TAX RETURN FILING SEASON

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

APRIL 19, 2016

Serial No. 114–OS11

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PUBLISHING OFFICE

22–230 WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON WAYS AND MEANS

KEVIN BRADY, Texas, *Chairman*

SAM JOHNSON, Texas
DEVIN NUNES, California
PATRICK J. TIBERI, Ohio
DAVID G. REICHERT, Washington
CHARLES W. BOUSTANY, JR., Louisiana
PETER J. ROSKAM, Illinois
TOM PRICE, Georgia
VERN BUCHANAN, Florida
ADRIAN SMITH, Nebraska
LYNN JENKINS, Kansas
ERIK PAULSEN, Minnesota
KENNY MARCHANT, Texas
DIANE BLACK, Tennessee
TOM REED, New York
TODD YOUNG, Indiana
MIKE KELLY, Pennsylvania
JIM RENACCI, Ohio
PAT MEEHAN, Pennsylvania
KRISTI NOEM, South Dakota
GEORGE HOLDING, North Carolina
JASON SMITH, Missouri
ROBERT J. DOLD, Illinois
TOM RICE, South Carolina

SANDER M. LEVIN, Michigan,
CHARLES B. RANGEL, New York
JIM MCDERMOTT, Washington
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
XAVIER BECERRA, California
LLOYD DOGGETT, Texas
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
EARL BLUMENAUER, Oregon
RON KIND, Wisconsin
BILL PASCRELL, JR., New Jersey
JOSEPH CROWLEY, New York
DANNY DAVIS, Illinois
LINDA SÁNCHEZ, California

DAVID STEWART, *Staff Director*
NICK GWYN, *Minority Chief of Staff*

SUBCOMMITTEE ON OVERSIGHT

PETER J. ROSKAM, Illinois, *Chairman*

PAT MEEHAN, Pennsylvania
GEORGE HOLDING, North Carolina
JASON SMITH, Missouri
TOM REED, New York
TOM RICE, South Carolina
KENNY MARCHANT, Texas

JOHN LEWIS, Georgia
JOSEPH CROWLEY, New York
CHARLES B. RANGEL, New York
DANNY DAVIS, Illinois

CONTENTS

TAX RETURN FILING SEASON

TUESDAY, APRIL 19, 2016

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON OVERSIGHT,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:00 a.m., in Room 1100, Longworth House Office Building, the Honorable Peter Roskam, [Chairman of the Subcommittee] presiding.

[The advisory announcing the hearing follows:]

WAYS AND MEANS
CHAIRMAN KEVIN BRADY

Chairman Roskam Announces Hearing on Tax Return Filing Season

House Committee on Ways and Means Subcommittee on Oversight Chairman Peter J. Roskam (R-IL) today announced that the Subcommittee will hold a hearing on the Tax Return Filing Season, as well as efforts to address identity theft related tax fraud and cybersecurity threats. The hearing will take place on Tuesday, April 19, 2016 at 10:00 AM in Room 1100 of the Longworth House Office Building.

Oral testimony at the hearing will be from the invited witnesses only. However, any individual or organization may submit a written statement for consideration by the Subcommittee and for inclusion in the printed record of the hearing.

Details for Submission of Written Comments:

Please Note: Any person(s) and/or organization(s) wishing to submit written comments for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, http://waysandmeans.house.gov, select "Hearings." Select the hearing for which you would like to make a submission, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word document, in compliance with the formatting requirements listed below, **by the close of business on Tuesday, May 3, 2016**. For questions, or if you encounter technical problems, please call (202) 225-3625 or (202) 225-2610.

Formatting Requirements:

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

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

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

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

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

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

Chairman ROSKAM. The subcommittee will come to order.

Welcome to the Ways and Means Subcommittee on the Internal Revenue Service's 2016 tax filing return season.

I think I speak for many Americans when I say that I am glad Tax Day is over. Today's hearing will review the results of the 2016 tax filing season. Additionally, we will focus on the growing threats of identity theft and cybersecurity.

Over 150 million Americans already have or soon will file tax returns for 2015. They expect and deserve an efficient IRS that works for them. Two key aspects of that are ensuring a smooth filing season and protecting taxpayer data.

Unfortunately, the IRS does not have the best track record with regard to either. Last year the Ways and Means Committee found that the IRS deliberately diverted user fees away from customer service, resulting in service that even the IRS Commissioner called "abysmal."

Through Congressional oversight and appropriations, the IRS was forced to prioritize customer service. The agency needs to act quickly to address identity theft, tax-related fraud issues, and cybersecurity issues.

Fraud related to identity theft is growing at an alarming rate. It is a serious crime that hurts millions of Americans and costs the government billions of dollars. In 2012, the Treasury Inspector General for Tax Administration, or TIGTA, reported the IRS could pay out $21 billion in fraudulent refunds over five years.

If you have your identity stolen, it can take months to get your life back together. TIGTA estimated it took an average of 278 days to resolve identity theft cases at the IRS. Nearly 20 percent of them were not even resolved correctly.

While the IRS has taken some steps to prevent and detect identity theft, the agency is not keeping up with the criminals. Law enforcement officers say tax fraud is so easy it has become an addiction for some criminals. Former drug dealers hold tax filing parties where they file hundreds of returns using stolen identities. As one suspect told police, "Why would I take the risk to sell drugs and get busted when I can put $10,000 on a card and do it from home all day long while the cartoons are on?"

In 2010, police in Miami, Florida uncovered an entire tax preparation company set up to file fraudulent returns. It stole over $2 million from taxpayers.

While law enforcement has had some success in this area, there are many sophisticated operations that continue unabated. As one police officer in Florida remarked, "You know, there are guys out there doing it better. We are catching the idiots."

Crime syndicates in Eastern Europe, for example, are ripping millions of dollars off the U.S. Government without ever setting foot in the country.

Last May the IRS announced criminals had broken into the Get Transcript function on the agency's Web site and accessed data on more than 100,000 Americans. The IRS suspended that specific program, but the problem continues. Over 700,000 people are now estimated to have had their sensitive information stolen.

Earlier this year, the agency also had to suspend its Identity Protection Personal Identification Numbers, or IP PIN online program.

IP PINs are given to previous victims of identity theft in order to protect their tax returns. But the IRS discovered at least 800 tax returns filed by fraudsters who had stolen IP PINs.

It is ironic and unsettling to see criminals access the very tool the IRS relies on to protect identity theft victims.

Identity thieves are increasingly relying on cybersecurity breaches and other attacks to obtain taxpayer data. And as the criminals evolve, we need to do the same.

A few years ago, criminals would use stolen names and Social Security numbers to fill out fraudulent returns just by guessing information. It is simpler to catch this type of fraud because some information is often incorrect and it can be flagged through data matching.

Nowadays with identity thieves obtaining their information through cybersecurity hacks, the criminals often have all of the information they need.

The IRS needs to focus on advanced fraud detection methods to keep up with increasingly sophistication of identity thieves. Does the IP address match the address on the return, for example? For electronically filed returns, were the forms filled out more quickly than a human preparer could fill them out?

The IRS needs to improve its information security. Both TIGTA and the GAO have raised concerns with the IRS's inability to protect taxpayer data. TIGTA found the IRS was fully meeting Federal information security standards only in three of ten areas, and there were three areas with significant weaknesses that put taxpayers at risk.

Last month, the GAO reported additional problems with IRS security, including outdated software.

Authentication is one of the biggest challenges. The IRS needs the ability to verify the people who are interacting with the agency are who they claim to be.

TIGTA and GAO have reported the IRS's current authentication standards are not enough to protect taxpayer data. We have seen those weaknesses play out in the IP PIN and Get Transcript hacks. These criminals were able to get in through the front door bypassing the IRS's authentication protocols.

The IRS has always had problems with its information technology, and now criminals are getting better at exploiting it.

Last year, the IRS convened a Security Summit of stakeholders and industry experts to try and address identity theft and cybersecurity. The agency has already announced that it is working with software providers to enhance identity and validation procedures.

Unfortunately, the IRS still has not made the common sense switch to multi-factor authentication. This is a common practice in the private sector. Most people have experienced it when they want to access their bank account online. The bank will not grant the user access until a code is sent to his or her phone or email account.

The IRS needs to move in this direction, and quickly. And let me be clear. This is not necessarily the gold standard that I am talking about. It is the bare minimum the IRS needs to do to ensure people accessing accounts and filing returns are who they claim to be.

And finally, I want to note that identity theft related tax fraud is not just committed by people outside of the IRS. As TIGTA will testify today, there have also been instances where the IRS's own employees used their positions to improperly access taxpayer data and claim fraudulent refunds.

This is obviously unacceptable and should be addressed immediately. How can the IRS expect taxpayers to trust its agents with sensitive information when it cannot prevent criminal activity among its own employees?

It is clear the IRS's existing efforts to address identity theft and cybersecurity attacks are not enough. Criminals are already exploiting these weaknesses, exposing taxpayers' identity and costing the government billions every year.

The troubled agency's failure to improve its information security puts us at risk, and we need to hold the IRS accountable for protecting taxpayer information and strengthening security.

I will now yield to the ranking member, Mr. Lewis, for the purpose of an opening statement.

Mr. LEWIS. Good morning. Mr. Chairman, I want to thank you for calling today's hearing. I also would like to thank the Commissioner and other witnesses for being here today.

Many of you know that this has been a difficult year for the IRS. Identity theft is on the rise, and millions of taxpayers are being harmed.

At the same time, Republicans continue to ask the agency to do more with less. I have said it before, and I think our colleague and my good friend, Mr. Davis, has said it, and I will say it again. You cannot squeeze blood from a turnip.

As one who has served on this Committee for a long time, I am particularly concerned about the new Republican mandate that directs the agencies to use private debt collectors. We have been down this road before. It is a waste, a distraction, and a disservice to the American taxpayers.

The previous private debt collection pilot program cost more than they collected. Taxpayers were harassed, not helped. I said they were harassed and not helped.

Across the country there is an increase in identity theft. Many of you read the news and have family and friends who have been victims. There are already many criminals impersonating the IRS. They seek to cheat taxpayers out of their hard earned money.

Confusion about whether the private debt collector was acting for the IRS was a problem ten years ago. With more criminals, the program is bound to do more harm than good. Bringing back private debt collection is a mistake, and it should be repealed. Congress should focus on giving the IRS the tools it needs to serve taxpayers.

Since 2010, funding for the IRS has been cut by around $1 billion. Last week the Republicans on this Committee passed a bill to cut the IRS by $400 million more each year. These budget cuts have resulted in the loss of 12,000 jobs, reducing employee training, delaying computer system upgrades. That is not good. It does not help.

Last week I was joined by Ways and Means Oversight Subcommittee Democrats in introducing the Taxpayers Protection Act

of 2016. This legislation responds to the recent recommendation from the National Taxpayer Advocate. My bill also includes good policy ideas offered by other committee members, by Mr. Pascrell and Mr. Becerra.

This legislation is a good, common sense policy. In addition to fighting identify theft and strengthening taxpayer protection, our bill will fully fund the President's fiscal year 2017 request for taxpayer service, increasing funding for low income taxpayer clinics, and repeal the terrible private tax debt collection program.

This bill is ripe and it is timely. I hope that it will receive the consideration of the full committee and the full Congress as soon as possible.

Mr. Chairman, again, I thank you for calling today's hearing. I hope that we will see more subcommittee activity on how to better serve and support American taxpayers. I look forward to hearing from today's witnesses, and again, I want to thank all of the witnesses for being here.

Thank you, Mr. Chairman, and I yield back.

Chairman ROSKAM. Thank you, Mr. Lewis.

We will have two panels today. Our first panel is our colleague, Congressman Jim Renacci from Ohio, who has had a personal experience in this arena that he is going to give us his perspective on. Not only does he have the background of serving on the Ways and Means Committee, but he also has a vast private sector background in terms of tax preparation and so forth with his insight as a CPA.

Mr. Renacci.

STATEMENT OF THE HONORABLE JIM RENACCI, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. RENACCI. Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, thank you for holding this important hearing. I am grateful for the opportunity to testify on the impact of tax-related identity theft on taxpayers in Northeast Ohio and across the country.

Let me start with my personal story. Last May I received a notice from the IRS stating they had some questions for me about my 2014 tax return. I found this troubling because I had yet not filed my return.

Because of the Tax Code's complexity, my return requires many forms that rarely arrive before the April 15th filing deadline. So like every year, I filed an extension for my 2014 return until October.

After receiving that IRS notice in May, I immediately called the IRS hoping to swiftly confirm that this was just an IRS error. Unfortunately, there was nothing quick about the call. It took almost two hours, and I did not get an answer.

My level of concern intensified, and I realized that something was very wrong. When I returned to Washington the next week for votes, I reached out to the IRS office here. I finally got some answers.

I learned that sometime in 2015, my personal information had been stolen. Someone then used the information to electronically file a fraudulent tax return for my wife and I. That fraudulent re-

turn, which included a fake W–2 from the U.S. House of Representatives, claimed a significant refund, and the return instructed that those proceeds go to a bank account outside the United States.

Thankfully, there were various red flags associated with this fraudulent return which the IRS caught before sending payment.

As a taxpayer and tax preparer for almost 30 years, it is apparent to me that identity theft is real. The ability to file for a refund electronically and receive a refund quickly via bank transfer can also cause significant issues related to identity theft.

Let me be clear. I do not want to return to paper returns and checks, but the ease of electronic filing and payments has exacerbated the problem. I know now more than ever we need additional safeguards to protect taxpayers.

I personally have heard from many Northeast Ohio taxpayers about their experiences dealing with tax related identity theft. My district office regularly assists constituents who are ID theft victims. I just never thought it would happen to me.

Of course, this is not just a Northeast Ohio problem. Tax-related identity theft is an evolving criminal activity that targets innocent taxpayers nationwide and robs the Treasury of billions of dollars each year.

I am committed to finding a way to crack down on the growing threat that has devastated millions of taxpayers. So last fall with Ranking Member Lewis, I introduced bipartisan legislation entitled "The Stolen Identity Refund Fraud Prevention Act of 2015."

This legislation is an important first step towards shielding taxpayer dollars from fees and reducing the hardship caused by this criminal activity. I was pleased that two core components from this legislation were included in the PATH Act that passed last December. One closes the large gap between when employers provide W–2s to their employees and when they are required to provide them to the government. While W–2 and non-employee compensation statements are due to employees by the end of January, before the PATH Act the deadline for filing them electronically with the government was not until the end of March.

In the last filing season, the IRS received over 90 million returns during that two-month window where the IRS was unable to verify key information before issuing refunds. Starting next filing season, the due date for filing W–2 information returns and non-employee compensation forms to the government will also be the end of January.

Closing this window was a key step in enabling the IRS to prevent the continued issuance of billions of dollars in fraudulent tax returns. Even though that provision does not go into effect until next filing season, I am pleased that some employees with large volumes of W–2s were proactive on this issue and agreed this filing season to voluntarily file their W–2s with the government early in this year. According to Tax Commissioner Koskinen's testimony last week before the Finance Committee, the IRS received over 25 million early submissions, most of which came by the end of January.

The second provision of my bill included in the PATH Act allows the IRS to require permitted truncated Social Security numbers on W–2s. Previously, while the IRS by regulation could require trun-

cated Social Security numbers on Forms 1099, they were prohibited by statute from doing the same on W–2s. This common sense provision will better protect sensitive taxpayer personal information that was previously at risk.

Mr. Chairman, tax-related identity theft is one of the most pressing challenges that we face in the world of tax administration. This complex and evolving threat requires cooperation from Congress, the IRS, state revenue agencies and industry stakeholders.

I would also like to applaud the IRS for creating the Security Summit initiative to collaborate in fighting tax-related identity theft, and I am pleased to hear that the public-private partnership has resulted in a greater sharing of resources to improve identity theft detection and prevention.

I look forward to continuing to work with all stakeholders to curb the growing threat.

Thank you for the opportunity to testify. I look forward to working with my colleagues on this Committee to mark up the remaining provisions of the Stolen Identity Refund Fraud Prevention Act of 2015.

[The prepared statement of Mr. Renacci follows:]

Written Testimony of Rep. James B. Renacci, OH-16
Before the House Ways and Means Oversight Subcommittee
April 19, 2016

Chairman Roskam, Ranking Member Lewis, and members of this Subcommittee, thank you for holding this important hearing. I am grateful for the opportunity to testify on the impact of tax-related identity theft on taxpayers in Northeast Ohio and across the country.

Let me start with my personal story. Last May, I received a notice from the IRS stating that they had some questions for me about my 2014 tax return.

I found this troubling because I had not yet filed.

Because of the tax code's complexity, my return requires many forms that rarely arrive before the traditional April 15th filing deadline. So, like every year, I filed an extension for my 2014 return until October.

After receiving that IRS notice in May, I immediately called the IRS, hoping to swiftly confirm that this was just an IRS error. Unfortunately, there was nothing quick about the call. It took almost two hours and I didn't get an answer

My level of concern intensified. And, I realized that something was very wrong.

When I returned to DC for votes, I reached out to the IRS here. I finally got some answers. I learned that—sometime in early 2015—my personal information had been stolen. Someone then used that information to electronically file a fraudulent tax return for my wife and I. That fraudulent return, which included a fake W-2 from the U.S. House of Representatives, claimed a significant refund. And the return instructed that those proceeds go to a bank account outside of the United States.

Thankfully, there were various red flags associated with this fraudulent return, which the IRS flagged before sending payment.

As a taxpayer and tax preparer for almost 30 years, it is apparent to me that identity theft is real. The ability to file for a refund electronically and receive a

refund quickly via bank transfer can also cause significant issues related to identify theft. Let me be clear, I don't want to return to paper returns and checks, but the ease of electronic filing and payments have exacerbated the problem. I know, now more than ever, we need additional safeguards to protect taxpayers.

I personally have heard from many Northeast Ohio taxpayers about their experiences dealing with tax-related identity theft. My district office regularly assists constituents who are ID theft victims. I just never thought it would happen to me.

Of course, this is not just a Northeast Ohio problem. Tax-related identity theft is an evolving criminal activity that targets innocent taxpayers nationwide and robs the Treasury of billions of dollars each year.

I am committed to finding a way to crack down on this growing threat that has devastated millions of taxpayers. So last fall—with Ranking Member Lewis—I introduced bipartisan legislation entitled the *Stolen Identity Refund Fraud Prevention Act of 2015*. This legislation is an important first step towards shielding taxpayer dollars from thieves and reducing the hardships caused by this criminal activity.

I was pleased that two core components from this legislation were included in the PATH Act that passed last December.

One closes the large gap between when employers provide W-2s to their employees and when they are required to provide them to the government. While W-2 and nonemployee compensation statements are due to employees by the end of January, before the PATH Act, the deadline for filing them electronically with the government was not until the end of March. Last filing season, the IRS received over 90 million returns during that 2 month window, where the IRS was unable to verify key information before issuing refunds.

Starting next filing season, the due date for filing W-2 information returns and nonemployee compensation forms with the government will also be the end of January. Closing this window is a key step in enabling the IRS to prevent the continued issuance of billions of dollars in fraudulent tax returns.

Even though that provision does not go into effect until next filing season, I am pleased that some employers that issue large volumes of W-2s were proactive on this issue & agreed this filing season to voluntarily file their W-2s with the government earlier in the year. According to Commissioner Koskinen's testimony last week before the Finance Committee, the IRS received over 25 million early submissions, most of which came by the end of January.

The second provision from my bill included in the PATH Act allows the IRS to require or permit truncated Social Security Numbers on W-2s. Previously, while the IRS by regulation could require truncated Social Security Numbers on Forms 1099, they were prohibited by statute from doing the same for W-2s. This common sense provision will better protect sensitive taxpayer personal information that was previously at risk.

While those two provisions are very helpful to combat tax-related identity theft, there are various other components of the bill that I hope will receive serious consideration by the Committee this year.

One is a centralized point of contact at the IRS for identity theft victims. Last year, I heard from tax-related identity theft victims who expressed frustration with having to repeatedly contact the IRS about their case. Each time they called, they had to explain their situation to IRS employees in various divisions, each of whom may have had no prior knowledge of their matter.

In response to that frustration, during the second half of last year, I understand that the IRS formed a victims' assistance unit to track a taxpayer's identity theft case from start to finish. The provision in my bill would signal that the unit has Congressional support and directs the IRS to maintain this unit to ensure that an identity theft victim has a centralized point of contact.

Another provision is improved taxpayer notification of suspected identity theft. I also heard last year from identity theft victims who had difficulty obtaining information about fraudulent returns filed in their names. Victims deserve to know the extent of their identity theft, including what personal information has been compromised, in order to take action to protect themselves and their

families. Under that provision, when the IRS determines that there has been an unauthorized use of a taxpayer's identity, this provision would require the IRS—as soon as practicable and without jeopardizing an investigation relating to tax administration—to notify the taxpayer.

The last one I will mention would provide taxpayers the opportunity to opt out of electronic filing. As I alluded to above, it's obvious that most tax-related identity theft occurs through electronically filed tax returns. The IRS, however, does not have a program which would allow taxpayers to elect to prevent the processing of an electronic return filed in their name. This provision would change that; it would allow a taxpayer to file an identity theft affidavit to elect to prevent the IRS from processing any electronically filed tax return submitted by the taxpayer or by any person purporting to be that taxpayer.

Mr. Chairman, tax-related identity theft is one of the most pressing challenges that we face in the world of tax administration. This complex and evolving threat requires cooperation from Congress, the IRS, state revenue agencies, and industry stakeholders. I applaud these parties for creating the Security Summit initiative to collaborate in fighting tax-related identity theft & I am pleased to hear that this public-private partnership has resulted in a greater sharing of resources to improve identity theft detection and prevention. While I am aware that not every tax-related identity theft problem is best served with a Congressional solution, I look forward to continuing to work with all stakeholders to curb this growing threat. Thank you for the opportunity to testify and I look forward to working with my colleagues on this Committee to mark-up remaining provisions of the *Stolen Identity Refund Fraud Prevention Act of 2015.*

Chairman ROSKAM. Mr. Renacci, thank you for your testimony.

I am just thinking about how aggressive it would be for somebody to actually file a fake W–2 with the U.S. House of Representatives on it. I mean, that is a demonstration of hubris, and as you pointed out, you know, the IRS caught it before the money went out. So let us give credit where credit is due.

So thank you for your attention and for your willingness to roll up your sleeves and to work on a bipartisan basis on these issues that affect all of us.

We will now hear from our second panel. It consists of three witnesses:

The Honorable John Koskinen, the Commissioner of the Internal Revenue Service;

Mr. Timothy Camus, who is the Deputy Inspector General for Investigations at the Treasury Inspector General for Tax Administration, or TIGTA;

And Ms. Jessica Lucas-Judy, who is the Acting Director for Tax Issues at the Government Accountability Office.

Commissioner Koskinen, welcome, and if we could begin with your testimony. You are recognized.

STATEMENT OF JOHN KOSKINEN, COMMISSIONER, INTERNAL REVENUE SERVICE

Mr. KOSKINEN. Thank you, Mr. Chairman and Ranking Member Lewis and Members of the Subcommittee. I appreciate the opportunity to appear before you today.

Let me start with an update on the 2016 filing season which ended yesterday for everyone but those living in Maine and Massachusetts, who must file by midnight tonight. For the rest of the country, I am pleased to report that the last day of filing individual tax returns, yesterday, went very smoothly with our systems receiving more than four million returns on that day alone.

We have received already and processed slightly over 130 million returns. Ninety percent of the refunds were processed within our 21-day goal and approximately 90 million refunds have already been issued.

In regard to taxpayer service, I am also pleased to be able to report that the IRS saw significant improvements during this filing season over last year largely due to the additional resources provided by Congress. A total of $290 million in additional funding was approved for the IRS for this fiscal year to improve service to taxpayers, strengthen cybersecurity and expand our ability to address identity theft, all of which we appreciate.

To illustrate how helpful this extra funding was, we designated $178 million to be used for taxpayer service, which among other things allowed us to add about 1,000 extra temporary employees to help improve our service on the phones during the filing season.

During the season, the average level of service on our toll free help lines this year has exceeded 70 percent, a vast improvement over last year's 37 percent. Unfortunately, once the seasonal employees are gone and the funding runs out, that number will drop significantly, but still the average for the phone service for the full year will probably be between 47 and 50 percent, still a significant improvement over last year.

The President's budget for 2017 provides for a level of phone service of about 70 percent for the entire year with an investment of approximately $150 million above current levels. This year has demonstrated that with additional funding, taxpayer service will improve significantly.

Let me now turn briefly to the IRS' ongoing efforts with regard to cybersecurity and identity theft. Securing our systems and taxpayer data continues to be a top priority for the IRS. Even within our constrained resources, we continue to devote significant time and attention to the challenge. We work continuously to protect our main computer systems from cyberattacks and to safeguard taxpayer information stored in our databases. These systems withstand more than one million malicious attempts to access them every day.

We are also continuing to battle a growing problem of stolen identity refund fraud. Over the past few years, we have made steady progress in protecting against fraudulent refund claims and criminally prosecuting those who engaged in this crime.

We have found the type of criminal we are dealing with has changed. The problem, as the chairman noted, used to be random individuals filing a few dozen or a few hundred false returns at a time. Now we are dealing more and more with organized crime syndicates here and around the world. They are gathering unimaginable amounts of personal data from sources outside the IRS so they can do a better job of impersonating taxpayers, evading our return processing filters and obtaining fraudulent refunds.

To improve our efforts against this complex, as noted, and against the evolving threat, as noted in March last year, we joined with the leaders of the electronic tax industry, the software industry and the states to create the Security Summit Group. This is an unprecedented partnership that is focused on making the tax filing experience safer and more secure for taxpayers in 2016 and beyond.

Our collaborative efforts have already shown concrete results this filing season. For example, Security Summit partners have helped us improve our ability to spot potentially false returns before they are processed, and they have increased the level of authentication for taxpayers when they use software or provide information for their preparers.

Over the past year, we have detected and stopped three instances of criminals masquerading as legitimate taxpayers on the basis of information stolen from places other than the IRS. One of the service's targets, as noted, was our Get Transcript online application used by taxpayers to quickly obtain a copy of their prior year return.

Another was the IP PIN, as the chairman noted. In all three cases we detected that criminals were trying to use our online tools to help them pretend to be legitimate taxpayers and sneak false returns past our filters.

The incidents have shown us that improving our reaction time to suspicious activity is not enough. We need to be able to anticipate the criminals' next moves in an attempt to stay ahead of them. The ongoing work of the Security Summit Group will be critical to our success here.

Congress can provide critical support by approving adequate resources for these efforts. Sustaining and increasing funding in this area will be critical as we move forward.

Another way Congress can help us is by passing legislative proposals to improve tax administration and cyber security. One of the most important requests we have made is for the reauthorization of streamlined critical pay authority, the loss of which has made it very difficult, if not impossible, to recruit and retain employees with expertise in highly technical areas such as information technology.

Mr. Chairman, Ranking Member Lewis, and Members of the Subcommittee, this concludes my statement, and after other presentations, I would be happy to take your questions.

[The prepared statement of Mr. Koskinen follows:]

WRITTEN TESTIMONY OF
JOHN A. KOSKINEN
COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE WAYS AND MEANS COMMITTEE
SUBCOMMITTEE ON OVERSIGHT
ON THE 2016 FILING SEASON, CYBERSECURITY AND PROTECTING
TAXPAYER INFORMATION
APRIL 19, 2016

PART I: UPDATE ON THE 2016 FILING SEASON

Chairman Roskam, Ranking Member Lewis and Members of the Subcommittee, thank you for the opportunity to testify today.

I am pleased to report that the 2016 filing season has gone smoothly in terms of tax return processing and the operation of our information technology (IT) systems. Through April 8 the IRS has received more than 107 million individual returns, on the way to an expected total of 150 million. We have issued more than 81 million refunds totaling more than $228 billion.

In regard to taxpayer service, the IRS saw significant improvements during this filing season over last year, largely due to additional resources provided by Congress. A total of $290 million in additional funding was approved for the IRS for Fiscal Year (FY) 2016, to improve service to taxpayers, strengthen cybersecurity and expand our ability to address identity theft, which we appreciate. This funding is the first significant increase in the IRS budget in six years and represents a positive development for the IRS and for the American taxpayer. I can assure the Congress that we are spending these resources wisely and efficiently.

We used approximately $178.4 million of this additional funding to add about 1,000 extra temporary employees to help improve our service on our toll-free phone lines. As a result, so far this filing season the telephone level of service is nearly 75 percent, which is a vast improvement over last year. The IRS has prioritized improving the level of taxpayer service on the phones during filing season, and was operating at historically low levels until the new appropriations were provided in December. When the funding for these additional employees runs out at the end of the filing season, the level of service on our phones will drop noticeably and we expect average phone services levels for the full year to be about 47 percent. This level will still be a major improvement over the 37 percent level of phone service last year. The President's 2017 Budget proposal

provides for a level of phone service above 70 percent for the full year with an investment of approximately $150 million above current levels.

Another, less visible, area of concern for us in regard to taxpayer service has been taxpayer correspondence. Typically, taxpayers correspond with the IRS after receiving a notice from the agency about an issue with their return. Our goal is to answer taxpayer correspondence within 45 days after we receive the letter.

Because of our constrained resources, we have been taking much longer to answer correspondence in recent years, though additional resources have allowed us to reduce our backlog slightly this year. However, additional improvements are needed. Our correspondence inventory is currently 923,000, with about one-third of that considered to be "over-age" – generally, unanswered after more than 45 days. The additional resources in our proposed FY 2017 budget would allow us to hire additional employees to make further improvements in this area.

During the current filing season, taxpayer demand for the services we provide online has been strong. As of April 9, we have had more than 291 million hits on our website, IRS.gov, and taxpayers have used the "Where's My Refund?" electronic tracking tool more than 254 million times. To give another example, our Online Payment Agreement application, which was streamlined and improved in 2014, has been used more than 187,000 times thus far in FY 2016.The growing demand for IRS online services underscores the need for adequate information technology and cybersecurity funding.

It is important to note that, even with the additional funding received for FY 2016, the IRS is still under significant financial constraints. This is illustrated by the fact that the IRS appropriation remains $900 million below the FY 2010 enacted level and that the $290 million increase is less than half the amount that had been requested for FY 2016 in the three critical areas mentioned above. In addition, the IRS must absorb mandated cost increases and inflation during FY 2016 that are greater than the additional funding provided.

As a result, we will need to continue the exception-only hiring policy that began in FY 2011, leaving us unable to replace most employees we lose this year through attrition. In fact, we expect the IRS workforce to continue to shrink by another 2,000 to 3,000 full-time employees during FY 2016, equaling a loss of over 17,000 since FY 2010.

While this decline in our workforce has been occurring, the number of individual returns filed grew by more than 10 million (or nearly 7 percent), from 153 million in 2010 to 163 million in 2015. Further increasing our workload, the IRS during this period has had to implement a number of significant legislative requirements, nearly all of which came with no additional funding.

For example, the IRS has worked diligently since the Affordable Care Act's enactment in 2010 to implement its tax-related provisions. Our most recent efforts began prior to the 2016 filing season, and involved preparing our systems for a reporting provision that applies to health coverage providers and certain large employers that took effect in 2015.

Another important legislative mandate is the Foreign Account Tax Compliance Act (FATCA). Most recently, implementation has involved preparing our systems to receive annual reports on accounts of U.S. taxpayers from foreign financial institutions (FFI). We currently have190,000 FFIs providing us with data under FATCA.

In FY 2016, several additional legislative mandates were put in place that carried no implementation funding with which to execute them – for example, new passport restrictions, a registration requirement for newly created 501(c)(4) organizations, and a program under which private contractors will collect taxes on some past-due accounts.

PART II: CYBERSECURITY AND PROTECTING TAXPAYER INFORMATION

Securing our systems and taxpayer data continues to be a top priority for the IRS. Even with our constrained resources as a result of repeatedly decreased funding over the past few years, we continue to devote significant time and attention to this challenge, which is twofold.

First, the IRS works continuously to protect our main computer systems from cyber incidents, intrusions and attacks, but our primary focus is to prevent criminals from accessing taxpayer information stored in our databases. These core tax processing systems remain secure, through a combination of cyber defenses, which currently withstand more than one million attempts to maliciously access our systems each day. Second, the IRS is waging an ongoing battle to protect taxpayers and their information as we confront the growing problem of stolen identity refund fraud. Our multipronged approach to this problem is discussed in more detail below.

As we confront these challenges, the IRS has also been working to expand and improve our ability to interact with taxpayers online. While we already engage taxpayers across numerous communications channels, we realize the need to meet taxpayers' increasing demand for digital services.

We are aware, however, that in building toward this enhanced online experience, we must continuously upgrade and improve our authentication protocols. The reality is criminals are becoming increasingly sophisticated and are gathering vast amounts of personal information as the result of data breaches at sources outside the IRS. We must balance the strongest possible authentication

processes with the ability of taxpayers to legitimately access their data and use IRS services online. It is important to note that cybercrime (theft by unauthorized access) and privacy breaches are increasing across the country in all areas of government and industry. Cyber criminals and their methods continue to grow in sophistication, frequency, brazenness, volume and impact. IRS will continue to be challenged in our ability to maintain currency with latest technologies, processes and counter-measures.

MAKING PROGRESS AGAINST IDENTITY THEFT

Discovering that your identity has been stolen by having your tax return rejected because someone else has already filed a return using your name and Social Security Number (SSN) can be a personal and traumatic experience. We are constantly working to improve our processes and methods to protect taxpayers from this situation. The problem of personal data being used to file fraudulent tax returns and illegally obtain refunds exploded from 2010 to 2012, and for a time overwhelmed private industry, law enforcement, and government agencies such as the IRS. Since then, we have been making steady progress within our reduced resources, both in terms of protecting against fraudulent refund claims and criminally prosecuting those who engage in this crime.

Thanks to the work of our Criminal Investigation Division, about 2,000 individuals have been convicted on federal charges related to refund fraud involving identity theft over the past few years. We currently have about 1,700 open investigations being worked by more than 400 IRS criminal investigators.

Meanwhile, we continue to improve our efforts at stopping fraudulent refunds from going out the door. For example, we have improved the filters that help us spot suspicious returns before they can be processed. Using those filters, we stopped 1.4 million returns last year that were confirmed to have been filed by identity thieves. By stopping those returns, we kept criminals from collecting about $8.7 billion in fraudulent refunds.

Importantly, the IRS also continues to help taxpayers who have been victims of identity theft. Last year, the IRS worked with victims to close more than 700,000 such cases.

But while we have stopped many crimes, we find that the type of criminal we are dealing with constantly evolves. Previously we were dealing with individuals stealing personal information and filing a few dozen or maybe a few hundred false tax returns, and while we still see this, the threat has grown to include organized crime syndicates here and in other countries.

Security Summit Group

To improve our efforts against this complex and evolving threat, the IRS held a sit-down meeting in March 2015 with leaders of the electronic tax industry, software industry and state tax officials. We agreed to build on our past cooperative efforts and find new ways to leverage our public-private partnership to help battle stolen identity refund fraud. Motivating us was the understanding that no single organization can fight this type of fraud alone.

This meeting led to the development of the Security Summit group, an unprecedented partnership that has focused our joint efforts on making sure the tax filing experience would be safer and more secure for taxpayers in 2016 and beyond. This is an important step for taxpayers and for tax administration, because the critical work being done by this group is giving everyone involved a better defense against stolen identity refund fraud.

Over the past year, the Security Summit group has made progress on a number of initiatives including:

- Summit group members identified and agreed to share 20 data components from Federal and state tax returns to improve fraud detection and prevention this filing season. For example, group members are sharing computer device identification data tied to the return's origin, as well as the improper or repetitive use of the numbers that identify the Internet "address" from where the return originates.

- Tax software providers agreed to enhance identity requirements and strengthen validation procedures for new and returning customers to protect their accounts from being taken over by criminals. This change is one of the most visible to taxpayers during the 2016 filing season, because it includes new verification procedures they need to follow to log in to their accounts. These actions will serve as the baseline for ongoing discussions and additional enhancements for the 2017 filing season.

- The Summit group created a new memorandum of understanding (MOU) regarding roles, responsibilities and information sharing pathways currently in circulation with states and industry. So far, 40 state departments of revenue and 21 tax industry members have signed the MOU, along with the IRS and endorsing organizations.

- Tax industry participants have aligned with the IRS and the states under the National Institute of Standards and Technology (NIST) cybersecurity framework to promote the protection of information technology infrastructure. The IRS and states currently operate consistently with this framework, as do many in the tax industry. Next steps in this area include follow-up sessions to develop strategy for how the NIST cybersecurity framework will be employed by all organizations within the tax industry.

- Summit group members agreed on the need to create a tax administration Information Sharing and Analysis Center (ISAC) to centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information.

- Recognizing the critical role that the nation's tax professionals play within the tax industry in both the Federal and state arenas, the Summit group created a team that will examine issues related to return preparers, such as how the preparer community can help prevent identity theft and refund fraud.

Our collaborative efforts are already showing concrete results this filing season. For example, Security Summit partners have helped the IRS improve its ability to spot potentially false returns before they are processed and thus before a possibly fraudulent refund is issued. Under our industry leads program, Security Summit partners and other external stakeholders such as banks provide information that allows us to improve our fraud filters, which in turn leads to more suspicious returns being identified for further review. In Calendar Year (CY) 2016 through mid-March, leads from industry partners directly resulted in the suspension of 27,000 returns on which a total of $119 million in refunds was claimed, up from 8,000 returns claiming $57 million during the same period last year.

Identity Theft Public Awareness Campaign

Despite the progress being made against stolen identity refund fraud, we recognized that we were missing an important partner in this effort – the taxpaying public. So in November 2015, with the strong support of all the Security Summit partners, we launched the "Taxes, Security, Together" campaign to raise awareness about actions people can take to protect themselves and avoid becoming victims of identity theft.

Many of the steps are basic common sense, but given that 150 million households file tax returns every year, we believe these steps cannot be stressed enough. People continue to fall prey to clever cybercriminals who trick them into giving up SSNs, bank account numbers, password information or other sensitive personal data. So having the public's help will greatly strengthen and improve our new tools we have to stop the crime of identity theft.

As part of this public awareness campaign, the IRS, in the weeks leading up to the 2016 filing season, issued weekly tax tips describing the actions people could take to protect their data. We have updated several publications for taxpayers and tax professionals. We have posted YouTube videos on this subject, and public-awareness information is being shared online across IRS.gov, state websites and platforms used by the tax software industry and many others in the

private-sector tax community. I would note our public awareness campaign is not confined to the tax filing season, but is an ongoing effort.

Our efforts to educate and inform members of the public about the need to protect themselves against identity thieves extend to businesses as well. Information returns, especially Form W-2, are becoming a major target of these criminals, as they seek new sources of information that will help them file false returns that have a better chance of going undetected by our fraud filters. In this effort, they attempt to trick companies into providing the information returns.

One scheme uncovered recently involved identity thieves posing as a company's chief executive and sending a legitimate-looking email to the payroll department requesting a list of all company employees and their Forms W-2. In March, the IRS issued an alert to payroll and human resources professionals warning them about this scam.

Identity thieves' efforts to obtain Forms W-2 have not stopped there. We are increasingly concerned about efforts to create counterfeit Forms W-2 that are filed along with the false returns to make the return appear legitimate. That concern led the IRS to launch a pilot program earlier this year testing the idea of adding a verification code to Form W-2 that would verify the integrity of Form W-2 data being submitted to the IRS.

For this pilot, the IRS partnered with four major payroll service providers. These providers added a special coded number on approximately 2 million individual Forms W-2 in a new box on the Form W-2 labeled "Verification Code." Each coded number is calculated based on a formula and key provided by the IRS, using data from the Form W-2 itself, so that each number generated was known only to the IRS, the payroll service provider, and the individual who received the Form W-2. The verification code cannot be reverse engineered. Since this identifier is unique, any changes to the Form W-2 information provided when filed are detected by the IRS. Individuals whose Forms W-2 were affected by the pilot and who used tax software to prepare their return entered the code when prompted to by the software program. The IRS plans to increase the scope of this pilot for the 2017 filing season by expanding the number and types of Form W-2 issuers involved in the test.

VERIFYING IDENTITIES AND STOPPING SUSPICIOUS ONLINE ACTIVITY

Following the OMB Guidance and NIST Standards

The IRS continues to make every effort to ensure that we provide tax account-related services only after verifying the identity of individuals seeking those services. This is true for all of our communications channels, some of which allow

for extremely strong assurance processes that are not possible in other channels.

For example, IRS employees at our Taxpayer Assistance Centers provide face-to-face help to taxpayers, and thus can easily verify identity through photo identification. This method provides the strongest possible level of assurance, but is obviously not feasible with phone or online interactions. Additionally, in-person assistance is more time-consuming for the taxpayer and costly for the IRS than the help we provide through other communications channels.

Given the ability of cybercriminals and identity thieves to evolve and improve their methods of stealing personal data, the need to properly verify the identity of taxpayers using online services is particularly great. In developing authentication procedures for online interactions with taxpayers, the IRS continues to follow the Office of Management and Budget (OMB) memorandum issued in 2003, *E-Authentication for Federal Agencies*.

This memorandum establishes criteria for determining the risk-based level of authentication assurance required for specific electronic applications and transactions. It requires agencies to review new and existing electronic transactions, to ensure authentication processes provide the appropriate level of assurance from among four levels, which are as follows:

Level 1: Little or no confidence in the asserted identity's validity;
Level 2: Some confidence in the asserted identity's validity;
Level 3: High confidence in the asserted identity's validity; and
Level 4: Very high confidence in the asserted identity's validity.

Each increase in level requires users to take additional steps to validate their identity and gain access to a given online transaction.

In addition to the OMB memorandum, we also follow the technical requirements set by NIST for the four levels of assurance defined in the OMB guidance. It is important to note that the NIST standards anticipate and require varying levels of assurance depending on the nature of a given online transaction and the information being exchanged.

In following the NIST standards, the IRS employs differing levels of authentication assurance among the various digital services used by taxpayers. For example, the level of authentication required for an online tool that only accepts payments from a taxpayer can reasonably be set lower than an application that provides the taxpayer with their personal tax information.

Thus, in establishing a risk assurance level to a particular online digital service, the IRS, in addition to assigning one of the four numerical levels of risk assurance, also assigns a letter representing the amount and types of validation

that a taxpayer would have to provide, in order to gain access to the digital service in question:

A: No credential required (OMB Level 1);
B: User ID and password required, but no identity proofing (OMB Level 1);
C: User ID and password, plus basic identity proofing – providing information such as name, address, date of birth, SSN (OMB Level 2);
D: Everything included in C above, plus knowledge-based authentication – answers to so-called "out of wallet" questions that only the legitimate taxpayer should know (OMB Level 2);
E: Everything included in D above, plus financial validation, such as providing the taxpayer's prior-year adjusted gross income (OMB Level 2);
F: Everything included in C above, plus financial validation and an additional authentication factor, such an authentication code texted or mailed to the user – so-called multifactor identification (OMB Level 3); and
G: In-person authentication.

Recent Unauthorized Attempts to Access IRS Online Services

Over the past year, unauthorized attempts were made to access online services on our website, IRS.gov. These attempts were not on our main computer system, which remains secure. Instead, in each situation criminals were attempting to use taxpayer information they had stolen from other sources to access IRS services by impersonating legitimate taxpayers, in order to file false tax returns and claim fraudulent refunds.

Each of the situations, which are described in more detail below – involving the Get Transcript online application, the Identity Protection Personal Identification Number (IP PIN) retrieval tool and the Get Your Electronic Filing PIN tool– illustrate both the progress we have made and the challenges we continue to face in detecting suspicious activity and ensuring the digital services we provide are used only by taxpayers who legitimately seek them.

For all three services, the improvements made to our system-monitoring capabilities allowed the IRS to uncover the suspicious activity. We continue to improve these monitoring capabilities and enhance our return processing filters so that we can thwart criminal activity as quickly as possible.

But improving our ability to react to these threats is not enough. The three situations are examples of how nimble criminals have become in attempting to access our systems by masquerading as legitimate taxpayers. In each case, those who were making the unauthorized attempts to gain access had already obtained vast amounts of stolen individual taxpayer data and were using it to help them get into our systems, with the ultimate goal of claiming a fraudulent refund. We are finding that, as the IRS improves monitoring capabilities and shuts off certain avenues of entry, identity thieves find new ways to file false

returns. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals have become more sophisticated at faking taxpayers' identities so they can evade those filters and successfully obtain fraudulent refunds.

Therefore, the IRS is working not just to react better and faster, but to anticipate the criminals' next moves and stay ahead of them. To fully protect taxpayers and the tax system, the IRS must not only keep pace with, but also get ahead of, criminals and criminal organizations, as they improve their efforts to obtain personal taxpayer information. The ongoing collaborative work of the Security Summit group along with additional funding received in FY 2016 as part of the Section 113 Administrative Provision have been crucial. The FY 2017 budget requests additional funding including a Departmentally-managed Cybersecurity Enhancement account which allows the IRS and the Department to leverage enterprise-wise services and capabilities.

Following are descriptions of the three situations referenced above involving suspicious online activity:

Get Transcript Application. The Get Transcript online application allows taxpayers to view and print a copy of their prior-year tax information, also known as a transcript, in a matter of minutes. Taxpayers use tax transcript information for a variety of non-tax administration, financial activities, such as verifying income when applying for a mortgage or financial aid.

Prior to the introduction of this online tool in January 2014, taxpayers needing a transcript had to order a transcript by mail, by phone, or in person at one of our Taxpayer Assistance Centers, and then have it mailed to them.

The development of the Get Transcript online application began in 2011. The IRS conducted a risk assessment and determined that the e-authentication risk assurance level appropriate for this application was 2D, which required the taxpayer to provide basic items of personal information and also answer out-of-wallet questions. At that time, this type of authentication process was the industry standard, routinely used by financial institutions to verify the identity of their customers conducting transactions online.

During the 2015 filing season, taxpayers used the Get Transcript online application to successfully obtain approximately 23 million transcripts. If this application had not existed and these taxpayers had to call or write us to order a transcript, it would have stretched the IRS's limited resources even further.

In May 2015, the IRS announced that criminals, using taxpayer information stolen elsewhere, had been able to access the Get Transcript online application. Shortly thereafter, we disabled the application. We are now strengthening the authentication process and expect to bring the Get Transcript application back

on-line, in the near future. In reevaluating the application, we have changed the risk assurance level for this application to 3F, which will require taxpayers to undergo a multifactor authentication process in order to gain access. In the meantime, taxpayers can still place an order for a transcript online, and have it mailed to their address of record.

The IRS, immediately focusing on last year's filing season, initially identified approximately 114,000 taxpayers whose transcripts had been accessed and approximately 111,000 additional taxpayers whose transcripts were targeted but not accessed. We offered credit monitoring, at our expense, to the group of 114,000 for which the unauthorized attempts at access were successful. We also promptly sent letters to all of these taxpayers to let them know that third parties may have obtained their personal information from sources outside the IRS in an attempt to obtain their tax return data using the Get Transcript online application.

Our review of the situation continued and, in August 2015, we identified another 220,000 taxpayers whose transcripts may have been accessed and approximately 170,000 taxpayers whose transcripts were targeted but not accessed. We again notified all of these taxpayers about the unauthorized attempts, and offered credit monitoring to the 220,000.

In addition, the Treasury Inspector General for Tax Administration (TIGTA) conducted a nine-month investigation looking back to the launch of the application in January 2014 for additional suspicious activity. This expanded review identified additional unauthorized attempts to access taxpayer information using the Get Transcript online application. This review found potential access of approximately 390,000 additional taxpayer accounts during the period from January 2014 through May 2015. An additional 295,000 taxpayer transcripts were targeted but access was not successful. Again, the IRS sent letters to these taxpayers alerting them to the unauthorized attempts, offering credit monitoring to those whose accounts were accessed.

The additional attempts uncovered by TIGTA brought the total number of potential unauthorized accesses to the Get Transcript online application to 724,000. So far, we have identified approximately 250,000 potentially fraudulent returns that were filed on behalf of these taxpayers, and we have stopped the majority of the known fraudulent refunds from going out.

I would note that our analysis of the attempts to access the Get Transcript online application is ongoing, and we may yet discover that some accesses classified as unauthorized were, in fact, legitimate. For example, family members, tax return preparers or financial institutions could have been using a single email address to attempt to access more than one account. However, in an abundance of caution, IRS notified any and all taxpayers whose accounts met these criteria.

Additionally, as a result of the Get Transcript online application problem, we added an extra layer of protection for taxpayers who use our online services. We started sending a letter, known as a CP301 notice, to taxpayers when they first create a login and password for any web application on IRS.gov. This notice tells the taxpayer that someone registered for an IRS online service using their information. If the taxpayer was not the one who registered, the notice instructs the taxpayer to contact the IRS. Mailing this notice conforms to NIST guidance, and is a best practice similar to that used by the Social Security Administration and other financial institutions.

Since we began sending these notices, we have disabled approximately 5,100 online accounts at the request of taxpayers who received a CP301. The majority of these accounts were disabled between January and March of this year, and we estimate that approximately 80 percent of these requests were related to the unauthorized attempts to access the IP PIN retrieval tool described below.

IP PIN Retrieval Tool. One aspect of the IRS's efforts to help taxpayers affected by identity theft involves the IP PIN, a unique identifier that authenticates a return filer as the legitimate taxpayer. If the IRS identifies a return as fraudulently filed, the IRS offers the legitimate taxpayer the ability to apply for an IP PIN for use when filing their next return. The IRS mails the IP PIN to the taxpayer's address of record, and the IP PIN is valid for only one filing season.

The IP PIN program began as a pilot in 2011, and since then has grown significantly. For the 2016 filing season, the IRS issued IP PINs to 2.7 million taxpayers previously identified by the IRS as victims of identity theft or participants in a pilot program. This pilot is for taxpayers living in Florida, Georgia and Washington, D.C. – three areas where there have been particularly high concentrations of stolen identity refund fraud – who can request an IP PIN regardless of whether the IRS has identified them as a victim of identity theft.

In 2015, the IRS developed an online tool that allowed taxpayers who had received an IP PIN to retrieve it if they lost or misplaced the number before filing their return. Taxpayers accessed this tool on IRS.gov by entering personal information to authenticate their identity. The retrieval tool has been used by only a small subset of all taxpayers receiving an IP PIN: this filing season, out of the 2.7 million who received an IP PIN, just 130,000, or about 5 percent, used the retrieval tool.

After discovering the problems with the Get Transcript online application, we began in July 2015 to monitor every request to recover a forgotten or lost IP PIN. In February 2016, as part of this proactive, ongoing security review, the IRS temporarily suspended this retrieval tool after detecting potentially unauthorized attempts to obtain IP PINs using the tool. Thus far, the IRS has confirmed and stopped about 5,000 false returns using a fraudulently obtained IP PIN. While our analysis is ongoing, at this time we do not believe any fraudulent refunds were issued as a result of successful unauthorized attempts to retrieve an IP PIN.

We are conducting a further review of this online tool and will strengthen its security features before bringing it back online. The IRS conducted an e-authentication risk assessment, following OMB guidelines, for the IP PIN retrieval tool, and has assigned an assurance level of 3F to this tool, so that taxpayers will have to undergo a multifactor authentication process to gain access once we bring the tool back online. Taxpayers who still need to retrieve a lost IP PIN in order to file their 2015 tax return can call the IRS, and we will mail the replacement IP PIN to the taxpayer's address of record.

Get Your Electronic Filing PIN Online Tool. Another way in which the IRS employs personal identification numbers involves the electronic signature on a tax return. When taxpayers electronically file a return, they sign their return by obtaining one of several types of PINs available through IRS.gov.

For example, the self-select PIN (SSP) method requires the taxpayer to use their prior-year adjusted gross income (AGI) or their prior-year SSP to authenticate their identity. They then select a five-digit PIN that can be any five numbers to enter as their electronic signature.

The IRS also provides an alternative to taxpayers unable to access their prior-year tax year return information for electronic signature authentication purposes. Using the Get Your Electronic Filing PIN application, taxpayers can enter identifying information and receive a temporary electronic filing PIN that can be used only for the current tax filing season. During FY 2015, taxpayers obtained approximately 25 million e-File PINs. On average, e-File PINs are used to sign about 12 million returns a year.

In January of this year, the IRS identified and halted an automated "bot" intrusion upon the Get Your Electronic Filing PIN application. In this intrusion, identity thieves employed malicious software, commonly known as "malware," to gain access to the application and generate e-File PINs for SSNs they had stolen from sources outside the IRS. Based on our review, we identified unauthorized attempts involving approximately 464,000 unique SSNs, of which 101,000 SSNs were used to successfully access an e-File PIN.

Nonetheless, our analysis of the situation found that no personal taxpayer data was compromised or disclosed by IRS systems, and no fraudulent refunds were issued. The IRS has taken steps to notify affected taxpayers by mail that their personal information was used in an attempt to access this IRS application. The IRS has also put returns filed under these SSNs through additional scrutiny to protect against future tax-related identity theft.

LOOKING TO THE FUTURE

Building an Authentication Framework

These incidents illustrate the challenges we face in developing appropriate authentication procedures for online transactions. The IRS takes protection of taxpayer data very seriously, and with that in mind, we must constantly strike a balance between citizen convenience and strong authentication and security protocols in an ever-changing cybercrime environment. The incidents also illustrate a wider truth about identity theft in general, which is that there are no perfect systems. No one, either in the public or private sector, can give an absolute guarantee that a system will never be compromised. For that reason, we continue our comprehensive efforts to update the security of our systems, protect taxpayers and their data, and investigate crimes related to stolen identity refund fraud.

We are reviewing our current e-authentication risk assessment process to ensure that the level of authentication risk for all current and future IRS online services accurately reflects the risk to the IRS and taxpayers should an authentication vulnerability occur.

We also realize that more needs to be done. A key element in our efforts to improve protections for existing online tools and new ones contemplated for the future is the development of a strong, coordinated and evolving authentication framework. This framework, once fully developed, will enable us to require multifactor authentication for all online tools and applications that warrant a high level of assurance.

To ensure proper development of our authentication framework, the IRS recently created a new position, the IRS Identity Assurance Executive. This executive will develop our Service-wide approach to authentication. In addition, we have engaged with the U.S. Digital Service (USDS), which uses the best of product design, engineering practices and technology professionals to build effective, efficient, and secure digital channels to transform the way government works for taxpayers.

We are joining forces with a team from USDS as we develop the future taxpayer digital experience and the foundational authentication standards that will enable secure digital exchanges between the IRS and taxpayers. In addition, we will leverage NIST standards to ensure that authentication processes used for all current and future online applications provide the required level of assurance for the determined level of authentication risk.

Going forward, we will continue to review and adjust our authentication protocols accordingly. The sophistication of today's cybercriminals and identity thieves requires us to continually reassess and modify these protocols.

Enhancing the Taxpayer Experience

Our efforts to detect and stop suspicious online activity and to develop a strong authentication framework are especially critical now, as the IRS builds toward the future and works to improve the online taxpayer experience for those taxpayers who prefer to communicate with us this way.

Within our tight budget constraints, the IRS has continued to analyze and develop plans for improving how the agency can fulfill its mission in the future, especially in delivering service to taxpayers.

We are looking forward to a new and improved way of doing business that involves a more robust online taxpayer experience. This is driven, in part, by business imperatives, since it costs between $40 and $60 to interact with a taxpayer in person, and less than $1 to interact online. But we also need to provide the best possible taxpayer experience, in response to taxpayer expectations and demands.

While we have spent the last several years developing new tools and applications to meet these taxpayer expectations and demands, we are now at the point where we believe the taxpayer experience needs to be taken to a new level. Our goal is to increase the availability and quality of self-service interactions, which will give taxpayers the ability to take care of their tax obligations online in a fast, secure and convenient manner.

The idea is that taxpayers would have an account with the IRS where they, or their preparers, could log in securely, get all the information about their account, and interact with the IRS as needed. Most things that taxpayers need to do to fulfill their federal tax obligations could be done virtually, and there would be much less need for in-person help, either by waiting in line at an IRS assistance center or calling the IRS.

As we improve the online experience, we understand the responsibility we have to serve the needs of all taxpayers, whatever their age, income, or location. We recognize there will always be taxpayers who do not have access to the internet, or who simply prefer not to conduct their transactions with the IRS online. The IRS remains committed to providing the services these taxpayers need. We do not intend to curtail the ability of taxpayers to deal with us by phone or in person.

In building toward the future of taxpayer service, we will need to strike a delicate balance with our efforts to improve our authentication protocols described above. Authentication protocols will need to be high, but not so high as to preclude taxpayers from legitimately using the online services we provide. As criminals become increasingly sophisticated, we will need to continue recalibrating our approach to authentication to continue maintaining this balance.

The Get Transcript online application is a good example of these tradeoffs. Under the original authentication method we required for the Get Transcript online application, we estimate that about 22 percent of legitimate taxpayers trying to access the application were unable to get through. We anticipate that under the multifactor authentication protocol to be implemented, an even higher percentage of taxpayers will be unable to use the tool. We will explain to taxpayers why these strong protections are necessary. All taxpayers will be able to order a transcript, online or by phone, and have it mailed to their address of record, if the online tool does not work for them, or if they prefer not to interact with us online.

Need for Adequate Resources and Legislative Solutions

An important consideration as we move into the future is the need for adequate resources to continue improving our efforts against identity theft and protecting our systems against cybercrime involving incidents, intrusions, and attacks. The IRS has been operating in an extremely difficult budget environment for several years, as our funding has been substantially reduced. In FY 2016, our funding level is more than $900 million lower than it had been in FY 2010.

Despite those reductions, the IRS still devotes significant resources to cybersecurity and identity theft, even though our total needs still exceeded our available funds.

As noted at the beginning of my testimony, Congress provided $290 million in additional funding for FY 2016, to improve service to taxpayers, strengthen cybersecurity and expand our ability to address identity theft. This action by lawmakers was a helpful development for the IRS and for taxpayers, and we appreciate it. Sustaining and increasing funds available for cybersecurity efforts at the IRS is critical this year and in the future. The IRS is using the new resources wisely and efficiently. This includes:

- ***Cybersecurity.*** We are using approximately $95.4 million to invest in a number of critical security improvements, including more effective monitoring of data traffic and replacement of technology that supports the development, maintenance and operation of IRS applications to make processes more secure, reliable and efficient. The funding will help us to improve systems and defenses across the entire IRS, thereby helping to protect taxpayer data. We are also investing in systems to allow for enhanced network segmentation, which involves further subdividing our network, so that if any vulnerabilities occur, they would be contained to just one portion of the network.

- ***Identity Theft.*** We are using approximately $16.1million to develop advanced secure access capabilities for applications such as Get Transcript, IP PIN and others. This will also fund advanced analytics and

detection of anomalies in returns filed. In addition, this investment will allow the IRS to partner with private industry and state tax agencies through the Security Summit to, for the first time, share information systemically about suspicious activity in the tax system.

Taxpayer Service. As described in detail above, we are using approximately $178.4 million provided in the additional $290 million to add about 1,000 extra temporary employees to help improve our service on our toll-free phone lines during the filing season.

The FY 2017 President's Budget sustains and bolsters funding for these important programs. This includes $90 million in additional funding to help prevent identity theft and refund fraud and to reduce improper payments. This funding will increase the capacity of our most important programs discussed above, including external leads and criminal investigations. New funds will allow the IRS to close almost 100,000 additional identity theft cases per year by helping victimized taxpayers who have engaged the IRS for assistance. The number of identity theft cases has grown from 188,000 in FY 2010 to 730,000 in FY 2014, and current resources can only close about 409,000 per year.

The FY 2017 President's Budget also requests cybersecurity funds provided through a Department wide Cybersecurity Enhancement account, which will bolster Treasury's overall cybersecurity posture. Of the nearly $110 million requested in the account, $54.7 million will directly support IRS cybersecurity efforts by securing data, improving continuous monitoring, and other initiatives. An additional $7.4 million will be used to continue development and implementation of electronic authentication systems currently being developed for the Get Transcript online application for our expanding set of digital services.

While adequate funding is critical to improving our cybersecurity efforts, Congress also provides important support to the IRS by passing legislative proposals that improve tax administration. An excellent example is the enactment last December of the requirement for companies to file Form W-2s and certain other information returns earlier in the year than now. Having W-2s earlier will make it easier for the IRS to verify the legitimacy of tax returns at the point of filing and to spot fraudulent returns.

Although the new law is not effective until the 2017 filing season, some employers that issue large volumes of W-2s agreed this year to voluntarily file them earlier in the year, so the benefit of the change is already beginning to be felt. This year we received early submissions of about 26 million W-2s, most of which came in by the end of January. The IRS is using this data in our program to verify claims of wages and withholding on individual income tax returns. We expect this to assist in the quicker release of refunds for those returns we are able to verify.

We have asked Congress for other changes to enhance tax administration and help us in our efforts to improve cybersecurity. An important proposal is the reauthorization of so-called streamlined critical pay authority, originally enacted in 1998, to assist the IRS in bringing in individuals from the private sector with the skills and expertise needed in certain highly specialized areas, including IT, international tax and analytics support. This authority, which ran effectively for many years, expired at the end of FY 2013 and was not renewed.

The loss of streamlined critical pay authority has created major challenges to our ability to retain employees with the necessary high-caliber expertise in the areas mentioned above. In fact, out of the many expert leaders and IT executives hired under critical pay authority, there are only 10 IT experts remaining at the IRS, and we anticipate there will be no staff left under critical pay authority by this time next year. The President's FY 2017 Budget proposes reinstating this authority, and I urge the Congress to approve this proposal.

Chairman Roskam, Ranking Member Lewis and Members of the Subcommittee, this concludes my statement. I would be happy to take your questions.

Chairman ROSKAM. Thank you, Commissioner.
Mr. Camus.

STATEMENT OF TIMOTHY CAMUS, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS AND TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, U.S. DEPARTMENT OF THE TREASURY

Mr. CAMUS. Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to discuss the Internal Revenue Service's 2016 tax filing season.

TIGTA continues to identify security of taxpayer data as fraudulent claims as major management challenges facing the IRS. Both challenges continue to play a significant role in this year's tax filing season.

Since 2012, TIGTA has issued a series of reports assessing the IRS' efforts to detect and prevent fraudulent tax refunds resulting from identity theft. The IRS has implemented many of TIGTA's recommendations and has continued its efforts to improve its detection processes.

However, tax related identity theft remains a major challenge for the IRS. At the same time, cybersecurity threats against the Federal Government continue to grow. The IRS is a prime target for attacks because of the extensive amounts of taxpayer data it stores and refund amounts it issues each year.

Because of this, the risk of unauthorized access to tax accounts, the potential theft of taxpayer information from the IRS and refund fraud will continue to grow. For example, in August 2015, the IRS reported that unauthorized users had been successful in obtaining information from the Get Transcript application for an estimated 334,000 taxpayer accounts.

To prevent further unauthorized accesses, the IRS disabled the application on its Web site. TIGTA's current review of the Get Transcript breach identified additional suspicious accesses to taxpayers' accounts that the IRS had not initially identified. We believe that more than 724,000 taxpayer transcripts may have been stolen.

TIGTA is participating in a multi-agency criminal investigation into this matter. We have also provided the IRS with some of our investigative observations to date in order to help them secure their e-authentication environment going forward.

We also reported in November 2015 that the IRS did not complete the required authentication risk assessment for its online identity protection personal identification number, or IP PIN application. We recommended that the IRS not reactivate this application for the 2016 filing season.

However, the IRS reactivated the application on January 19th, 2016.

We issued a second recommendation to the IRS on February 24th to remove the IP PIN application from its public Web site. On March 7th, the IRIS reported that it was temporarily suspending the use of the IP PIN application. The IRS also reported that 800 stolen IP PINs had been used to file fraudulent tax returns.

Tax refund fraud and identity theft issues are not limited to unscrupulous individuals operating from outside of the IRS. We have

conducted a number of significant investigations involving identity theft by IRS employees.

In one recent prosecution case, we identified an IRS employee who, through her access to IRS data systems, stole the information of hundreds of taxpayers. She subsequently used this information in an attempt to obtain between $550,000 and $1.5 million in fraudulent refunds.

We believe the IRS must prioritize its focus on insider threat posed by IRS employees by increasing and improving its application audit trails.

Other challenges to the IRS' ability to efficiently administer the Nation's tax laws include a telephone impersonation scam. Since October 2013, we have received over one million complaints from taxpayers who reported that individuals called them, claimed to be IRS employees, and then demanded money.

This scam is the largest, most pervasive impersonation scam in the history of our agency. It has claimed over 5,700 victims with reported losses totaling more than $31 million to date.

We also continue to receive reports of individuals who have become victims of lottery winning scams, and we are also seeing an increase in the number of reported IRS fishing attempts.

TIGTA and our law enforcement partners have made several arrests in connection with many of these scams, and we have over 100 investigations currently underway. As the number and sophistication of threats to taxpayer information will likely increase, they will be a continued focus of our audit and investigative coverage, and we will continue to provide the IRS with information necessary to protect taxpayers.

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to share my views.

[The prepared statement of Mr. Camus follows:]

TESTIMONY
OF
TIMOTHY P. CAMUS
DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON OVERSIGHT
U.S. HOUSE OF REPRESENTATIVES

"The 2016 Tax Filing Season"
April 19, 2016

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to testify on the topic of tax scams and schemes faced by the Internal Revenue Service (IRS) during the 2016 tax return filing season.

The Treasury Inspector General for Tax Administration (TIGTA) is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of IRS operations, including the IRS Chief Counsel. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA plays a critical role in ensuring the approximately 86,000 IRS employees[1] who collected over $3.3 trillion in tax revenue, processed over 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2015,[2] have done so in an effective and efficient manner while minimizing the risks of waste, fraud, and abuse.

TIGTA's Office of Audit (OA) reviews all aspects of Federal tax administration and provides recommendations to improve IRS systems and operations; ensure the fair and equitable treatment of taxpayers; and detect and prevent waste, fraud, and abuse in tax administration. The Office of Audit places an emphasis on statutory coverage required by the IRS Restructuring and Reform Act of 1998 (RRA 98)[3] and other laws, as well as on areas of concern raised by Congress, the Secretary of the Treasury, the Commissioner of Internal Revenue, and other key stakeholders. The OA has examined

---

[1] Total IRS staffing as of October 3, 2015. Included in the total are approximately 15,400 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2015.*
[3] Pub. L. No. 105-206, 112 Stat. 685 (1998) (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

specific high-risk issues such as identity theft, refund fraud, improper payments, information technology, security vulnerabilities, complex modernized computer systems, tax collections and revenue, and waste and abuse in IRS operations.

TIGTA's Office of Investigations (OI) protects the integrity of the IRS by investigating allegations of IRS employee misconduct, external threats to IRS employees and facilities, and other attempts to impede or otherwise interfere with the IRS's ability to collect taxes. Specifically, OI investigates misconduct by IRS employees which manifests itself in many ways, including unauthorized access to taxpayer information and the use of the information for the purposes of identity theft; extortion; theft of government property; Section 1203 taxpayer abuses; false statements; and other financial fraud. For example, as will soon be reported in our upcoming Semiannual Report to Congress, in the past six months, TIGTA investigations resulted in Federal prosecution action on six IRS employees whose criminal activity impacted over 240 taxpayers and cost the Government the payment of hundreds of thousands of dollars in fraudulent refunds. Although the six IRS employees involved in this criminal activity represent a very small percentage of the total IRS employee population, their actions negatively impacted the public's perception of the integrity of the Federal tax system; therefore, allegations of IRS employee misconduct will remain one of our primary investigative priorities.

Since the summer of 2013, a significant amount of OI's workload has consisted of investigating a telephone impersonation scam in which more than one million intended victims have received unsolicited telephone calls from individuals falsely claiming to be IRS or Department of the Treasury employees. The callers demand money under the pretense that the victim owes unpaid taxes. To date, over 5,700 victims have purportedly paid more than $31 million to these criminals.

In the last several years, threats directed at the IRS have remained the second largest component of OI's work. Physical violence, harassment, and intimidation of IRS employees continue to pose challenges to the implementation of a fair and effective system of tax administration. The Office of Investigations is statutorily charged to investigate threats made against IRS employees, facilities, and data and is committed to ensuring the safety of IRS employees as well as the taxpayers who conduct business at the approximately 550 IRS offices[4].

In this section of my testimony, I will briefly discuss the status of the 2016 tax return Filing Season and the tax scams and schemes that the IRS is currently facing as

---

[4] IRS, *Management's Discussion & Analysis, Fiscal Year 2015.*

it administers our Nation's tax laws.

STATUS OF THE 2016 FILING SEASON

The annual tax return filing season[5] is a critical time for the IRS as this is when most individuals file their income tax returns and contact the IRS if they have questions about specific tax laws or filing procedures. During Calendar Year (CY) 2016, the IRS expects to receive more than 150 million individual income tax returns, approximately 19 million paper filed and 131 million filed electronically (e-filed).

Among the continuing challenges the IRS faces each year in processing tax returns are the implementation of new tax law changes and changes resulting from expired tax provisions. Before the filing season begins, the IRS must identify the tax law and administrative changes affecting the upcoming filing season. Once these have been identified, the IRS must revise the various tax forms, instructions, and publications affected by the changes. It also must reprogram its computer systems to ensure that tax returns are accurately processed based on changes in the tax law. Errors in the IRS's tax return processing systems may delay tax refunds, affect the accuracy of taxpayer accounts, or result in incorrect taxpayer notices.

For the 2016 Filing Season, the IRS was challenged by the late passage of legislation that extended a number of expired tax provisions.[6] To reduce the impact on the filing season, the IRS monitored the status of the legislation and took steps to implement the extension of these provisions prior to their enactment. These efforts enabled the IRS to begin accepting and processing individual tax returns on January 19, 2016, as scheduled. As of March 4, 2016, the IRS had received more than 66.7 million tax returns—more than 62.6 million (93.9 percent) of which were e-filed and more than 4 million (6.1 percent) of which were filed on paper. The IRS has issued more than 53.5 million refunds totaling more than $160 billion.

Implementation of provisions of the Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act of 2010[7] (collectively referred to as the Affordable Care Act or ACA) will also continue to present challenges for the IRS in the 2016 Filing Season. As of February 25, 2016, the IRS had processed 1.4 million tax returns that reported $4.4 billion in Premium Tax Credits that were either received

---

[5] The period from January 1 through mid-April when most individual income tax returns are filed.
[6] TIGTA, Ref. No. 2016-40-034, *Interim Results of the 2016 Filing Season* (Mar. 2016).
[7] Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the Internal Revenue Code and 42 U.S.C.), as amended by the Heath Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.

in advance or claimed at the time of filing. As of March 3, 2016, the IRS had received approximately 47 million tax returns reporting that all members of the taxpayer's family maintained minimum essential coverage as required by the ACA. In addition, more than 2.7 million taxpayers reported shared responsibility payments totaling $1 billion for not maintaining the required health insurance coverage.

For the 2016 Filing Season, taxpayers have several options to choose from when they need assistance from the IRS, including assistance through the toll-free telephone lines,[8] face-to-face assistance at the Taxpayer Assistance Centers (TAC) or Volunteer Program sites, and self-assistance through IRS.gov and various other social media channels (*e.g.*, Twitter, Facebook, and YouTube). The IRS continues to increase its dependence on technology-based services and external partners that direct taxpayers to the most cost-effective IRS or partner channel available to provide the needed service. The IRS notes that this approach allows it to focus limited toll-free and walk-in resources on customer issues that can be best resolved with person-to-person interaction. However, the cuts made by the IRS in its traditional services continue to significantly affect a number of areas.

For example, the IRS reports that, as of March 5, 2016, approximately 46.1 million attempts had been made to contact the IRS via its toll-free assistance lines for the 2016 Filing Season. Assistors have answered approximately 7.3 million calls and have achieved a 72.8 percent Level of Service[9] with a 9.6 minute Average Speed of Answer.[10] As a result of the IRS receiving additional funding for customer service in FY 2016, the IRS is forecasting a 65 percent Level of Service for the 2016 Filing Season, which is an increase from the 38 percent it originally forecasted. Overall, the IRS is forecasting a 47 percent Level of Service for the full fiscal year, which is an increase from its original forecast of 34 percent. We are currently assessing the IRS's process for allocating its Customer Service budget.

In addition, each year many taxpayers seek assistance from one of the IRS's 376 walk-in offices, called TACs. However, the IRS estimates that the number of taxpayers it will assist at its TACs will continue to decrease. The IRS assisted 5.6 million taxpayers in FY 2015 and plans to assist 4.7 million taxpayers in FY 2016, which represents a 16 percent decline from FY 2015.

---

[8] The IRS refers to the suite of 29 telephone lines to which taxpayers can make calls as "Customer Account Services Toll-Free".
[9] The primary measure of service to taxpayers. It is the relative success rate of taxpayers who call for live assistance on the IRS toll-free telephone lines.
[10] The average number of seconds taxpayers waited in the assistor queue (on hold) before receiving services.

However, the IRS has implemented initiatives to better assist those individuals seeking assistance from a TAC. For example, in CY 2015, the IRS began providing services at selected TACs by appointment, in an attempt to alleviate long lines that sometimes occur at many TACs and to help ensure that taxpayers' issues are resolved. The IRS reports that as of February 29, 2016,[11] 166,569 taxpayers had scheduled an appointment. The IRS also offers Virtual Service Delivery, which integrates video and audio technology to allow taxpayers to see and hear an assistor located at a remote TAC. For the 2016 Filing Season, the IRS is offering Virtual Service Delivery at 35 locations, which include 24 TACs and 11 Volunteer Program sites. The IRS reports that 8,137 taxpayers had used the service as of February 29, 2016.

TAX REFUND FRAUD

The IRS is continuing to expand its efforts to detect tax-refund fraud. The IRS reports that, as of March 5, 2016, it had identified 42,148 tax returns with nearly $227 million claimed in fraudulent refunds. Moreover, it had prevented the issuance of $180.6 million (79.6 percent) in fraudulent refunds and also identified 20,224 potentially fraudulent tax returns filed by prisoners during this year's filing season. The IRS also reports that, as of February 29, 2016, it had identified and confirmed 31,578 fraudulent tax returns and prevented the issuance of $193.8 million in fraudulent tax refunds as a result of its identity-theft filters. Finally, the IRS is continuing to expand on its use of controls to identify fraudulent refund claims before they are accepted into the processing system. As of February 29, 2016, it had identified approximately 35,000 fraudulent e-filed tax returns and approximately 741 fraudulent paper tax returns.

TIGTA continues to identify fraudulent claims as an IRS major management challenge. As such, we continue to evaluate the IRS's efforts to improve fraudulent tax return filing detection processes, including its efforts to implement TIGTA's recommendations.

In November 2015,[12] TIGTA reported that a programming error resulted in over $27 million in refunds being erroneously issued for more than 13,000 Tax Year (TY) 2013 returns before the income and withholding had been screened and verified. Each of these tax returns was identified by the IRS as potentially fraudulent. In addition,

---

[11] For Fiscal Year 2016 – October 1, 2015 through February 29, 2016.
[12] TIGTA, Ref. No. 2016-40-006, *Improvements Are Needed to Better Ensure That Refunds Claimed on Potentially Fraudulent Tax Returns Are Not Erroneously Released* (Nov. 2015).

TIGTA reported that ineffective monitoring of potentially fraudulent tax returns had resulted in the erroneous release of $19 million in refunds for 3,910 TY 2013 tax returns. Each of these returns was selected by the IRS; however there was no indication that tax examiners had verified the returns prior to the refund being issued. The IRS agreed with TIGTA recommendations to address the concerns identified.

Clearly, tax-related identify theft is a major challenge still facing the IRS. Since 2012, TIGTA has issued a series of reports assessing the IRS's efforts to detect and prevent fraudulent tax refunds resulting from identity theft. In July 2012, we reported that the impact of identity theft on tax administration is significantly greater than the amount the IRS detects and prevents. Our analysis of TY 2010 tax returns identified approximately 1.5 million undetected tax returns with potentially fraudulent tax refunds, totaling in excess of $5.2 billion, which had the characteristics of identity theft confirmed by the IRS.[13]

For example, in response to our reporting that the IRS did not have a process to measure the impact of identity theft, the IRS initiated a research project in CY 2012 to develop a measurement process to assess its efforts to defend against identity theft and identify areas that require additional effort. For the 2014 Filing Season, the IRS reported that identity thieves had been successful in receiving approximately $3.1 billion in fraudulent tax refunds. TIGTA is evaluating the accuracy of the IRS's measurement process and expects to issue its report early next fiscal year.

The IRS has implemented many of TIGTA's recommendations and has continued in its efforts to improve its detection processes. In the 2014 Filing Season, the IRS reported that it had detected and prevented approximately $21.5 billion in identity theft refund fraud.

The IRS is locking the tax accounts of deceased individuals to prevent others from filing a tax return using their names and Social Security Numbers (SSN). The IRS locked approximately 30.2 million taxpayer accounts between January 2011 and December 31, 2015. For Processing Year 2015, the IRS rejected approximately 77,000 fraudulent e-filed tax returns and prevented about 16,000 paper-filed tax returns through the use of these locks as of April 30, 2015.

The IRS also continues to expand the number of filters it uses to detect identity theft refund fraud at the time tax returns are processed. Those filters increased from

---

[13] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

11 filters for the 2012 Filing Season to 183 filters for the 2016 Filing Season. Tax returns identified by these filters are held during processing until the IRS can verify the taxpayers' identities. As of December 31, 2015, the IRS reported that it had identified and confirmed more than one million fraudulent tax returns and prevented the issuance of nearly $6.8 billion in fraudulent tax refunds as a result of the identity theft filters.

After TIGTA continued to identify large volumes of undetected potentially fraudulent tax returns with tax refunds issued to the same address or deposited into the same bank account, the IRS developed and implemented a clustering filter tool during the 2013 Filing Season. This tool groups tax returns based on characteristics that include address and bank routing numbers. Tax returns identified are held from processing until the IRS can verify the taxpayer's identity. As of December 31, 2015, the IRS reported that, using this tool, it identified 835,183 tax returns claiming approximately $4.3 billion in potentially fraudulent tax refunds.

A new process, also implemented during the 2015 Filing Season, limits the number of direct deposit refunds that can be sent to a single bank account to three deposits. The IRS converts the fourth and subsequent direct deposit refund requests to a specific account to a paper refund check and mails the check to the taxpayer's address of record. In August 2015, we reported that programming errors resulted in some direct deposit refunds not converting to a paper check as required.[14]

As noted earlier in my testimony, unfortunately, tax refund fraud and identity theft is not limited to unscrupulous individuals operating from outside of the IRS; there is also an insider threat posed by IRS employees who use their official positions and access to IRS information in furtherance of these schemes. For example, one of the most significant recent cases involved an IRS employee who, through their access to IRS data, stole the IRS information of hundreds of taxpayers, and then used that information in an attempt to obtain between $550,000 and $1.5 million in fraudulent refunds. The employee was able to successfully steal over $438,000 in fraudulent refunds.[15] We detected this criminal activity through our ability to review the audit trails of accesses made by IRS employees to the IRS computer systems. We remain very concerned that as the IRS has modernized its systems over the last several years, it has not built in adequate audit trails that would allow us to detect an IRS employee's unauthorized access to taxpayer information. Although we are discussing this vulnerability with the IRS Information Technology leadership, the pace of progress is not acceptable. For example, currently only 12 of the 82 applications subject to the risk

---

[14] TIGTA, Ref. No. 2015-40-080, *Results of the 2015 Filing Season* (Aug. 2015).
[15] N.D. Ala. Plea Agreement Nakeisha Hall filed Feb. 8, 2016.

of unauthorized access and theft of taxpayer information are currently transmitting accurate and complete audit trail data. The IRS estimates that it will have this vulnerability addressed between FY 2021 and FY 2027.

In December 2015, Congress passed legislation to address TIGTA's ongoing concern about limitations in the IRS's ability to prevent the continued issuance of billions of dollars in fraudulent tax refunds.[16] We reported that the IRS did not have timely access to third-party income and withholding information needed to make substantial improvements in its fraud detection efforts. The recently enacted legislation now requires the annual filing of income and withholding information by January 31, beginning in 2017.[17] Access to this information at the beginning of the filing season is the single most important tool to detect and prevent tax fraud-related identity theft. TIGTA will be reviewing the IRS's use of the income and withholding information returns as part of its FY 2017 assessment of efforts to detect and prevent identity theft.

Identity theft also affects businesses. In September 2015, TIGTA determined that processing filters could be developed to identify business tax returns containing certain characteristics that could indicate potential identity-theft cases.[18] TIGTA also reported that State information sharing agreements do not address business identity theft and that actions are needed to better promote awareness of business identity theft. The IRS agreed with our recommendations.

In order to continue to improve its detection efforts, the IRS needs expanded capabilities in its fraud detection system. The IRS's current fraud detection system does not allow the IRS to change or adjust identification filters throughout the processing year. The IRS is developing and testing a replacement fraud detection system, called the Return Review Program (RRP), which the IRS believes will provide new and improved capabilities that advance its fraud detection and prevention to a higher level.

The IRS conducted a pilot test of the RRP scoring and models during Processing Year 2014 to assess its effectiveness in identifying potential identity-theft tax returns. In December 2015, TIGTA reported that although the pilot successfully identified tax returns involving identity theft that were not identified by the IRS's other

---

[16] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. Q, § 201 (2015).
[17] *Id.*
[18] TIGTA, Ref. No. 2015-40-082, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* (Sept. 2015).

fraud detection systems, it did not detect all the fraudulent tax returns identified by its existing fraud detection systems.[19]

IRS ASSISTANCE TO VICTIMS OF IDENTITY THEFT

TIGTA has identified continuing issues with victim assistance. In September 2013, TIGTA reported that, on average, it took the IRS 312 days to resolve tax accounts of identity-theft victims due a refund in FY 2012.[20] In March 2015, we reported that taxpayers were still experiencing long delays in resolving their tax accounts and that the IRS continued to make errors on the victims' tax accounts.[21] Our review of a statistically valid sample of 100 identity-theft tax accounts resolved by the IRS during FY 2013 identified that the IRS took an average of 278 days to resolve the tax accounts and did not correctly resolve 17 of the 100 accounts (17 percent) we reviewed. We estimate that of the 267,692 taxpayer cases resolved during this period, 25,565 (10 percent) may have been resolved incorrectly resulting in delayed or incorrect refunds and requiring the IRS to reopen cases to resolve the errors.

In October 2008, the IRS formed the Identity Protection Specialized Unit (IPSU) as part of its strategy to reduce taxpayer burden caused by identity theft. The IPSU is a dedicated unit for victims of identity theft to have their questions answered and obtain assistance in resolving their identity-theft issues quickly and effectively. In October 2015, we reported that the majority of identity-theft victims are no longer provided with an IPSU single point of contact.[22] The IRS indicated that budgetary constraints did not allow for a single employee to be assigned to each identity-theft victim. However, the IRS has stated that it remains committed to providing identity-theft victims with the centralized IPSU hotline to obtain assistance. The IRS noted that obtaining assistance via contact with the hotline does not depend on the availability of a single IRS representative, who may be unavailable because he or she is performing other casework. We also found that the IPSU's process does not ensure that taxpayers are timely informed about the IRS's receipt of their supporting documentation or the status of their identity-theft claims.

---

[19] TIGTA, Ref. No. 2016-40-008, *Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection* (Dec. 2015).
[20] TIGTA, Ref. No. 2013-40-129, *Case Processing Delays and Tax Account Errors Increased Hardship for Victims of Identity Theft* (Sept. 2013).
[21] TIGTA, Ref. No. 2015-40-024, *Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds* (Mar. 2015).
[22] TIGTA, Ref. No. 2016-40-003, *Improvements Are Needed in the Identity Protection Specialized Unit to Better Assist Victims of Identity Theft* (Oct. 2015).

On May 4, 2015, the IRS announced the final phase of its plan to consolidate its identity-theft assistance and compliance activities into a new organization called the Identity Theft Victim Assistance Directorate. The IRS indicated that this new directorate aims to provide consistent treatment to victims of tax-related identity theft. We plan to review the IRS's implementation of this organization as part of our FY 2016 audit coverage.

IRS "GET TRANSCRIPT" DATA BREACH

The risk of unauthorized access to tax accounts and the potential theft of taxpayer information from the IRS will continue to grow as the IRS focuses its efforts on delivering online tools to taxpayers. The IRS plans to increase the availability and quality of self-service interactions, allowing it to free up in-person resources for taxpayers who truly need them. The IRS's goal is to eventually provide taxpayers with dynamic online account access that includes viewing their recent payments, making minor changes and adjustments to their accounts, and corresponding digitally with the IRS. As tax administration evolves, the challenge of providing adequate data security will continue.

In a report issued in November 2015, TIGTA found that although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, it has not established a Service-wide approach to managing its authentication needs.[23] As a result, the level of authentication the IRS uses for its various services is not consistent. The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system.

Unscrupulous individuals constantly seek to identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information. For example, on May 26, 2015, the IRS announced that individuals using taxpayer-specific data had attempted to gain unauthorized access to tax information[24] through the e-authentication portal and into the Get Transcript application. According to the IRS, one or more individuals succeeded in clearing the IRS's authentication process, which required knowledge of information about individual taxpayers, including

---

[23] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
[24] The tax information that can be accessed on the Get Transcript application can include the current and three prior years of tax returns, nine years of tax account information, and wage and income information.

Social Security information, date of birth, tax filing status, and street address. The unauthorized accesses resulted in the IRS disabling the application.

Office of Management Budget (OMB) standards require Federal agencies to conduct an assessment of the risk of authentication error for each online service or application they provide. An authentication error occurs when an agency confirms the identity provided by an individual, despite the fact that the individual is not who he or she claims to be. In addition, the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Special Publication 800-63 establishes specific requirements that agencies' authentication processes must meet to provide a specific level of authentication assurance. However, we found that, although the IRS has established processes and procedures to authenticate individuals requesting online access to IRS services, these processes and procedures do not comply with Government standards for assessing authentication risk and establishing adequate authentication processes.

The IRS assessed the risk of the Get Transcript application as required. However, the IRS determined that the authentication risk associated with Get Transcript was low to both the IRS and taxpayers. The IRS defines a low risk rating as one in which the likelihood of an imposter obtaining and using the information available on an application is low. In addition, a low risk rating indicates that controls are in place to prevent, or at least significantly impede, an imposter from accessing the information. As a result, the IRS has implemented single-factor authentication to access the Get Transcript application.

In August 2015, the IRS indicated that unauthorized users had been successful[25] in obtaining information on the Get Transcript application for an estimated 334,000 taxpayer accounts. TIGTA's current review[26] of the Get Transcript breach has identified additional suspicious accesses to taxpayers' accounts that the IRS had not identified. Based on TIGTA's analysis of Get Transcript access logs, the IRS reported on February 26, 2016 that potentially unauthorized users had been successful in obtaining access to an additional 390,000 taxpayer accounts, for a total of over 724,000 stolen transcripts. The IRS also reported that an additional 295,000 taxpayer transcripts had been targeted but the access attempts had not been successful. TIGTA was able to identify these additional unauthorized accesses due to our use of advanced analytics and cross-discipline approaches. The IRS had not

---

[25] A successful access is one in which the unauthorized users successfully answered identity proofing and knowledge-based authentication questions required to gain access to taxpayer account information.
[26] TIGTA, Audit No. 201540027, *Evaluation of Assistance Provided to Victims of the Get Transcript Data Breach*, report planned for May 2016.

previously identified these accesses because of limitations in the scope of its analysis, including its method of identifying suspicious e-mail accounts and the timeframe it analyzed.

In response to TIGTA's identification of the additional accesses, the IRS started mailing notification letters on February 29, 2016 to the affected taxpayers and placing identity-theft markers on their tax accounts. It should be noted that the actual number of individuals whose personal information was available to the potentially unauthorized individuals accessing these tax accounts is significantly larger than the number of taxpayers whose accounts were accessed in that these tax accounts include certain information on individuals other than the taxpayers listed on these tax returns (*e.g.*, spouses and dependents).

We are currently evaluating the appropriateness of the IRS's response to the Get Transcript incident and the IRS's proposed solutions to address the authentication weakness that allowed the incident to occur.[27] To date, we have learned that the IRS is working with the U.S. Digital Service[28] on its new e-authentication and authorization policies and procedures.

In addition, TIGTA is participating in a multi-agency investigation into this matter, and we have provided the IRS with some of our investigative observations to date in order to help them secure the e-authentication environment in the future. During its investigation, TIGTA has observed that the unauthorized accesses and the thefts of tax transcripts from the Get Transcript application have been occurring for some time, not long after the application was initially made available to the public until the IRS disabled it in May 2015. In addition to the investigative activity based on the May 2015 data breach, TIGTA is also investigating an additional 22 other cases involving transcripts that were stolen from the Get Transcript application and then used to file fraudulent refund tax returns.

For example, in one case, our investigation revealed that the defendant broke into the Get Transcript application and obtained 22 transcripts. He then filed over 100 fraudulent tax returns seeking $500,000 in fraudulent IRS refunds.[29] In a separate case, the defendant and co-conspirators stole over 1,200 transcripts from the Get Transcript application. They then used the stolen information to file over 2,900

---

[27] TIGTA, Audit No. 201520006, *Review of Progress to Improve Electronic Authentication*, report planned for July 2016.
[28] The U.S. Digital Service is part of Executive Office of the President. Its goal is to improve and simplify the digital services that people and businesses have with the Government.
[29] Department of Justice Press Release, S.D. Fla dated Mar. 1, 2016.

fraudulent tax returns seeking $25 million in refunds. The IRS stopped most of the fraudulent refunds, but ultimately paid $4.7 million in fraudulent refunds to the defendant and his co-conspirators.[30] In both cases, the Get Transcript information was stolen from between early February 2015 and April 30, 2015.

Finally, we also reported in November 2015 that the IRS did not complete the required authentication risk assessment for its online Identity Protection Personal Identification Number (IP PIN)[31] application. On January 8, 2016, we recommended that the IRS not reactivate its online IP PIN application for the 2016 Filing Season, due to concerns that the IP PIN authentication process requires knowledge of the same taxpayer information that was used by the individuals who breached the Get Transcript application. Notwithstanding our recommendation, the IRS reactivated the application on January 19, 2016. We issued a second recommendation to the IRS on February 24, 2016, advising it to disable the IP PIN application from its public website to prevent any further abuse.

On March 7, 2016, the IRS reported that it was temporarily suspending use of the IP PIN application as part of an ongoing security review. The IRS also reported that 800 stolen IP PINs had been used to file fraudulent refund returns. The IRS advised that it is conducting a further review of the application that allows taxpayers to retrieve their IP PINs online and is looking at further strengthening its security features. The IRS does not anticipate having the technology in place to provide multifactor authentication capability for either the Get Transcript or IP PIN application before the summer of 2016.

No single authentication method or process will prevent criminals from filing identity-theft tax returns or attempting to inappropriately access IRS services. However, strong authentication processes can reduce the risk of such activity by making it harder and more costly for individuals to gain unauthorized access to resources and information. Therefore, it is important that the IRS ensure that its authentication processes are in compliance with NIST standards to provide the highest degree of assurance that valuable taxpayer information is protected from criminals.

---

[30] D. Or. Indictment Michael O. Kazeem filed Feb. 4, 2016.
[31] To provide relief to tax-related identity-theft victims, the IRS issues IP PINs to taxpayers who are confirmed by the IRS as victims of identity theft, taxpayers who are at a high risk of becoming a victim such as taxpayers who call reporting a lost or stolen wallet or purse, as well as taxpayers who live in three locations that the IRS has identified as having a high rate of identity theft (Florida, Georgia and the District of Columbia).

TELEPHONE IMPERSONATION SCAM

As noted earlier in my testimony, the telephone impersonation scam continues to be one of TIGTA's top priorities; it has also landed at the top of the IRS's "Dirty Dozen" tax scams. The numbers of complaints we have received about this scam continues to climb, cementing its status as the largest, most pervasive impersonation scam in the history of our agency. It has claimed thousands of victims, including victims in every State represented on this committee, with reported losses totaling more than $31 million to date.

We started receiving reports of this particular phone scam in August 2013. As the reporting continued through the Fall, we started to specifically track this crime in October 2013. TIGTA currently receives between 10,000 and 19,000 reports of these calls each week. To date, TIGTA has received more than one million reports of these calls. As of April 4, 2016, 5,770 victims of this scam have reported to TIGTA they have collectively paid a total of more than $31 million, an average of approximately $5,370 per victim. The highest reported loss by any one individual exceeded $500,000. In addition, more than 1,275 of these victims reported that they also provided sensitive identity information to the scammers.

Here is how the scam works: The intended victim receives an unsolicited telephone call from a live person or from an automated call dialer. The caller, using a fake name and sometimes a fictitious employee badge number, claims to be an IRS or Treasury employee. The scammers use Voice over Internet Protocol technology to hide their tracks and create false telephone numbers that show up on the victim's caller ID system. For example, the scammers may make it appear as though the calls are originating from Washington, D.C., or elsewhere in the U.S.

The callers may even know the last four digits of the victim's SSN or other personal information about the victim. The caller claims that the intended victim owes the IRS taxes and that, if those taxes are not paid immediately, the victim will be arrested or charged in a lawsuit. Other threats for non-payment include the loss of a driver's license, deportation, or loss of a business license. They often leave "urgent" messages to return telephone calls and they often call the victim multiple times.

According to the victims we have interviewed, the scammers who made the threatening statements as described above then demanded that the victims immediately pay the money using prepaid debit cards, wire transfers, Western Union payments or MoneyGram payments in order to avoid being immediately arrested. They are typically warned that if they hang up, local police will come to their homes to arrest them immediately. Sometimes the scammers also send bogus IRS e-mails to

support their claims that they work for the IRS. By the time the victims realize that they have been scammed, the funds are long gone.

Over time, the scam has evolved from live callers demanding payment using prepaid debit cards to scammers using automated call dialers, or "robo-dialers," to place thousands of calls very rapidly. When the intended victim answers the phone, the automated voice states that the victim owes the IRS taxes. The victims are informed that if they do not immediately call a telephone number provided in the message, they will face arrest and possibly a lawsuit.

TIGTA has made several arrests in connection with this scam and has numerous investigations underway. In one of the largest prosecutions on this scam that we have had to date, in July 2015, an individual plead guilty to organizing an impersonation scam ring and was sentenced to over 14 years of incarceration and a $1 million dollar forfeiture. While we cannot provide specific details of our additional ongoing investigations out of concern that it will hinder our ability to prosecute those responsible, we can describe for you some of the other steps TIGTA is taking to combat this scam.

To thwart scammers using robo-dialers, we have created and instituted an "Advise and Disrupt" strategy. The strategy involves cataloguing the telephone numbers that were reported by intended victims. We then use our own automated call dialers to make calls to those telephone numbers to advise the scammers that their activity is criminal and to cease and desist their activity. As of April 8, 2016, we have placed more than 59,000 automated calls back to the scammers.

Also, we are working with the telephone companies to have the scammers' telephone numbers shut down as soon as possible. Of the 626 telephone numbers that have been reported by victims, we have successfully shut down over 75 percent of them, some of them within one week of the number's being reported to us.

TIGTA is also publishing those telephone numbers that have been used by the scammers on the Internet. This provides intended victims an additional tool to help them determine if the call is part of a scam. All they have to do is type the telephone number in any search engine, and the response will indicate whether the telephone number has been identified as part of the impersonation scam. These efforts are producing results: our data show it now takes hundreds of calls to defraud one victim, whereas in the beginning of the scam it took only double digit attempts.

In addition, TIGTA is engaged in public outreach efforts to educate taxpayers

about the scam. These efforts include publishing press releases, granting television interviews, issuing public service announcements, and providing testimony to the Congress. The criminals view this scam as they do many others; it is a crime of opportunity. Unfortunately, while we plan on arresting and prosecuting more individuals, the scam will not stop until people stop paying the scammers money. Our best chance at defeating this crime is to educate people so they do not become victims in the first place. Every innocent taxpayer we protect from this crime is a victory.

ADVANCE FEE "LOTTERY WINNING" SCAMS AND PHISHING

We continue to receive reports of people who have become victims of lottery winnings scams and we are also seeing an uptick in the number of reported phishing attempts. The lottery scam is a continuation of an older scam and it starts with an unsolicited e-mail or telephone call from an impersonator to an unsuspecting victim. The caller tells the intended victim that they have won a lottery or other valuable prize, however; in order to collect the prize, the victim must send money to prepay the tax on the winnings to the IRS. The lottery scam often, but not always, originates from outside of the U.S., and it continues to be a successful crime because it capitalizes on a very common dream: getting rich quick and hitting the jackpot.

In a recent investigation, one individual was sentenced after pleading guilty to money laundering[32] and another individual was sentenced to 33 months of incarceration after pleading guilty to conspiracy to commit mail and wire fraud for their roles in a lottery scheme.[33] Overall, the scammers defrauded approximately $380,000 from at least 20 victims.[34]

In another case in the District of Nevada, on March 16, 2016, three individuals were indicted for conspiracy, mail fraud, wire fraud, and money laundering in connection with a telemarketing lottery scheme that was intended to target victims over the age of 55. Under the guise of collecting money for the Federal taxes associated with a lottery prize, the defendants and others called at least 66 victims in 22 states. The defendants caused the victims to send approximately $97,000 via MoneyGram and at least $366,000 via Western Union wire transfers. The defendants also caused victims to send at least $389,000 in fraudulently induced payments through the U.S. mail, UPS and FedEx. As a result of the scheme, the defendants

---

[32] N.D. Ga. Judgment Kecia Place filed Nov. 19, 2015.
[33] N.D. Ga. Amended Judgment Kenneth Kaufman filed Jan. 7, 2016.
[34] N.D. Ga. Indictment Kenneth Kaufman and Kecia Place filed Mar. 18, 2015.

and others collected over $1 million in fraudulently obtained funds from their victims.[35] Prosecution action is ongoing.

In yet another case, we were successful in having a defendant extradited from the United Kingdom for his role in a lottery scheme where he targeted and victimized a citizen in West Virginia.[36]

This year, we have also seen a resurgence of criminals using a technique called phishing to swindle and victimize taxpayers into paying money or providing financial information by tricking the victims into believing they are receiving an e-mail from the IRS. In one current version, taxpayers are receiving e-mails purporting to be from the IRS which asks the taxpayers to confirm their tax return information. This information will then more than likely be used to file fraudulent refund returns or to commit other forms of identity theft.

A new phishing scheme involves scammers sending e-mails purporting to be a business's Chief Executive or Financial Officer. These e-mails notify the employees there has been a mistake on their Form W-2, *Wage and Tax Statement*, and directs the employees to either e-mail their Form W-2 to the sender, or to provide information that was on the Form W-2 for verification. Both approaches result in the theft of the employee's identity information.

As with the other scams, the phishing scam preys on people who simply want to comply with the law and other requests. The IRS will not send e-mails to taxpayers requesting their personal or financial information. If someone receives an e-mail of this nature, they should forward it to phishing@irs.gov prior to clicking on any links that may be contained in the e-mail.

We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system. As such, we plan to provide continuing audit and investigative coverage of the IRS's efforts to operate efficiently and effectively and to expand our oversight related to cybersecurity.

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee thank you for the opportunity to share my views.

---

[35] D. Nev. Indictment Willie Montgomery, Tanika Armstrong, and Reginald Lowe filed Mar. 16, 2016.
[36] N.D. W.Va. Indictment Davel Young filed Sep. 4, 2013.

Timothy P. Camus
Deputy Inspector General for Investigations

Mr. Timothy P. Camus has served in the Treasury Inspector General for Tax Administration (TIGTA) and the Internal Revenue Service Inspection Service, TIGTA's predecessor organization, as a Special Agent, for 25 years.

After an exemplary investigative career, Mr. Camus was promoted into TIGTA management. In June 2003, Mr. Camus became a member of the Senior Executive Service, and in January 2011, he was promoted to the position of the Deputy Inspector General for Investigations for TIGTA. As the Deputy Inspector General for Investigations, Mr. Camus is responsible for overseeing and leading all aspects of TIGTA's law enforcement mission.

During his law enforcement career, Mr. Camus has successfully investigated domestic terrorism, death threats made against public officials, bribery and extortion cases, as well as thefts of Government property and all other facets of white collar crime and fraud that impact the IRS. In 2008, Mr. Camus was awarded the Presidential Rank Award for Meritorious Service.

Chairman ROSKAM. Thank you.
Ms. Lucas-Judy.

STATEMENT OF JESSICA LUCAS-JUDY, ACTING DIRECTOR, STRATEGIC ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. LUCAS-JUDY. Chairman Roskam, Ranking Member Lewis, Members of the Subcommittee, thank you for inviting me to testify on three opportunities that GAO identified for IRS:

First, improving customer service;

Second, combating identity theft refund fraud; and

Third, enhancing information security.

During the filing season IRS deals with millions of transactions. The scale of these operations presents challenges for customer service and for protecting taxpayers' personal and financial information. Congress provided IRS with an additional $290 million this year to improve these areas.

Regarding the first area of opportunity, customer service, the 2016 filing season was generally smooth. IRS provided a higher level of telephone service than it did in 2015. More people who wanted to speak to a live assister were able to get through, and the wait times were much shorter.

However, as you heard, IRS expects telephone service to decline now that the filing season is over. GAO has recommended that IRS benchmark its telephone service with other call centers to identify potential improvements.

Of course, IRS provides much more than just phone service. It handles correspondence, and it also provides services online, among other things. We have made recommendations to help IRS strategically manage these duties.

For example, in 2013, GAO recommended IRS develop a long-term strategy for new online services. IRS recently told us that its new Future State Initiative will provide better service to taxpayers, but this initiative is in its early stages.

We have also suggested Congress require Treasury and IRS to develop a comprehensive customer service strategy that incorporates elements of our prior recommendations.

The second area of opportunity is identity theft refund fraud. IRS estimates it paid more than $3 billion dollars in identity theft refunds in 2014, and that is just from schemes already known. IRS has made it easier for people to report suspected fraud, and it is working with state and industry partners to share potential leads and strengthen fraud filters.

Stronger pre-refund and post-refund strategies would help IRS combat this persistent and evolving threat. For example, IRS is considering a number of tools to enhance authentication, making sure the person filing the return is who they say they are.

However, some of these could impose significant burdens on taxpayers and the IRS, and it is unclear how well they work. GAO recommended IRS assess the costs and benefits of its authentication tools.

It is also important that IRS identify fraudulent returns before the money goes out the door. IRS currently issues refunds after matching names and Social Security numbers and filtering for cer-

tain indicators of fraud but does not match wage information reported by employers on W–2s.

Historically W–2s had been available to IRS after it issued most refunds. Matching W–2s with information on tax returns to detect fraud before paying refunds could save some of the billions of dollars currently lost to fraud.

The 2016 Consolidated Appropriations Act makes some of that information available earlier, which should help address this issue.

The third area of opportunity is cybersecurity. While IRS has implemented some controls, taxpayer data continues to be exposed to unnecessary risk due in part to inconsistent implementation of IRS' security programs.

To illustrate, we found that IRS used easily guessable passwords on servers that were supporting key systems. IRS also allowed access to certain systems beyond what users needed to do their jobs and did not encrypt sensitive data on some of the key systems that we reviewed.

Importantly IRS did not fully address deficiencies we had identified in prior reviews or ensure that its actions corrected the problem. For instance, in our most recent review, IRS told us it had addressed 28 of our prior recommendations, but we found that nine of those had not been implemented effectively.

Last month GAO made 43 recommendations to address newly identified weaknesses. Implementing these and our 49 outstanding recommendations would better protect sensitive information.

In summary, as more IRS services are conducted online, it would be important for IRS to ensure it has proper safeguards in place and is using the full range of information to combat identity theft refund fraud and protect taxpayer data.

We urge Congress, Treasury, and IRS to implement GAO's recommendations in the three areas we identified: benchmarking IRS' phone service and developing comprehensive customer service and online strategies; assessing authentication tools and conducting pre-refund matching; and addressing vulnerabilities in IRS' information security systems to better protect taxpayer data.

Chairman Roskam, Ranking Member Lewis, Members of the Subcommittee, this concludes my prepared remarks, and I will be happy to answer any questions you may have.

[The prepared statement of Ms. Lucas-Judy follows:]

United States Government Accountability Office
Testimony
Before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

For Release on Delivery
Expected at 10 a.m. ET
Tuesday, April 19, 2016

TAX FILING

IRS Needs a Comprehensive Customer Service Strategy and Needs to Better Combat Identity Theft Refund Fraud and Protect Taxpayer Data

Statement of Jessica K. Lucas-Judy, Acting Director, Strategic Issues

GAO Highlights

Highlights of GAO-16-578T, a testimony before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

April 19, 2016

TAX FILING

IRS Needs a Comprehensive Customer Service Strategy and Needs to Better Combat Identity Theft Refund Fraud and Protect Taxpayer Data

Why GAO Did This Study

IRS provides service to tens of millions of taxpayers and processes most tax returns during the filing season. It is also a time when legitimate taxpayers may learn that they are a victim of IDT refund fraud, which occurs when a thief files a fraudulent return using a legitimate taxpayer's identity and claims a refund. In 2015, GAO added IDT refund fraud to its high-risk area on the enforcement of tax laws and expanded its government-wide high-risk area on federal information security to include the protection of personally identifiable information. With IRS's reliance on computerized systems, recent data breaches at IRS highlight the vulnerability of sensitive taxpayer information.

This statement discusses IRS's efforts to address (1) customer service declines, (2) IDT refund fraud challenges, and (3) information security weaknesses. This statement is based on GAO reports issued between 2012 and 2016 and includes updates of selected data.

What GAO Recommends

GAO previously suggested that Congress consider requiring that Treasury work with IRS to develop a customer service strategy, and providing Treasury with the authority to lower the annual threshold for e-filing W-2s. GAO made prior recommendations to IRS to combat IDT refund fraud, such as assessing the costs, benefits, and risks of taxpayer authentication options, and 45 new recommendations to further improve IRS's information security controls and the implementation of its agency-wide information security program.

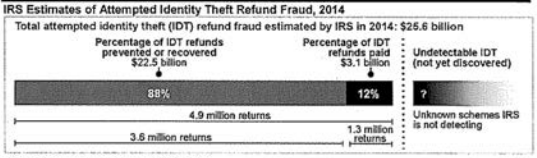
View GAO-16-578T. For more information, contact Jessica K. Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov, or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Internal Revenue Service (IRS) improved phone service to taxpayers during the 2016 filing season compared to last year. According to IRS, this is due in part to the additional $290 million in funding Congress provided to improve customer service, identity theft (IDT) refund fraud, and cybersecurity efforts. However, IRS expects its performance for the entire fiscal year will not reach the levels of earlier years. In 2012 and 2014, GAO made recommendations for IRS to improve customer service, which it has yet to implement. Consequently, in December 2015, GAO suggested that Congress require the Department of the Treasury (Treasury) to work with IRS to develop a comprehensive customer service strategy that incorporates elements of these prior recommendations.

IDT refund fraud poses a significant challenge. Although the full extent of this fraud is unknown, IRS estimates it paid $3.1 billion in IDT fraudulent refunds in filing season 2014, while preventing the processing of $22.5 billion in fraudulent refunds (see figure).

IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-578T

IRS has taken steps to combat IDT refund fraud, such as increasing resources dedicated to combating the problem. However, as GAO reported in August 2014 and January 2015, additional actions can further assist the agency, including assessing the costs, benefits, and risks of improving methods for authenticating taxpayers. In addition, the Consolidated Appropriations Act, 2016 included a provision to accelerate filings of W-2 information from employers to the IRS that would help IRS with pre-refund matching. GAO suggested that Congress provide Treasury with authority to lower the threshold for e-filing W-2s, which would further enhance pre-refund matching.

In March 2016, GAO reported that IRS had instituted numerous controls over key financial and tax processing systems; however, it had not always effectively implemented other controls intended to properly restrict access to systems and information, among other security measures. While IRS had improved some of its access controls, weaknesses remained in controls over key systems for identifying and authenticating users, authorizing users' level of rights and privileges, and encrypting sensitive data. These weaknesses were due in part to IRS's inconsistent implementation of its agency-wide security program, including not fully implementing 49 prior GAO recommendations. GAO concluded that these weaknesses collectively constituted a significant deficiency for the purposes of financial reporting for fiscal year 2015. As a result, taxpayer and financial data continue to be exposed to increased risk.

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee:

Thank you for the opportunity to testify on the Internal Revenue Service's (IRS) 2016 filing season performance, identity theft (IDT) refund fraud and information security.

The filing season—which ended yesterday for most of the country—is the time when millions of taxpayers contact IRS over the phone, through written correspondence, in person, and via IRS's website.[1] It is also during this period that IRS processes most of the approximately 150 million individual tax returns it will receive, conducts initial screening for compliance, and issues more than 100 million refunds. The scale of these operations alone presents challenges, in addition to ensuring the security of taxpayers' personal and financial information. Customer service is one of those challenges.

Another major challenge for IRS during the filing season is the growing and evolving problem of IDT refund fraud and IRS efforts to prevent, detect, and resolve it. This crime occurs when a refund-seeking fraudster obtains an individual's Social Security number, date of birth, or other personally identifiable information (PII) and uses it to file a fraudulent tax return seeking a refund.[2] This crime costs the federal government billions of dollars in both IDT refunds paid to fraudsters and costs incurred by IRS in its efforts to combat it. Further, it burdens legitimate taxpayers because authenticating the victims' identities is likely to delay processing their returns and refunds, in those cases where a legitimate refund is due. Moreover, the victim's PII can potentially be used to commit other crimes. Given current and emerging risks, in 2015 we expanded the enforcement of our tax laws high-risk area to include IRS's efforts to address IDT refund fraud.[3]

[1]This year, most taxpayers had until April 18 to file a tax return with IRS.

[2]PII is information about an individual, including information that can be used to distinguish or trace their identity, such as name, Social Security number, mother's maiden name, or biometric records, as well as any other personal information that is linked or linkable to an individual. This statement discusses IDT refund fraud and not employment fraud. IDT employment fraud occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job.

[3]See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

In carrying out its mission to collect taxes, process tax returns, and enforce U.S. tax laws during the filing season and beyond, IRS relies extensively on computerized systems and on information security controls to protect the confidentiality, integrity, and availability of sensitive personal and financial information for each U.S. taxpayer. We first designated federal information security as a government-wide high-risk area in 1997. As we did with IDT refund fraud, in 2015 we expanded this area to include protecting the privacy of PII that is collected, maintained, and shared by both federal and nonfederal entities as a government-wide high-risk area.[4] Two recent information security incidents at IRS highlight the challenges and importance of ensuring that controls protecting taxpayer data are effectively implemented:

- In June 2015, the Commissioner of the IRS testified that unauthorized third parties had gained access to taxpayer information from its Get Transcript service.[5] According to IRS officials, criminals used taxpayer-specific data acquired from nondepartment sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included such PII as Social Security information, dates of birth, and street addresses. In an August 2015 update, IRS updated this number to be about 114,000, and reported that an additional 220,000 accounts had been inappropriately accessed. In a February 2016 update, the agency reported that an additional 390,000 accounts had been accessed. Thus, IRS has reported a total of about 724,000 accounts that were inappropriately accessed. The online Get Transcript service has been unavailable since May 2015.

- In March 2016, IRS stated that as part of its ongoing security review, it had temporarily suspended the Identity Protection Personal Identification Number (IP PIN) service on IRS.gov. The IP PIN is a single-use identification number provided to taxpayers who are victims

[4]GAO-15-290.

[5]The Get Transcript service provides users, via the IRS website, the ability to view, print, and download tax account, tax return, and record of account transcripts; wage and income documents; and proof of nonfiling transcripts. Taxpayers can also obtain transcripts by calling, writing, or walking into an IRS office.

of IDT to help prevent future IDT refund fraud.[6] The service on IRS's website allowed taxpayers to retrieve their IP PINs online. Taxpayers passed IRS's authentication checks by confirming their identities through site inquiries, asking for personal, financial, and tax-related information. The IRS stated that it was conducting further review of the IP PIN service and is looking at further strengthening the security features before resuming service. As of April 13, this online service was still suspended.

In response to challenges in these three areas, in fiscal year 2016, Congress provided IRS with $290 million in additional funding intended to improve customer service, IDT identification and prevention, and cybersecurity efforts.[7] According to IRS's spending plan this funding will be used to invest in (1) increased telephone level of service, including reduced wait times and improved performance on IRS's Taxpayer Protection Program/Identity Theft Toll Free Line ($178.4 million); (2) cybersecurity including network security improvements, protection from unauthorized access, and enhanced insider threat detection ($95.4 million); and (3) IDT refund fraud prevention ($16.1 million).

My statement today focuses on IRS's efforts to address (1) declines in customer service, (2) the challenge of identity theft refund fraud, and (3) information security weaknesses we have identified.

My statement is based in part on our previous reports issued between December 2012 and April 2016. Detailed descriptions of the scope and methodology for each of these reports can be found in each of the reports cited within this statement. We updated selected data in this statement with 2016 data from IRS on individual income tax return processing and telephone service, as well as IRS's fiscal year 2016 spending plan for the additional $290 million in appropriated funds. We also incorporated IRS statements on recent data breaches and IRS actions to address our past recommendations. To assess data reliability, we reviewed IRS data and

[6]In January 2014, IRS offered a limited IP PIN pilot program to eligible taxpayers in Florida, Georgia, and the District of Columbia. Taxpayers must confirm their identities with IRS to receive an IP PIN. IP PINs help prevent future IDT refund fraud because, once issued, the IP PIN must accompany their electronically filed tax return or else IRS will reject the return. If a paper return has a missing or incorrect IP PIN, IRS delays processing the return while the agency determines if it was filed by the legitimate taxpayer. See GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, GAO-14-633 (Washington, D.C.: Aug. 20, 2014), for more details on IRS's IP PIN service.

[7]Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. E, § 113, 129 Stat. 2242 (Dec. 18, 2015). Funding is available to IRS until September 30, 2017.

documentation and assessed it for data limitations. We found the data to be sufficiently reliable for our purposes. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our work to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

IRS Improved its Telephone Service for the 2016 Filing Season but Still Needs to Develop a Comprehensive Customer Service Strategy

In addition to processing approximately 150 million individual tax returns and issuing more than 100 million refunds during the filing season, IRS provides a range of taxpayer services, including through telephones, written correspondence, and on its website.[8]

Based on recent data from IRS, compared to last year, IRS's telephone service has improved in the 2016 filing season. From January 1 through March 26, 2016, IRS received about 38.2 million calls to its automated and live assistor telephone lines—a slight decrease compared to the same period last year.[9] Of the 14.7 million calls seeking live assistance, IRS had answered 9.9 million calls—a 72 percent increase over the 5.7 million calls answered during the same period last year. Further, the average wait time to speak to an assistor also decreased from 24 to 10 minutes.

IRS anticipated that 65 percent of callers seeking live assistance would receive it this filing season, which ended April 18. IRS's performance for telephone service during the filing season as of March 26, 2016 has exceeded IRS's anticipated level—74 percent of callers have received live assistance.

[8]The filing season generally runs between January and mid-April.

[9]Total call volume to IRS's toll free telephone lines include automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected.

IRS attributed this year's improvements to a number of factors. As noted above, of the additional $290 million IRS received in December 2015, it allocated $178.4 million (61.5 percent) for taxpayer services to make measurable improvements in its telephone level of service. With the funds, IRS hired 1,000 assistors who began answering taxpayer calls in March, in addition to the approximately 2,000 seasonal assistors it had hired in fall 2015.[10] To help answer taxpayer calls before March, IRS officials told us that they detailed 275 staff from one of its compliance functions to answer telephone calls.[11] IRS officials said they believe this step was necessary because the additional funding came too late in the year to hire and train assistors to fully cover the filing season. IRS also plans to use about 600 full-time equivalents of overtime for assistors to answer telephone calls and respond to correspondence in fiscal year 2016. This compares to fewer than 60 full-time equivalents of overtime used in fiscal year 2015.

However, IRS expects that the telephone level of service will decline after the filing season. As a result, the telephone level of service for the entire 2016 fiscal year is expected to be at 47 percent.[12] As we reported in March 2016, IRS's telephone level of service for the fiscal year has yet to reach the levels it had achieved in earlier years (see figure 1).[13]

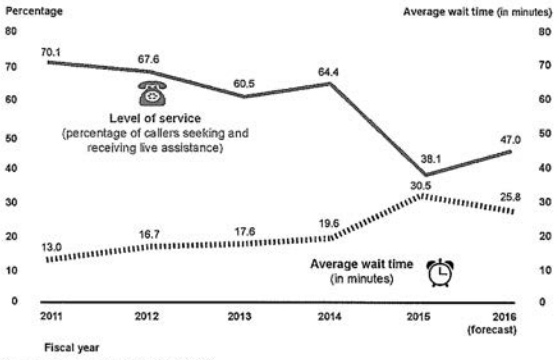
[10]In contrast, IRS reduced the number of assistors answering telephone calls between fiscal years 2010 and 2015, which contributed to the lowest level of telephone service in fiscal year 2015 compared to recent years.

[11]IRS has not yet determined the amount of foregone revenue from taking this action.

[12]IRS's projected telephone level of service for the filing season covers the period between January 1, 2016 and April 23, 2016.

[13]GAO, *Internal Revenue Service: Preliminary Observations on the Fiscal Year 2017 Budget Request and 2016 Filing Season Performance*, GAO-16-459R (Washington, D.C.: Mar. 8, 2016).

Figure 1: IRS Telephone Level of Service and Average Telephone Wait Time, Fiscal Year 2011 through Fiscal Year 2016 Performance Forecast



Source: GAO analysis of IRS data. | GAO-16-578T

In addition to answering telephone calls, IRS responds to millions of letters and other correspondence from taxpayers. In 2015, we reported that the percentage of correspondence cases in IRS's inventory classified as "overage"—cases generally not processed within 45 days of receipt by IRS—has stayed close to 50 percent since fiscal 2013.[14] Minimizing overaged correspondence is important because delayed responses may prompt taxpayers to write again, call, or visit a walk-in site. Moreover, an increasing overage rate could lead to more interest paid to taxpayers who are owed refunds.

In March 2016, IRS officials attributed improvements made this filing season, in part, to assistors working overtime. These officials reported that IRS's office that responds to taxpayer inquiries and handles

[14]IRS can classify correspondence in its inventory as "overage" from 30 to 180 days after IRS receives them depending on the type of work performed by assistors. For example, correspondence cases generated internally age 75 days from the date IRS receives such cases, while international adjustment cases generated by taxpayers age 90 days from the date IRS receives them. See GAO, *2015 Tax Filing Season: Deteriorating Taxpayer Service Underscores Need for a Comprehensive Strategy and Process Efficiencies*, GAO-16-151 (Washington, D.C.: Dec. 16, 2015).

adjustments had slightly more than 700,000 correspondence cases in inventory at the end of January and expect about 1 million cases in inventory by the end of April. They described IRS's correspondence inventory as manageable, but steadily increasing. Officials said that, after the filing deadline, assistors will turn their attention to correspondence.

IRS also offers online services to millions of taxpayers through its website, including tax forms and interactive tax assistance features. According to IRS, the agency wants to expand online service to provide greater convenience to taxpayers which has the potential to reduce costs in other areas, such as its telephone operations.

Implementing Our Prior Recommendations Could Help IRS Improve Customer Service

We have made recommendations to IRS and the Department of the Treasury (Treasury), as well as a matter for congressional consideration, to assist IRS in improving its customer service. Examples include:

Telephone and Correspondence. In December 2012, we recommended that IRS define appropriate levels of service for telephones as well as correspondence.[15] IRS neither agreed nor disagreed with this recommendation and, as of October 2015, the agency had not developed these customer service goals. While IRS has taken some steps to modify services provided to taxpayers, a strategy would help determine the resources needed to achieve customer service goals. Recognizing the importance of such as strategy, in December 2014, we recommended that IRS systematically and periodically compare its telephone service to the best in business to identify gaps between actual and desired performance.[16] IRS disagreed with this recommendation, noting that it is difficult to identify comparable organizations. We do not agree with IRS's position; many organizations run call centers that would provide ample opportunities to benchmark IRS's performance.

Recognizing the need to improve performance responding to taxpayer correspondence, in December 2015, we recommended to Treasury that it include overage rates for handling taxpayer correspondence as a part of

[15]GAO, *2012 Tax Filing: IRS Faces Challenges Providing Service to Taxpayers and Could Collect Balances Due More Effectively*, GAO-13-156 (Washington, D.C.: Dec. 18, 2012).

[16]GAO, *Tax Filing Season: 2014 Performance Highlights the Need to Better Manage Taxpayer Service and Future Risks*, GAO-15-163 (Washington, D.C.: Dec. 16, 2014).

Treasury's performance goals. Treasury neither agreed nor disagreed with this recommendation.

Online Services. In April 2013, we recommended that IRS develop a long-term online strategy that should, for example, develop business cases for all new online services.[17] In March 2016, IRS officials reported that IRS's Future State initiative is intended to provide better service to taxpayers through multiple channels of communication, including online.[18] We have not yet assessed IRS's Future State initiative. However, a long-term comprehensive strategy for online services should help ensure that IRS is maximizing the benefit to taxpayers from this investment and reduce costs in other areas, such as for IRS's telephone operations.

Comprehensive Customer Service Strategy. In fall 2015, Treasury and IRS officials said they had no plans to develop a comprehensive customer service strategy or specific goals for telephone service tied to the best in the business and customer expectations. These officials told us that the agencies' existing efforts were sufficient. However, we continue to believe that, without such a strategy, Treasury and IRS can neither measure nor effectively communicate to Congress the types and levels of customer service taxpayers should expect and the resources needed to reach those levels. Therefore, in December 2015, we suggested that Congress consider requiring that Treasury work with IRS to develop a comprehensive customer service strategy.[19] In April 2016, IRS officials told us that the agency has established a team to consider our prior recommendations in developing a comprehensive customer service strategy or goals for telephone service.

Billions of Dollars Have Been Lost to IDT Refund Fraud, and IRS Faces Challenges in Combating This Evolving Threat

During the filing season many taxpayers learn that their private information has been stolen and they have been victims of IDT refund fraud. This generally occurs when the taxpayer attempts to file a tax

[17]GAO, *IRS Website: Long-Term Strategy Needed to Improve Interactive Services*, GAO-13-435 (Washington, D.C.: Apr. 16, 2013).

[18]According to IRS, the agency is working to transform its operations in order to modernize the taxpayer experience and empower its workforce to operate more efficiently—which will make filing simpler for taxpayers and increase voluntary compliance.

[19]GAO-16-151.

return only to learn that one has already been filed under the taxpayer's name. For these taxpayers, IRS has taken action to improve customer service related to IDT refund fraud. As we reported in March 2016, between the 2011 and 2015 filing seasons, IRS experienced a 430 percent increase in the number of telephone calls to its Identity Theft Toll-Free Line.[20] As of March 19, 2016, IRS had received more than 1.1 million calls to this line.[21] During this time, 77 percent of callers seeking assistance on this telephone line received it compared to 54 percent during the same period last year. Average wait times during the same period have also decreased—taxpayers were waiting an average of 14 minutes to talk to an assistor, a decrease from 27 minutes last year.

As we reported in April 2016, billions of dollars have been lost to IDT refund fraud and this crime continues to be an evolving threat.[22] IRS develops estimates of the extent of IDT refund fraud to help direct its efforts to identify and prevent the crime. While its estimates have inherent uncertainty, IRS estimated that it prevented or recovered $22.5 billion in fraudulent IDT refunds in filing season 2014 (see figure 2).[23] However, IRS also estimated, where data were available, that it paid $3.1 billion in fraudulent IDT refunds. Because of the difficulties in knowing the amount of undetectable fraud, the actual amount could differ from these estimates.

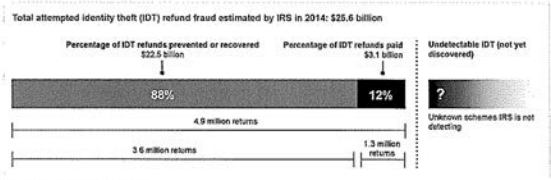
[20]GAO-16-459R.

[21]Total call volume to IRS's identity theft protection toll-free telephone line includes automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected.

[22]GAO, *2016 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO-16-375SP (Washington, D.C.: Apr. 13, 2016).

[23]IRS's 2014 estimates cannot be compared to 2013 estimates because of substantial methodology changes to better reflect new IDT refund fraud schemes and to improve the accuracy of its estimates, according to IRS officials. We are reviewing IRS's IDT refund fraud estimates as part of ongoing work.

Figure 2: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-578T

IRS has taken steps to address IDT refund fraud; however, it remains a persistent and continually changing threat. IRS recognized the challenge of IDT refund fraud in its fiscal year 2014-2017 strategic plan and increased resources dedicated to combating IDT and other types of refund fraud.[24] In fiscal year 2015, IRS reported that it staffed more than 4,000 full-time equivalents and spent about $470 million on all refund fraud and IDT activities.[25] As described above, IRS received an additional $290 million in fiscal year 2016 to improve customer service, IDT identification and prevention, and cybersecurity efforts. The agency plans to use $16.1 million of this funding to help prevent IDT refund fraud, among other things. As we reported in April 2016, the administration requested an additional $90 million and an additional 491 full-time equivalents for fiscal year 2017 to help prevent IDT refund fraud and reduce other improper payments.[26] IRS estimates that this $90 million investment in IDT refund fraud and other improper payment prevention would help it protect $612 million in revenue in fiscal year 2017, as well as protect revenue in future years.

As we previously reported, IRS also works with third parties, such as tax preparation industry participants, states, and financial institutions to try to

[24]IRS, *Strategic Plan*: FY2014-2017, (Washington, D.C.: June 2014).

[25]IRS officials told us they do not track spending for IDT activities separately from other types of refund fraud. A full-time equivalent reflects the total number of regular straight-time hours (i.e., not including overtime or holiday hours) worked by employees divided by the number of compensable hours applicable to each fiscal year.

[26]See GAO-16-375SP. Improper payments are payments that should not have been made or that were made in an incorrect amount (including overpayments and underpayments).

detect and prevent IDT refund fraud.[27] In March 2015, the Commissioner of the IRS convened a Security Summit with industry and states to improve information sharing and authentication. IRS officials said that 40 state departments of revenue and 20 tax industry participants have officially signed a partnership agreement to enact recommendations developed and agreed to by summit participants. IRS plans to invest a portion of the $16.1 million it received in fiscal year 2016 into identity theft prevention and refund fraud mitigation actions from the Security Summit. These efforts include developing an Information Sharing and Analysis Center where IRS, states, and industry can share information to combat IDT refund fraud.

Even though IRS has prioritized combating IDT refund fraud, fraudsters adapt their schemes to identify weaknesses in IDT defenses, such as gaining access to taxpayers' tax return transcripts through IRS's online Get Transcript service.[28] According to IRS officials, with access to tax transcripts, fraudsters can create historically consistent returns that are hard to distinguish from a return filed by a legitimate taxpayer. This can make it more difficult for IRS to identify and detect IDT refund fraud.

Stronger Pre-refund and Post-refund Strategies Can Help Combat IDT Refund Fraud

Because identity thieves are "adaptive adversaries" who are constantly learning and changing their tactics as IRS develops new IDT strategies, IRS will need stronger pre-refund and post-refund strategies to combat this persistent and evolving threat. While there are no simple solutions, our past work has highlighted ways IRS can combat this threat.

Improved authentication. Improving authentication could help IRS prevent fraud before issuing refunds. In January 2015, we reported that IRS's authentication tools have limitations and recommended that IRS assess the costs, benefits and risks of its authentication tools.[29] For

[27]GAO, *Information Security: IRS Needs to Further Improve Controls over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud*, GAO-16-589T (Washington, D.C.: Apr. 12, 2016).

[28]As mentioned above, the online Get Transcript service has been unavailable since May 2015.

[29]GAO, *Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud but IRS Lacks an Estimate of Costs, Benefits and Risks*, GAO-15-119 (Washington, D.C.: Jan. 20, 2015).

example, individuals can obtain an e-file PIN by providing their name, Social Security number, date of birth, address, and filing status for IRS's e-file PIN application. Identity thieves can easily find this information, allowing them to bypass some, if not all, of IRS's automatic checks according to our analysis and interviews with tax software and return preparer associations and companies. After filing an IDT return using an e-file PIN, the fraudulent return would proceed through IRS's normal return processing.

In response to our recommendation, in November 2015, IRS developed guidance for its Identity Assurance Office to assess costs, benefits, and risk. According to IRS officials, this analysis will inform decision-making on authentication-related issues. IRS also noted that the methods of analysis for the authentication tools will vary depending on the different costs and other factors for authenticating taxpayers in different channels, such as online, phone, or in-person. In February 2016, IRS officials told us that the Identity Assurance Office plans to complete a strategic plan for taxpayer authentication across the agency in September 2016. While IRS is taking steps, it will still be vulnerable until it completes and uses the results of its analysis of costs, benefits, and risks to inform decision-making.

W-2 Pre-refund Matching. Another pre-refund strategy is earlier matching of employer-reported wage information to taxpayers' returns before issuing refunds. As we reported in August 2014, thieves committing IDT refund fraud take advantage of IRS's "look-back" compliance model.[30] Under this model, rather than holding refunds until completing all compliance checks, IRS issues refunds after conducting selected reviews, such as verifying identity by matching names and Social Security numbers and filtering for indications of fraud.[31] However, we found that the wage information that employers report on the Form W-2, *Wage and Tax Statement* (W-2), has generally been unavailable to IRS until after it issues most refunds. According to IRS, pre-refund matching would potentially save a substantial part of the billions of taxpayer dollars currently lost to fraudsters.

[30]GAO-14-633.

[31]These reviews can detect inconsistencies, allowing IRS to resolve any issues and—in some cases—prevent refunds.

- *Increasing electronically-filed (e-file) W-2s.* In December 2015, the Consolidated Appropriations Act, 2016 amended the tax code to accelerate W-2 filing deadlines to January 31.[32] This represents important progress. Building on that, other policy changes may also be needed in concert with moving W-2 deadlines. Agency officials and third-party stakeholders told us that these changes include lowering the employee threshold requirement for employers to e-file W-2s.[33] Because of the additional time and resources associated with processing paper W-2s submitted by employers, Social Security Administration officials told us that a change in the e-file threshold would be needed to sufficiently increase the number of e-filed W-2s. Backlogs in paper W-2s could result in IRS receiving W-2 data after the end of the filing season. Therefore, we have suggested that Congress should consider providing the Secretary of the Treasury with the regulatory authority to lower the threshold for electronic filing of W-2s from 250 returns annually to between 5 to 10 returns, as appropriate.

- *Assessing the costs and benefits of pre-refund W-2 matching.* In August 2014 we reported that the wage information that employers report on Form W-2 is unavailable to IRS until after it issues most refunds.[34] Also, if IRS had access to W-2 data earlier, it could match such information to taxpayers' returns and identify discrepancies before issuing billions of dollars of fraudulent IDT refunds. We recommended that IRS assess the costs and benefits of accelerating W-2 deadlines.

  In response to our recommendation, IRS provided us with a report in September 2015 discussing (1) adjustments to IRS systems and work processes needed to use accelerated W-2 information, (2) the potential impacts on internal and external stakeholders, and (3) other changes needed to match W-2 data to tax returns prior to issuing refunds, such as delaying refunds until W-2 data

[32]Pub. L. No. 114-113, div. Q, § 201, 129 Stat. 2242 (Dec. 18, 2015). This change goes into effect for W-2s reporting payments made in 2016 and filed in 2017.

[33]Currently, employers who file 250 or more W-2s annually must electronically file those forms. 26 C.F.R. § 301.6011-2(b)(2). IRS is generally prohibited from requiring those filing fewer than 250 returns annually to e-file. 26 U.S.C. § 6011(e)(2)(A). For details, see GAO-14-633.

[34]GAO-14-633.

are available. IRS's analysis for this report will help it determine how to best implement pre-refund W-2 matching, given the new January 31 deadline for filing W-2s.

Improving feedback on external leads. A post-refund strategy to combat IDT refund fraud involves IRS's External Leads Program. This program involves financial institutions and other external parties providing information about emerging IDT refund trends and fraudulent returns that have passed through IRS detection systems. In August 2014, we reported that IRS provided limited feedback to external parties on IDT leads they submitted and offered external parties limited general information on IDT refund fraud trends. We recommended that IRS provide actionable feedback to all lead-generating third parties, and IRS neither agreed nor disagreed.[35]

However, in response to our recommendation, IRS took a number of steps. First, in November 2015, IRS reported that it had developed a database to track leads submitted by financial institutions and the results of those leads. IRS also stated that it had held two sessions with financial institutions to provide feedback on external leads provided to IRS. Second, in December 2015, IRS officials told us that the agency sent a customer satisfaction survey asking financial institutions for feedback on the external leads process. The agency was also considering other ways to provide feedback to financial institutions. Third, in April 2016, IRS officials told us that they plan to analyze preliminary survey results by mid-April 2016. Finally, IRS officials reported that the agency shared information with financial institutions in March 2016 and plans to do so on a quarterly basis. The next information sharing session is scheduled in June 2016. We are following up with IRS on these activities to determine the extent to which IRS has addressed our recommendation.

[35]GAO-14-633.

Although IRS Has Made Improvements, Information Security Weaknesses Continue to Place Taxpayer and Financial Data at Risk

In addition to securing taxpayer information to help prevent IDT refund fraud, there are additional concerns for maintaining security of taxpayer data. As we reported in March 2016,[36] IRS has implemented numerous controls over key financial and tax processing systems; however, it had not always effectively implemented access and other controls,[37] including elements of its information security program.

Access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. These controls include identification and authentication, authorization, cryptography, audit and monitoring, and physical security controls, among others. In our most recent review in March 2016, we found that IRS had improved access controls, but some weaknesses remain.[38] Examples include:

- **Identifying and authenticating** users—such as through user account-password combinations—provides the basis for establishing accountability and controlling access to a system. IRS established policies for identification and authentication, including requiring multifactor authentication for local and network access accounts, and establishing password complexity and expiration requirements.[39] It also improved identification and authentication controls by, for example, expanding the use of an automated mechanism to centrally manage, apply, and verify password requirements. However,

[36]GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-398 (Washington, D.C.: Mar. 28, 2016).

[37]Information security controls include logical and physical access controls, configuration management, and continuity of operations. These controls are designed to ensure that access to data is properly restricted, physical access to sensitive computing resources and facilities is protected, systems are securely configured to avoid exposure to known vulnerabilities, and backup and recovery plans are adequate and tested to ensure the continuity of essential operations.

[38]GAO-16-398.

[39]Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric).

weaknesses in identification and authentication controls remained. For example, the agency used easily guessable passwords on servers supporting key systems.

- **Authorization controls** limit what actions users are able to perform after being allowed into a system. They should be based on the concept of "least privilege," granting users the least amount of rights and privileges necessary to perform their duties. While IRS established policies for authorizing access to its systems, we found that it continued to permit excessive access in some cases. For example, users were granted rights and permissions in excess of what they needed to perform their duties, including for an application used to process electronic tax payment information and a database on a human resources system.

- **Cryptography controls** protect sensitive data and computer programs by rendering data unintelligible to unauthorized users and protecting the integrity of transmitted or stored data. IRS policies require the use of encryption and it continued to expand its use of encryption to protect sensitive data. However, key systems we reviewed had not been configured to encrypt sensitive user authentication data.

IRS also had weaknesses in configuration management controls, which are intended to prevent unauthorized changes to information system resources (e.g., software and hardware), and provide assurance that systems are configured and operating securely. Specifically, while IRS developed policies for managing the configuration of its information technology (IT) systems and improved some configuration management controls, it did not, for example, ensure security patch updates were applied in a timely manner to databases supporting two key systems we reviewed, including a patch that had been available since August 2012.

To its credit, IRS had established contingency plans for the systems we reviewed, which help ensure that when unexpected events occur, critical operations can continue without interruption or can be promptly resumed, and that information resources are protected. Specifically, IRS had established policies for developing contingency plans for its information systems and for testing those plans, as well as for implementing and enforcing backup procedures. Moreover, the agency had documented and tested contingency plans for its systems and improved continuity of operations controls for several systems.

Nevertheless, the control weaknesses we found can be attributed in part to IRS's inconsistent implementation of elements of its agency-wide information security program. The agency established a comprehensive framework for its program, including assessing risk for its systems, developing system security plans, and providing employees with security awareness and specialized training. However, IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring access.

In addition, the agency had not fully addressed previously identified deficiencies or ensured that its corrective actions were effective. During our most recent review, IRS told us it had addressed 28 of our prior recommendations; however, we determined that 9 of these had not been effectively implemented.

We concluded in our November 2015 report that the collective effect of the deficiencies in information security from prior years that continued to exist in fiscal year 2015, along with the new deficiencies we identified, were serious enough to merit the attention of those charged with governance of IRS and therefore represented a significant deficiency in IRS's internal control over financial reporting systems as of September 30, 2015.[40]

Implementing GAO Recommendations Can Help IRS Better Protect Sensitive Taxpayer and Financial Data

To assist IRS in fully implementing its agency-wide information security program, we made two new recommendations to more effectively implement security-related policies and plans.[41] In addition, to assist IRS in strengthening security controls over the financial and tax processing systems we reviewed, we made 43 technical recommendations in a

[40]A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. For additional information, see GAO, *Financial Audit: IRS's Fiscal Years 2015 and 2014 Financial Statements*, GAO-16-146 (Washington, D.C.: Nov. 12, 2015).

[41]GAO-16-398.

separate report with limited distribution to address 26 new weaknesses in access controls and configuration management.[42]

Implementing these recommendations—in addition to the 49 outstanding recommendations from previous audits—will help IRS improve its controls for identifying and authenticating users. This, in turn, will allow IRS to limit users' access to the minimum necessary to perform their job-related functions, protect sensitive data when they are stored or in transit, audit and monitor system activities, and physically secure its IT facilities and resources.

In commenting on drafts of our reports presenting the results of our fiscal year 2015 audit, the IRS Commissioner stated that while the agency agreed with our new recommendations, it will review them to ensure that its actions include sustainable fixes that implement appropriate security controls balanced against IT and human capital resource limitations.

In conclusion, this year's tax filing season has generally gone smoothly and IRS has improved customer service. While IRS has some initiatives to review customer service and consider improvements, it still needs to develop a comprehensive strategy for customer service that will meet the needs of taxpayers. This strategy could include setting customer service goals as well as benchmarking and monitoring performance.

IRS also needs to strengthen its defenses for addressing IDT refund fraud that is informed by assessing the cost, benefits, and risks of IRS's various authentication options.

Finally, weaknesses in information security can also increase the risk posed by IDT refund fraud. While IRS has made progress in implementing information security controls, it needs to continue to address weaknesses in access controls and configuration management and consistently implement all elements of its information security program. The risks to which the IRS and the public are exposed have been illustrated by recent incidents involving public-facing applications, highlighting the importance of securing systems that contain sensitive taxpayer and financial data.

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, this concludes my statement. I look forward to answering any questions that you may have at this time.

[42]GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-397SU (Washington, D.C.: Mar. 28, 2016).

Contacts and Staff Acknowledgments

If you have any questions regarding this statement, please contact Jessica K. Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov, James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov, Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Nancy Kingsbury at (202) 512-2928 or kingsburyn@gao.gov. Other key contributors to this statement include Neil A. Pinney, Joanna M. Stamatiades, and Jeffrey Knott, (assistant directors); Dawn E. Bidne; Mark Canter; James Cook; Shannon J. Finnegan; Lee McCracken; Justin Palk; J. Daniel Paulk; Erin Saunders Rath; and Daniel Swartz.

Chairman ROSKAM. Thank each one of you for your perspectives. They are very valuable.

Now we will go to inquiries from the members. Let us go to Mr. Reed from New York.

Mr. REED. Well, thank you, Mr. Chairman, and thank you to the panelists for being here today.

Commissioner, I wanted to go to some of the information you shared in your testimony, in your written testimony, in regards to the Security Summit and the Information Sharing and Assessment Center that was discussed in coming out of there.

So in the spirit of true oversight, not a "got you" question, but what is the status of the Information Sharing Center and when can we expect it to be up and running?

Mr. KOSKINEN. The status is we are working both internally and also with our summit partners to design it. It will be somewhat unique. There are a couple of other ISACs, as they are called, in the government that we have looked at. None of them quite apply to this.

We jointly with them all have security concerns obviously. Our hope would be to have it totally operational by the next tax season, but the technology features are such that we think we may or may not make that deadline, but we are all committed, the private sector partners with us, as quickly as we can to have it up.

What it will do is basically allow the private sector and the states to more easily have access to the information that is being shared. Right now everybody gives it to us and then we process it and give it back out. So it is not that people are not sharing the information. It will just be much more efficient if we can get the ISAC up and running.

Mr. REED. Okay. So one of the barriers you said was the technological barrier. What are the technological barriers that you are uncovering with establishing that center?

Mr. KOSKINEN. The technology there is just setting up. We have the governance structure already underway. So it is primarily just the technology. Can we set up the database in a secure way and the accesses for it to go forward?

Mr. REED. Is that hardware technology, software technology?

Mr. KOSKINEN. It is a combination. You know, we have this somewhat antiquated system with many moving parts to be able to collect the data, make sure it gets into our filters appropriately and gets back out in a secure way. It is primarily a programming and software challenge.

Mr. REED. Okay. That is helpful.

And you know you and I have talked numerous times before, and one of the things that I drive in my private life as well as public life is metrics. What are the expectations? What are we going to hold you accountable to?

So in the spirit of hoping to meet that deadline of having the ISAC center up and running by next tax season, what are you going to gauge yourself as the IRS to make sure that the ISAC operation is functioning and delivering on the security measures that you want to see happen in that arena?

Mr. KOSKINEN. I think our measure is that by this time next year it will be up and running. Our goal, aspirational, is to try to

see if we can get it up early enough to be at the front end of the filing season, but we would be delighted to report back to you.

The measure underneath it all, that is a system. It is the amount of data being shared, and then it is really the impact on how many of these returns can we catch. So we are monitoring carefully the number of returns we stop, and to the extent we can, as a result the increase in those as a result of the partnership.

Mr. REED. All right. So I am not going to let you off that easy. So the goal is to get it up and running by this time next year.

Mr. KOSKINEN. Right.

Mr. REED. And then you are going to monitor the data and you are going to gauge the data. How are you going to measure that? What does that mean? What is the metric?

I mean I hope the goal is not just we are going to get it up and running, and we hope it is going to do a great job, and we will come next year and say it is doing a great job, Congressman.

Mr. KOSKINEN. Right.

Mr. REED. You are getting millions of dollars potentially invested here. What are we going to hold you accountable for?

Mr. KOSKINEN. The ultimate goal is to catch and stop fraudulent refunds before they go out.

Mr. REED. So how much of an improvement in that arena can we expect from you as a result of this ISAC?

Mr. KOSKINEN. We do not have a number that we can work against yet. We know last year we stopped slightly over four million.

Mr. REED. Will you have that number when the ISAC is up and running?

Mr. KOSKINEN. Yes. We know last year we stopped four million suspicious returns, a million and a half of which were proven identity theft which were $8 billion of refunds prevented from going out. That is a baseline.

The goal would be to not only stop refunds, but to trap identify theft refunds.

Mr. REED. And how much?

Mr. KOSKINEN. And if we are successful, to some extent those numbers should go down. In other words, if we are successful at closing off systems and having better authentication on the front end, the goal would be to have the number of fraudulent returns filed not only stopped, but to go down. If we can get fraudulent returns under a million, that would be terrific.

Mr. REED. So get the fraudulent returns down to a million as a metric that we could hold you to?

Mr. KOSKINEN. I think the metric would be we had a million and a half we stopped in 2014. Can we lower that metric noticeably and significantly?

Mr. REED. And that would be about a million, down to about a million if I heard you correctly?

Mr. KOSKINEN. Well, my partners and I have to figure out what is a reasonable goal.

Mr. REED. That is what I am really looking for, are those actual hard metrics that we can hold you accountable to because what other metric are you going to deploy to make sure to see if this ISAC is a success?

Mr. KOSKINEN. The two metrics that I think are most important to everyone are: can we get the number of fraudulent returns filed down? And can we get the amount of fraudulent payments made down?

Mr. REED. To what?

Mr. KOSKINEN. Well, the goal would be obviously illusory to get them down to zero.

Mr. REED. Okay.

Mr. KOSKINEN. I mean we could fight it there, but we are not going to get them to zero.

Mr. REED. We all agree we cannot get to zero, but what is the goal you are going to be at from today to a year from now or a year after the ISAC center is up and running?

Mr. KOSKINEN. Well, as I said, our numbers for 2014 were 3.8 billion. We would like to get that number under three billion. We would like to get it under two billion at some day, but we are dealing with increasingly well-funded, sophisticated criminals, organized criminals around the world.

Mr. REED. I appreciate the work, and I appreciate the threat that you have. I just want to make sure we have a clear metric as we move forward, and we have discussed that before.

Mr. KOSKINEN. Yes.

Mr. REED. It is meant in good faith just to hold everyone honestly accountable.

With that I yield back.

Chairman ROSKAM. Mr. Lewis.

Mr. LEWIS. Thank you very much, Mr. Chairman.

Mr. Commissioner, thank you for your testimony this morning.

What concern do you have, and if you have some concern, could you share with us about restarting this program of private debt collectors?

Mr. KOSKINEN. Well, our concern goes to the issues that Mr. Camus talked about, and that is we jointly with them have been for the last couple of years battling phone scams, people impersonating IRS employees trying to shake down nervous or frightened taxpayers.

Historically we have run private debt collection systems twice before and they have never generated significant funding for the government. We are committed because the Congress gave it to us as a requirement; we are committed to do everything we can to make the program work.

But one of the complications this year as we put the program in place will be how to deal with the phone scams that are going on. So we have already had a bidder's conference with potential participants, trying to work with them as to how we jointly, and I am a big believer in partnerships as you know; how we jointly can figure out how to make this work.

One thing we are looking at it is, as I have told people publicly for two years, if you are surprised to be hearing from us, you are not hearing from us. People should have gotten letters from us long before they ever hear from us on the phone.

So one of the ideas we have is that we would send a letter to a taxpayer saying, "Your account has now been assigned to a given debt collector."

The debt collector then would write the same taxpayer saying, "We are Company X and your account has been assigned to us. We will be calling you."

So, again, a taxpayer would be in the situation of not being surprised when they got a call from the IRS. So we could continue to advise taxpayers if you are surprised, it is a scam.

The other thing we are trying to tell everybody is if you are going to pay your taxes in response to any inquiry, the check goes to the United States Treasury. The money does not go into a debit card account. It does not go into a bank account. It goes to the United States Treasury.

Mr. LEWIS. Mr. Commissioner, not too long ago, just maybe about three months ago I received a call at my home here on Capitol Hill. The person said, "I am from the IRS. We are going to sue you."

And I said, "Sue me for what?"

The person hung up. I tried to trace the number. I could not trace it.

How do we warn the American people that there are people out there that are not representing the IRS?

Mr. KOSKINEN. As I said, we have been working on this for over two years. I get clippings services every day, and there are good news articles at the local level, television stories either warning about the scam every year, and regularly we put out warnings about a range of scams.

I have been dismayed at the persistence of the calls. The IG has done a very good job with us of collecting the data. They have been working with the Department of Justice prosecuting as we go on, and as they have noted, the number of people falling prey to the calls is dropping as a percentage, but the calls continue.

The IG does a report that they share with us every week. There are 15 to 18,000 reported calls every week, and that is just the tip of the iceberg.

So all we can do and what we are trying to do is flood the zone as it were, regularly and consistently, again, trying to get people to understand in simple terms. As I say, if you are surprised to be hearing from us, you are not hearing from us.

The second thing is we never threaten you. We never say something is going to happen in 24 hours if you do not act, and the third thing is we will never tell you to put money anywhere but in the accounts of the U.S. Treasury in a check to the United States Treasury.

And if we can continue to get that message out, my hope is the percentage, now small, of people who fall prey to this will decline. People being subject to it are elderly, low income people, and recent immigrants who tend to be more nervous and frightened or easily scared. And they are the people whose heart you go out to most when you read about they have sent $1,000, $3,000 in effect into criminals' hands.

Mr. LEWIS. Mr. Inspector, do you share these concerns?

Mr. CAMUS. Yes, sir, we are very concerned about this scam. As I said in my testimony, it is the most persistent scam. We continue to try to do a public awareness. I personally, although I have a face

for radio, I recorded a public service announcement that we continue to try to market and get out on the YouTube channels.

People every week fall victim to this, and as the Commissioner noted, between 15 and 20,000 calls are made each week and reported to us. We are very concerned about this as a continuing crime, but we do have some prosecutions coming up in the future that we hope will help us warn taxpayers not to fall prey to this criminal activity.

Mr. LEWIS. Thank you very much.

I yield back, Mr. Chairman.

Chairman ROSKAM. Mr. Meehan.

Mr. MEEHAN. I thank you, Mr. Chairman.

I thank the ranking member for bringing up that issue. I suspect everybody on this dais got one of those phone calls. I did. My wife did.

Mr. KOSKINEN. I have gotten one. When I got it I thought there must be somebody at the IRS I could talk to about this.

[Laughter.]

Mr. MEEHAN. We did the same press conference and got tremendous coverage and alert, but people are still once they get that call very, very scared, and there is one discrepancy that is not my questioning, but we say that we never go after people and ask for, you know, demand, but there are some collection services that are out there potentially speaking on behalf of the IRS with some level of legitimacy, and I think that is an issue that we need to be able to confirm, that you will never get a phone call from anybody representing the IRS, but a lot of work for us to do.

Listen. As technology changes, we are utilizing it more, and I have seen a tremendous shift in utilization of e-filing and other kinds of things, which I assume makes it a little easier for you to be able to handle the returns that you get, Commissioner, but we are struggling on the front end with the authentication issue. Are you who you say you are?

And obviously in the beginning, we began with just name, Social Security number, and some of the other things, all of which are readily available for somebody not even hacking into your system oftentimes by getting information from taxpayers.

Now, I know that there have been some efforts in the IRS to strengthen its authentication system, but there has also been criticism that notwithstanding those efforts, things have not even reached the standards of what is expected of a governmental agency.

So can you give me a sense on where this is going? I am aware that even within the agency you are looking at 2016, setting a standard, trying to get there, but because authentication is so important not just on the back end, but on the front end as well, to assure that the initial inquiry is accurate.

Can you talk to me about authentication?

Mr. KOSKINEN. Yes.

Mr. MEEHAN. Where we are going and how we can fix this and get it better?

Mr. KOSKINEN. Yes. It is obviously critical for all the reasons you state. It goes to the heart of our ability to expand our online

services because if we are going to expand those, we have to expand them for legitimate taxpayers.

So as noted, when we first designed Get Transcript four or five years ago, so-called out-of-wallet questions were a standard means of authentication on the theory that you ask questions only the taxpayer should know.

It turns out with all of the data breaches, all of the information available on social media, it is increasingly easy, not totally simple, for criminals with enough personal data to, in fact, be able to masquerade as you. As I used to say, they can answer sometimes your questions better than you because they remember the year you bought the Volvo. They know that. You may not remember it.

So what has happened with the evolution of the sophistication of criminals is simply relying on out-of-wallet questions no longer is the sort of standard you should use. We have gone to multi-factor authentication.

In simple terms, multi-factor authentication, and you have done it with your online services, you will change a password or do something, and you will get sent to another account, to an iPhone, to your iPad, someplace else, a code that you enter back in, and that is a two-factor authentication. They know you are online. They also know that you have got possession of a device that the criminals do not have.

Our problem is we do not right now have email addresses or telephone numbers regularly for taxpayers. We correspond with people by paper.

Mr. MEEHAN. Well, that is what your Identity Assurance Office is looking at some of these things. Where are they going to be going with this in 2016? Because the assessment by the Inspector General was that you are going to assess costs and risks and other kinds of things.

Mr. KOSKINEN. Yes. So what we are testing right now, before getting Get Transcript back up or IP PINs, is a multi-factor authentication where through a credit service, and which now would be the first to do that, who, when you go onto the credit service they have your phone number and other information, where we would correspond with the taxpayer online. We would then send to their iPhone or iPad a code. They would pick that code up and come back in, and we would be satisfied that even the criminal knew your out-of-wallet questions, which you still have to answer, they probably do not have possession of your cell phone.

The difficulty is that is a good system, and it will make it much more difficult for criminals. The problem is it will make it a little harder for taxpayers as well.

Mr. MEEHAN. Right, finding the right balance.

Mr. KOSKINEN. Yes. Our estimate is, judging that we have talked to the British and we have talked to everybody we can talk to, that at the front end if we can get 50 percent of taxpayers through, that will be helpful.

I would remind everybody on the out-of-wallet questions, our experience was 22 percent of taxpayers could not answer their out-of-wallet question, and half the criminals could not answer them.

Mr. MEEHAN. Well, that is the problem. Everybody nowadays has a million different pins and other kinds of things. You forget

what you gave them in terms of the identifying information. You cannot answer your own questions.

Mr. KOSKINEN. Yes.

Mr. MEEHAN. How do we get to a system in which we can effectively address that?

Mr. KOSKINEN. Well, again, the multi-factor does not require you to remember the number you get. Every time you need it a new number will be sent to your iPhone, your iPad or texted to you, and you will use that new six-digit number just to authenticate, again, that you are who you are, and it will be harder for a criminal to duplicate that because they will not have possession of the alternate or the multi-factor part of the authentication.

The problem will be and our goal will be over time to make that work smoothly enough with data enough that we could get back to the 80 percent level. We will probably never have an authentication system that everybody can get through. So the balance is how do we keep criminals out without keeping all of the taxpayers out at the same time.

Chairman ROSKAM. Mr. Rangel.

Mr. RANGEL. Thank you so much for calling this hearing, Mr. Chairman.

It seems as though the criminals have been bipartisan in their attempt to defraud innocent congressional people. So that is one way to bring us together, through the criminal element.

Years ago we had hearings, and the IRS indicated it sent out 30,000 letters to taxpayers telling them that their tax debt was being sent to private debt collectors, and then the debt collectors were required to send a letter to the taxpayers, but it turned out that some 30,000 letters were returned to the IRS. In other words, it did not appear at that time that the IRS was effective in notifying the taxpayers.

Do you have any problems in your office as to whether or not you are effectively reaching the taxpayers?

Mr. KOSKINEN. Our information and our experience is that we were able to reach, give or take a little, 75 to 80 percent of the taxpayers. The problem is people move every year, and give or take a little, 15 to 20, 25 percent of people are moving every year.

Mr. RANGEL. Okay. The second question I have has to deal with the effectiveness of the investigation and the prosecution of these people. We hear about the victims, but as a former Federal prosecutor, I do not ever remember reading about a criminal that is conducting these fraudulent calls ever being arrested and sent to jail.

Do you have any details as to what are you doing in the prosecution department to let the people know that you are being effective?

Mr. KOSKINEN. Right. I will distinguish that Mr. Camus is the expert on that.

Mr. RANGEL. I know. I was particularly talking to Mr. Camus.

Mr. KOSKINEN. Yes, we have prosecuted over 2,000 people for identity theft.

Mr. RANGEL. I know. I am asking you how do you get that out there?

Mr. KOSKINEN. But for phone scams, I give you Mr. Camus.

Mr. RANGEL. That is who I want.

Mr. CAMUS. Yes, sir. We have had a couple of high level cases. The challenge that we have had is we find ourselves chasing a lot of the runners who are just converting the money into various forms.

But last July we had a conviction of an individual who was responsible for over a million dollars in damage to his victims. He got sentenced to 14 years in Federal prison. So we have had cases on occasion.

We are currently working with the Department of Justice on a cluster of cases that we hope, to answer your question, that when we get those prosecutions we will use those as a springboard to warn people on a grand scale that this is going on. If you get contacted out of the blue by somebody claiming to be from the IRS or the Treasury Department and you have not heard from them before, as the Commissioner said, you are probably getting scammed.

Mr. RANGEL. I hate to say we are from the Congress and we are here to help you, but quite frankly, are these fly-by-night individuals? Is this an organized national scheme?

These people seem to be pretty well organized. As a matter of fact, they are outsmarting the IRS and, therefore, the Congress and the Nation. But who are these people? How are they classified?

What is going on?

Mr. CAMUS. One of the biggest challenges, sir, is that initially the scam started out as being a centralized group of people. Then once the criminals started to realize through warning taxpayers not to fall for it, other criminals saw, boy, if I just pick up the telephone and call somebody and threaten them, I can collect money.

Mr. RANGEL. So you do not really think this is organized?

Mr. CAMUS. I think this is centered now, sir, to a point where there are all kinds of different folks making these types of phone calls because when you think about it, from a criminal point of view, they have very little invested in this crime. They are just picking up the phone and calling people, and if they get two or three victims a day, that is good money.

Mr. RANGEL. I think we ought to take this up with the Justice Department.

Getting back to the debt collectors, forgetting the outside criminals, do you really think the debt collectors are doing a better job than the IRS trained collectors in the past?

Mr. KOSKINEN. I think what we are committed to doing is to run this program as well as we can and——

Mr. RANGEL. That was not my question.

Mr. KOSKINEN. No, and see what the answer is.

Mr. RANGEL. My question is that the Congress directed you use the private sector debt collectors.

Mr. KOSKINEN. Right.

Mr. RANGEL. And I am asking, based on your experience, do you find that to be more effective than when the IRS trained the collectors?

Mr. KOSKINEN. Well, the last two times it has been tried by the IRS it did not turn out to be more effective. It turned out IRS employees were more effective.

There were questions raised about how those programs are run and the costs of them. We now do have a statutory mandate.

Mr. RANGEL. Who trains these private debt collectors? Because debt collectors can be very, very mean, rude. Do you train them now?

Mr. KOSKINEN. We will, in fact, work with the companies to provide appropriate training as to they need to know something about their authority and they need to know something about debt collection.

We will try to and select and monitor, with the Inspector General, the performance of these organizations to make sure that they are legitimate companies, but there is always that risk. But as I say, we are committed, and I think it is important for the Congress to understand to run this program as well as we can, as best as we can, we will have a fair test of how effective it is.

I do not want anybody thinking that we are dragging our feet.

Mr. RANGEL. Mr. Chairman, I want to thank you for this hearing. I think there is a wide range of areas that we can work with the IRS and be cooperative in a bipartisan way. This is one heck of a good beginning, and I did not like the Commissioner saying what they are trying to do. I think we ought to have other hearings to find out what can we help them to do it.

We are not challenging their good intent, but there are a lot of things that have to be done, and it looks as though we are throwing up our hands saying we are doing the best we can.

We are not blaming you, but we have to work more closely together.

Thank you for having these hearings.

Chairman ROSKAM. Thank you.

Mr. Rice.

Mr. RICE. Mr. Koskinen, I would like to start with you, sir.

You know, I was a tax payer and CPA for 25 years, and I dealt with the IRS hundreds of times, and most of those times in my time I found them to be professional, and they are doing a difficult job in a difficult circumstance.

But we have a voluntary compliance system. It does not work if the taxpayers do not work with us, and in order for the taxpayers to do that, they have to have a level of confidence in the IRS. They have to know that the IRS is competent and that they are honest, and that they are not going to target them for anything other than their tax liability, and that they are going to act in an ethical way.

And in looking at what has happened in these last five years with scandal after scandal after scandal, from Lois Lerner targeting people who do not believe the way the Administration believes, purely for their political beliefs, and then the lies and the obfuscation and the cover-up in the investigation of that, and then redirecting taxpayer funds from taxpayer assistance to other things and allowing taxpayers to call in and not be responded to at a rate of two-thirds of the people calling in not being responded to, and then apparent, you know, disregard or incompetence in protecting taxpayer info, in taking basic measures to avoid sending out fraudulent refunds.

It just looks to me like and nobody being held accountable in any of this, you know, nobody getting fired, nobody being held account-

able in any way. It looks to me like the IRS has so undermined its credibility, and a lot of this happened before you got there, but it so undermined its own credibility in the last five years, it is almost beyond my comprehension.

It is almost like if they had set out to do it intentionally, I do not know what else they could have done to further undermine their credibility than what they have done in the last five years.

So I am just really worried. You know, this is not just something that is a one-time thing or it only happens every once in a great while. It is just every year it seems like there is another scandal, one after another after another, a cascade.

And, my friend, there is an old saying. If you find yourself in a hole, the first thing you need to do is quit digging, right?

So my question to you, I have got some questions here that the group here wants me to ask you, but my question to you first is: how do we stop this cascade of scandals? How do we start working on rebuilding the credibility of this institution that is so fundamental to this country?

Because I do not see it happening right now. Is there some method, quality control? Is there some process that you're undertaking to foresee instead of us being totally reactionary to scandal after scandal after scandal and eroding the taxpayer confidence?

Is there something you are doing to try to head this off and stop this endless cascade?

Mr. KOSKINEN. One of the things we are doing that is important, and there are two basic things. One is to get people to understand our responses to the challenges and the work we are doing to fix them, and to the extent that I am a big believer in transparency, we have hearings. I think the hearings should point out the problems. There has been less focus on the solutions.

We have taken every recommendation and implemented that have been made by the Inspector General in response to the (C)(4) issue of social welfare organizations not being handled promptly. We have taken every recommendation of the Senate Finance Committee, both its bipartisan recommendations, the majority report and the minority report.

We have tried to make it clear that if anyone has any indication, our goal is to make sure people, as you say, are treated fairly no matter who they voted for, what party they belong to, where they go to church. I think that is fundamental.

The second thing that we have done is we have set up a risk management program for the entire agency and are working to have every employee of the IRS from the front line on up view themselves as a risk manager so that they understand my view, and I mean it, as bad news is good news. The only problem we cannot solve is the problem we do not know about.

As I said at my confirmation hearing two and a half years ago, it would be fun to say we will never make a mistake. There will never be a problem. We run the world's most complicated Tax Code. We deal with 150 million Americans. We have 85,000 employees. The better goal, it seems to me, is to say that if there is a problem, we will find it quickly, we will fix it quickly, and we will be transparent about it.

And I think if the public understands not that there will never be a problem, but if there is a problem our goal is to find it quickly, to fix it quickly, and to be transparent about it, then we will be on the road toward restoring confidence in the agency.

Mr. RICE. Friend, that is reactive and not proactive.

Mr. KOSKINEN. No, if I get employees on the front line to raise their hand when they see a problem, that is proactive. That is not reactive. General Motors' ignition switch is my favorite example. A lot of people knew about the ignition switch problem. It is just nobody at the top knew. My goal is to make sure that any time any employee knows anything is going on, they will raise their hand and let us know.

We are proactive in terms of implementing all of the recommendations that the IG made and the Senate Finance Committee and others have made about how to make sure we never have a management failure such as we had with the (C)(4).

We also have a valuable partnership with the IG and GAO. We take their recommendations seriously and implement them, but I think it is important for people to understand the culture of this organization. We have wonderful employees, dedicated to the mission. The culture is that if there is a problem, we reward messengers, do not shoot them; that we really mean it, that we want to find out whenever we have a problem and a situation occurs, as quickly as we can we can fix it.

I think if the public understood that inevitably there will be issues, but we have a system designed to find them as quickly as we can, where employees are empowered, feel responsible to let us know, they will then feel that problems will not get hidden. They are not going to go on forever; that we are, in fact, going to fix them as quickly as we can, and we will let you know about it.

Chairman ROSKAM. The time has expired.

Mr. RICE. People need to be held accountable.

Chairman ROSKAM. Mr. Davis.

Mr. DAVIS.

Mr. KOSKINEN. Yes.

Mr. DAVIS. Thank you very much, Mr. Chairman, and I, too, want to thank you for calling this hearing.

And I want to thank our witnesses for being here with us today.

Mr. Chairman, I am troubled a bit by the policy of using private tax collectors who could earn up to 25 percent of what they collect, and I know that we often have the discussion relative to what is most effective, public or private, but it seems to me that this policy sets up a perverse incentive for private industry to harass and confuse taxpayers while costing the Federal Government money.

My office often receives calls from constituents who have received fraudulent calls purportedly from Treasury or the IRS, as well as I get calls from constituents who have been targeted by mean-spirited debt collectors who threaten and frighten them.

A recent call involved a constituent whose daughter with learning issues had given her credit card number to the person who called from the Treasury.

Of course, I continue to be concerned and am troubled by whether or not we are trying to get from an agency without having all of the resources that they really need.

Commissioner, I guess I am trying to get at, you know, based on the discussion that we are having right now and that we have had this morning, it seems as though in some ways we are between the rock and a hard place, that, on one hand, we are trying to prevent fraudulent activity from occurring and, on the other hand, it seems as though we do not have what we need even in the way of investigatory personnel or people to really deal with the pervasiveness of the issue. And I guess the agency is trying to do what it can.

Are there any other approaches that you can think of that might help us to deal more effectively with these problems?

Mr. KOSKINEN. Well, clearly, resources are an important part of it. Ninety-five million of the money we got this year in additional funding have gone to cybersecurity to allow us to buy better monitoring systems, to begin to retire antiquated equipment that is at greater risk. The budget for 2017 requests additional funding for that.

It also is a procedural issue. One of the reasons I called the CEOs, tax preparers, software developers, payroll providers and state commissioners together a year ago was because we needed to change the paradigm. As I told them, the goal was not to tell them what to do. The goal was to create a partnership because no one of us by ourselves can deal with the complexity and sophistication of the criminals we are facing.

So by bringing the entire tax, what we call the ecosystem together, dealing with taxpayers at the front end when they use the software or deal with their preparers, dealing with the returns when they come through the states and the IRS, and then dealing with financial institutions when the refunds are deposited, we can, in fact, begin to have a more coordinated strategy to fight back against the criminals.

And I think it is an important step forward as we go. We do not have a line of sight into the taxpayers directly. They deal with software companies. They deal with preparers, but the preparers and software companies can give us identification of what are the ideas from the computers which they are using to file the returns. Are they filing quickly or not so quickly?

We have plenty of data elements that we now have we did not have before. So part of it is resources, making sure we are doing the best we can and we have been constrained for some time. Part of it is, as I say, changing the paradigm, trying to figure out, as I say, if we can, can we get beyond reactive and start to be able to anticipate where it is going to happen?

We have been warning preparers for a year that as we get better at stopping false returns, the next place that the criminals are going to go is attacking preparers and hacking into their system because then they have all the information they need in that way, and we see some of that happening.

But, again, the preparers have been very good. They are very sensitive about that, setting security standards across the industry that they are setting. We can require them, but we require them after they have said this is what they need.

Mr. DAVIS. Thank you very much.

Mr. Chairman, I think we might want to take a look at our policy perspective in terms of trying to get further insight into solving the problems.

Mr. KOSKINEN. Thank you.

Chairman ROSKAM. Mr. Holding.

Mr. HOLDING. Thank you, Mr. Chairman.

You know, in order to properly protect taxpayer data, we need to authenticate as we have discussed on the front end so that only valid users can access the systems, but the reality is we have to also minimize the damage that bad actors can do if they access the system.

Both GAO and TIGTA have reported the IRS is not making sure that the only people who are accessing the information are the folks that have authorization to do so. So my first question to Ms. Lucas-Judy and to Mr. Camus is: identify for me succinctly what do you think are the most serious problems with the IRS' information security.

So, Mr. Camus, if you could kick it off. Give it to me in a sentence.

Mr. CAMUS. The insider threat in addition to some of the things we talked about with Get Transcript and IP PIN. We are concerned that the 55,000 IRS employees who have access to the most sensitive data of every taxpayer do not do horrible things with that data and commit identity theft themselves.

Mr. HOLDING. Ms. Lucas-Judy.

Ms. LUCAS-JUDY. The GAO has found that IRS could do more to authenticate the users and make sure that systems are protected. They could do more to ensure that the level of access that is provided is just what people need to do their jobs.

And then also another place was installing security patches for software as soon as it is available. IRS' own guidelines call for a risk-based approach to installing patches to software, and what we found was that they were not adhering to their own guidelines there.

Mr. HOLDING. Interesting. I want to quickly move over, Mr. Commissioner, to the law enforcement side of the IRS. As a former U.S. Attorney I firmly understand and appreciate the great value of the work done by the Criminal Investigative Division. You always want to have an IRS CID agent on your case.

So it is curious to listen to the testimony this morning about the continuing prevalence in tax related crimes, such as identity theft and fraud, and you mentioned the additional funding provided to the IRS during fiscal year 2016. I believe you said $290 million.

So how much of that was directed toward the CID, the Criminal Investigative Division?

Mr. KOSKINEN. The bulk of the money went first at 178 million to taxpayer services; 95 million to cybersecurity and improving the systems. There was no additional funding. Some of the systems are used by CID and we have been supporting the systems, but there are no additional personnel that were added to CID.

We are down about 5,000 revenue agents, officers, and criminal investigators over the last five years.

Mr. HOLDING. So, I mean, it occurs to me you are talking about these crimes being committed. So who is going to investigate these

crimes and put the cases together and bring them to the prosecutor, bring them to the U.S. Attorney's Office and ask them to prosecute?

So I do not understand why you are not placing more of a premium on the criminal investigation.

Mr. KOSKINEN. We are. Five or six years ago before the explosion of identity theft CID spent about three percent of their time on this. They are now up to 20 percent of their time. So they have, in fact, assigned a high priority to identity theft and refund fraud.

Mr. HOLDING. Mr. Commissioner, interestingly, you know, I have taken a look at CID's business report from fiscal year 2015, and I see a notable decrease in the number of investigations initiated and a troubling trend overall with the number of Special Agents and professional staff since 2010.

You cannot deter crime unless you are prosecuting crime.

Mr. KOSKINEN. That is right, and we need more people, and the only way to get the people is to fund them, and over the last five years, six years, our budget is down a billion dollars. We are down 15,000 employees. We are going to shrink another two to 3,000 this year, and that is going to include shrinkage in CID agents, revenue agents and revenue officers.

It is a point I have been making for two and a half years.

Mr. HOLDING. Commissioner, when you are faced with a budget, I mean, you have to look at what you need to do with the money that you are given, and by shrinking the Criminal Investigative Division and really limiting the number of prosecutions, I mean, it is defeating in and of itself.

You know prosecution and the penalties that come with successful prosecution are the ways to deter crime. Holding them up as an example, you know, we have heard over and over again that, you know, criminal organizations are getting more interested in committing tax fraud because they know they are not going to get prosecuted.

My time has expired, Mr. Chairman. So I yield back.

Mr. KOSKINEN. If I could, Mr. Chairman, just note our funding goes to enforcement, taxpayer service, and information technology. As the budget gets cut, everything has been cut. They are all a priority. Now, we would put more money into enforcement. We would put more money into taxpayer service. We would put more money into information technology if we had it.

One of the things I hope we will do with the $290 million is demonstrate to the Congress if you give us the funding, we will demonstrate to you exactly the improvements you bought with that additional funding. The converse is true as well. If you do not give us the money, we will not be able to increase enforcement, improve taxpayer service or improve protection.

Chairman ROSKAM. We have a first-time caller, a long-time listener. Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman, Mr. Roskam, and Ranking Member Lewis for holding this hearing.

Yesterday was tax day, a very important day in the calendar, and millions of Americans have been busy filing their taxes this season and trust that private information is secure.

You have heard from the Commissioner about the drastic underfunding and undercutting. Those are facts or they are fables. I happen to believe they are facts. And I want to commend you for weathering storm that we have been experiencing over the last couple of years.

I think the storm is from men and women of good faith, but I think their priorities are misdirected. Identity theft and tax fraud are a growing problem, growing problems being carried out by very, very sophisticated criminals who we usually assist.

As technology changes and criminal syndicates hone in on American tax returns, we need to help, be able to keep up. Just this year a man was changed in Federal court in Newark, New Jersey for being sent nearly $343,000 in fraudulent tax refund checks, cashing them in New Jersey bank accounts.

Too often the victims are not alerted and not able to get the help they need to correct the problem, and I think Mr. Holding is on target. If we do not prosecute, what good does it all mean?

Organized crime last year, syndicates accessed past tax returns in more than 100,000 people to file fraudulent returns, and the IRS sent nearly 50 million in refunds before detecting the crime. Using Social Security numbers—and that is a whole other issue which we have struggled with since the Homeland Security Department was put together and the committee was put together—birth dates, street addresses, other personal information, hackers completed a multi-step authentication process and requested tax returns and other filings, then used that information to file fraudulent returns.

I introduced a piece of legislation, H.R. 3981, the Identity Theft and Tax Fraud Prevention Act, that would take a number of steps to address the issue. It would create a single point of contact for identity theft victims. I think that is a big issue as I read the materials.

Provide a taxpayer notification of suspected identity theft; create criminal penalties for tax fraud through identity theft; increase taxpayer repair penalties for improper use of personal information; and reduce the display in the use of Social Security numbers all over the place.

Retailers demanded it because we demanded it in many of the Homeland Security pieces of legislation that we passed.

I am proud to sponsor that legislation, this legislation, with Congressman Lewis, the Taxpayer Protection Act of 2016. It builds on these provisions and adds hopefully some meaningful reforms like the elimination of private debt collectors, and we will debate that, and increase funding for taxpayer services.

Mr. Commissioner, I know that both the GAO and TIGTA found in a 2014 report on cybersecurity that identify theft victims are no longer provided with a single point of contact in the IRS. The IRS has indicated that budgetary constraints do not allow for a single employee.

Could you please comment on that and how that if we did have enough it would benefit the taxpayers?

Mr. KOSKINEN. What we have done, which we think is a significant step forward, is bring all of the identity theft assistance programs into one area. It used to be in our various divisions.

Mr. PASCRELL. Right.

Mr. KOSKINEN. So there is now a single point of contact. In other words, the taxpayer is not going to get referred to different divisions of the IRS with their problem, and we think that that has been effective this year. We think the time it takes to resolve a taxpayer account problem is down to our goal of 120 days and we would like to shrink it. It was at one point almost a year.

The problem an individual point of contact is then when you call, they may be on vacation. They may be out of town. If you call any other call center, you never get them. The key is to have it centralized so that people know what the status of the case is so when the taxpayer calls back in, that single point of contact can continue the discussion rather than start all over again. And we think that that is important.

Mr. PASCRELL. Good. Thank you, Mr. Chairman.

Chairman ROSKAM. Chairman Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman.

Commissioner, it is always good to see you. I have two issues I would like to talk to you about. First, as you know, last year's tax deal included the Johnson, Larson Wrongful Conviction Tax Relief Act.

Now, back in January we wrote you about the importance of quick implementation, and as you know, our bill would allow those who previously paid taxes on their restitution to be able to file for a refund when they ordinarily could not do so because too many years have gone by, and as you know, they only have this year to file for such a refund.

Mr. Commissioner, it is April already, and I want to know what you and the IRS are doing to get the word out about this important relief.

Mr. KOSKINEN. We every year—because you are exactly right; the statute runs out—early in the filing season try to make, again, a full national release of the amount of money that is out there, the states in which it is available, trying to encourage people.

Usually what has happened, they had a job; they got withholding; and then they forgot about it. They did not have to file. They forgot about the act that they should have filed to get the refund or the money back.

Every year we do our best to remind taxpayers of that situation, and we issue a kind of national public campaign to get people aware of that.

Mr. JOHNSON. Are you doing that right now?

Mr. KOSKINEN. We have done that right now probably six weeks or so ago. We actually went state by state, and we had a lot of good coverage in Oregon and Massachusetts, Mississippi people saying, "This is the amount of money that in this state taxpayers have if they would just file."

Mr. JOHNSON. Okay. My second issue involves illegal immigrants and their use of Social Security numbers. I know this has been brought up before, but it is too important of an issue for me to stay silent.

As you know, as Chairman of the Social Security Subcommittee, one of my longstanding priorities has been to protect Americans' identities, and as we have heard today, the IRS struggles to respond to identity theft.

At last week's Senate Finance Committee hearing you were asked about troubling practice of illegal immigrants stealing Americans' Social Security numbers to get a job and then filing tax returns using their own names and their own individual tax identification numbers. What I find absolutely outrageous is your suggesting that when it comes to illegal immigrants, the IRS could not really be bothered when it comes to these folks stealing Americans' Social Security numbers, and I think that is wrong, and it ought to stop now.

What is the status of the pilot program you began in 2014 that sends notices to suspected victims of identity theft?

Mr. KOSKINEN. I do not have the update to that. I will get that for you, but again, as I said, the point is anyone with a job earning money is required to pay taxes whether they are undocumented for one reason or another or whether they simply cannot get a Social Security number. They apply to us and authenticate themselves and are given what is called an ITIN.

Our role is to make sure that those tax payments are made and credited appropriately. Oftentimes to get a job, you need a Social Security number. They may have borrowed one. They may get one from a relative. You can buy them for ten or $15 on the Web.

The problem is if people think we are in the immigration business of tracking through and finding out what is going on with those Social Security numbers, we are not going to get people paying the taxes they owed because of their nervousness.

We are though looking at can we advise because the Social Security number just comes as an adjunct either on a W–2. Sometimes we do not even know what the Social Security number is. The return is filed without a W–2, but the taxes are paid.

So we are doing, as you note, a review to see what would the implications be of notifying people that somebody has used their Social Security number for a job, not to file a return. The return does not come with a Social Security number as the identifier, but so that it is out there.

We already, as noted earlier when we talked, even when on some of the accesses to our applications the criminals were not able to get through, if they tried and we track that, we notified all of those taxpayers that their Social Security number was in the hands of criminals, and while it was not successfully used to get any information from the IRS, we think it is important for taxpayers to know if criminals have access to their Social Security numbers.

So we are trying with a pilot program to figure out exactly what can we do without discouraging people from paying their taxes to let people know whether their Social Security number is being used.

Mr. JOHNSON. Well, the status of the pilot program you began in 2014, it sends notices to suspected victims of identity theft is important.

And, Mr. Camus, I understand that the IG has a report coming out on the pilot program. What are your thoughts?

And has the IRS made any progress in stopping the improper use of Social Security numbers?

Mr. CAMUS. Sir, we will be issuing our report hopefully in June, and we will be able to address your issues and concerns in that report.

Mr. JOHNSON. Okay. Mr. Commissioner, that the IRS can track when illegal activity has occurred but fails to notify the victims of these crimes is plain wrong. Mr. Commissioner, the IRS must do better. Americans rightly expect the IRS to stand up for them and protect their Social Security numbers.

Thank you, Mr. Chairman. I yield back.

Chairman ROSKAM. Mr. Marchant.

Mr. MARCHANT. Thank you, Mr. Chairman.

Like Representative Johnson, I felt like the hearing that took place earlier this week or last week was very alarming. I got a lot of input from my constituents about the responses that were made at that time. So I would like to just discuss that a little bit further and get your thoughts.

Your responses basically said they are undocumented aliens. They are paying taxes. That is in everybody's interest to have them pay the taxes they owe.

So is it your position that a person that is in the country illegally and is breaking the law because they are in the country illegally and undocumented, it is the law that they pay income tax on their earnings?

Mr. KOSKINEN. Yes. And in fact, whenever there have been over the last 30 or 40 years, any amnesty programs or programs to allow people here in undocumented status to become green card holders or citizens, the first thing they have to establish is that they paid taxes on any earnings while they were in the United States.

So the reason a number of people file with ITINs who are here legally but just cannot get a Social Security number, they are not American citizens. But the reason undocumented residents are filing and paying their taxes is just for that reason, that in fact some day they are going to have to establish that they paid them.

And our job is, in fact, to collect those taxes.

Mr. MARCHANT. Is it a crime or is it illegal for a person to obtain a job by giving another person's Social Security number?

Mr. KOSKINEN. I am not sure what the legal implications are because we are not in the immigration business, but I am sure it is not allowed. I do not know what the nature of——

Mr. MARCHANT. If my son gave his cousin's Social Security number on his tax return, if somebody in the United States is here legally and they give a false Social Security number or another person's Social Security number, are they creating some kind of fraud with the IRS?

Mr. KOSKINEN. Again, I would stress the Social Security number is not used to file with the IRS. So in your case your son would be giving the Social Security number to someone to allow him to get a job and they would be using that Social Security number with their employer.

With us, they would be filing with an ITIN. So the Social Security number is not used to file with us. The Social Security number, whether it is bought, borrowed or stolen, is used to get a job.

Mr. MARCHANT. To get to a logical conclusion of this, but a Social Security number triggers the deduction of Social Security tax. It triggers all kinds of deductions, and it triggers all kinds of forms that get sent to the Social Security Administration and then gets filed when they file their tax return, right?

Mr. KOSKINEN. No. Actually what they are filing with us is simply whatever information they have of their revenues and expenses or taxes. The Social Security Administration and the Immigration——

Mr. MARCHANT. But it will ultimately either be a W–2 or a 1099, correct?

Mr. KOSKINEN. Yes, but as noted, we have been collecting and paying out taxes without those W–2s being identified. Our problem is to make sure that the people who owe the taxes are paying them.

Mr. MARCHANT. So many of these people obtaining the earned income tax credit and the child tax credit have not even presented a 1099 or a W–2 on their tax return?

Mr. KOSKINEN. You are only eligible for the earned income tax credit if you actually file with a Social Security number and have a legitimate Social Security number. ITIN holders are not eligible.

Mr. MARCHANT. Okay. So but if you file with the Social Security number that you used to get the job, that the employer uses to issue you a W–2, is the Social Security number on the W–2 the one that the employee gave them that is not correct or is it the ITIN number that you obtain from the IRS?

Mr. KOSKINEN. The W–2 will not have the ITIN number. The W–2 will have a Social Security number that the employer accepted when the employee got the job.

Mr. MARCHANT. But it is an inaccurate document. The IRS, I assume, is using a W–2 that is an inaccurate document.

Mr. KOSKINEN. Well, it is an inaccurate document if it has a Social Security number not there. The numbers on the document will be accurate. It will reflect accurately the income and withholding.

Mr. MARCHANT. So the IRS just disregards the inaccuracy, the parts of the document that are inaccurate, but they will take the income part.

Mr. KOSKINEN. Again, the Immigration Service works with employers to make sure that people are legitimately getting jobs. Social Security enforces whether the payments are being made appropriately. Our job is are people paying taxes on the earnings they have. If the W–2 comes in and says I earned $14,000 and here is my tax payment, that is what our job is.

If we start going into the immigration business, we are going to have a lot of people decide, "Well, I cannot file with the IRS because that is going to trigger a set of government inquiries".

Mr. MARCHANT. Well, I would not say that you are necessarily in the immigration business if you were just saying to the taxpayer, "You are giving me inaccurate information on your tax return," and that in itself should raise some red flag as when it begins to be paying credits out, whether they be earned income tax credits——

Mr. KOSKINEN. The information they are giving us is accurate. That is the Social Security number they have been using, the revenues and the withholding and that are accurate numbers, and again, the statute provides we are supposed to be collecting that tax, not going behind it and figuring out whether they legitimately had that job.

If they had the job and got paid, if they are paying their taxes, they have an obligation to pay them. If they are filing, the W–2 has accurate information about revenue and expenses. That is what we are supposed to be doing.

Now, as I said, whether the use of that Social Security number, again it is taxpayer information whether we can provide that and in what forms we can notify taxpayers, somebody has gotten a job with their Social Security number.

Chairman ROSKAM. Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Commissioner earlier we were discussing the funds going towards taxpayer services for wait times and various items. The IRS has discretion over roughly $500 million in funds that they collect from fees that they can appropriate any way that they want.

Could you tell me why you all have decided from 2014 to 2015 to cut almost $130 million that was used in 2014 for taxpayer assistance?

Mr. KOSKINEN. Because for that year, as you will recall, we had a budget cut of $350 million, and inflationary and payroll costs of $250 million. So we had $600 million that we had to make up, and the way we made that up was allocating those user fees.

Some portion of them, about 50 million, went to taxpayer service. A big chunk of them went to information technology, and ID theft. In other words, again, we end up having to do enforcement, taxpayer service, and information technology.

As our budget gets cut, everything has to get cut to some extent. There are priorities. Last year, as I testified before this Committee, if we had put the 100 million there, we would not have had the money to spend both in implementing. We have got a whole set of unfunded statutory mandates. Private debt collection is an unfunded mandate. The health coverage tax care program is an unfunded mandate. The ABLE Act is an unfunded mandate. Going after people who owe more than $50,000 and having their passports taken away is an unfunded mandate. The Point of Contacts Compliance Act is an unfunded mandate.

Mr. SMITH. Okay. Let me ask you a question. In regards to taxpayer assistance, did Congress leave your funding level for taxpayer assistance to help taxpayers?

Mr. KOSKINEN. Yes. What the——

Mr. SMITH. We did leave it at level funding?

Mr. KOSKINEN. You left it, and we did not change that level of funding. What the Congress has not done——

Mr. SMITH. You changed the level——

Mr. KOSKINEN. What Congress has not done for the past four or five years is fully fund the cost of taxpayer service.

Mr. SMITH. Okay. What I am talking about is taxpayer assistance. So when Congress in the line item budget, we appropriated level funding for taxpayer assistance; is that correct?

Mr. KOSKINEN. Yes, and we spent that money.

Mr. SMITH. Okay. That was my question.

The other question is the fund that you all have complete discretion of, which is the user fees, you have complete discretion of user fees, correct?

Mr. KOSKINEN. Yes. We file a spending plan with the appropriators.

Mr. SMITH. Okay. That was my question. You answered that.

My other question is that in 2014 you appropriated $183 million for taxpayer assistance; is that correct?

Mr. KOSKINEN. In 2014, yes.

Mr. SMITH. Yes. In 2015, you appropriated 49 million for taxpayer assistance; is that correct?

Mr. KOSKINEN. That is correct.

Mr. SMITH. So it was your decision to cut taxpayer assistance by $130 million; is that correct?

Mr. KOSKINEN. Yes.

Mr. SMITH. Thank you.

Mr. Chairman, that is all I have.

Mr. KOSKINEN. If I could just expand, we also cut tax enforcement.

Chairman ROSKAM. The time has expired.

Mr. KOSKINEN. We also cut information technology.

Chairman ROSKAM. Mr. Koskinen, you will have an opportunity.

Mr. Renacci.

Mr. RENACCI. Thank you, Mr. Chairman.

And I do want to thank you for the opportunity to testify and also being part of the hearing from this side of the dais, and I do hope to work with my colleagues on the committee to really mark up the remaining provisions of the Stolen Identity Refund Fraud Prevention Act of 2015, which does address some of these issues.

Mr. Commissioner, you said something pretty interesting. You said, "We run the world's most complicated Tax Code," you as the IRS. That is kind of interesting because I think the real answer is we have to simplify the Tax Code, and that probably would be the best way of reducing the overhead that you have, if we could get to that part.

And I do want to applaud you for creating the Security Summit Initiative. I think that is an important part of moving forward.

But I want to ask you about the IP PIN program, and I know Mr. Camus talked about this. I understand the current IP program is available to all taxpayers previously identified by the IRS as victim's identity theft. Actually I have one of those ID numbers right now as well, and participants from the pilot program, which are people living in Florida, Georgia, Washington, D.C., which are areas of high risk of ID theft.

Do you think expanding the program to the taxpayers who request one regardless of states would further crack down on the tax related ID theft, and does the security breach connected to the IP PIN retrieval tool give you pause in doing so?

Mr. KOSKINEN. No, the breach was for people who were trying to retrieve their PIN. Last year we mailed 2.7 million IP PINs out

to the taxpayers, but they lose them. They forget about them, and then they need to get one.

So we had about 135,000 on it. About five percent of people try to access it online. So continuing to mail them out to the address of record we think is a secure method of providing them. The problem we have is when they forget them because they cannot file without them. How do we get them access to those?

What we are going to do is we will bring that back up with the multi-factor authentication, but taxpayers also will be able to go online and have the IP PIN mailed to them. It will just take them five to seven days longer to get it.

But in terms of the PIN itself, one of the reasons is in some ways you kind of move it here and it moves there. One of the reasons that criminals were trying to access the IP PIN was they discovered that the IP PINs were stopping them when they had stolen or bought Social Security numbers from filing successfully.

So their next move was, okay, if I need an IP PIN, I will go get the IP PIN. There is no taxpayer identification involved in that access. It is just a way of being able to file. They already had the necessary fraudulent information to file.

So our goal is to continue providing IP PINs to victims of identity theft and those in the pilot program areas, but we will continue to provide them by mail. For next year the re-authentication will be by mail unless you can work your way through the multi-factor authentication.

Mr. RENACCI. So do you think expanding it to other states would be helpful?

Mr. KOSKINEN. Yes, we have explored that as to what if we just got rid of Social Security numbers as an identifier and gave everybody an IP PIN. There is a substantial cost in that and a burden to taxpayers to try to then keep track of those PINs. We think that ultimately we are better off if we can improve authentication and deal with authorities like the Congress has given us. Get W–2s earlier to be able to match and make sure that we have the right people because IP PINs themselves can get lost, stolen or used, and so they are not by themselves, you know, totally a magical percentage, but we are expanding them, as I say. We sent out 2.7 million this year and continue to expand them.

The pilot program was attest to see how many people would like to have them. A relatively small percentage of people have opted in that direction, but that means that we may be able to offer it to more people because we will not get overwhelmed by it, and it will give some people who want that additional security a better feeling.

Mr. RENACCI. Thank you.

Ms. Lucas-Judy, can you talk a bit about the process of what happens to W–2s once they get to the government, specifically timing between being received by the Social Security Administration and where they are transmitted to the IRS? Because I understand there is a delay there.

And then do you know the difference in timing between when the IRS receives an electronically filed W–2s from the Social Security Administration as compared to paper filed W–2s with the Social Security at the same time?

Mr. KOSKINEN. You are given an additional—I am sorry.

Ms. LUCAS-JUDY. So there is a delay and there has been a delay historically in IRS receiving the W–2 information and being able to use that to match wage data against what is on the tax return before providing a refund, and so that is why we advocated for the deadline to be earlier, and we also had recommended that IRS assess the cost and benefits and figure out how it was going to implement pre-refund matching once it did start receiving the W–2s earlier.

So, you know, we are happy that IRS has implemented that recommendation, and will be able to hopefully take the information that it is getting in the next filing season with earlier W–2s and be able to use that as part of its——

Mr. RENACCI. How significant a delay is the paper W–2? That is the big question.

Ms. LUCAS-JUDY. The paper W–2s come in several weeks later. It can take weeks longer to process those, to receive those and process those as opposed to the electronic filing.

Mr. RENACCI. Is that a month, three weeks, six weeks?

Ms. LUCAS-JUDY. I would have to get back to you on the exact amount.

Mr. RENACCI. Thank you.

I yield back.

Chairman ROSKAM. Mr. Kelly.

Mr. KELLY. Thank you, Chairman.

I thank you all for being here.

Mr. Rangel said something that really made a lot of sense to me, and really everybody that is here today either up here in the dais, we all work for the same people, hard-working American taxpayers, and I think sometimes the exchanges go back and forth like we are actually at odds with each other, and I do not think we are.

But I will say this, and Mr. Koskinen, you are right. A 78,000 page Tax Code is the problem. It is so complicated, and it creates an awful lot of problems for people.

I have also gone through this process like Mr. Lewis where I got phone calls from people saying, "This is the IRS. You have got a problem."

I came home one time after being in session. My wife said, "Please, something is wrong with the IRS."

I said, "Why do you say this?"

She said, "Because they called us."

I said, "That is not the IRS."

She said, "How do you know?"

I said, "They never call. You would have gotten a letter."

But think about this. The culture of fear that comes with the IRS as an agency, I am not saying that is your intention. I am saying that is what people feel.

Why do they respond to these people who call them? Because they are scared to death that they have done something wrong and they are scared to death that the outcomes are going to be poor for them, that somehow they are going to be put through some type of a process that they just do not want to go through.

So we talk to each other about these things all the time, but we never fix them. The problem is the code. When President Clinton

first ran for office he said very simply it is the economy, stupid. Right now it is the Tax Code, stupid.

How long are we going to go on? And every one of you are doing the same thing for the same purposes. We have to have an IRS. We have to have a way to collect revenue, but by the same token, are we going to be at this level of fear that every day hard-working American taxpayers fear a letter or a call from the IRS?

There is nothing that strikes fear in the hearts of the American people more than the IRS getting involved with them. I am not saying it is your fault. I am saying it is a result of where we are.

I look at these things, and, Commissioner, an $11 billion a year budget, that is not a little bit. Eighty-two thousand people.

I come from the private sector, and unfortunately in government the answer to every single problem is to throw more money at it. In the private sector is to get it fixed or you will not be in business anymore, and I think this is where we have this real disconnect. We think that in the government the answer is always to grow it bigger. It has got to expand the number of dollars.

For me in the private sector it is how would I prioritize those dollars to fit the needs that I need, not just putting them where I want to from time to time, but on a priority from the most needed to the least needed to the best service I could provide to make sure my customer base stays intact.

And so when I look at all of you, I mean, you are all doing the same thing.

And, Mr. Camus, thank you. You have given up a quarter of a century to serve this country. That is phenomenal. Ms. Lucas-Judy, thank you for what you are doing, but you are all working for the same process and that is to help hard-working American taxpayers.

Commissioner, I know you are working within a very difficult situation, but the reality of all this is we can have hearing after hearing after hearing. If we do not fix our Tax Code, all this is going to lead to is hearing after hearing after hearing and more suggestions of what we could do to fix it.

So do you all have any suggestion other than—I know what you are dealing with right now is a disease, but what is the cure?

So, Ms. Lucas-Judy, the one thing that could happen today in Congress that would make it easier for the American taxpayers, not easier for their representatives, but for the American taxpayers?

Ms. LUCAS-JUDY. Well, we have recommended that Congress give Treasury the authority to lower the threshold for e-filing of information returns from the current 250 down to five to ten because that would provide information electronically earlier for IRS to do its W–2 matching.

We have also recommended that it require Treasury and IRS to work together on a comprehensive customer service strategy to figure out what kind of services that IRS wants to be able to provide, what is it going to cost, you know, what is the right balance between online and——

Mr. KELLY. I just want to interrupt for a minute because what you are responding to is under the current code with 78,000 pages. That still is the underlying problem, is it not?

This thing is so big and so unmanageable that the average person cannot do it on herself or himself. They just cannot. They are scared to death they are going to make a mistake.

So that is what I keep going back to. Mr. Camus, outside of major tax reform, how could we ever get this system into something that is actually manageable and understandable by the hard-working American taxpayer?

That is who we are leaving out of the equation.

Mr. CAMUS. Mr. Kelly, you are absolutely right, you know, and we all serve America and we are very proud. The 400 men and women and the 836 men and women in my agency are proud to come to work every day to make America better and serve America. That is why we take these issues so seriously.

In our view one of the things that can help would be as we make recommendations to the IRS, that sometimes there could be support or some oversight into making sure that they are implemented. Sometimes that does mean resources or their decisions that are being made. That is maybe a discussion we could have, to make sure that the recommendations that we make when we view something at the IRS and have discussions with the Commissioner and his staff, that we could actually bring those to life.

The GAO recommendations are a good point. We talk about recommendations over and over again, but how do we bring those to life and make sure they actually happen for the American taxpayer?

Mr. KOSKINEN. Well, I totally agree with you that tax simplification is core to the issue. It would make our lives simpler. It would make taxpayers' lives simpler. The code really is a mess. So as I have made it clear, while the policy of tax simplification and Tax Code is the domain of Congress and the White House, anything we can do to be supportive of simplifying the Administration of the Tax Code, which is our responsibility, we are happy to do.

I would note, just to make you feel hopefully a little better, the OECD just published statistics that noted that it cost us 50 percent of what the average cost of collection is around the world. Germany, France, England, Australia, Canada spend twice as much to collect a dollar of revenue as the IRS does.

So we need to be efficient. They are our taxpayer dollars we are spending, and I agree that every problem does not have a monetary solution to it, hence the Security Summit, but on the other hand, there is a point at which as you have more and more work to do, as I have said, and you and I have talked, nobody I know in the private sector says, "I think I will take my revenue arm, my accounts receivable arm," whatever you think it is, "and starve it for funds and just see how it does."

In other words, most of those businesses say, "Wherever I produce the revenue, I want to protect that while I am becoming efficient and trying to run the organization."

Mr. KELLY. It is the only way to survive. You are right. Thank you.

And I yield back.

Chairman ROSKAM. I want to thank our panel and the members for actively participating.

Let me just ask a couple of other questions, but make one point. Just to step back from this whole process for a second, I have got to share with you an interaction that I had last week with a group of visiting parliamentarians from emerging democracies. This is part of an effort of the House Democracy Partnership. It is a relationship the House has with emerging democracies around the world.

And we had a panel and a discussion, and to go back and forth with parliamentarians of other countries that are emerging and really struggling with the voices of authoritarianism within their own countries, and you talk about this process, and if they were to be witnesses here today, this would be a marvel to them, an absolute marvel, that you have got an oversight process. We have got these two co-equal branches of government that are tussling it out and sort of arguing and so forth and presenting different perspectives.

But in the great scheme of things, we have got a lot to be thankful for. I know we have got very serious challenges that we have got to deal with, but you compare what we are dealing with with what is going on around the world, and we have got a lot to be thankful for.

And the disposition and the talent of the members as well as our witnesses today are all part of the solution. So end of sermon, but I think it is an important point to make.

Commissioner, you mentioned the multi-factor authentication process. Let me take you back to a hearing that you did not attend, but we had as a subcommittee. It was last year, I think, and we had invited in the person who is in charge of fighting fraud at Medicare, and we asked a very simple question: what is the fraud and erroneous payments rate?

And he said the number is 12.7 percent, and all of our jaws just dropped.

We had on a similar panel that same day the person who is in charge of fighting fraud at Visa and asked him the same question. What is your fraud rate? And he said it was .06 percent.

So there is this high contrast between what the public sector was doing and what the private sector is doing.

On this multi-factor authentication, this is not new ground. It is out there in the private sector. What is your expectation of when this would be implemented at the IRS? Is this a matter of months in your view? Is this a matter of years in your view?

Can you just give us a sense of scope and scale?

Mr. KOSKINEN. I said some time ago we would have it in the spring, and if you define that broadly, we are running internal tests on it right now. We are having security experts——

Chairman ROSKAM. Okay. I mean, that is reasonable.

Mr. KOSKINEN. Sometime in the next couple of months it will be up.

Chairman ROSKAM. Mr. Camus, do you have an expectation that that is realistic, that what the Commissioner is talking about to have that multi-factor authentication in place in that time frame based on your experience. Do you think that is realistic?

Mr. CAMUS. I think it is a significant challenge, but I know they are dedicated to doing that, and our agents have consulted with

them on things that we have seen in our investigation of the breaches. So we are sharing that information with them, but it is a significant undertaking and a very complex one.

Chairman ROSKAM. Okay. Ms. Lucas-Judy, what is your opinion on whether the Commissioner's time line is realistic?

Ms. LUCAS-JUDY. I agree that it would be complicated. It would probably take a while, and there is a lot for them to consider. We do think it is important that they take a measured approach and consider very carefully the costs, the benefits, the risks of any of the authentication tools before they go forward and implement them.

Chairman ROSKAM. Okay. Let me just shift gears and, Ms. Lucas-Judy, stick with you for a second. The Commissioner mentioned in response to Mr. Rice's inquiry about recommendations from GAO as it relates to the management failure surrounding the targeting issue, and if I understood the Commissioner, he said that they have been implemented, those recommendations.

Is that your understanding? Have those recommendations been fully implemented or are there things that yet have to be implemented? What is your understanding?

Ms. LUCAS-JUDY. I would have to get back with you to be sure. I am pretty certain that the recommendations are still open.

Mr. KOSKINEN. I think the recommendations were from the Inspector General that I testified.

Chairman ROSKAM. Okay.

Mr. KOSKINEN. As well as the Senate Finance Committee.

Chairman ROSKAM. Okay. Then I stand corrected.

Mr. Camus, is that your understanding, that TIGTA's recommendations have been fully implemented on the targeting mismanagement?

Mr. CAMUS. I believe we did a recent audit report that was favorable in that regard, but I can get that audit report reference for you.

Chairman ROSKAM. Okay. Just so that we are clear and thank you for making that clarification.

Ms. Lucas-Judy, could you give us a sense? So we have heard this testimony today about the nature of the changing fraud schemes. It was fairly pedestrian in the past. The fraudsters are moving at the same rate of technology, becoming more and more sophisticated.

In the past it was basically get a name and get a Social Security number and manipulate something.

Do you have a sense of how we should be thinking about fraudsters now that have access to all of the information? So a fraudster based on the data breaches and all of these other areas are not guessing John Lewis, date of birth, you know, what his favorite drink is, Coca-Cola by the way. He is working the hometown product. But they are coming in the front door with all of the information.

Do you have an opinion or recommendation in terms of what we should be thinking about and that changing nature of the way the technology is driving the crime?

Do you follow my question?

Ms. LUCAS-JUDY. I think so.

Chairman ROSKAM. You had a very quizzical look on your face. Go ahead.

Ms. LUCAS-JUDY. We are currently looking at the characteristics of identity theft refund fraud to, you know, try to determine if there are any patterns in terms of, you know, where it is coming from, location, other characteristics, and we are going to be reporting out on that later this year.

But in general, I mean, we have said before that it needs to be a multipronged, multilayered approach to fighting identity theft refund fraud, you know, trying to get at the situation up front, during the processing, and then afterwards following up with leads from partners, and again, you know, analyzing that information, developing metrics to determine how effective the leads program is and sharing information that is actionable with the folks that are providing the leads information so that they can help strengthen their own security posture.

Chairman ROSKAM. Mr. Camus, on the idea of a refund deposit being made to an account, electronically made, it is my understanding that the IRS has changed its policy, and they have limited the amount of deposits that will be made into a single account.

Can you give us a sense of that, you know, what your understanding is of that?

Because I think implicit is the recognition that it would have been ridiculous over a period of time to have hundreds of refunds going to a single account, and the IRS has changed that policy.

Now, my understanding is that they will put three refunds into a single account, but is there still an issue as to where a paper check could go, that it could go to more than one address?

Do you follow me on the nature of this question?

And can you give us some insight for this? Because it is really troubling, and I think like we are in the midst of it, but we are not quite done dealing with it. Can you give us a sense of that?

Mr. CAMUS. Yes, you hit the nail on the head. It is a very complex issue because taxpayers, if you have seen one taxpayer, you have seen one taxpayer. Each taxpayer can have their own set of circumstances.

So the IRS did, in fact, take a look at that issue based on some recommendations, and they agreed that any more than three deposits to a single bank account is questionable even if it is maybe a family member that has the bank account on behalf of all the people.

So limiting those bank accounts, limiting those deposits to a single bank account to three people, their filters have caught about 885,000 questionable returns using that screen.

We also think thought that mailing then subsequent paper checks could cause a problem because who is to say that the criminals have not gone in and changed the address of record? That is one of the concerns that we have when we talk to the Commissioner's staff about all the ways that criminals from all over the world look at this $3.3 trillion that is collected or the 400 billion that gets issued in refunds. That is a very ripe area for criminal enterprise, and they are constantly looking at it and testing it.

So we think the limiting the refunds to three is good. We are looking at that, and we will be writing an audit report on the effects of that.

Chairman ROSKAM. Okay. Commissioner, thank you for your time today, and I have just got sort of just a closing question and just a general inquiry.

So some of the concerns that were either articulated or implied today are no surprise to you. You have heard some of these things in the past. One of the areas that I think is really worthy of exploration is this. The allocation of resources as it relates to technology has from my point of view underperformed, and your head of IT came up, and we had a briefing. I think it was last year. Do not hold my feet to the fire, but you remember when you came up and you brought your team.

And one of the things that he said to me startled me, and we were criticizing, you know, as is sort of our pattern, and he said, "Well,"—and this is as it relates to the IG spending—and he said, "We do not look at it as a failure. We look at it as we have learned what does not work."

Now, that is great if you are Thomas Edison and this is Menlo Park, but that is not what we are dealing with, and I am not trying to be cavalier or flippant. My view is, look, some of this technology has been explored and robust in the private sector, and it has been allocated, and the example I used a couple of minutes ago about the use of Visa's technology as it relates to Medicare, it is deployed. It is successful.

So what is the level of complication that has made it so difficult for the Internal Revenue Service to transition and to be successful on these themes?

And this is in the context of an agency that has been successful in moving through and implementing the Affordable Care Act. And one of the reasons we are not talking about the Affordable Care Act today is because the IRS has been successful largely in implementing a terribly complicated new law and did it pretty well.

So why should the IRS not be held to account? If you can do it with the Affordable Care Act and be successful, what is to say it cannot be done on cybersecurity and these identity theft questions?

That is how it looks to me. Am I misperceiving this? What new information? Because I am not believing that it is just money. I just am not buying it, and if that is sort of what it distills down to, then okay. We are shirts and skins, and I guess that is just the way it is.

I do not think that is it. I think that there is something else going on, and I am interested just in your perspective. What else do you think is going on?

Mr. KOSKINEN. I think the biggest difference is with the Affordable Care Act or when we get tax extenders, it is a fixed target. You know exactly what it is you are going to do. It is complicated. We run an antiquated system, as you know, that we are trying to upgrade.

When you are dealing with identity theft and refund fraud, as you have noted and this hearing has discussed, you are dealing with a moving target that as you push down here and stop it there, it moves and evolves.

That is to say we are now dealing with and part of the reason for the Security Summit is the ways of getting refund fraud information is not just stealing it in the public domain, and it is not trying to access IRS systems. It is, in fact, accessing all private sector systems so that the reason the states are so enthusiastic is they are fighting the same battle, and it changes every year.

So we are moving. It is as if you change the rule of the football game every year, and last year's rules have now been changed, and we have got to play with a different game and a different set of rules, and it will continue to be a moving target.

But I do think that it is important for us to continue to fight that battle. As I say, my goal is for us to get to a point where instead of just reacting and stopping in their latest incarnation, we can begin to anticipate where are they going next? If we have stopped them here, what is the next likely place they will go?

One of the things we are getting with leads from private sector and the states is what are they seeing that is different. What are the patterns that are going on out there that did not happen last year? Last year, you know, there were actually suddenly refund fraud attacks on states, not the Federal Government but on state systems.

This year we are seeing other things. That is why our data elements that we are involved with. We have over 200 filters now that have evolved over time. Those 200 filters five years ago would have stopped everything. They do not stop everything today because, in fact, we are fixing the plane while it flies, but we do not know the direction it is going every year.

Chairman ROSKAM. So just in closing, I think that there is an opportunity here, and you heard it from both sides of the aisle. There is a level of concern and a level of anxiety. From my point of view, the IRS has demonstrated a capacity to deal with some very significant, challenging things.

I will stipulate that the implementation of the Affordable Care Act as you have described it is a fixed target and date certain and so forth.

I think we have a season right now where there is a lot of interest on both sides in trying to drive towards some of these solutions, and I think that we should seize on that opportunity.

But I want to thank each of you for your time today and for the members who have chosen to participate.

The meeting is adjourned.

[Whereupon, at 12:05 p.m., the subcommittee was adjourned.]

[Questions for the record follow:]

Rep. Peter Roskam (IL-6) Question for the Record
Committee on Ways and Means
Oversight Subcommittee
Hearing on Tax Return Filing Season
April 19, 2016

Commissioner Koskinen:

There have been cases where hundreds of refunds are deposited into a single bank account. In response, the IRS has limited the number of direct deposits to a single account to three. But after that the IRS will still mail the checks to the address on file. Is that enough to address the problem?

Internal research suggests that the limit on the number of refunds that may be directly deposited to a single account has had a positive impact on our efforts to deter refund fraud and identity theft. To successfully perpetrate refund fraud, fraudulent filers must have a way to receive the refund payment. When the check is mailed to a physical address instead of direct deposited, it creates an additional challenge for the fraudulent filer. Perpetrators of fraud are exposed to a higher risk of detection and prosecution if they must retrieve refunds from a physical location. In addition, when a paper check based on a fraudulent filing is delivered to a physical address, the check is often received by the real taxpayer and returned to the IRS.

Additionally, there have been schemes where fraudsters obtain Electronic Filing Identification Numbers (EFINs). How many refunds may be sent to a single account if the tax preparer has an EFIN? Could fraudsters potentially use EFINs in order to have more than three deposits sent to one account?

The same direct deposit limit (i.e., no more than three refunds may be sent by direct deposit to a single account) applies to tax preparers using an EFIN. Generally, Treasury's Bureau of Fiscal Service and IRS rules prohibit the deposit of refund checks payable to individual taxpayers to business accounts. IRS rules require a refund check to be in the name of the taxpayer and sent directly to the taxpayer (or an agent if the taxpayer has filed a power of attorney specifically authorizing the agent to receive a paper refund check). Financial institutions are to deposit tax refunds to individuals paid by direct deposit to an account in the name of the taxpayer unless made to a pooled account in limited cases. No exception to these rules exists for tax return preparers. Return preparers cannot receive waivers from these rules from either the government or their customers.

Rep. Erik Paulsen (MN-03) Question for the Record
Committee on Ways and Means
Oversight Subcommittee
Hearing on Tax Return Filing Season
April 19, 2016

Commissioner Koskinen:

I am encouraged by the IRS's efforts to combat identity theft through initiatives such as the Identification Protection Personal Information Number (IP PIN) pilot program.

However, it is unclear whether or not the IRS is involved in similar efforts with other agencies, such as the National Institute of Standards and Technology (NIST) and its National Strategy for Trusted Identities in Cyberspace initiative. It is my understanding that NIST has funded its own pilot program through the initiative to create an opt-in, electronic ID (e-ID) program that uses a common identifier – in this case, a face as it appears on a driver's license – and a feature that allows the IRS to alert the taxpayer through his or her cell phone of tax filings and refunds, as a means of confirming that the taxpayer is aware of those filings or refunds.

Both the IP PIN and e-ID pilot programs are underway in the state of Georgia, but it does not appear as though the IRS and NIST are coordinating their efforts.

Is the IRS working with NIST as you both operate pilot programs with the same goal in the same state?

Additionally, following the November 2015 TIGTA report (https://www.treasury.gov/tigta/auditreports/2016reports/201640007fr.pdf) that found that the IRS is not meeting NIST ID standards, does the IRS intend to explore the NIST e-ID approach?

The IRS extensively engages with the National Institute of Standards and Technology (NIST) on a variety of issues, including soliciting NIST guidance on appropriate application of NIST standards to IRS web authentication. We also continue to explore options for increasing cybersecurity that emerge through the National Strategy for Trusted Identities in Cyberspace (NSTIC) pilots, industry at-large, or pilots pursued by other government agencies.

At this time, the IRS is not part of the e-ID pilot program because of certain limitations of the pilot program. For instance, the IRS IP PIN is a nationwide program whereas the e-ID pilot program is a relatively short-term, geographically limited program. Also, in general, NSTIC pilots are intended to test new technologies or processes and may not be 100% compliant with today's NIST standards.

However, the IRS is adopting the NIST cybersecurity framework to promote the protection of information technology infrastructure as part of the Security Summit effort. Tax industry participants have aligned with IRS and state tax administrations to work to develop strategies for applying the NIST cybersecurity framework to all organizations within the tax industry.

Additionally, the IRS is developing an enterprise identity assurance strategy across taxpayer contact channels to ensure secure access to tax information for taxpayers across all contact mediums (e.g.

online, phone, in person). The Identity Assurance Strategy is planned for completion by early Fall of 2016.

Rep. Sam Johnson (TX-3) Question for the Record
Committee on Ways and Means
Oversight Subcommittee
Hearing on Tax Return Filing Season
April 19, 2016

Commissioner Koskinen:

With respect to PL 114-113 /Division Q/Title III/Sec. 304 (exclusion for wrongfully incarcerated individuals), please provide information with respect to the how the IRS is implementing this section in particular the waiver of limitations.

On February 6, 2016, the IRS updated the Internal Revenue Manual describing internal procedures to implement the new exclusion from gross income under section 139F, including waiver of any provision preventing a claim for credit or refund of any overpayment of tax resulting from application of section 139F if the claim is filed within one year of the date of enactment of section 139F. A wrongfully incarcerated individual, who included in income an award he or she received in a prior year that meets the requirements of the Wrongful Incarceration Exclusion, must file an amended federal income tax return (Form 1040X) for that prior year in order to exclude the award from income and claim a refund. Form 1040X instructions were revised January 2016 to include information addressing wrongfully incarcerated individuals. We are working on a communication strategy which includes a news release and Frequently Asked Questions (FAQs), both of which we expect to release soon.

Also, how is the IRS conducting outreach with respect to the waiver of limitations to ensure that eligible individuals can benefit by the deadline?

The instructions for how to claim a credit for any overpayment of tax resulting from application of section 139F already have been included in the Form 1040X instructions. Additional communications specifically focused on requesting a waiver of limitations on claiming a credit or refund, including Frequently Asked Questions (FAQs) posted to IRS.gov, are expected to be released to the public next month.

[Submission for the record follows:]

Anthony M. Reardon

National President

National Treasury Employees Union

Statement for the Record

For

House Ways and Means Subcommittee on Oversight

Hearing on

"Internal Revenue Service Budget Request for FY 2017 and the 2016 Filing Season"

April 19, 2016

1750 H Street, N.W. • Washington, D.C. 20006 • (202) 572-5500

Chairman Roskam, Ranking Member Lewis and distinguished members of the subcommittee, I would like to thank you for allowing me to provide comments on the IRS budget request for FY 2017. As President of the National Treasury Employees Union (NTEU), I have the honor of representing over 150,000 federal workers in 31 agencies, including the men and women at the IRS.

Mr. Chairman, NTEU strongly supports the Administration's FY 2017 budget request of $12.28 billion for the IRS, an increase of more than $1 billion above the current FY 2016 level. We are particularly pleased the Administration's request would provide the IRS with the additional resources necessary to restore customer service levels that have fallen in recent years due to funding cuts totaling almost $1 billion, and to begin rebuilding its depleted workforce which is down more than 15,000 full-time employees since FY 2010. The IRS has warned that without this additional funding, the IRS will lose another 2,000 to 3,000 full time employees which will further undermine its ability to serve taxpayers and enforce our nation's tax laws.

Taxpayer Services

Providing quality customer service to the taxpayer is an important part of IRS efforts to help the taxpaying public understand its tax obligations while making it easier to comply. Unfortunately, the IRS' ability to provide excellent taxpayer service has been severely challenged due to reduced funding in recent years and the cuts mandated by sequestration. Without additional resources, further degradation in taxpayer services will occur, jeopardizing our voluntary compliance system.

Impact of Funding Reductions on IRS Taxpayer Services

Mr. Chairman, funding reductions in recent years have had a devastating impact on IRS' ability to provide taxpayers, including victims of identity theft, with the service they need in a timely manner. Since FY 2010, the IRS has absorbed $1.2 billion in cuts despite the fact that they are handling more than 10 million additional tax returns a year, and the number and complexity of tax refund fraud cases are on the rise. The funding cuts have resulted in a reduction of about 34 percent in the number of assistors answering telephone calls between fiscal years 2010 and 2015 and contributed to the lowest level of telephone service in fiscal year 2015 compared to recent years. In addition, reduced funding forced the IRS to implement a number of service initiatives during FY 2015 that included reducing or eliminating certain telephone and walk-in services, and redirecting taxpayers toward other service channels such as IRS's website.

In a recent letter to Congress, the IRS highlighted some of the adverse impacts these reductions had on the IRS' ability to deliver taxpayer services during the 2015 filing season. These include:

•A reduction in the percentage of callers seeking live assistance who received it (telephone level of service) to 38 percent,—down from 74 percent in FY 2010.

•Taxpayers waiting about 23 minutes on average for an IRS representative to get on the line, with more than 60 percent of calls going unanswered. This represents a sharp decline from 2010, when the IRS answered three-quarters of calls and had an average wait time of just under 11 minutes.

•The IRS was not able to answer any tax-law questions except "basic" ones during the last filing season and no tax law questions after the filing season, leaving the roughly 15 million taxpayers who filed later in the year unable to get answers to their questions by calling or visiting IRS offices.

•The IRS historically has prepared tax returns for taxpayers who need help, particularly for low income, elderly, and disabled taxpayers. Eleven years ago, it prepared some 476,000 returns. That number declined significantly over the past decade, and last year the IRS announced it will no longer prepare returns at all.

In addition, as a result of budget cuts, the IRS was forced to reduce staff devoted to face-to-face assistance at walk-in sites by about 4 percent in FY 2015 compared to the previous year, and directed customers to self-service options. However, the percentage of customers at walk-in sites waiting for longer than 30 minutes for service increased by 7 percentage points (from about 25 to 32 percent) during the same period.

The importance of providing taxpayers with timely assistance over the phone or in person is of particular importance for victims of identity theft and other types of tax refund fraud. These cases are extremely complex cases to resolve, frequently touching on multiple issues and multiple tax years and the process of resolving these cases can be very frustrating for victims.

While the IRS has made considerable progress in this area, additional work remains. Fighting identity theft is an ongoing battle as identity thieves continue to create new ways of stealing personal information and using it for their gain. Therefore, it is critical that the IRS has the resources and staffing necessary to prevent refund fraud from occurring in the first place, investigate identity theft-related crimes when they do occur and help taxpayers who have been victimized by identity thieves as quickly as possible.

NTEU appreciates the $290 million that congress provided for FY 2016 to help improve the customer service representative level of service rate, among other things. With this additional funding, the IRS was able to hire 1,000 seasonal telephone assistors and project these additional employees will help increase the phone level of service to 65 percent for the current filing season. However, because these hires are only temporary, the IRS has warned the overall level of service will drop back down to 47 percent for FY 2016 when these employees are let go.

That is why NTEU strongly supports the President's request of $2.4 billion in funding for taxpayer services in FY 2017. This funding will allow the IRS to increase the telephone level of service to 70 percent, provide assistance to victims of identity theft in a timely manner, and

help taxpayers understand their obligations, correctly file their returns, and pay taxes due in a timely manner.

Mr. Chairman, it is evident that drastic funding reductions in recent years have seriously eroded the IRS' ability to provide taxpayers with the services they need. Without the additional funding proposed in the Administration's budget request, taxpayers will continue experiencing a degradation of services, including longer wait times to receive assistance over the telephone, increasing correspondence inventories, including letters from victims of identity theft and taxpayers seeking to resolve issues with taxes due or looking to set up payment plans.

Enforcement

Mr. Chairman, NTEU believes a strong enforcement program that respects taxpayer rights, and minimizes taxpayer burden, plays a critical role in IRS' efforts to enhance voluntary compliance, combat the rising incidence of identity theft and reduce the tax gap.

Impact on Efforts to Reduce the Federal Deficit

Unfortunately, funding reductions in recent years are undermining IRS' ability to maximize taxpayer compliance, prevent tax evasion and reduce the deficit. The adverse impact of insufficient funding on IRS' capacity to collect revenue critical to reducing the federal deficit is clear. In FY 2015, on a budget of $10.9 billion, the IRS collected $3.3 trillion, roughly 93 percent of federal government receipts. According to the IRS, every dollar invested in IRS enforcement programs generates roughly $6 in increased revenues, but reduced funding for enforcement programs in recent years has led to a steady decline in enforcement revenue since FY 2007. In FY 2015, IRS enforcement activities brought in $54.2 billion, down $5 billion from the $59.2 billion of FY 2007.

The reduction in revenue can be partly attributed to a reduction in the total number of IRS enforcement personnel, including revenue officers and revenue agents as well as employees in the correspondence audit program. Between FY 2014 and FY 2015, the total number of revenue officers and revenue agents fell nine percent from 15,775 to 14,376, while reduced staffing in the correspondence audit program resulted in roughly 16,000 fewer case closures and potentially $75 million in lost revenue.

Without sufficient staffing to effectively enforce the law to ensure compliance with tax responsibilities and combat fraud, our voluntary tax compliance system is at risk. And as the IRS Commissioner has repeatedly noted, a simple one-percent decline in the compliance rate translates into $30 billion in lost revenue for the government.

Sufficient enforcement staffing is also critical if the IRS is to make further progress on closing the tax gap, which is the amount of tax owed by taxpayers that is not paid on time. According to the IRS, the amount of tax not timely paid is $450 billion, translating to a noncompliance rate of almost 17 percent.

While the tax gap can never be completely eliminated, even an incremental reduction in the amount of unpaid taxes would provide critical resources for the federal government. At a time when Congress is debating painful choices of program cuts and tax increases to address the federal budget deficit, NTEU believes it makes sense to invest in one of the most effective deficit reduction tools: collecting revenue that is owed, but hasn't yet been paid.

That is why NTEU was happy to see the Administration's budget request would provide a total of $5.2 billion to support IRS enforcement activities, an increase of more than $356 million over the current level. The increased funding is designed to protect revenue by identifying fraud, including tax related identity theft, and strengthen examination and collection programs. The increase is also supported by a program integrity cap adjustment totaling $514 million, which includes funding for both the Enforcement ($231 million) and the Operations Support ($283 million) accounts. This additional funding is designed to restore enforcement of current tax laws to acceptable levels, investigate transnational organized crime, pursue abusive tax schemes and enforce the new Foreign Account Tax Compliance Act (FACTA). According to the Administration, the cap adjustment will help generate $46 billion in net savings over the next 10 years. This estimate does not account for the deterrent effect of IRS enforcement programs, estimated to be at least three times larger than the direct revenue impact.

CONCLUSION

Mr. Chairman, thank you for the opportunity to provide NTEU's views on the Administration's FY 2017 budget request for the IRS and the 2016 filing season. NTEU believes that only by restoring critical funding for effective enforcement and taxpayer service programs can the IRS provide America's taxpayers with quality service while maximizing revenue collection that is critical to reducing the federal deficit.

○