

Hearing on 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 114-OS11

Printed for the use of the Committee on Ways and Means

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

C O N T E N T S

[Advisory of April 19, 2016 announcing the hearing](#)

WITNESSES

Timothy Camus

Deputy Inspector General for Investigations and Treasury Inspector General for Tax Administration, U.S.

Department of Treasury

Witness Statement [[PDF](#)]

The Honorable John Koskinen

Commissioner, Internal Revenue Service

Witness Statement [[PDF](#)]

Jessica Lucas-Judy

Acting Director, Strategic Issues, U.S. Government Accountability Office.

Witness Statement [[PDF](#)]

The Honorable James B. Renacci

Member of Congress, Washington D.C.

Witness Statement [[PDF](#)]

Hearing on Tax Return Filing Season

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

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

*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 the 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 Webs 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 by passing 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.

*Chairman Roskam. 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 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 HON. 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 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 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 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 truncated 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.

*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 exceed 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.

*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.

*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, combatting 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 certain 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.

*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 accountable 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 under-funding 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 form 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](#)

[Public Submissions for the Record](#)