S. HRG. 114–857

# PROTECTING SENIORS FROM IDENTITY THEFT: IS THE FEDERAL GOVERNMENT DOING ENOUGH?

## HEARING

BEFORE THE

## SPECIAL COMMITTEE ON AGING

## UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

OCTOBER 7, 2015

**Serial No. 114–14**

Printed for the use of the Special Committee on Aging

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
48–680 PDF WASHINGTON : 2022

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, Maine, *Chairman*

ORRIN G. HATCH, Utah
MARK KIRK, Illinois
JEFF FLAKE, Arizona
TIM SCOTT, South Carolina
BOB CORKER, Tennessee
DEAN HELLER, Nevada
TOM COTTON, Arkansas
DAVID PERDUE, Georgia
THOM TILLIS, North Carolina
BEN SASSE, Nebraska

CLAIRE MCCASKILL, Missouri
BILL NELSON, Florida
ROBERT P. CASEY, JR., Pennsylvania
SHELDON WHITEHOUSE, Rhode Island
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY, Indiana
ELIZABETH WARREN, Massachusetts
TIM KAINE, Virginia

---

PRISCILLA HANLEY, *Majority Staff Director*
DERRON PARKS, *Minority Staff Director*

# C O N T E N T S


Page

Opening Statement of Senator Susan M. Collins, Chairman ..... 1
Opening Statement of Senator Claire McCaskill, Ranking Member ..... 3

PANEL OF WITNESSES

Sean Cavanaugh, Deputy Administrator and Director, Center for Medicare, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services ..... 5
Gary Cantrell, Deputy Inspector General for Investigations, Office of Inspector General, U.S. Department of Health and Human Services ..... 7
Betty Balderston, Statewide Coordinator, Maine Senior Medicare Patrol ..... 8
Marc Rotenberg, President, Electronic Privacy Information Center ..... 9

APPENDIX

PREPARED WITNESS STATEMENTS

Sean Cavanaugh, Deputy Administrator and Director, Center for Medicare, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services ..... 27
Gary Cantrell, Deputy Inspector General for Investigations, Office of Inspector General, U.S. Department of Health and Human Services ..... 35
Betty Balderston, Statewide Coordinator, Maine Senior Medicare Patrol ..... 45
Marc Rotenberg, President, Electronic Privacy Information Center ..... 49

QUESTIONS FOR THE RECORD

Sean Cavanaugh, Deputy Administrator and Director, Center for Medicare, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services ..... 61
Gary Cantrell, Deputy Inspector General for Investigations, Office of Inspector General, U.S. Department of Health and Human Services ..... 62

# PROTECTING SENIORS FROM IDENTITY THEFT: IS THE FEDERAL GOVERNMENT DOING ENOUGH?

**WEDNESDAY, OCTOBER 7, 2015**

U.S. SENATE,
SPECIAL COMMITTEE ON AGING,
*Washington, DC.*

The Committee met, pursuant to notice, at 2:09 p.m., Room 562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Tillis, McCaskill, Casey, and Donnelly.

## OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

The CHAIRMAN. Good afternoon. The Committee will come to order.

First, let me explain to our witnesses and those who are here today the unusual situation on the Senate floor in which we find ourselves. Much to our surprise, two votes were scheduled for 2:00 p.m. I have cast the first of those votes. My colleague and Ranking Member Senator McCaskill is on her way to cast that vote. Then the second vote will occur, and we each will have to go vote and have a short recess. Also complicating this afternoon's schedule is a classified briefing on Syria.

I will beg the indulgence of our witnesses for less than a full attendance today due to conflicting events, such as the two votes on the DOD policy bill and also the classified briefing on Syria. Nevertheless, I do want to welcome you all here today.

It comes as no surprise that Americans are very concerned about the risk of identity theft. According to a recent Harris poll, 70 percent of respondents cited identity theft as among their greatest security-related concerns, ahead of terrorism, personal safety, and natural disasters.

Last year, more than 332,000 Americans reported being victimized by someone who had stolen their identity. According to the Federal Trade Commission, 28 percent of those identity theft complaints were reported by seniors. This is not a new problem. In fact, the FTC reports that identity theft has been its number one consumer complaint over the past 15 years.

More than a decade ago, the Government Accountability Office cited the widespread use of Social Security numbers as identifiers by both public and private sector organizations as a major factor allowing criminals to commit identity theft. Subsequently, in 2007,

the Office of Management and Budget directed all Federal agencies to develop plans for reducing the unnecessary use of Social Security numbers as identifiers in order to help protect individuals against identity theft.

Since then, many Federal agencies that had used Social Security numbers as identifiers, including the Department of Defense and the Department of Veterans Affairs have removed these numbers from their identification cards. Private health insurers and State agencies have also discontinued their use of Social Security numbers. Yet, the Centers for Medicare and Medicaid Services, which provides Medicare cards for 55 million seniors and disabled individuals, still has not.

While five years have elapsed since the OMB order to reduce unnecessary use of Social Security numbers, the GAO found in 2012 and again in 2013 that CMS's efforts lagged behind other agencies and the private sector. As a consequence, the 55 million Medicare cards in use today still clearly display an individual's Social Security number.

Last March, Ranking Member McCaskill and I wrote to CMS to ask what steps the agency was taking to remove Social Security numbers from Medicare cards. In its response, CMS told us that it would, "likely take approximately two to three years to make the necessary system modifications, conduct an outreach and education campaign, and issue new cards."

Since it was increasingly clear that CMS officials were going to continue to drag their feet, in April, Congress passed and the President signed into law, a law that requires CMS to remove Social Security numbers from all Medicare cards.

In May, ten members of this Committee joined Ranking Member McCaskill and me in sending yet another letter to CMS, asking that we be further updated of its plans. In its response to this letter, CMS told us that they now anticipated that it would take four years to complete the project and that communications activities would continue through April 2019. In other words, CMS has actually lengthened its estimate of the time needed to solve this problem first identified by the GAO eleven years ago.

This afternoon's hearing will allow us to hear from CMS why its completion of this important project, which is essential to help protect seniors from identity theft, has taken so long.

For the victims of identity theft, the stakes are high. Identity thieves can drain bank accounts, make unauthorized credit card charges, and damage credit reports. When medical identity theft occurs, the thief can obtain medical care, buy drugs, and submit fake billings to Medicare. Some identity thieves have even used stolen personal information to obtain medical care for themselves or others. This can actually put lives at risk if the theft is not detected and the wrong information winds up in a victim's medical file.

Moreover, it is not at all unusual for a victim of medical identity theft to be unaware that his or her personal information has been stolen. According to a 2015 study sponsored by the Medical Identity Theft and Fraud Alliance, on average, victims learn about the theft of their information more than three months following the crime. Some victims may never know how or when their medical identity

was stolen because the criminals often hold the stolen information for months or even years before using or selling it.

Our witness from the Office of the Inspector General will discuss what the OIG and its law enforcement partners are doing to combat medical identity theft and health care fraud.

I also want to take a moment to give a special welcome to Betty Balderston from Winthrop, Maine. Ms. Balderston is the statewide Coordinator for the Senior Medicare Patrol in our State. Senior Medicare Patrol volunteers work locally to empower seniors and their families to fight health care fraud and abuse and to help them to identify identity theft.

We can reduce the likelihood of identity theft through tougher prosecution, consumer education, and by removing Social Security numbers from Medicare cards without endless delays. I look forward to hearing from our witnesses.

Senator McCaskill, I have explained the difficult schedule we are all operating under today. Please proceed with your statement.

**OPENING STATEMENT OF SENATOR CLAIRE MCCASKILL, RANKING MEMBER**

Senator MCCASKILL. Thank you so much. Thank you, Chairman Collins.

I am pleased we are holding a hearing on such an important issue. Given the recent passage of H.R. 2, the Medicare Access and CHIP Reauthorization Act of 2015, this hearing is both timely and very necessary. Today, we will again examine a problem causing significant angst to many Americans, especially our seniors.

Identity theft occurs when personal identifying information, like a Social Security number, is stolen to fraudulently establish lines of credit, to make unauthorized credit card charges, and to drain bank accounts. More specific, medical identity theft, the fastest growing form of health care fraud, occurs when stolen personal information is used to submit fraudulent billings to Medicare or Medicaid, or to apply and actually receive Social Security benefits.

Social Security numbers are exceptionally valuable to an identity thief. Therefore, the visual display of Social Security numbers on Medicare cards has played a significant role in putting Medicare beneficiaries, including more than 41 million seniors, at risk of identity theft.

Our seniors are particularly vulnerable. They use their Social Security numbers for a variety of reasons, including financial transactions and to obtain health services. More often than not, seniors carry their Medicare cards with them, as instructed by providers, which makes them more susceptible to identity thieves. Removal of the Social Security number from the Medicare card is a critical step toward hopefully reducing the number of seniors who are currently being targeted.

Moreover, we have seen an alarming number of cybersecurity breaches of health care providers in the last several years. That means in addition to stealing information directly out of a senior's pocket, thieves can simply hack into a Medicare provider's system and take thousands of Social Security numbers.

In 2007, the Office of Management and Budget issued requirements for the protection of personally identifiable information.

These requirements directed all Federal agencies to reduce and eliminate usage of Social Security numbers. Since then, Federal agencies, such as the Department of Defense and the Department of Veterans Affairs, moved away from Social Security numbers as identification. Additionally, private health insurance companies, universities, and states have abandoned the practice of using Social Security numbers as identifiers.

Yet, the CMS, the Centers for Medicare and Medicaid Services, continues to place Social Security numbers on more than 50 million Medicare cards currently in use. In fact, CMS has made minimal steps toward removing Social Security numbers from Medicare cards despite continued warnings from the Government Accountability Office in 2004, in 2012, in 2013, and 2015 that the practice places millions of people at risk of not only identity theft, but severe financial loss.

In 2014, the Federal Trade Commission reported that Missouri ranked fourth among states for identity theft and fraud complaints. That is after ranking 23rd the previous year. A 77 percent increase in complaints is not only substantial, it is alarming.

Transitioning from the use of Social Security numbers as identifiers to an alternative identifier is no doubt an arduous task. However, there is no excuse for inaction when the safety and financial security of our seniors is at stake. Though CMS has offered a proposed plan and timeline, it has been, "planning to switch from using Social Security numbers as identifiers to alternative identifiers for almost a decade."

The time for action has long passed. Now that funding has been allocated, there is no time to waste. Our seniors cannot afford to wait. My hope is that through this hearing, we get a sense of CMS's plan, implementation process, and timeline to permanently remove Social Security numbers from Medicare cards to better protect our seniors.

I thank Chairman Collins for her attention to this issue. She has been dogged in her pursuit of getting Social Security numbers off Medicare cards, and I look forward to hearing from our witnesses. I know she has probably explained we have an important security briefing on Syria for the Armed Services Committee, and so I do not want anyone to think I do not think this is important if I slip out long enough to get the secure briefing. My hope is to return before the hearing is concluded.

Thank you very much, Chairman.

The CHAIRMAN. Thank you.

I would now like to call on our colleague, Senator Tillis. He, too, is on Armed Services and has to attend that classified briefing, so I am going to ask if he has some comments he would like to make.

Senator Tillis.

Senator TILLIS. Thank you, Madam Chair.

I did want to apologize. We were late because we had a vote, and we have to leave a little bit early to get off to a security briefing. Senator McCaskill and I rode up in the elevator together and we were talking about how glad we were that the Chair is holding this hearing.

I do not understand the difficulty here. I mean, this is a blinding flash of the obvious in terms of what we need to do. Why you have

been thinking it for 10 years and not taking action makes no sense to me. It defies any best practices in other government organizations and certainly in the private sector.

I appreciate you all for the work that you are doing. I think that this is not a discussion about trying to sort out what needs to be done. It is really a discussion why it is not already done.

I hope to get back so that I can hear some of your testimony and have an opportunity to ask you questions, but I thank you all for being here, and I know that I think I speak for many members of this Committee that we all agree that this is action that needs to be taken promptly in defense for our seniors. Thank you.

The CHAIRMAN. Thank you very much.

Now, we will turn to our panel of witnesses. First, we will hear from Mr. Sean Cavanaugh. He is the Deputy Administrator and Director of the Center for Medicare at the Centers for Medicare and Medicaid Services.

Next, we will hear from Gary Cantrell, the Deputy Inspector General for Investigations at the Department of Health and Human Services.

We will then hear from our witness from the great State of Maine, Betty Balderston, the statewide Coordinator for the Maine Senior Medicare Patrol. She has done an impressive job of recruiting some 80 volunteers across the State to assist her, and I am looking forward to hearing her testimony.

Finally, we will hear from Marc Rotenberg, the Executive Director of the Electronic Privacy Information Center.

We thank you all for joining us and we will start with your testimony, Mr. Cavanaugh.

## STATEMENT OF SEAN CAVANAUGH, DEPUTY ADMINISTRATOR AND DIRECTOR, CENTER FOR MEDICARE, CENTERS FOR MEDICARE AND MEDICAID SERVICES, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. CAVANAUGH. Good afternoon, Chairman Collins, Ranking Member McCaskill, and Senator Tillis. Thank you for inviting me to testify today on CMS's work to remove Social Security numbers from Medicare cards.

When the Medicare program was created in 1965, it was administered by the Social Security Administration. While CMS is now responsible for the management of Medicare, the Social Security Administration still enrolls beneficiaries and both agencies rely on interrelated systems to coordinate Social Security and Medicare eligibility.

Upon enrollment, Medicare beneficiaries are assigned identification numbers, known as Health Insurance Claim Numbers, or HICNs, which are based upon a beneficiary's Social Security number. Providers use the HICN when they submit claims for services and supplies. CMS and its contractors also use the HICN to process claims, authorize payments, and issue beneficiary communications.

Thanks to the Medicare Access and CHIP Reauthorization Act, or MACRA, which was enacted earlier this year, CMS will eliminate the Social Security number-based identifier on Medicare cards by April 2019. CMS has already begun the process of replacing the

current HICN with a Medicare Beneficiary Identifier, or MBI, which will help beneficiaries better safeguard their personal information by reducing the exposure of their Social Security numbers. CMS will be able to terminate a compromised MBI and issue a new number as soon as it is reported as compromised, similar to how credit card companies respond to stolen card numbers.

This is a substantial undertaking requiring coordination with Federal, State, and private stakeholders, updating and modifying numerous IT systems, and conducting extensive outreach to beneficiaries, providers, and other stakeholders. CMS must accomplish these tasks without disrupting beneficiaries access to care or payments to providers. CMS will assure a smooth transition by moving forward thoughtfully and taking lessons learned from other large scale, complex IT projects.

CMS will develop, test, and execute systems modifications in a way that ensures compatibility with multiple outside systems, including every entity that bills Medicare. This work will affect more than 75 systems within CMS and 57 unique State, territorial, and Federal partners' IT systems. For example, the Social Security Administration and the Railroad Retirement Board will need to modify their eligibility enrollment systems, and the Medicare Administrative Contractors will need to modify systems to authorize coverage and process claims.

Once systems modifications are in place, CMS will initiate an extensive and phased outreach program for an estimated 60 million Medicare beneficiaries. We will have a series of communications that will inform beneficiaries that they will be receiving a new card, instruct them on how the new card should be used, and how to dispose of their old card. We will also work with Medicare providers on this transition and instruct them on how to use MBIs to submit claims and conduct other transactions. We must also ensure that private health plans, other insurers, and State Medicaid agencies are instructed on how to use MBIs so they can continue their coordination of benefit activities.

Throughout this transition, CMS will continue to prevent and detect fraud by educating beneficiaries about the risks of medical identity theft. Information is available online and in the "Medicare and You" handbook, which is distributed to all Medicare households each fall. In these publications, beneficiaries are advised to guard personal information, check medical bills and billing summaries, be wary of telemarketers and anyone who offers free medical equipment or services, and alert CMS or the Inspector General if they see signs of fraud.

In addition, we will continue to add compromised HICNs to our Compromised Number Checklist. This data base includes compromised provider and beneficiary numbers obtained through fraud investigations and complaints from providers or beneficiaries. CMS uses the checklist to inform sophisticated analytics through the Fraud Prevention System. This system identifies aberrant and suspicious billing patterns. Output from the Fraud Prevention System helps CMS focus its investigative resources on the misuse of HICNs and other egregious behavior. Through these investigations, CMS may make referrals to law enforcement or take other admin-

istrative actions, including revoking a provider's billing privileges or implement a payment suspension.

The transition from HICNs to MBIs is complex. It requires complicated Federal, State, and private sector systems modifications and significant outreach to beneficiaries and providers. CMS is fully committed to completing this project on time to protect Medicare beneficiaries and the trust funds from fraud while minimizing confusion and disruption from denied claims or access to services.

Thank you for your continued interest in Medicare and the beneficiaries we serve and we look forward to working with you to protect and strengthen the program. Thank you.

The CHAIRMAN. Thank you very much.

Mr. Cantrell.

**STATEMENT OF GARY CANTRELL, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**

Mr. CANTRELL. Good afternoon, Chairman Collins, and thank you for the opportunity to talk today about OIG's efforts to combat medical identity theft in Medicare.

Medical identity theft can create patient safety risk and impose financial burdens on those affected and may also lead to significant financial losses for Medicare. Of concern are external threats posed by criminal enterprises and professional identity thieves, as well as internal threats from company owners, employees, practitioners, and patients who participate in these fraud schemes.

Combating medical identity theft is among OIG's highest priorities. OIG advances our mission through a robust program of investigations, audits, evaluations, and compliance efforts. Combining data analytics with field intelligence, we identify areas most vulnerable to fraud and deploy our resources to ensure the greatest impact from our work.

OIG works closely with the Department of Justice, CMS, and other Federal and State law enforcement partners to bring those who commit fraud against our program and beneficiaries to justice. Our Medicare Fraud Strike Force Teams located in nine cities throughout the country exemplify this approach. The OIG and our partners are committed to fighting and preventing fraud, waste, and abuse.

Our efforts have produced significant results, including over 4,300 criminal and civil actions, over 11,000 exclusions, and nearly $11 billion in investigative receivables in the last three years. Since 1997, we have recovered more than $27 billion to the Medicare Trust Fund.

Despite these successes, more needs to be done. Fraud schemes are constantly evolving and migrating. Identity theft is now a common component of many fraud schemes we encounter. The patient and provider identifiers represent the keys to Medicare reimbursement, and as a result, both are targeted for identity theft.

We have seen a variety of identity theft-related schemes in our enforcement work. Our cases include company owners that pay kickbacks to identity thieves for patient information, health care providers that steal the identity of another practitioner, and pa-

tients who participate in fraud schemes by selling their sensitive data for some sort of monetary gain or kickback.

Annual Medicare spending is approaching $600 billion. An estimated 10,000 individuals become newly eligible each day. As the program continues to grow and evolve, criminals will continue to target the Medicare program for fraud. The need to protect the beneficiaries it serves from identity theft has never been more important.

It will take an all hands-on deck approach. This includes targeted enforcement, such as our Medicare Fraud Strike Force teams, in collaboration with our external partners, including our program integrity and private sector contacts.

It is also critical that we continue to educate our seniors so they can take steps to avoid being victimized by identity thieves. I would like to commend the Senior Medicare Patrol for their efforts in this area and express our commitment to work with the SMPs to educate seniors about identity theft.

We would also like to thank Congress for your efforts to prevent medical identity theft, including this important hearing and recent legislation that requires the removal of the Social Security number from Medicare cards. We appreciate your sustained commitment toward our mission and your interest in this vital issue of protecting our seniors from identity theft.

Finally, we encourage seniors to notify OIG's hotline if they suspect the fraudulent use of their Medicare number, either by visiting our website or by calling 1–800-HHS-TIPS.

Thank you for the opportunity to speak with you today, and I would look forward to any questions you have.

The CHAIRMAN. Thank you very much for your testimony.

Ms. Balderston.

**STATEMENT OF BETTY BALDERSTON, STATEWIDE COORDINATOR, MAINE SENIOR MEDICARE PATROL**

Ms. BALDERSTON. Chairman Collins, I am honored to be here today to share information about the SMP projects in Maine and across the country and how we educate, empower, and provide assistance to Medicare beneficiaries, their families, and their caregivers to prevent Medicare errors, fraud, and abuse, including identity theft.

Since my written testimony provides statistics and other details about our ongoing efforts to provide outreach, education, counseling, and assistance to seniors and people with disabilities receiving Medicare, I will focus my oral comments on the types of scams that have been reported and that relate to identity theft.

In 2013, the Maine SMP received reports of callers claiming to represent Medicare and providing information about the issuance of new Medicare cards. The caller requested the person's Medicare number and their financial information. This same scam has surfaced again since Congress ordered Social Security numbers be removed from Medicare cards.

According to reports from SMPs in other states, callers claiming to be from Medicare have contacted Medicare beneficiaries about other scams that include replacing their Medicare plan with an Obamacare plan and setting up home visits. In each instance, the

caller requested personal information, including the beneficiary's Medicare number.

On behalf of the SMPs nationwide, I applaud the efforts of Congress to eliminate the use of Social Security numbers on Medicare cards. This change will help address the issue of identity theft.

However, our work is not finished. Scam artists are always ready to take advantage of the country's most vulnerable individuals, including seniors and people with disabilities. They are experts in gaining trust and stealing money and benefits from unsuspecting victims.

A few years ago at a health care fraud panel presentation in Bangor, Maine, a senior reported he was a victim of identity theft, impacting his life for the previous five years.

The SMPs are the front-line boots-on-the-ground programs that provide outreach, education, counseling, and assistance to individuals every day. Our volunteer programs work, with seniors helping seniors every single day to help our vulnerable citizens remain safe and to protect their identities.

As the Centers for Medicare and Medicaid Services continue their work of transitioning to new Medicare cards, the SMP programs nationwide will continue our work, providing education about identity theft to Medicare beneficiaries, their families and caregivers, empowering them to protect their identities and to safeguard the Medicare program.

I would like to thank CMS for its recent outreach and education campaign on Medicare fraud that includes television ads, a blog, and a You Tube video. I am proud to say that one of our Maine SMP volunteers, Stan Cohen, is actually part of that TV ad, providing information on the importance of reading Medicare statements. In rural states like Maine, TV ads are the most effective way of reaching Medicare beneficiaries statewide with our important messages.

By all of us continuing to work together, we can make a difference in the lives of seniors and people with disabilities nationwide, empowering them to protect themselves against fraud and scams.

Thank you again for the opportunity to be here today on behalf of the Senior Medicare Patrol programs, and I am happy to answer any questions you may have.

The CHAIRMAN. Thank you very much.

Mr. Rotenberg.

## STATEMENT OF MARC ROTENBERG, PRESIDENT, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Chairman Collins, members of the Committee, thank you for the opportunity to be here today. My name is Marc Rotenberg. I am President of the Electronic Privacy Information Center. I also teach privacy law at Georgetown. I have been studying privacy issues related to the Social Security number for almost 25 years, and I just want to say how very grateful we are for your work on the Social Security number issue.

There is no number that is more critical in record linkage and data base management in the United States, and there is no number that poses a greater risk to personal privacy and financial secu-

rity. It is very important to continue to remove the Social Security number from identification documents that are used in the United States.

In my testimony, I provide a great deal of history about the use and misuse of the SSN for personal identification. In my oral testimony, I would like to just highlight a few of the key points which I think underscore the need for the CMS to move quickly to take the SSN off the Medicare card.

Now, as you know, this is not a new issue for Congress. In fact, back in 1973, a very famous report called "Records, Computers, and the Rights of Citizens" explicitly recommended that the SSN be removed from record management systems in the United States, and the Privacy Act of 1974, which was passed the following year, has a very specific provision, and it essentially tries to limit the use of the SSN across the Federal agencies, but as we all know, even with that restriction in place, the SSN continues to be used in the Federal Government and in the private sector.

In 1991, I testified before a House committee, and I warned at that time that the use of the SSN would contribute to increasing financial fraud in the United States. We did not even have the term "identity theft" at the time. All we knew back then was that the Social Security number was being used by criminals to gain access to people's bank accounts and their financial records.

In the 1990's, we also worked with the IRS to get the SSN off of the mailings that come from the IRS. We also worked with State governments to get the SSN out of State record systems, and we even had a case in Virginia where we got the SSN out of the voting rolls.

Now, as you have described, from about 2004, the GAO and other government reports made clear the need to get the SSN off of patient record identity documents, because what we have now seen is that in no sector is the problem of identity theft more severe than it is in the medical records sector. All of the reports point to the highest level of data breach and identity theft taking place in the medical records sector. That is where Americans are most vulnerable, and that is also where the elderly are particularly vulnerable. The Department of Justice and the Federal Trade Commission have both pointed to the increasing levels of identity theft among the American elderly based on the availability of the Social Security number.

Now, I have studied recently some of the history associated with the CMS and I simply do not understand the delay. We looked at the other Federal agencies and we looked at the Department of Defense, which has an extraordinarily complex record management program across many, many different components, and it is clear that the Department of Defense over the last several years has moved very aggressively and purposefully to get the Social Security number off DOD identity documents to make sure that that number is not even embedded in the magnetic strip, and I think the Department of Defense should be commended for the very good work they have done on behalf of servicemembers and their families, but it is not only DOD. Health care providers, the Harvard Community Healthcare Program took the SSN off of their identity documents. State governments have passed laws to have the SSN

removed from the private payment identity documents. Every institution in this country is moving to get the Social Security number off of health ID documents.

I think it is abundantly clear at this point in time that the greater delay is leaving Americans at risk, and American elderly communities are those who are most vulnerable, so thank you again for holding this hearing.

The CHAIRMAN. Thank you for your excellent testimony.

Senator Donnelly, have you voted yet on the second vote?

Senator DONNELLY. I have.

The CHAIRMAN. Senator Donnelly, I am going to go into recess so that I can go vote, but if you want to——

Senator DONNELLY. I have to go to the briefing.

The CHAIRMAN. You have to go to the classified briefing. We have a lot of overlap on our Committee. Thank you for coming by. I know this is an issue that you care deeply about.

We will take an approximately 15-minute recess so that I can go to the floor, vote, and then I will return. Thank you for your patience.

[Recess.]

The CHAIRMAN. The Committee will resume the hearing, and let me welcome our colleague, Senator Casey. We are very glad that you could join us, and again, my apologies for the unpredictable Senate schedule that we have to cope with.

Mr. Cavanaugh, let me start my questions with you. In 2004, more than a decade ago, the GAO reported that Social Security numbers are "a key piece of information used in identity thefts." At the time of that report in 2004, most states had already taken Social Security numbers off of their drivers' licenses in recognition of this threat.

Then we had a series of other reports. One of our witnesses, Mr. Rotenberg, mentioned a landmark that also could have been added to this list.

In 2007, OPM issued a governmentwide order telling agencies to drop the use of Social Security numbers as an identifier. The Department of Defense, the Veterans Affairs Department complied. Several more states, private insurers, Harvard Pilgrim, as was mentioned, also stopped using it as an identifier.

Then in 2008, we had the Inspector General of the Social Security Administration recommending the removal of the Social Security number from Medicare cards.

In 2012, the same recommendation came from the Inspector General of HHS, the broader Department.

I would add to this chart that Congress has weighed in on this issue many times, including this year in April as part of the change in the formula for doctors' reimbursements, passing a requirement that ordered—mandated—the Medicare agency to remove the SSN from the card.

Now, I do recognize you are dealing with 55 to 60, I believe you said, million Americans and that this is a big project, but the Department of Defense, as another witness pointed out today, is hardly a small agency. The VA also deals with millions of Americans, and both those departments managed to get the Social Security numbers off of their ID cards four years ago, so why has it taken

so long for CMS to tackle this issue? Why do you now predict that you are going to need the entire four years, to 2019, which is, after all, 15 years after the first red flag about this issue, before the numbers are no longer on the Medicare cards?

Mr. CAVANAUGH. Thank you, Chairman, for the question. It is an excellent and fair question. The short answer to your first question of what took us so long is funding, and in that respect, I applaud Congress, but specifically the leadership that this Committee has shown. As you know, the President's budget this year requested funding for this project, and just months after the President's budget was issued, Congress acted through MACRA and provided the funding, so we are pleased that we have a path forward. We have hit the ground running and we are working on a project that will get the Social Security numbers off the Medicare cards.

We had, prior to that funding, made some incremental improvements, so for example, we have over 16 million Medicare beneficiaries in private Medicare Advantage plans, and at our direction, the Medicare Advantage plans have gotten the Social Security number off the cards that they use. We have gotten the HICN number of some of our communications with beneficiaries, such as the summary notices that go out quarterly, but I think, it is most importantly to do the job right and to do it completely, we needed the funding that Congress has provided, so we thank you for that and we look forward to accomplishing this.

As to the question of why it is going to take time, I think it is important to understand two things. One, as you pointed out, and I appreciate you recognizing it, it is a complex technological challenge. There are within CMS over 75 systems that need to be updated, but more importantly, and unlike our colleagues at DOD and VA, we deal with many external partners, be they states, our administrative contractors, the Social Security Administration, so technologically, we are going to have to coordinate with them and make sure their systems are changed at the same time.

The wild card in all this is how we roll it out to beneficiaries and providers. As you know—so, we anticipate when we roll this out, there will be 60 million Medicare beneficiaries. There are closer to 55, 56 million today. There are also, importantly, 1.5 million providers who bill Medicare. We have made a decision at CMS not to throw a switch one day and send all the cards out at one time and change the world in one fell swoop.

A significant part of the calendar and timeline that we have established is a phased rollout that will give us time to educate both beneficiaries and providers on why the card is being changed, what they should do with it, to try to help distinguish this action from some of the fraudulent actions that you have heard about, because we have been training Medicare beneficiaries to be very suspicious about mailings and things like this, so we have got to make sure they understand this is one they can trust, so I think that is part of the timeline that often gets overlooked.

We recently learned about the importance of really doing an extended outreach and education with the ICD–10 implementation, which just started recently, so we worked with providers over several years in that case, and I think it really accrued to our benefit and to the benefit of providers.

Again, we thank Congress for the funding. I think it set us on a path to get where we all want to be, which is to get the number off the cards.

The CHAIRMAN. Mr. Cavanaugh, 10,000 Americans are turning age 65 every day and, thus, eligible for Medicare. Would it not make sense to use an incremental approach and start with those new beneficiaries? You are not going to have to swap the cards out. There is no educational effort involved because they are coming in for the first time and getting their card, and I can tell you, though I will be interested if Mr. Rotenberg can add to this, that I believe health care providers would adapt in a nanosecond to this change and, indeed, welcome this change.

Why would you not start with those 10,000 new beneficiaries that are coming into your offices around the country every day to enroll in Medicare? There is no education requirement. Why does that not make sense, and that would not be an expensive effort.

Mr. CAVANAUGH. You are correct, and that is a very attractive option. The problem, and the reason we are not pursuing that track, is that it is not simply a matter of issuing a card with a certain number on it. All of our internal systems, and as I mentioned, there are over 75 of them, look to the number to identify a beneficiary, and all these systems need to be changed to recognize the new MBI, which will be different than the HICN, and to communicate with our external partners so that they know what these are, so there is a technology side to this that needs to precede the change in the number, so it would be wonderful if we could throw a switch today and begin filtering these out, but unfortunately, we have explored this and we do not think it works.

The CHAIRMAN. Mr. Rotenberg, you have dealt with health care insurers that have dropped the use of the Social Security number as an identifier. You said in your opening statement that it is the single most important set of numbers that an individual has when it comes to being vulnerable to identity theft. Do you think this would be difficult for health care providers to adapt to?

Mr. ROTENBERG. Chairman Collins, in fairness, I have not managed a transition of the type that CMS is obviously facing, but my sense is that your intuition is correct. In other words, the advantage of the incremental implementation avoids many of the difficulties that transitions necessarily raise. I am actually concerned, as I know Mr. Cavanaugh must be, about an education process that asks people to distinguish between a trustworthy communication and one that is not. That is already an opening for a new form of identity theft, and my thinking would be, let us do everything possible to try to avoid that.

Paradoxically, public education is actually an indicator that the system transition is probably not adequately managed, because a smooth system transition would be completely transparent to the end user. They would not be aware of the change, and I think your point, that the ideal moment at which to implement a new numbering scheme is with the issuance of a new card. That is the experience at the State level with the driver's license. That is the experience in universities with student IDs, and I think it is the experience at the State level with most of the private insurers. Take that moment when you have a new beneficiary and you are about to

issue a card to issue the correct card that minimizes the privacy risk.

The CHAIRMAN. Thank you.

Senator Casey.

Senator CASEY. Thank you, Madam Chair. I appreciate this hearing and I want to thank the panel for being here today. I missed your testimony, but I will try, based upon your written testimony, to pose a few questions.

Mr. Cavanaugh, I would start with you with regard to the two parts of your testimony, one that says that if you have a health insurance claims number compromise, that that individual will still get care, but also at the same time you are saying that right now, CMS cannot issue new numbers, so I am trying to get a sense of what that means for—in the real world of the beneficiary and the provider.

For example, for the provider, if they are in the case of having—dealing with an individual, or dealing with a claim where the individual's number has been compromised, what does that mean for that individual in terms of them? Will that provider have claims withheld? I guess that is part one, and then on the beneficiary end of this, will you also see instances where the beneficiary is refused services?

Mr. CAVANAUGH. Thank you for the question, Senator. No, so, as the current—as the checklist works, the number when it is identified as compromised goes into the system and then we start running analytics to look for suspicious behavior on the use of that number. We do not block use of the number, importantly, so the beneficiary who is using it legitimately can continue doing so, and similarly, providers who are billing legitimate services can continue doing so.

I know there has been some concern that the fraudulent user of that number could accumulate services in a way that disadvantages the beneficiary, for example, services that are subject to a cap. We have asked and are willing to investigate any circumstances. We have not seen any specific circumstances, but it is a potential.

I want to assure you, the beneficiary continues to receive services while we conduct an investigation about the use of their number.

Senator CASEY. Is it your testimony that the provider would not be adversely impacted, as well, in this instance where you have a compromised number?

Mr. CAVANAUGH. That is correct. The legitimate provider would not be adversely impacted. What we would be looking for is providers who are using the number in a suspicious way which would trigger an investigation either by us or our law enforcement partners.

Senator CASEY. Because of the numbers here, and I open this to the panel, the numbers are extraordinary in terms of fraud and in terms of the instances of fraud and it being the number one consumer complaint, so in the real world of families and beneficiaries, does anyone on the panel have an opinion about ways to be proactive when it comes to the family—warning signs that they should look for, on the one hand, and also proactive steps in light

of those warning signs? Does anyone have any thoughts about that? Ms. Balderston.

Ms. BALDERSTON. I could speak to that. Some of the outreach and education that we do is to address exactly what you just suggested, and it is to get people to pay attention to their Medicare statements, to what is going on with their Medicare account, and a lot of our efforts are spent trying to personalize that, that this is not just a government program, but it is their health insurance.

I think one of the most important things that CMS has created is myMedicare.gov, which allows people to set up their own Medicare account. We talk a lot about that with seniors, with their caregivers and their families, and the importance of utilizing that website so that they can look and see what is going on all the time, real time, with a person's Medicare account, because now that Medicare statements are only issued quarterly, it can be quite some time before somebody might notice something is going on with their Medicare account, so the myMedicare.gov site can be really helpful in that.

Having said that, coming from a very rural State like Maine and a very old State like Maine, there are a lot of people that do not have access to websites, and so much of our education has been focused on the new Baby Boomers that are aging into Medicare and families and caregivers of existing Medicare beneficiaries.

Mr. ROTENBERG. Senator Casey?

Senator CASEY. Yes.

Mr. ROTENBERG. If I could just add a word, I wanted to commend, by the way, Ms. Balderston and her group for the very important work that they are doing, because for families that do run into issues around identity theft, it is very important that someone is available to assist them, and I really do want to thank you for that work.

I will also say, the best outcome is to prevent the incident from occurring, because once a family confronts the problem, it is a very difficult problem. Identity theft is unlike other types of crime. If someone breaks into your car and steals the camera because you have left it in the back seat, you will know it. The camera is gone and the window is broken.

People who sit on stolen Social Security numbers and bank account numbers can wait weeks or months. There can be one theft. There can be multiple thefts. The FTC, the Department of Justice, will tell you this is a very difficult crime to solve, and the best thing to do is to prevent it from occurring.

If I may say one other thing, as I said in my opening testimony, I have been working on this issue for many years. In the early years, we thought the problem could be largely solved by preventing the display of the Social Security number, so a lot has been done over the years to take the SSN off of identity documents, but in fairness, I have to tell you, today, that with data breaches and criminal hacking, the data bases themselves are vulnerable, which means that it is not enough to simply take the SSN off the identity document.

If you are collecting the SSN in the administration of a system, you have to ensure that it is secure. You have to have that data encrypted, because if people get access to it, it will be misused. The

best starting point is to take the SSN off the ID document, but the other thing we have learned is that if you collect the SSN, you have to protect it.

Senator CASEY. Thank you very much. Madam Chair, thank you.

The CHAIRMAN. Thank you.

Ms. Balderston, you described a scam that I had not heard of prior to reading your testimony, where seniors will get a call from someone saying that they are issuing a new Medicare card and then they manage to get the Social Security number, the financial information, date of birth, all of the information that could be used to commit a really serious financial fraud.

I am a little concerned when I hear about the talk of an educational campaign that there is a new card coming that that will feed into the kind of fraud that you described so well in your testimony. Could you comment on that?

Ms. BALDERSTON. Thank you, Chairman, for bringing that up. I, too, have been worried about the same thing, and I think that by working together, all of us working together and sharing information with consumers about what is coming up and what is happening—and I think the value of the SMP programs are we are local programs in our own states. People know us. We work together with partners that are in communities throughout our states. In Maine, as I am sure you are aware, we work with the Area Agencies on Aging and people know and trust them.

I think for Maine and many other states like Maine, that really is the secret to helping people understand, is to use the trusted sources that are already in place and work together with CMS and others as they roll out this campaign so that we, as the boots on the ground, as I described earlier, and a familiar face and voice in our various states, that we can help get that message out to people.

The CHAIRMAN. Well, I think that is an excellent suggestion for Medicare to follow, and your presence really does make a difference, and the work of the Area Agencies on Aging is just tremendous in the State of Maine, I know from personal experience, so I think that is an excellent suggestion.

I still worry about the opportunity for criminals to take advantage of that, which is why I so strongly believe that the first step should be the new enrollees and get them their card. Their first card should be the card without any Social Security number on it and then figure out how we go from there.

Mr. Cantrell, I remember years ago holding hearings on Medicare fraud and we actually had a witness who said that he used to deal drugs, but that he could make a lot more money and it was a lot safer for him to be involved in Medicare fraud. Can you explain to us in a little more detail some of the Medicare identity theft cases that you have been dealing with? You had an astonishing number of the amount of recoveries you have been able to do, for which I salute you, and I think you said $27 billion was being lost in waste, fraud, and abuse.

This area of medical identity theft is a little different from the kind of provider fraud that we have seen in the past or people pretending to be providers and billing Medicare. Could you talk to us about what you are seeing in the area of medical identity theft.

Mr. CANTRELL. Absolutely, Chairman Collins. We have seen identity theft as a common theme throughout many types of fraud schemes. In some cases, there are individuals who have no intention of providing any legitimate service to anyone, but with the identity of the Medicare patient and the provider, they can submit bills with the intent of stealing money from Medicare, so there are some who are just straight-out criminal networks creating ghost companies, billing for services that were never rendered.

We have also seen, unfortunately, some legitimate providers, or providers who provide some level of service using identity theft as a means of perpetuating fraud to gain additional reimbursement for services that they either did not provide or for patients who they did not see. We have seen in some cases insider threats at physician offices or at medical facilities where identities have been stolen and either are used for—to further Medicare fraud, or in some cases we have seen that data being passed on and used to commit tax fraud, so our patients can become victims to other types of fraud as a result of the theft of this data, in many cases.

It ranges from people who will knock on the door of a facility or a nursing home where lots of Medicare beneficiaries are present and talk them into the need for a free service or some care that they maybe do not need and get their identifying information and begin billing for it, to the straight-up, no one has ever contacted this individual, but they have traded this information on the street somehow, some way. In the worst cases, we see what we call patient recruiters who will even go out and offer payment for exchange of what they call the red, white, and blue, the Medicare card, and that number on it, which is the key to Medicare reimbursement.

The CHAIRMAN. In some cases, you have actually seen a Medicare beneficiary sell the information or be paid for the information and actually be a co-conspirator in the fraud?

Mr. CANTRELL. That is correct, Chairman Collins.

The CHAIRMAN. I always hate to think of any senior doing anything wrong——but I guess it does happen occasionally.

Mr. CANTRELL. Unfortunately, they can be susceptible to these types of bribes, if you will, especially if they are financially not secure and someone is offering them a couple hundred dollars for either—and they do not have to do anything else, or maybe they get a trip to an adult day care center and they get some level of service that is not necessary that they did not need that would not have been prescribed by a legitimate physician.

The CHAIRMAN. Mr. Cavanaugh, I have read what is in many ways an excellent brochure that the U.S. Administration on Aging puts out. I think it is used by a lot of the Medicare Patrol volunteers to try to educate people, and I was struck, however, by the irony of the cover of this brochure, which otherwise has excellent information, because what is the cover but a beneficiary actually holding up the Medicare card showing the Social Security number on it. Does that trouble you?

Mr. CAVANAUGH. I noticed the same thing. I took some solace in the fact that this seems to be a dummy card, so this is not——

The CHAIRMAN. It is true. It does say "Joe Doe" and it has zeroes, but still, are you not sending a bit of a mixed message here? After

all, I think the Social Security Administration first advised the public to stop carrying Social Security cards and Medicare cards that displayed the Social Security number clear back in 1994 and started printing, "Do Not Carry It With You" on the cards in 2002. Medicare in this brochure also has, "Don't carry your Medicare or Medicaid card with you unless you need it. Only take it to doctors' appointments, visits to a hospital or clinic, or trips to the pharmacy." Is it not sending a mixed message to say that inside and then on the outside have someone hold up the card?

Mr. CAVANAUGH. Just to be clear, this is not a CMS publication, but I do think the publication has some excellent advice. Yes. I think probably a better picture could have been used, but this is, I think, a production of the Senior Medicare Patrol who do outstanding work and we appreciate their partnership in Combating Medicare fraud.

The CHAIRMAN. Actually, it is funded by the Department of Health and Human Services, and we are told that it was CMS that provided all the graphics.

Mr. CAVANAUGH. Then it is an unfortunate choice, I agree, but I just want to emphasize that the information in here is really solid. The work the Senior Medicare Patrol does is great, because I do think an educated and attentive beneficiary is the best first line of defense on identity theft.

The CHAIRMAN. I certainly agree with you on the work done by the Senior Medicare Patrol. I think they do a fabulous job, and I also agree with you that the information inside the brochure and the examples that are given are excellent and very helpful, but it is ironic, at best, and really unfortunate that the graphic that CMS designed shows that card. It sort of contradicts the message inside.

Mr. CAVANAUGH. The good news is, thanks to the leadership of you and the Congress, we will in the future not have to worry about that. We will still discourage people from flashing their cards like that, but we will have the Social Security number off the cards.

The CHAIRMAN. Good. Mr. Cantrell, you have looked at this issue. You are familiar with the GAO reports that go way, way back to 2004. I do not know whether you are involved in those earlier studies——

Mr. CANTRELL. No, Chairman.

The CHAIRMAN [continuing]. or you are too young to have been involved in those earlier studies, but what is your assessment of the responsiveness of CMS to GAO's recommendations in 2004, 2012, 2013?

Mr. CANTRELL. Well, I certainly believe from an anti-fraud perspective, the earlier and the sooner we can get the Social Security number off a card, the better. It has definitely been used to commit fraud against the Medicare program over the years since I have been here. I started with HHS OIG in 1996. It continues to be used in Medicare fraud schemes, and now we have seen, as a result of some of these identity thieves, fraud in other areas outside of the Medicare program, so we are looking forward to the day when the Social Security number is no longer used on the Medicare cards.

The CHAIRMAN. Thank you.

Ms. Balderston, when you work with seniors in Maine, how do you try to get the message across? Do you speak to senior groups in the state? Do you work with the AARP as well as the Area Agencies on Aging to try to get the message across of, be careful with this card?

Ms. BALDERSTON. Thank you, Chairman Collins. The answer is yes, we do all of those things. We do presentations to senior groups, to retiree groups. We do outreach through newsletters, through the Area Agencies on Aging as well as other partners that we have, like the Maine Association of Retirees, and we do education with the Maine Residence Service Coordinators Association, whose membership are people that work in senior housing facilities. They are the gatekeepers protecting the people that live in those facilities.

We have a broad partnership, both within Maine and, I think, around the country with our programs, to work with other organizations that work with seniors and people with disabilities in order to get the message out. In states like Maine that are so rural and so large, that is the only way that we can get our message out, is by working together with lots of other partners.

We also in Maine and in about half of the other states, the SMP programs also partner with the State Health Insurance Assistance Programs, the SHIP programs, and in Maine, as we are coming upon the Medicare open enrollment period here in just—ooh, next week—part of the counseling that the SHIP counselors do is also to provide our information. They provide them with advice on looking at their Medicare statements to make sure that Medicare is not paying for a service or supply that they did not receive. They are encouraged to use personal health journals to track what is going on with their health care so that when they get statements, they have something to check it against, and we really try to be proactive in getting people involved in paying attention to their health insurance and their health care. We also promote the preventive services under Medicare.

The CHAIRMAN. A friend of mine who receives Medicare in Maine was telling me that one of the things that upsets him is the Social Security number, the Medicare number is on statements that he receives from his bank because he automatically pays his Medicare premiums from his bank, but they send him a notice confirming that the transfer has occurred, and then right on that notice is his Social Security number. Have you seen that as a problem?

Ms. BALDERSTON. I have not seen that. I was not aware that that was happening, but that sounds like something perhaps we need to work with the Bankers Association.

The CHAIRMAN. I mention it to you because I happened to meet with the Bankers just this week in Maine, and as you may know, Maine has a wonderful program called Senior$afe, which is aimed at preventing the exploitation financially of our seniors and I think it is an excellent model for other states to follow, as well. Again, I want to thank you for the work that you do.

I am curious about one final point for you, and that is how many of your 80 volunteers that you have are seniors themselves?

Ms. BALDERSTON. Most of them are. I would say probably a good 85 to 90 percent are seniors, and we have really good volunteers. These are—a lot of these people have been professionals in their

working life. When we train volunteers, one of the questions that I often ask them when they first come to us is what brought you here. Of all the volunteer opportunities that are available to you in Maine, why would you come here? The answer is always the same, because they care about people.

They have been in situations where they have tried to figure out their own Medicare or their Medicare for a loved one and it is a very, very complicated health insurance program, and so, these people come so that they can help their families and their neighbors and people that life in their areas so that it is not as complicated, not as confusing, and so that people do not become victims of crimes like we have been talking about here today.

The CHAIRMAN. Thank you very much.

I want to give each of our witnesses a chance for any final comment that you would like to make, any advice to us before I close out the hearing. Mr. Rotenberg.

Mr. ROTENBERG. Well, again, Chairman Collins, thank you so much for your work and leadership on this issue. This is one that affects millions of Americans and it is a great thing that you are holding this hearing.

As I tried to suggest during my testimony, the misuse of the Social Security number is a long-running problem in this country. There is a lot more that still needs to be done. We need to make the record systems more secure. We need to protect against other forms of identity theft, but I think there is no question that the right starting point is to get the Social Security number off of identity documents, particularly in the medical sector. That is where the greatest risk of identity theft exists.

The CHAIRMAN. Thank you.

Ms. Balderston.

Ms. BALDERSTON. Thank you, Chairman Collins. My one closing remark would be the ongoing support of both Congress and a variety of Federal agencies for the work that we do, and hopefully, we can continue to work together to help fight these crimes and make all of our states a better and safer place for our seniors and our people with disabilities.

The CHAIRMAN. Thank you.

Mr. Cantrell.

Mr. CANTRELL. Yes. I will just say that, once again, thank you for having this hearing. It is an important issue to us. It does directly lead to fraud in the Medicare program and other areas. We are looking forward to the time when the Social Security number is no longer on the card. It will take all of us at the table and throughout the U.S. to continue to protect this information. As was mentioned earlier, these systems that contain the Social Security numbers, even if it is not on the card, there is a treasure trove of data that is available if it is not properly secured, so I encourage us to continue to look to ways to properly secure this data.

The CHAIRMAN. Thank you.

Mr. Cavanaugh.

Mr. CAVANAUGH. Thank you. Again, I want to thank your leadership, this Committee's leadership in getting us the funding so we can all get to where we agree that we need to be, which is to get the numbers off the card, but to echo Mr. Cantrell's remarks, this

will be an important step in preventing fraud. It will not be the final step, and so, we look forward to working with you to make sure we have other ways to protect both the beneficiaries and the Trust Fund.

The CHAIRMAN. Just think, if we could recapture or cut in half that $27 billion that is lost to waste, fraud, and abuse because the Social Security number makes us so vulnerable to that kind of fraud, what good things we could do with that money, including shoring up the Social Security Disability Insurance Trust Fund, which is going to go broke next year if we do not act. It would also be very reassuring to America's seniors, since they rank identity theft so high in their lists of concerns.

I do appreciate your sincerity in recognizing the seriousness of this problem, but I would be remiss if I did not express the frustration of the 12 members of this Committee that have written to you with the slow pace, and I really urge you to look at an incremental approach, starting with new beneficiaries, where you would not have to swap out cards and there would not be the educational effort that you are concerned about, and there would not be the opening for the fraudsters who are going to call up the beneficiary and say, hey, we have got your new Medicare card and all we need is, which is what I fear is going to happen. We are going to have to have a really effective public outreach campaign to prevent more fraud from happening during that period, but surely, surely, you ought to be able to start by the beginning of next year, in my judgment, with the new beneficiaries that are coming in and giving them a new card-—their first card—with an identifier that is not the Social Security number. I really hope that you will work toward that goal.

Working together, I am convinced that we can solve this problem, but I do not want in the year 2019 to be calling CMS before this Committee and find out that we have done yet another study, or that we are having technical problems, or that we really have not made the progress that other departments have demonstrated can be made through a concerted effort.

I want to thank all of you for being here today and for your testimony, and again to apologize that it turned out to be a day—this is the life in the U.S. Senate—where we could not control all of the competing votes and briefings that were going on.

For that reason, I strongly suspect that many Committee members will be submitting additional questions to you for the record, and they will have until Friday, October 16th, to submit those questions for the record.

I want to thank you for your cooperation today. Let us get this problem solved.

This hearing is adjourned. Thank you.

[Whereupon, at 3:38 p.m., the Committee was adjourned.]

# APPENDIX

## Prepared Witness Statements

**STATEMENT OF**

**SEAN CAVANAUGH**

**DEPUTY ADMINISTRATOR AND DIRECTOR,**
**CENTER FOR MEDICARE,**
**CENTERS FOR MEDICARE & MEDICAID SERVICES**

**ON**

**PROTECTING SENIORS FROM IDENTITY THEFT: IS THE FEDERAL GOVERNMENT DOING ENOUGH?**

**BEFORE THE**
**U.S. SENATE SPECIAL COMMITTEE ON AGING**

**OCTOBER 7, 2015**

**Statement of Sean Cavanaugh on**
**Protecting Seniors From Identity Theft: Is The Federal Government Doing Enough?**
**Senate Special Committee on Aging**
**October 7, 2015**

Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for this opportunity to discuss the Centers for Medicare & Medicaid Services' (CMS') work to remove the Social Security Number (SSN) from beneficiaries' Medicare cards. This effort is an important step in protecting beneficiaries from becoming victims of identity theft. Identity theft disrupts lives, damages credit ratings, and can result in inaccuracies on medical records. Medicare fraud wastes taxpayer dollars, and CMS appreciates the Committee's focus on this important topic.

Under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), by April 2019, CMS will eliminate the use of beneficiaries' SSNs as the source of the primary identifier on Medicare cards. CMS has begun the process to redesign Medicare cards by removing the current SSN-based identifier and replacing it with a Medicare Beneficiary Identifier (MBI). For the first time, CMS will be able to terminate a Medicare number as soon as we confirm that is has been compromised and issue a new number to a beneficiary, similar to how credit card companies address stolen card numbers. Being able to immediately deactivate a compromised MBI will enable CMS to quickly respond and better prevent further misuse of a compromised number.

Transitioning to a new MBI will help Medicare beneficiaries better safeguard their personal information by reducing the exposure of their SSNs. This is a complex, multi-year effort that requires both coordination between Federal, state, and private-sector stakeholders as well as an extensive outreach and education program for Medicare beneficiaries, providers, and other stakeholders. CMS will continue our efforts to educate beneficiaries about the risks of medical identity theft, how they can protect their information, and prevent and detect fraud that stems from medical identity theft.

**History of Social Security Numbers Within Medicare**

From the creation of the Medicare program under the Social Security Act in 1965 until 1977, the Medicare program was administered by the Social Security Administration (SSA). While CMS is now responsible for the management of Medicare, SSA and CMS continue to rely on interrelated systems to coordinate both Social Security and Medicare eligibility. Medicare cards include a Health Insurance Claim Number (HICN) which is used as the beneficiary identification number for Medicare. Generally, the HICN is based upon a beneficiary's SSN, or in cases where a beneficiary's Medicare eligibility is based on the employment status and Medicare payroll tax contributions of another person, his or her spouse or parent's SSN. After determining Medicare eligibility, SSA transmits the SSN and beneficiary identification code (BIC) (the identifying suffix that follows the Medicare number) to CMS for entry into the CMS Enrollment Database, the data repository for individuals who are or have ever been enrolled in Medicare. CMS then issues the Medicare card with the HICN to the beneficiary. Often, when receiving care, the beneficiary shows the provider or supplier their Medicare card with the HICN, just as an individual with private insurance uses their insurance card. The provider or supplier then uses the Medicare card information to check eligibility and to bill Medicare, a process that involves multiple CMS systems.

CMS uses the HICN to identify beneficiaries in more than 75 CMS systems, and in CMS communications with other Federal partners. Likewise, providers are required by CMS to use the HICN identifier when they submit claims in order to receive payment for treatments, services, and supplies. CMS and its contractors' systems use the HICN to check for duplicate claims, apply claims and medical policy edits, authorize or deny payment of claims, issue Medicare Summary Notices (MSNs), and conduct printing and mailing operations.

**Replacing Health Insurance Claim Numbers with Medicare Beneficiary Identifiers**

The initiative to remove SSNs from Medicare cards by replacing HICNs with MBIs is a substantial undertaking. In April 2015, MACRA provided $320 million for this critical initiative. The replacement process will require coordinating with Federal, state, and private sector stakeholders; updating and modifying numerous internal IT systems; and conducting an extensive outreach and education campaign for beneficiaries, providers, and other stakeholders.

CMS is working to accomplish these tasks without disrupting payments to providers, business processes, or beneficiaries' access to care. Taking lessons learned from CMS' implementation of other large-scale, complex IT systems, CMS is developing a thoughtful and measured approach to assure a smooth transition from the first day of use of the MBI.

CMS anticipates that the changes brought about through the shift from HICNs to MBIs will affect more than 75 complex CMS systems, as well as 57 unique State and Territorial eligibility and enrollment and Federal partners' IT systems. For example, SSA and the Railroad Retirement Board (RRB) will need to modify their eligibility and enrollment systems, and the Medicare Administrative Contractors (MACs) and other business partners will need to modify systems to authorize coverage and process claims. Additionally, private insurers and states, including State Medicaid Agencies, will need to modify their systems to process crossover claims.

CMS has been meeting with SSA and RRB to discuss the strategy, timeline, and assumptions for removing the SSN from Medicare cards. CMS will also meet with states and private health plans to coordinate new processes for crossover claims. In addition, CMS has already started the process of procuring a systems integrator to coordinate this multi-faceted project.[1]

CMS will need to develop, test, and execute systems modifications in a way that ensures compatibility with the systems of states, insurers, providers, and every other entity that bills Medicare while avoiding disruption to payment and business processes and beneficiaries' access to care. Once system modifications are in place, issuing new Medicare cards will require an extensive and phased outreach and education program for an estimated 60 million[2] Medicare beneficiaries, as well as providers, private health plans, other insurers, clearinghouses, states, and other stakeholders. We will have a series of communications that will inform beneficiaries that they will be receiving a new card, instruct them on when and how the new card should be used, and inform them how to dispose of their old card. In order to prevent bad actors from taking advantage of potential confusion to gain access to personal information, it will be important to

[1] CMS Small Business Sources Sought, Solicitation Number 160626, https://www.fbo.gov/index?s=opportunity&mode=form&id=baa6a5c5f4d213295219629196f2bd44&tab=core&_cview=0

[2] https://www.cbo.gov/sites/default/files/cbofiles/attachments/44205-2015-03-Medicare.pdf

clearly communicate with our beneficiaries about the timing of and steps necessary to obtain a new card. Additionally, we will have a series of communications to inform Medicare providers of these changes and instruct them on how to use the new identifier to submit claims and other transactions. We must also ensure that private health plans, other insurers, and State Medicaid Agencies are instructed on how to use MBIs so that they can continue their coordination of benefits activities. CMS anticipates that communication activities will begin in January 2018 and continue through April 2019, allowing CMS to meet the deadline established in MACRA.

**Working with Beneficiaries to Prevent Medical Identity Theft**

The initiative to remove SSNs from Medicare cards will build upon efforts that CMS has already engaged in to protect against identity theft. CMS has already removed SSNs from many types of communications, including MSNs mailed to beneficiaries on a quarterly basis, and we have prohibited private Medicare health ( Medicare Advantage) and Prescription Drug (Part D) plans from using SSNs on enrollees' insurance cards (*e.g.*, insurance cards for Medicare Advantage, cost contract, and Part D enrollees).

Beneficiary involvement is a key component of all of CMS' anti-fraud efforts. Alert and vigilant beneficiaries, family members, and caregivers are some of our most valuable partners in stopping fraudulent activity. Information from beneficiaries and other parties helps us to quickly identify potentially fraudulent practices, stop payment to suspect providers and suppliers for inappropriate services or items, and prevent further abuses in the program. CMS has made it easier for beneficiaries to help us fight fraud, waste, and abuse. In 2013, CMS began sending redesigned MSNs,[3] the explanation of benefits for people with Medicare fee-for-service, to make it easier for beneficiaries to spot fraud or errors. The new MSNs include clearer language, descriptions and definitions, and have a dedicated section that tells beneficiaries how to spot potential fraud, waste, and abuse. Beneficiaries are encouraged to report fraud, waste, and abuse to 1-800-MEDICARE, and this is promoted in the re-designed MSN.

CMS engages in a variety of outreach efforts to inform beneficiaries about the risk of medical identity theft and to educate them on steps they can take to protect their personally identifiable

[3] http://blog.medicare.gov/2013/06/06/redesigned-with-you-in-mind-your-medicare-summary-notice/

information. Information is available online and in The Medicare & You handbook, which is distributed to all Medicare households each fall. These resources explain the importance of personal information and how it is used by Medicare; they also include instructions on contacting the appropriate authorities when Medicare fraud, including medical identity theft, is suspected. In these publications, Medicare beneficiaries are advised to take preventive action against identity theft, including:

- Guarding personal information such as Medicare identifiers and SSNs, and only sharing personal information with providers, plans, and suppliers approved by Medicare (a list of approved suppliers is available on Medicare.gov). Importantly, do not give personal information to anyone who calls or comes to the door uninvited, including individuals claiming to be conducting a health survey. Medicare and Medicaid do not send representatives to homes to sell products or services.
- Checking medical bills, MSNs, explanations of benefits, and credit reports for accuracy; use a calendar to record the receipt of services and compare this to Medicare statements.
- Being suspicious of anyone who offers free medical equipment or services; if it is free, they do not need a Medicare number. Do not accept offers of money or gifts for free medical care.
- Not letting anyone borrow or use a Medicare ID card or identity in exchange for goods or services; this is illegal.

CMS has also been partnering with the Administration for Community Living to lend support to the Senior Medicare Patrol (SMP) program, a volunteer-based national program that educates Medicare beneficiaries, their families, and caregivers to prevent, detect, and report Medicare fraud, waste and abuse. The SMP program empowers Medicare beneficiaries through increased awareness and understanding of health care programs and educates them on how to recognize and report fraud. During 2014, SMP program grantees' staff and more than 5,000 volunteers reached over 650,000 people with group education sessions and one-on-one counseling.[4] SMP projects also work to resolve beneficiary complaints of potential fraud in partnership with state and national fraud control and consumer protection entities, including Medicare contractors,

[4] http://www.smpresource.org/Handler.ashx?Item_ID=3A7D6D74-1D4F-4FA6-A8AE-2979022F185F

State Medicaid fraud control units, State attorneys general, the Department of Health and Human Services Office of Inspector General (HHS OIG), and the Federal Trade Commission (FTC).

**Addressing Identity Theft and Compromised Numbers**

We recognize that despite efforts to safeguard beneficiary information, medical identity theft can still occur. Identity theft complaints from Medicare beneficiaries are received from a number of sources such as calls from beneficiaries and their caregivers to 1-800-MEDICARE, the HHS OIG's Hotline (1-800-HHS-TIPS), our MACs, SMP volunteers, or CMS Regional Offices. CMS has protocols in place to take action when the Agency learns that a beneficiary's number has been compromised. First and foremost, a beneficiary can still receive needed medical care if they have been a victim of identity theft. When a Medicare beneficiary suspects that someone is using their SSN we refer them to the FTC's ID Theft Hotline and the Fraud Hotline of the HHS OIG to file a complaint. In addition, CMS tracks and triages complaints to determine whether the number appears to have been misused, and to ensure that the appropriate corrective actions are taken. If a HICN is compromised, CMS cannot currently issue a new HICN. Once CMS begins issuing MBIs, we will be able to terminate compromised MBIs and issue new beneficiary identification numbers to more immediately mitigate potential fraud.

Currently, if a HICN has been compromised, it is added to our Compromised Numbers Checklist (CNC) database. The CNC is a web-based system that allows direct entry and retrieval of compromised Medicare provider and beneficiary numbers by CMS and CMS contractors. The CNC includes compromised provider and beneficiary numbers obtained through fraud investigations and complaints from providers or beneficiaries. In addition, complaints of identity theft that come into the 1-800-MEDICARE Hotline and CMS contractors (such as Medicare Drug Integrity Contractors, Zone Program Integrity Contractors, or MACs) may be added to the database. For each number, the database includes a specific reason code describing why the number is considered compromised and categorizes the risk as low, medium, or high.

CMS uses the compromised numbers in the CNC database to inform sophisticated analytics through the Fraud Prevention System (FPS). The FPS is an advanced analytics system that identifies and prevents inappropriate payments in Medicare. Through this system, CMS and its

contractors use the CNC data, along with other external data, to identify aberrant and suspicious billing patterns or relationships. Based on the results, CMS focuses its investigative resources on the most egregious behavior. Through the investigations, CMS may provide education or take appropriate administrative action, including revoking a provider's billing privileges, implementing a payment suspension, implementing prepayment edits, requesting an overpayment, or referring the provider to law enforcement.

**Moving Forward**

Redesigning the Medicare card to remove the SSN-based identifier is a multifaceted initiative that will require complex IT modifications by numerous Federal and state agencies, as well as private partners. It also necessitates significant outreach and education among Medicare beneficiaries and providers. Given how much is at stake, CMS' objectives are to complete the transition to the new cards in a timely fashion that not only improves security, but also minimizes member confusion and disruption from denied claims or access to services. Thank you for your interest in our progress towards removing the SSN from Medicare cards. I look forward to working with the Committee on this important endeavor.

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

---

**Testimony Before the United States Senate**
**Special Committee on Aging**

---

***"Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?"***

Testimony of:
Gary Cantrell
Deputy Inspector General for Investigations

Office of Inspector General
Department of Health and Human Services

**October 7, 2015**
**2:00 pm**
**Location: Dirksen Senate Office Building, Room 562**

Testimony of: **Gary Cantrell**
Deputy Inspector General for Investigations
Office of Inspector General, U.S., Department of Health and Human Services

Good afternoon, Chairman Collins, Ranking Member McCaskill, and distinguished members of the Committee. I am Gary Cantrell, Deputy Inspector General for Investigations with the U.S. Department of Health and Human Services (HHS) – Office of Inspector General (OIG). I appreciate the opportunity to appear before you to discuss medical identity theft in Federal health care programs and our efforts to fight this threat.

Our mission at OIG is to protect the integrity of HHS programs as well as the health and welfare of program beneficiaries. A majority of OIG's resources go toward the oversight of Medicare and Medicaid programs that represent a significant part of the Federal budget and that affect this country's most vulnerable citizens. In a given year, the amount of work conducted in each category is set by the purpose limitations in OIG's appropriations.

OIG is a leader in the fight against Medicare fraud. We use data analytics to detect and investigate program fraud and to target our resources for maximum results. Our partnerships with other Government entities and the private sector are also invaluable to our enforcement successes. Medical identity theft represents a growing danger to patients and health care programs, including Medicare and Medicaid. We commend the Committee's efforts to draw much-needed attention to this type of fraud. Today's testimony discusses OIG's enforcement efforts to detect, prevent, and investigate health care fraud involving medical identity theft in Federal health care programs.

**OIG IS A LEADER IN THE FIGHT AGAINST MEDICARE FRAUD**

OIG advances our mission through a robust program of investigations, audits, evaluations, enforcement actions, and compliance efforts. In today's testimony, I focus on our law enforcement activities, led by my division, the Office of Investigations. We collaborate with our OIG colleagues, which include attorneys, evaluators, auditors, and data analytics experts. The Office of Investigations is the law enforcement component of OIG and investigates fraud and abuse against HHS programs. Our special agents have full law enforcement authority and affect a broad range of actions, including the execution of search warrants and arrests. We use traditional, as well as state-of-the art investigative techniques and innovative data analytics to fulfill our mission.

Our OIG investigations have produced record-setting results. During the last 3 fiscal years (FYs 2013-2015), OIG investigations have resulted in over $10.9 billion in investigative receivables (dollars ordered or agreed to be paid to government programs as a result of

criminal, civil, or administrative judgments or settlements); 2,856 criminal actions; 1,446 civil actions; and 11,343 program exclusions.

The return on investment for our work is significant. OIG, and our HHS and Department of Justice (DOJ) partners, have returned $7.70 for every $1 invested in the Health Care Fraud and Abuse Control Program (HCFAC).[1] HCFAC is OIG's largest funding source. Since HCFAC's inception in 1997, its activities have returned more than $27.8 billion to the Medicare Trust Funds. HCFAC's continued success confirms the soundness of a collaborative approach to identify and prosecute the most egregious instances of health care fraud, to prevent future fraud, and to protect program beneficiaries.

**MEDICAL IDENTITY THEFT POSES SERIOUS RISKS TO PATIENTS AND HEALTH CARE PROGRAMS**

Medical identity theft is the appropriation or misuse of a patient's or a provider's medical identifying information (such as a Medicare identification number) to fraudulently obtain or bill for medical care, prescription drugs, or supplies. It can affect beneficiaries or providers. Such theft can create patient safety risks and impose financial burdens on those affected. It can lead to erroneous entries in beneficiaries' medical histories and even lead to the wrong medical treatment. Medical identity theft may also lead to significant financial losses for the Medicare Trust Funds and taxpayers.[2] OIG has seen a variety of such fraud, as well as related schemes that go beyond the traditional boundaries of medical identity theft.

Medical identity theft includes the theft of Personally Identifiable Information (PII), such as Social Security numbers, dates of birth, and credit card and bank account information that are highly valued by identity thieves. It may also include Protected Health Information (PHI), such as health history, medical diagnoses, services rendered, or health care billing or payment information. We primarily see the theft of PII in our enforcement work, but whether the information compromised is PII or PHI, the theft of this sensitive information can result in significant financial loss, damaged credit scores, and costly legal problems. Of grave concern is the possibility that someone's PHI could be compromised and result in patient harm because of incorrect information in a personal medical record (either hardcopy or electronic). A false diagnosis, an inaccurate blood type, or even an incorrect medication included or omitted in an official medical record could result in serious patient harm. For the purposes of today's testimony, I will refer to the types of information involved in medical identity theft as sensitive information.

---

[1] Data from the *Health Care Fraud and Abuse Control Program FY 2014 Report*, available at http://oig.hhs.gov/publications/docs/hcfac/FY2014-hcfac.pdf.

[2] HHS-OIG report: *CMS Response to Breaches and Medical Identity Theft*, October 2012 (OEI-02-10-00040)

**MEDICAL IDENTITY THEFT CAN TAKE MANY FORMS**

Medical identity theft fraud is perpetrated by a broad range of bad actors – from health care providers to criminal enterprises. Health care providers who commit medical identity theft often rely on a relationship of trust with an unsuspecting patient. Health care providers can include physicians, nurses, pharmacists, ambulance drivers, and medical assistants. Health care providers and other non-provider employees in the health care industry pose a particular challenge because of their often unrestricted access to sensitive information. Also of concern is the number of Medicare and Medicaid beneficiaries who are either tricked into providing sensitive information, or at worst, are co-conspirators in the fraud scheme.

While each medical identity theft case is unique, these cases can generally be categorized into external and internal threats. External threats often include the involvement of con artists and professional identity thieves who target vulnerable seniors and program beneficiaries, often through social engineering. Of concern is the external threat posed by criminal enterprises. Internal threats include health care company owners, employees, physicians, non-physician practitioners, and patients who participate in a fraud scheme. Additional detail regarding these external and internal threats is discussed below.

**OIG IS DEDICATED TO FIGHTING HEALTH CARE FRAUD BY CRIMINAL ENTERPRISES, WHICH POSE SIGNIFICANT THREATS TO MEDICARE AND ITS BENEFICIARIES**

OIG dedicates significant resources to investigate health care fraud schemes perpetrated by both domestic and transnational organized criminal enterprises. Some transnational criminal enterprises recruit individuals from their countries of origin to execute illicit acts and shield the leaders from direct involvement in the execution of the schemes. Others target individuals from their country of origin as fraud victims because of a high level of trust and strong cultural ties. Health care fraud schemes by transnational criminal enterprises often involve the theft or sale of sensitive information, which is used to defraud Medicare and other health care programs.

We view complex health care fraud schemes perpetrated by criminal enterprises as a priority. These groups take a systematic, organized approach to committing fraud. Criminal enterprises have become a pervasive problem in fraud schemes involving home health, durable medical equipment (DME), prescription drugs, transportation, and medical clinic settings. Criminal enterprises may solicit persons to use as "straw" business owners for a sham corporation, or they may steal physician or other identities to bill Medicare and other health insurance carriers for false claims. They often hire recruiters to buy lists of patient names and identification numbers, or identify parties willing to participate in the fraud schemes. These groups pose a threat to the integrity of HHS programs because their primary

objective is to organize with the intent of stealing as much money from Federal health programs as quickly as possible. Two examples of criminal enterprises involved in medical identity theft schemes are included below.

In one case, a transnational criminal organization established a "ghost" medical clinic using stolen information from a physician in the local area. Members of the conspiracy enrolled the clinic in Medicare, established bank accounts, linked the bank accounts to a fictitious address (a mailbox store), registered the clinic with the Secretary of State, and began to bill Medicare. All together, the "ghost" clinic billed Medicare over $1 million, with Medicare paying about $350,000 worth of claims. The money that was paid was laundered through out-of-state banks and shell businesses by members of the conspiracy. The supervisor of the conspiracy was sentenced to 57 months in prison and others have been indicted.

In another identity theft case, a mastermind was sentenced to 37 months in prison for his involvement in an Armenian-American organized criminal enterprise engaged in a wide range of fraudulent activity, including the operation of a $100 million Medicare billing ring. In this national, multiagency investigation, a large-scale law enforcement operation was conducted that involved the arrest of over 50 individuals in multiple states. At the time, it was the largest Medicare fraud scheme ever perpetrated by a single criminal enterprise and charged by DOJ. According to the indictment, the defendants stole the identities of numerous physicians and thousands of Medicare beneficiaries and operated at least 118 different phony clinics in 25 states for the purposes of submitting Medicare claims for reimbursement.

**OIG HAS ALSO UNCOVERED INSIDER THREATS INVOLVING PROVIDER AND PATIENT CO-CONSPIRATORS**

Those who work in the health profession could have access to significant amounts of sensitive information. The following examples are illustrative of our work in this area.

*In Some Cases, Health Care Company Owners Mastermind Fraud Schemes*
Health care company owners are a particular problem in medical identity theft schemes because they may mastermind a fraud scheme without the knowledge of the company employees or patients. In one case, OIG investigated a home health agency owner who paid illegal kickbacks to patient recruiters to obtain the information of Medicare beneficiaries; this information was used to submit over $12 million in false claims to Medicare for home health services that were not medically necessary or never provided. The owner also created fictitious patient files in an attempt to deceive a Medicare auditor and make it appear as though home health services were provided and medically necessary. The defendant was sentenced to 80 months in prison and ordered to pay $14.1 million in restitution.

In another matter, OIG investigated a fraud case in which a hospice owner paid an individual large amounts of money to illegally obtain names and other sensitive information for multiple Medicare beneficiaries. The hospice owner used that illegally obtained beneficiary information to fraudulently bill Medicare for millions of dollars of hospice services that were never provided or were for beneficiaries who were not eligible for those services. The hospice owner was sentenced to 70 months imprisonment and 3 years of supervised release. The individual who sold the sensitive information for illegal use was sentenced to 14 months imprisonment and 3 years of supervised release.

*Unscrupulous Health Care Employees Present Fraud Vulnerabilities*

Health care company employees present a unique challenge to the problem of medical identity theft because of their knowledge about program vulnerabilities and level of access to sensitive information. In a recent Medicare Fraud Strike Force case, a visiting physician group billed Medicare over $4 million using deceased patient information for home health services. The medical biller, office administrator, and medical director also billed for services that were never provided, using information from former medical professionals without their knowledge. The company's administrator and biller forged physician signatures on medical documents, and directed physicians to create false documentation to support billing for services that were never rendered. The medical biller was sentenced to 45 months in prison for her role in the scheme, while the office administrator was sentenced to more than 7 years in prison. The medical director pleaded guilty and is awaiting sentencing.

*Physicians and Other Health Care Providers Have Also Committed Identity Theft and Fraud*

Medical identity theft is not limited to health care employees and can include clinicians, such as physicians and nurses. For example, OIG jointly investigated a case in which a physician violated his agreement with the United States to be excluded from all Federal health care programs for 10 years. After his exclusion, the physician developed a sophisticated scheme to defraud Medicare and Medicaid and to continue collecting Federal reimbursement. This scheme involved shell owners, forged signatures, and theft of the identity of another doctor to fraudulently bill Medicare and Medicaid for laboratory services. The physician was convicted of multiple charges related to health care fraud, bankruptcy fraud, filing false tax returns, and aggravated identity theft. He was sentenced to over 8 years in prison and 3 years of supervised release, was fined over $2.6 million and ordered to pay restitution of over $260,000. He was also ordered to forfeit over $1 million.

OIG has investigated numerous cases involving nonphysician health care practitioners who commit medical identity theft. In one case, OIG investigated a pharmacy chain owner who engaged in a health care fraud scheme by submitting false claims for prescription refills. The pharmacy owner billed Medicare and Medicaid for prescription refills when the beneficiaries had not requested refills and indeed did not receive the refills. The medications targeted for these refills were often expensive HIV and cancer medications intended for very

ill customers. The pharmacy owner, along with co-conspirators, falsely used the names and sensitive information of hundreds of beneficiaries to conduct this fraud. The defendant was convicted of health care fraud and aggravated identity theft.

*Although Program Beneficiaries Are Typically Victims of Medical Identity Theft, in Some Cases They Are Co-Conspirators*

Patient co-conspirators can be a significant problem in medical identity theft schemes by selling their sensitive information (usually their Medicare or Medicaid numbers) to identity thieves for a small kickback. OIG continues to investigate cases in which patients sell their sensitive information and receive medically unnecessary (often sham) services in exchange for a kickback.

One example involving prescription drug fraud involved a physician who wrote illegal prescriptions for complicit beneficiaries, who were transported by the vanload to his practice. There they received medically unnecessary prescriptions for oxycodone-based products. The pseudo-patients provided their Medicare, Medicaid, and private insurance information that was used to pay for the prescriptions, then passed more than 700,000 pills to 6 different drug trafficking organizations. The physician, along with 61 of his associates, received a combined 253 years in prison. The physician himself received 20 years and was ordered to forfeit $10 million.

In one high-profile case, an OIG investigation into a medical clinic unraveled a $20 million fraud scheme in which thousands of anti-psychotic medications were fraudulently prescribed, using stolen Medicare beneficiary identities and recruited homeless veterans. The clinic owner conspired with her mother-in-law to fill the fraudulent prescriptions at various pharmacies. Once the drugs were filled, the clinic purchased the prescriptions from recruited veterans being treated for drug addiction and schizophrenia. After purchasing the drugs from beneficiary co-conspirators, the clinic diverted the drugs to the black market, where they were sold to other pharmacies and rebilled to health care programs. To date, 16 defendants have been convicted for their roles in this scheme. The clinic owner has pleaded guilty to conspiracy to commit health care fraud and identity theft and has been sentenced to 8 years for overseeing the conspiracy.

## OIG IS LEVERAGING A RANGE OF OPPORTUNITIES TO COMBAT FRAUD INVOLVING MEDICAL IDENTITY THEFT

*Data Analytics Support OIG Fraud Identification and Investigation*

OIG is a front-runner in the use of data analytics to detect and investigate health care fraud. We use innovative analytic methods to analyze billions of records and data points to identify trends that may indicate fraud, geographical hot spots, emerging schemes, and individual providers of concern. At the macro level, we analyze data patterns to assess fraud risks

across a spectrum of services and geographic areas to prioritize and deploy our resources. At the micro level, we use data analytics, including near-real-time data, to identify fraud suspects and conduct our investigations efficiently and effectively.

*Medicare Fraud Strike Forces Exemplify Enforcement Success*

The remarkable success of the Medicare Fraud Strike Force (Strike Force) showcases the effectiveness of our use of data analytics to detect and investigate health care fraud, including schemes that involve medical identity theft. The Strike Force effort began in March 2007, and in 2009 HHS and DOJ announced the formal creation of the Health Care Fraud Prevention and Enforcement Action Team, a joint agency initiative known as HEAT. A key component of HEAT is the Strike Force, which harnesses the efforts of OIG and DOJ, including headquarters, Offices of U.S. Attorneys, and the Federal Bureau of Investigation, along with State and local law enforcement, to fight Medicare fraud in geographic hot spots. The Strike Force teams use near-real-time data to pinpoint fraud hot spots and aberrant billing as it occurs. This coordinated and data-driven approach to identifying, investigating, and prosecuting fraud has produced record-breaking results. Since its inception in March 2007, the Strike Force has charged over 2,300 defendants who collectively have billed the Medicare program over $7 billion.

HEAT actions have led to a 75 percent increase in individuals charged with criminal health care fraud during the initial stages, and the program has maintained significant enforcement success throughout its history. Through HEAT, we have expanded Strike Force teams to operate in nine locations: Miami, Florida; Detroit, Michigan; southern Texas; Los Angeles, California; Tampa, Florida; Brooklyn, New York; southern Louisiana; Chicago, Illinois; and Dallas, Texas.

In a recent example, a national Strike Force operation in June 2015 resulted in charges against 243 individuals, including 46 doctors, nurses, and other licensed medical professionals, for their alleged participation in multiple Medicare and Medicaid fraud schemes involving about $712 million in false billings. The defendants were charged with various health care fraud-related crimes, including conspiracy to commit health care fraud, violations of the anti-kickback statutes, money laundering and aggravated identity theft. The charges were based on a variety of alleged fraud schemes involving various medical treatments and services, including home health care, psychotherapy, physical and occupational therapy, DME, and pharmacy fraud. This coordinated takedown was the largest in Strike Force history, both in terms of the number of defendants charged and loss amount. The cases are currently being investigated and prosecuted by Strike Force teams.

*OIG Is Maximizing Its Fraud Fighting Impact Through External Partnerships*

In addition to internal collaboration, OIG continuously engages with external stakeholders to enhance the relevance and impact of our work to combat health care fraud, as demonstrated

by our leadership in the Healthcare Fraud Prevention Partnership (HFPP)[3], our association with the National Health Care Anti-Fraud Association (NHCAA), and our support to the Senior Medicare Patrol (SMP).

The HFPP is a groundbreaking partnership between the Federal and private sectors to share data and information for the purposes of detecting and combating fraud, waste, and abuse in health care. The HFPP was created as a voluntary public-private partnership, between the Federal Government, State officials, private health insurance organizations, and health care antifraud associations. The NHCAA is the leading national nonprofit organization focused exclusively on combating health care fraud and abuse.[4] The NHCAA mission is to protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution, and prevention of health care fraud and abuse. Both organizations are engaged in efforts to combat the problem of medical identity theft.

OIG, through OI, has worked collaboratively with the SMP[5] to combat medical identity theft. In conjunction with the SMP, OI agents conduct regular presentations designed to educate Medicare and Medicaid beneficiaries on the threat of medical identity theft, and how to protect their sensitive information.

*Consumer Education Efforts Are a Key Tool for Preventing Fraud*

While data-driven efforts and our external partnerships are invaluable to our enforcement successes, we are not focused solely on enforcement. The best way to combat fraud is by preventing it in the first place, and OIG's oversight efforts support all aspects of program integrity. We strive to cultivate a culture of compliance in the industry through various efforts, including education and guidance. Robust oversight of medical identity theft goes beyond enforcement efforts, and the need to educate providers and consumers (those who could be targeted as victims or co-conspirators) is a critical part of the solution.

OIG conducts a wide variety of consumer education efforts, including offering multiple resources on our public web site at http://oig.hhs.gov/fraud/medical-id-theft/. Our resources include a medical identity theft brochure that is available in an easy-to-read printable format and translated into multiple languages. OIG has also made a significant effort to highlight the problem of medical identity theft through media outreach, including through national television appearances on shows, such as *Good Morning America*, and in widely read journals such as the New England Journal of Medicine and publications such as *USA Today* and the *Wall Street Journal*.

---

[3] For more information on HFPP, visit: http://hfpp.cms.gov/.
[4] For more information on NHCAA, visit: http://www.nhcaa.org/.
[5] For more information on SMP, visit http://www.smpresource.org/.

*Removal of SSNs from Medicare Cards Is an Important Step Toward Preventing Medical Identity Theft*

Mitigating the problem of medical identity theft requires an "all hands on deck" approach. We want to thank Congress for its effort to prevent medical identity theft. Because of the Members of this Committee and Congress in passing the CHIP Reauthorization Act of 2015, the removal of Social Security numbers from Medicare cards is now underway. This is an important first step in protecting Medicare beneficiaries' sensitive information, and we thank the Members of this Committee for the attention they continue to place on this important issue.

**CONCLUSION**

OIG is committed to our continuing oversight of HHS programs and protecting them and their beneficiaries from fraud, waste, and abuse. We will continue to leverage our analytic, investigative, and oversight tools, as well as our partnerships within the law enforcement and program integrity communities, to maximize our efforts. We will continue our enforcement efforts to detect, investigate, and prevent medical identity theft in the Federal health care programs, and will remain vigilant to emerging trends, such as the growing threat of cyber breaches affecting our programs.

We would like to express our appreciation to Congress for its sustained commitment toward our mission and appreciate the Committee's interest in the vital issue of protecting Medicare and other HHS programs and their beneficiaries from fraud. This concludes my testimony. I would be happy to answer your questions. Thank you.

# Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?

Testimony of Betty Balderston
Statewide Coordinator for the Maine Senior Medicare Patrol
Legal Services for the Elderly

Before the Special Committee on Aging
United States Senate

October 7, 2015

Chairman Collins, Ranking Member McCaskill, and Members of the Committee, I am Betty Balderston, Statewide Coordinator for the Maine Senior Medicare Patrol (SMP) at Legal Services for the Elderly. I am honored to be here today to share information on how the SMP programs in Maine and across the country provide outreach, counseling, education and assistance to Medicare beneficiaries, their families and their caregivers, empowering them to prevent Medicare errors, fraud and abuse, including Medical Identity Theft.

According to the August 21, 2015 Memorandum Report: Performance Data for the Senior Medicare Patrol Projects from the Office of Inspector General, in 2014 the 53 SMP projects nationwide had 5,294 active volunteers, conducted 14,692 group education sessions and 202,862 one-on-one counseling sessions. As a result of this outreach, education and counseling, the OIG reported that the SMP projects achieved $942,159 in Medicare and Medicaid recoveries, savings and cost avoidance. The report emphasized that the SMP projects may not be receiving full credit for savings attributable to their work, since it is not always possible to track referrals to Medicare contractors or law enforcement from beneficiaries who have learned to detect fraud, waste, and abuse from the projects. In addition, the report states that the projects were unable to track the substantial savings derived from a sentinel effect whereby fraud and errors are reduced by Medicare beneficiaries' scrutiny of their bills.

In partnership with the Maine Department of Health and Human Services-Office of Aging and Disability Services (OADS), Legal Services for the Elderly (LSE) and

Maine's Area Agencies on Aging (AAAs), the Maine SMP recruits, trains, manages and supports over 80 volunteers statewide, most of them seniors themselves. These volunteers provide presentations on a variety of Medicare issues that include information about benefits, costs and how Mainers can protect themselves from fraud and scams. Since the Maine SMP works in conjunction with the Maine State Health Insurance Assistance Program (SHIP), volunteers also provide one-on-one counseling sessions where Mainers receive information on Medicare benefits, costs, and programs that can help pay for costs, as well as information on the importance of reading Medicare statements and reporting any issues with those statements, such as Medicare paying for services and/or supplies that were never received. The Maine SMP also serves as a resource for Medicare beneficiaries, their families and caregivers for assistance with billing issues, as well as reporting possible healthcare fraud and other types of scams to the appropriate State and Federal agencies. Since Maine is a large, rural state, the SMP/SHIP programs have a long history of working with a variety of local, regional and national partners and collaborators to meet the needs of Mainers statewide. In addition to OADS, LSE and the AAAs, partnerships also include the Administration for Community Living (ACL), the Centers for Medicare and Medicaid Services (CMS), the Office of Inspector General (OIG), the Maine Attorney General's Office, AARP, the Long-Term Care Ombudsman Program, the Maine Resident Service Coordinators Association, state and local law enforcement, and others.

Although Maine does not have a high rate of healthcare fraud, we have received complaints related to Medical Identity Theft. In January 2013, at the request of the Maine SMP, the Maine Attorney General's Office issued a Consumer Alert warning consumers about recent reports of calls from individuals claiming to represent Medicare (see attached). The callers claimed that Medicare was issuing new Medicare cards and asked for the consumer's Medicare number, the name of their financial institution and their financial routing and account numbers. The Consumer Alert advised anyone who provided this information to review their Medicare statements carefully for the next year and to contact 1-800-Medicare immediately if anything questionable appeared on their Medicare statements. Mainers were also instructed to notify their financial institution

about the possibility of their account being compromised. In the alert, Attorney General Janet Mills was quoted as saying "Mainers can protect themselves by never giving any personal information to anyone over the phone." Since Congress ordered Social Security numbers be removed from Medicare cards, these types of calls are continuing.

Similar scams have been reported by SMP programs in other states. According to the SMP National Resource Center, shortly after the Affordable Care Act was signed, the Missouri SMP reported that a man claiming to represent Medicare visited senior housing facilities in St. Charles, claiming Medicare beneficiaries needed to replace their Medicare plans with an "Obamacare" plan due to healthcare reform. In July of this year, the California SMP reported that a Medicare beneficiary received a call from someone claiming to be from Medicare who wanted to set up a home visit. The beneficiary provided her name, address, telephone number and Medicare number. Since no one showed up for this scheduled home visit, the beneficiary believed that her personal information had been stolen.

These are just a few examples of the scams that are perpetrated against Medicare beneficiaries across this country every day. On behalf of the SMPs nationwide, I applaud the efforts of Congress to eliminate the use of Social Security numbers on Medicare cards. This change will help address the issue of Medical Identity Theft, as well as Identity Theft. However, our work is not finished. Scam artists are always ready to take advantage of people in every state in this country, especially vulnerable seniors and people with disabilities. They are experts at gaining trust and stealing money and benefits from unsuspecting victims. The SMPs are the front-line, boots-on-the-ground programs that provide outreach, education, counseling and assistance to individuals every day. Our volunteer programs work, with seniors helping seniors, every single day, to help some of our most vulnerable citizens remain safe and to protect their identities. Over the next four years, as CMS continues their work of transitioning to new Medicare cards, the SMP programs nationwide will continue our work, providing education about Medical Identity Theft to Medicare beneficiaries, their families and caregivers, empowering them to protect their identities and to safeguard the Medicare program.

By working together, we *are* making a difference in the lives of seniors and people with disabilities nationwide, empowering them to protect themselves against fraud and scams, assisting them when their personal information has been compromised and educating them about Medicare benefits and costs. With 10,000 baby boomers aging into Medicare every day, our work is more important than ever before, helping the Medicare program to be sustainable for the future. We look forward to ongoing support from Congress, the OIG, CMS and other partners as we continue our mission to Protect, Detect and Report health care fraud.

Thank you, again, for the opportunity to provide a brief glimpse of the important work of the Senior Medicare Patrol Programs. I would be happy to answer any questions you may have.

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown Law

Hearing on

"Protecting Seniors from Identity Theft:
Is the Federal Government Doing Enough?"

Before the

U.S. Senate Special Committee on Aging

October 7, 2015
562 Dirksen Senate Office Building
Washington, DC

## I. Introduction

Chairman Collins and Members of the Senate Committee, thank you for the opportunity to testify today regarding the use of SSNs on Medicare cards and the risks facing senior citizens in the United States. My name is Marc Rotenberg, and I am President of the Electronic Privacy Information Center ("EPIC"). I also teach Information Privacy Law at Georgetown Law. I am a former chair of the ABA Committee on Privacy and Information Security and the coauthor of a forthcoming casebook on privacy law.[1]

EPIC is a non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has participated in the leading cases involving the privacy of the Social Security Number ("SSN") and has frequently testified in Congress about the need to establish privacy safeguards for the SSN to prevent the misuse of personal information.[2] EPIC also maintains an archive of information about the SSN online.[3]

We appreciate the Special Committee's interest in SSN privacy issues. It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater risk to personal

---

[1] ANITA L. ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY (WEST 2016). *See also,* MARC ROTENBERG, JULIA HORWITZ, & JERAMIE SCOTT, EDS. PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS (THE NEW PRESS 2015).

[2] *See, e.g., Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993) ("Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling"); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994) ("the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs"); Marc Rotenberg, Exec. Dir., EPIC, *Testimony at a Hearing on Protecting the Privacy of the Social Security Number from Identity Theft, Before the H. Ways & Means Subcom. on Social Security*, 110th Cong. (June 21, 2007), available at https://epic.org/privacy/ssn/idtheft_test_062107.pdf; Marc Rotenberg, Exec. Dir., EPIC, *Testimony at a Joint Hearing on Social Security Numbers & Identity Theft, Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001), available at http://www.epic.org/privacy/ssn/testimony_11_08_2001.html.

[3] Social Security Numbers, EPIC, https://epic.org/privacy/ssn/.

privacy. The use of the number for identification poses an ongoing risk of identity theft, financial fraud, and other forms of crime.

## II. Social Security Number History and the Importance of Limiting SSN Collection

The Social Security Number is the classic example of "mission creep," a particular designed for a specific, limited purpose has been transformed for additional, unintended purposes, often with disastrous results. The pervasiveness of the SSN and its use to both identify and authenticate individuals threatens privacy and financial security.

These risks associated with the expanded use of the SSN and identification cards underscore the importance of the hearing today. But this problem has been well known to Congress for many years.

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the SSN that show a striking resemblance to the problems we face today. Although the term "identify theft" was not yet in use, a detailed report, prepared by Willis Ware and leading technical experts and legal scholars, made clear the risks from the expanded use of the Social Security Number.[4]

The Report of the Ware Commission provided the cornerstone of the landmark Privacy Act of 1974. In enacting the Privacy Act, Congress recognized the dangers of widespread use of the SSN as a universal identifier, and included provisions to limit its use. The Privacy Act makes it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN. Section 7 of the Privacy Act specifically provides that any agency requesting that an individual disclose

---

[4] Department of Health, Education, and Welfare (HEW), *Records Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973) (Ware Commission report), available at https://www.epic.org/privacy/hew1973report/

his or her SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it."[5] This section reflects a presumption that the Social Security number should not be used for recordkeeping purposes unrelated to Social Security and taxation. In its report supporting adoption of Section 7, the Senate Committee stated that the widespread use of the SSN as a universal identifier in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation."[6] Since passage of the Privacy Act, concern about SSN confidentiality and misuse has become even more compelling.

It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater risk to personal privacy. We have urged the Congress to implement SSN privacy protections for over two decades, beginning in 1991 when I first testified before a House Committee at a hearing on the "Use of Social Security Number as a National Identifier."[7] The U.S. Government Accountability Office has urged Congress to remove SSNs from government documents since 2004.[8] In 2006, the growing misuse of the SSN and associated identity theft risks prompted President George W. Bush to establish an Identity Theft Taskforce. In a 2008 audit, the Inspector General for the Social Security

---

[5] Privacy Act of 1974, 5 U.S.C. § 552 (a) (2006).
[6] S.Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6943.
[7] Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991). republished Marc Rotenberg, "The Use of the Social Security Number as a National Identifier," *Computers & Society*, vol. 22, nos. 2, 3, 4 (October 1991).
[8] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-768T, SOCIAL SECURITY NUMBERS: USE IS WIDESPREAD AND PROTECTIONS VARY (2004).

Administration recommended swift removal of SSNs from Medicaid cards, supported by the following observation:

> Despite the increasing threat of identity theft, CMS continued to display SSNs on identification cards it issued to Medicare beneficiaries. Displaying such information on Medicare cards unnecessarily places millions of individuals at-risk for identity theft. This is particularly troubling because CMS instructs individuals, many of whom are elderly, to carry their Medicare card with them when away from home. We do not believe a Federal agency should place more value on convenience than the security of its beneficiaries' personal information.[9]

The SSN is central to identity theft in the United States. In 2014, 17.6 million U.S. residents experienced identity theft.[10] Elderly Americans are most at risk of identity theft and the problem is getting worse. According to the U.S. Department of Justice, "[m]ore persons age 65 or older were identity theft victims in 2014 (2.6 million) than in 2012 (2.1 million). The number of identity theft victims in all other age groups measured did not significantly change from 2012 to 2014."[11] According to the FTC's most recent Consumer Sentinel Network (CSN) Data Book, 39% of identity theft victims in 2014 were age 50 or older.[12]

Increasing data breaches in the healthcare industry compound the threat to seniors posed by the use of SSNs on Medicare cards. According to one 2015 study, 91 percent of healthcare organizations had experienced a data breach in the past twenty four months,

---

[9] U.S. SOC. SEC. ADMIN., OFFICE OF THE INSPECTOR GEN., A-08-08-18026, REMOVING SOCIAL SECURITY NUMBERS FROM MEDICARE CARDS (2008), http://oig.ssa.gov/sites/default/files/audit/full/html/A-08-08-18026.html.

[10] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, 17.6 MILLION U.S. RESIDENTS EXPERIENCED IDENTITY THEFT IN 2014 (Sept. 27, 2015), http://www.bjs.gov/content/pub/press/vit14pr.cfm.

[11] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ 248991, VICTIMS OF IDENTITY THEFT, 2014 3 (2014), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[12] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY – DECEMBER 2014 14 (2015), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

and 40 percent has more than five data breaches during that time period.[13] Another study found that 42.5% of all data breaches in 2014 occurred in this field, outpacing breaches in all other sectors. A third study warns of the persistent and growing threat of healthcare breaches.[14]

Given the rising frequency of healthcare data breaches, the use of SSNs on Medicare cards places an already vulnerable population at even greater risk for identity theft. In addition, the crime of medical identity theft – when someone uses another individual's identity to obtain medical goods and services – can cause significant harm to victims.[15]

The need to find a solution to the problem of the widespread use of the SSN is critical.

## III. Solutions to Prevent the Misuse of SSNs and Identity Theft Risks

Fortunately, CMS does not need to look far to find a model for removing and replacing SSNs on Medicare cards. The U.S. Department of Defense has engaged in similar efforts over the past several years. According to DOD's published materials on the SSN Reduction Plan,

> In response to an increasing awareness of the growing need to protect the safety of Service members and their families' identity information, the Department of Defense (DoD) has begun to eliminate the Social Security Numbers (SSN) from DoD identification (ID) cards. In support of this

---

[13] The Ponemon Institute, *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data* (May 2015), https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data.

[14] Experian, *2015 Second Annual Data Breach Industry Forecast* 2 (2015), https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182

[15] *Medical Identity Theft*, WORLD PRIVACY FORUM, https://www.worldprivacyforum.org/category/med-id-theft/ (last visited Oct. 5, 2015).

initiative, a three-phased plan for the removal of the SSN on all DoD ID cards was announced.[16]

The DoD stopped printing SSNs on all DoD ID cards as of June 2011. SSNs are being replaced with DoD ID Numbers on all ID cards, and DoD Benefits Numbers on cards that provide healthcare benefits. The U.S. Department of Veterans Affairs also introduced new Veterans Health Identification Cards in 2014 that removed SSNs from the cards' magnetic strips and barcodes.[17]

Recognizing the huge risk of printing SSNs on identification cards, numerous states have already required private insurers to eliminate the practice. Arizona,[18] Colorado,[19] Georgia,[20] Hawaii,[21] Illinois,[22] New Jersey,[23] North Carolina,[24] Texas,[25] Utah,[26] Virginia,[27] and Washington[28] all have laws prohibiting the printing of an individual's SSN on his or her insurance card. Other state laws limit the use of SSNs in higher education,[29] by private businesses,[30] by state agencies,[31] and financial

---

[16] Def. Human Res. Activity, Dep't of Def., *Removal of the Social Security Number (SSN) From DoD ID Cards*, http://www.cac.mil/docs/SSNReductionUpdate_201409.pdf (last visited Oct. 5, 2015).
[17] Hans Petersen, *New ID Cards for Vets Enrolled in VA Health Care*, U.S. DEP'T OF VETERANS AFFAIRS (Feb. 24, 2014) http://www.va.gov/health/newsfeatures/2014/february/new-id-cards-for-vets-enrolled-in-va-health-care.asp.
[18] Ariz. Rev. Stat. § sec. 44-1373.
[19] Colo. Rev. Stat. § 10-3-129.
[20] Ga. Code Ann. § 33-24-57.1.
[21] Haw. Rev. Stat. § 487J-2.
[22] 815 Ill. Comp. Stat. § 505/2QQ.
[23] N.J. Stat. Ann. C.56:8-164.
[24] N.C. Gen. Stat. sec 75-62.
[25] Tex. Bus. & Com. Code § 35.58.
[26] Utah Code § 31A 21-110.
[27] Va. Code sec 59.1-443.2.
[28] Wash. Rev. Code Ann. sec 48.43.022.
[29] *See e.g.* N.Y. Educ. Code sec. 2-b; W. Va. Code Ann. sec. 18-2-5f; Ariz. Rev. Stat. Sec. 15-1823.
[30] *See e.g.* R.I. Gen. Laws 6-13-17.
[31] *See e.g.* Ala. Code sec. 41-13-6; Cal. Civ. Code sec. 1798.85.

institutions.[32] In 2004, Congress passed legislation prohibiting the display of SSNs on state drivers' licenses.[33]

Many private organizations that provide comprehensive health services do not use the SSN as a patient identifier. For example, the Harvard Community Health Plan, with over half a million subscribers, uses a separate number for patient identification in its automated records system. The SSN is collected for administrative use but is not publicly disclosed. Nearly a decade ago, the Blue Cross Blue Shield Association mandated that its members replace SSNs with Subscriber ID numbers by January 1, 2006.[34] Today, most private health insurance companies have abandoned the use of SSNs as patient identifiers in light of identity theft concerns.[35]

To safeguard against privacy threats that SSNs present, universities have routinely adopted policies prohibiting the use of SSNs for student ID numbers and cards. For example, Georgetown University's "Policy on the Use, Collection, and Retention of Social Security Numbers by Georgetown University" states:

> The University will take steps necessary and appropriate to guard the confidentiality of SSNs and to eliminate or minimize its exposure to liability and other harms arising from unauthorized access to, or data breaches involving, SSNs. No use of the SSN, or any part of the SSN, is permitted except as authorized under this Policy. SSNs are highly confidential information and must be handled in accordance with applicable law pursuant to this policy.[36]

---

[32] *See e.g.* Fla. Stat. Ann. sec 659.062; Mass. Gen. Laws. Ann. ch. 167B, sec. 14.
[33] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 § 7214, 118 Stat. 3638, 3832 (codified at 42 U.S.C. § 405(c)(2)(C)(vi)(II) (2012).
[34] *Empire Physician Sourcebook*, EMPIRE BLUE CROSS BLUE SHIELD, https://www.empireblue.com/provider/noapplication/f4/s2/t0/pw_e209016.pdf?refer=ehpprovider (last visited Oct. 5, 2015).
[35] Robert Pear, *New Cards for Medicare Recipients Will Omit Social Security Numbers*, N.Y. TIMES (Apr. 20, 2015), http://www.nytimes.com/2015/04/21/us/new-law-to-strip-social-security-numbers-from-medicare-cards.html?_r=0.
[36] Georgetown University Information Security Office, *Policy on the Use, Collection, and Retention of Social Security Numbers by Georgetown University*, https://security.georgetown.edu/technology-policies/use-collection-retention-policy.

The policy holds:

> **SSNs, or any part of the SSN, are NOT permitted:**
> 1. As the primary record key, or sort key, in any University database or other business system or operation
> 2. As an identifier among University departments or with external University affiliates
> 3. To be transferred by the University to external entities (i.e. benefits providers)[37]

In lieu of SSNs, Georgetown uses the "Georgetown University ID, a "nine digit number beginning with the numeral "8" listed on each person's GU identification card, [which] may be used to identify, track, and provide services to individuals for all University electronic and paper data systems and processes."[38]

Georgetown's policy is partially adapted from Northwestern's SSNs policy, which states in relevant part:

> 1. [T]he University does not permit the use of a SSN as the primary identifier for any person or entity in any system, except where the SSN is required or permitted by law, and permitted by University policy. . . .
>
> 4. Except where the SSN is required by law, the University ID (EMPLID) replaces use of the SSN and will be used in all future electronic and paper data systems and processes to identify, track, and service individuals associated with the University. The University ID will be permanently and uniquely associated with the individual to whom it is originally assigned.[39]

---

[37] *Id.*
[38] *Id.*
[39] Northwestern University Information Technology, *Information Security Policy and Standards: Secure Handling of Social Security Numbers*, http://www.it.northwestern.edu/policies/SSN_policy.html. *See also* Virginia Tech Office of the University Registrar, *Student Identification Numbers*, https://www.registrar.vt.edu/faculty/privacy/student-numbers.html; University of Pittsburgh, *Use and Management of Social Security Numbers and University Primary ID ("UPI") Numbers*, https://www.cfo.pitt.edu/policies/policy/10/10-02-08.html; University of New Mexico, *The Pathfinder – UNM Student Handbook*, "Student ID Number and Social Security Numbers," https://pathfinder.unm.edu/common/policies/student-id-number-policy.html.

EPIC favors technological innovation that enables the development of context-dependent identifiers. For the purpose of Medicare cards, a context-dependent identifier would be a specific number assigned to an individual for the specific purpose of Medicare patient identification. An example of this is the Medical Identification Number used in Canada. This would be conceptually similar to a student ID number, driver's license number, bank account number, utility bill number, the list goes on.[40] Rather than using the SSN to identify and authenticate an individual across these various contexts, individuals would be assigned separate numbers depending on the context. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number gets compromised, all of the numbers are not spoiled and identity thieves cannot access all of your accounts. All of your accounts can become compartmentalized, enhancing their security.

## IV. Conclusion

Given the growing risk of identity theft coupled to the SSN and the fact that other federal agencies have already removed the SSN from identity cards, there is simply no excuse for further delay by CMS. We urge the committee to ensure that the problem is addressed before the elderly in America face the ever-greater risk of financial fraud and medical fraud.

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

---

[40] Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991).

## Questions for the Record

**U.S. Senate Special Committee on Aging**
**"Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?"**
**October 7, 2015**
**Questions for the Record**
**Mr. Sean Cavanaugh**

**Senator Claire McCaskill**

**Question:**

According to GAO, CMS has several recommendations from both GAO's 2012 and 2013 reports on CMS' Need to Pursue a Solution for Removing Social Security Numbers from Cards. Notwithstanding how challenging it is to remove the numbers, why hasn't CMS fully responded to these recommendations?

**Question:**

Taking into consideration that CMS is still in the planning stages, having not identified a clear plan to transition to a new Medicare Beneficiary Identifier (MBI), what assurances does this Committee have that CMS will not be before the Committee in 2019 having missed the implementation goal?

**Question:**

During the hearing, you mentioned that you have begun the process to redesign Medicare cards by removing current SSN –based identifiers, and that you are "developing a thoughtful and measured approach for a smooth transition." Can you please provide a detailed description (including a monthly timeline) of CMS' SSN removal plan?

**Question:**

Can you please provide a detailed description (including a monthly timeline) of how CMS plans to update and consolidate its 75 legacy systems?

**"At this time, responses are not available for printing. Please contact the U.S. Special Committee on Aging for further updates and to perhaps obtain a hard copy, if available."**

**U.S. Senate Special Committee on Aging**
**"Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?"**
**October 7, 2015**
**Questions for the Record**
**Mr. Gary Cantrell**

**Senator Claire McCaskill**

**Question:**

During the hearing, you spoke briefly about a health care company owner's role in medical identity theft schemes. What additional safeguards should be put in place to prevent these fraudsters from opening health care companies?

**Question:**

What do you see is the biggest challenge that law enforcement agencies face when attempting to bring down the criminal enterprises that you mentioned in your testimony?

**Question:**

About how long does it take to identify, investigate, and ultimately prosecute the average health care fraud case?

**"At this time, responses are not available for printing. Please contact the U.S. Special Committee on Aging for further updates and to perhaps obtain a hard copy, if available."**

○