(3), 42 U.S.C. §§ 1306 and 1320b-7).

   For instance, our State Verification & Exchange System (SVES) provides SSN verifications and benefit information to States and some Federal agencies. States use the information to administer State-run federally funded assistance programs such as Unemployment Insurance, Supplemental Nutrition Assistance Program, Temporary Assistance to Needy Families, Medicaid, and Children's Health Insurance Programs. All 50 States use SVES, as do the District of Columbia, Guam, Puerto Rico, and Virgin Islands.

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

5. **Broader adoption of eCBSV would help recoup costs sooner without the anticipated price increase. We have heard that many online and fintech lenders are not using this program due to challenges with adoption in an "instant credit" environment.**

   Are there any non-price factors inhibiting financial institutions from fully utilizing eCBSV?

   We designed a system that is responsive to the financial industry's needs within our legislative, regulatory, and fiscal constraints, and eCBSV fulfills the Banking Bill's requirement to offer real-time responses. We worked closely with the financial industry throughout the eCBSV development and rollout. We participate in monthly discussions with the Big Tent Coalition, an alliance formed by the financial industry, as well as with eCBSV Permitted Entities to engage the industry and solicit effective feedback. When they have

raised non-price factors, we have tried to address them, such as by allowing the necessary consent language to be incorporated into financial institutions' broader consent processes.

6. **One underlying issue that seems to be contributing to the high number of unreimbursed costs is the original transaction and usage estimates used by SSA in building the system varied significantly from those estimates provided by industry and have continued to significantly shift year after year. In December 2019, SSA based its cost estimates for the eCBSV pilot phase on 10 participating entities in FY 2020 submitting an anticipated volume of 307,000,000 transactions; actual transactions in FY 2020 were much lower. Despite that lower number, in November 2020, SSA based cost estimates on 123 participating entities in FY 2021 submitting an anticipated volume of 1,100,000,000 transactions; again, actual numbers were much lower. In January 2022, SSA based its revised tier structure on 45 participating entities in FY 2022 submitting an anticipated volume of 280,000,000 transactions. At that time, SSA also stated that it anticipated recovering the development costs over a three-year period, assuming projected enrollments and transaction volumes meet SSA's projections.**

   How has SSA considered their historical projections versus actual usage in designing the new pricing system? Has private industry provided any input on how their usage would change under this new pricing regime? How would that shift in industry usage affect time to recoup costs?

   Participation in eCBSV has been markedly lower than estimated. As of August 1, 2023, we have 23 Permitted Entities enrolled directly with some acting as service providers and 1,967 Financial Institutions enrolled indirectly behind a service provider.

   Our original fee tiers were based on applications submitted by 123 entities expressing interest in using eCBSV. When we developed the revised tier structure and associated fees published in the January 2022 Federal Register Notice, we reached out to the industry for an updated estimate of entities and volumes.[2] We based our tier increase on this estimate, but the actual entities and volume again came in much lower. Therefore, we conducted our recent FY 2023 breakeven analysis using current entities and volume based on actual experience.

[2] SSA, Notice of Open Enrollment and Fee Increase for Our Electronic Consent Based Social Security Number Verification Service, 87 Fed. Reg. 2475 (Jan. 2022): https://www.federalregister.gov/documents/2022/01/14/2022-00638/notice-of-open-enrollment-and-fee-increase-for-our-electronic-consent-based-social-security-number.

Representative Kildee

1. **I understand that the Social Security Administration (SSA) is required by law to recoup the costs of developing and operating the Electronic Consent Based SSN Verification Service (eCBSV) because Trust Fund resources cannot be used for non-program purposes such as eCBSV. Can you provide further explanation regarding this requirement and the timeline by which these costs must be recovered?**

   By law Social Security's discretionary Limitation on Administrative Expenses appropriation cannot be used to fund non-mission work, such as eCBSV.

   Section 215 of the *Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018* (P.L. 115-174, referred to as the "Banking Bill") required us to create an SSN verification system. The Banking Bill specifically requires that we fully recover our costs of developing and operating the system from users, and authorizes us to establish and adjust user charges to ensure we do so. Our Limitation on Administrative Expenses (LAE) resources fund the eCBSV project until sufficient reimbursements from the users allow us to break even. Our LAE account is an annual-year account; appropriation law limits the amount of time we can use LAE to that first fiscal year and limits the timeline to recover funds to the subsequent five years.

   The total cost for developing and operating eCBSV is $53 million through FY 2022. Of this amount, $38 million remains unrecovered/unreimbursed. On May 9, 2023, we published a Federal Register Notice announcing changes in the eCBSV subscription tier structure and associated fees.[3] These changes are intended to ensure we fully recover these costs in advance of appropriation law time limits, while limiting the amount of time during which LAE funds are used for non-mission work, assuming projected enrollments and transaction volumes meet these projections.

2. **At the hearing, testimony was submitted suggesting that the number of users of the eCBSV system should be expanded to bring per-user costs down. On page 6 of SSA's testimony, you note that SSA is "working to expand the ability of Federal benefits programs to use the service." Can you provide further information on this, including a timeline for implementation?**

   The statement in our testimony that "we are working to expand the ability of Federal benefits programs to use this service as part of their identity verification processes" refers to our intent to improve SSN verification services broadly, not eCBSV in particular. While government agencies do not use eCBSV, we provide similar SSN verification services through numerous other forms of electronic exchanges. We perform over 2 billion SSN verifications annually for State and Federal agencies, among others, to confirm whether the information they provide matches our records. The Fall 2022 and Spring 2023 Unified Agendas noted that we are contemplating a proposed regulation, "Social Security Number

[3] SSA, Notice of Fee Increase for Our Electronic Consent Based Social Security Number Verification Service, 88 Fed. Reg. 29959 (May 2023): https://www.federalregister.gov/documents/2023/05/09/2023-09753/notice-of-fee-increase-for-our-electronic-consent-based-social-security-number-verification-service.

Use in Government Records," which would clarify the circumstances under which SSA may disclose SSN information to other Federal agencies.[4] We are planning to expand the policy, and make process improvements, but do not currently have any additional information to share.

[4] SSA, Social Security Number Use in Government Records, RIN 0960-AI80, Unified Agenda (Sept. 2022): https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=0960-AI80; and SSA, Social Security Number Use in Government Records, RIN 0960-AI80, Unified Agenda (April 2023): https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=0960-AI80.

Representative Malliotakis

1. **In 2020, financial institutions lost around $20 billion from synthetic identity fraud. How is the SSA working with financial institutions to combat synthetic identity fraud?**

   Our electronic Consent Based Social Security Number Verification (eCBSV) service is specifically designed to combat synthetic identity fraud by allowing financial institutions to verify whether an individual's name, Social Security Number (SSN), and date of birth combination matches the information in our records. We worked closely with the financial industry throughout the eCBSV development and rollout. As of June 28, 2023, eCBSV has processed more than 149 million transactions.

   We participate in ongoing monthly discussions with the Big Tent Coalition, an alliance formed by the financial industry, as well as with eCBSV Permitted Entities to engage the industry and solicit effective feedback.

2. **Since the peak of identify fraud during the COVID-19 pandemic, has SSA made any progress combatting fraudsters and securing Americans SSN's?**

   SSA's Office of the Inspector General (OIG) received increased imposter scam reports in mid-2020 through mid-2021.[5] We strengthened our efforts to educate the public about how to protect their sensitive information from fraudsters. The scam numbers began to decline in April 2021 and have since remained steady.[6] Nevertheless, in partnership with our OIG, we continue to fight these scams using multiple methods to deliver the message to the public.

   To strengthen our multi-faceted efforts to educate the public, we released public service announcements, worked with external groups and agencies to raise awareness, and partnered with the United States Postal Service to display identity scam prevention posters in Post Offices around the country. We provide our employees with the latest information to ensure they can help individuals who call and visit our offices. We ask them to help educate their friends, families, and communities. We use social media to reach individuals, advising them to "guard their [SSN] card" and sensitive information.

   For instance, in Q2 of FY 2023, our latest Public Service Announcement[7] on scams generated 131 million impressions. Other useful public education tools included our scam FAQ web page[8] (336K page views in Q3 of FY 2023), our main scam web page[9] (478K page views), our Spanish language scam web page[10] (26K page views), the scam banner on

[5] SSA OIG, Quarterly Scam Update to Congress (March 2022): https://oig.ssa.gov/assets/uploads/quarterly-scam-report-issue-3.pdf
[6] SSA OIG, Quarterly Scam Update to Congress (March 2023): https://oig.ssa.gov/assets/uploads/quarterly-scam-report-issue-7.pdf
[7] SSA, SSA Scam Awareness PSA 60 (Oct. 2021): https://www.youtube.com/watch?v=0l5RX73PnFY
[8] SSA, What should I do if I get a call claiming there's a problem with my Social Security number or account? (March 2023): https://faq.ssa.gov/en-us/Topic/article/KA-10018.
[9] SSA, Protect Yourself From Scams (n.d.): https://www.ssa.gov/scam/.
[10] SSA, Protéjase de las estafas (n.d.): https://www.ssa.gov/espanol/estafas/.

SSA.gov[11] (143K clicks), and paid social media campaign of Facebook/Instagram ads promoting scam awareness (22 million impressions). We also added a scam warning message on the outside of 108 million notice envelopes sent to customers this quarter, and published scam alerts and warnings on televisions in our field office waiting rooms nationwide.

We prioritize research each year to shape our interventions, response, communications, and outreach. Recent studies funded by SSA include *Identity Theft Victimization among Older Americans*[12] and *Scam Susceptibility and Fraud Victimization.*[13]

We collaborate closely with our OIG to keep our customers and our employees informed of developing threats against their personal information. This year, working with our OIG, we observed the fourth annual "Slam the Scam" day[14] during the Federal Trade Commission (FTC)'s National Consumer Protection Week, continuing our efforts to ensure the public can identify fraud attempts, understands how to respond, and stays up to date on best practices to protect their information.

3. How would requiring States to compare unemployment claimants to database of deceased individuals in the Social Security Administration's Death Master File prevent fraudsters from stealing identities of deceased individuals?

SSN verifications and death indicators are important tools to help prevent and detect identity theft. Our verification services return a death indicator if our records indicate that the individual is deceased.

We perform over 2 billion SSN verifications annually for State and Federal agencies, among others, to confirm whether the information they provide matches our records. For instance, our State Verification & Exchange System (SVES) provides SSN verifications, death indicators, and benefit information to States and some Federal agencies. States can use the information to administer State-run Federally funded assistance programs such as Unemployment Insurance, Supplemental Nutrition Assistance Program, Temporary Assistance to Needy Families, Medicaid, and Children's Health Insurance Programs. All 50 States use SVES, as do the District of Columbia, Guam, Puerto Rico, and Virgin Islands.

4. Many people are unknowing victims of identity theft, and this sometimes results in missing benefits or money owed. When this happens and your agency is made aware of fraud, what actions do you take to protect the victim? Case after case that comes to my office needs my staff to intercede, how does the average citizen

---

[11] SSA web home page (n.d.): https://www.ssa.gov/.
[12] Marguerite DeLiema, David Burnes, and Lynn Langton, Consequences and Response to Identity Theft Victimization among Older Americans, WI21-11, Center for Financial Security, University of Wisconsin-Madison (Sept. 2021): https://cfsrdrc.wisc.edu/files/working-papers/WI21-11_DeLiema-Burnes_Final-Paper_9.29.21-(2).pdf.
[13] Aparajita Sur, Marguerite DeLiema, and Ethan Brown, Contextual and Social Predictors of Scam Susceptibility and Fraud Victimization, WP 2021-429, University of Michigan Retirement and Disability Research Center (Sept. 2021): https://mrdrc.isr.umich.edu/publications/papers/pdf/wp429.pdf.
[14] SSA, Social Security and OIG Hold Annual Slam the Scam Day – Press Release (March 2023): https://www.ssa.gov/news/press/releases/2023/#3-2023-1.

who doesn't know to use their Representative for assistance get help when the issuing agency couldn't detect the fraud in the first place?

We appreciate the assistance of Congressional offices in resolving casework. We understand the frustration, distress, and economic hardship that SSN misuse and identity theft cause victims. If an individual suspects their identity has been stolen, they can contact us directly and we can correct SSA program-related issues.

As a matter of practice, online and in our offices, we also provide individuals who suspect their identities have been stolen with up-to-date information about steps they can take to work with credit bureaus, law enforcement agencies, and the Federal Trade Commission. We encourage individuals to consider contacting the IRS because an identity thief might use a stolen SSN to file a tax return. We develop cases of possible SSA-program related fraud and refer them to our Office of the Inspector General (OIG) for investigation as appropriate. Individuals who suspect their identities have been stolen can place a block on their online SSA account to prevent anyone from viewing their record or being able to change direct deposit information online or by phone without contacting us.

5. **My office has delt with casework of people who were denied unemployment benefits because someone else was using their Social Security Number. One week without a paycheck can be detrimental to many families. Are there safeguards in place to assist these individuals who are denied benefits due to fraud?**

SSA offers tools for Federal and State partners to improve program administration and prevent fraud. We perform over 2 billion SSN verifications annually; these verifications are an important tool for agencies in protecting the integrity of their programs. For instance, our SVES system is available to States for administering State-run federally funded assistance programs such as Unemployment Insurance. Using SVES and our other verification services, States can verify unemployment applicants' SSN information *before* paying benefits.

6. **How does SSA work with law enforcement to crack down and prosecute fraudsters?**

SSA's Office of the General Counsel employs 35 criminal fraud prosecutors who are embedded in various U.S. Attorney's Offices around the country as Special Assistant U.S. Attorneys. These prosecutors work with the SSA OIG and other law enforcement agencies to investigate and prosecute fraud against the agency's benefits programs as well as misuse of SSNs, identity theft, and imposter scams in Federal court.

We work closely with SSA's OIG to educate the public on threats and scams, and to prevent and root out fraud. We operate the anti-fraud Cooperative Disability Investigations (CDI) Program jointly with OIG and law enforcement partners. The CDI Program is an important anti-fraud initiative that combats fraud within Social Security disability programs by reviewing questionable disability claims and investigating cases of suspected disability fraud to stop payment before it occurs, or as soon as fraud is suspected. Each CDI unit consists of an SSA OIG special agent who serves as a team leader, and personnel from SSA, State

disability determination services (DDS), and State or local law enforcement partners. Today, 50 CDI units cover all 50 States, the District of Columbia, Puerto Rico, and all U.S. territories.

We also partner with SSA OIG to keep our customers and our employees informed of developing threats against their personal information. This year, we jointly observed the fourth annual "Slam the Scam" day during the FTC's National Consumer Protection Week, continuing our work to ensure the public can identify fraud attempts, understands how to respond, and stays up to date on best practices to protect their information.

SSA OIG collects and investigates reports of suspected fraud or scams regarding Social Security benefits or SSNs, often in close collaboration with law enforcement. We would defer to the testimony of SSA OIG for further details on this work.

PUBLIC SUBMISSIONS FOR THE RECORD

U.S. HOUSE OF REPRESENTATIVES
WAYS AND MEANS SUBCOMMITTEE
ON SOCIAL SECURITY

SSA's Role in Combatting ID Fraud

Statement for the record from:
National Council of SSA Field Operations Locals
AFGE Council 220
Representing bargaining unit employees in Social Security Field Offices, Tele-Service Centers and Workload Support Units Nationwide

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

On behalf of the American Federation of Government Employees, AFL-CIO (AFGE) which represents over 750,000 federal employees at over 70 different agencies, I thank you for holding this important hearing on Social Security Administration's (SSA) role in combatting identity fraud.

AFGE represents over 42,000 SSA employees and I am the President of AFGE Council 220, representing employees in SSA field offices, tele-service centers, and workload support units nationwide. Over the last decade Social Security beneficiaries have increased by 25% while SSA's operating budgets have decreased by 17% and hiring is by down 50%. By the end of FY 2022 SSA staffing levels reached a 25-year low, and employee surveys have found SSA to be the worst large agency to work for in the Federal government.

Despite a decade of Congressional underfunding that has failed to keep up with inflation and the increased public demand for services, according to the Partnership for Public Service, SSA is ranked second overall as the public's most trustworthy Federal agency. The reason for this is simple, the hard work of dedicated SSA employee in serving the American public. SSA employees are vetted with background checks upon entering public service and are fully trained on how to protect the public's Personal Identifiable Information (PII).

But workers at SSA are struggling with an underfunded operating budget, and it is leading to an employee morale and attrition crisis while workloads mount and public service deteriorates. As the SSA workforce dwindles, we are seeing the agency relying more and more on the assistance of community partners to help the public with their claims, new Social Security number applications, replacement card applications, and reviews of eligibility in an effort to keep up with public need.

Congress needs to fully fund Social Security so sensitive information stays within the hands of trusted, vetted, and trained Social Security employees, and so the agency may continue to be a steward and protect the PII of the American public. Failing to adequately fund the Social Security Administration, which is manned by professional, security vetted public employees, is a disservice to the public as it opens them up to further attacks by scammers and cybercriminals.

Employees at Social Security, who have been through a thorough background investigation conducted by the Defense Counterintelligence and Security Agency and Office of Personnel Management's Nation Background Investigation Bureau, have the training and clearance to work with the sensitive information that is required to process the claims and other matters for the people that depend on the various services as provided by the Social Security Administration.

Congress must meet its responsibility and appropriate adequate funds so that the Agency has enough staff and the agency and employees have the tools they need to continue to protect both the integrity and security of the Social Security Administration's programs, trust funds and customer PII.

Thank you for hosting this hearing on Social Security. We look forward to working with the Committee to ensure SSA can better protect the personal information of the American public. If you have further questions about any of these issues, please contact Jeff Cruz at jeff.cruz@afge.org.

Sincerely,

Jessica LaPointe
AFGE Council 220 President

Sherry Jackson
AFGE Council 220 2nd Vice President

○