SCAM SPOTTING: CAN THE IRS EFFECTIVELY PROTECT SMALL BUSINESS INFORMATION?

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

HEARING HELD
APRIL 6, 2017

Small Business Committee Document Number 115–015
Available via the GPO Website: www.fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE
24–837 WASHINGTON : 2017

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

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUETKEMEYER, Missouri
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
TRENT KELLY, Mississippi
ROD BLUM, Iowa
JAMES COMER, Kentucky
JENNIFFER GONZÁLEZ-COLÓN, Puerto Rico
DON BACON, Nebraska
BRIAN FITZPATRICK, Pennsylvania
ROGER MARSHALL, Kansas
VACANT
NYDIA VELÁZQUEZ, New York, *Ranking Member*
DWIGHT EVANS, Pennsylvania
STEPHANIE MURPHY, Florida
AL LAWSON, JR., Florida
YVETTE CLARK, New York
JUDY CHU, California
ALMA ADAMS, North Carolina
ADRIANO ESPAILLAT, New York
BRAD SCHNEIDER, Illinois
VACANT

KEVIN FITZPATRICK, *Staff Director*
JAN OLIVER, *Deputy Staff Director and Chief Counsel*
ADAM MINEHARDT, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESS

APPENDIX

SCAM SPOTTING: CAN THE IRS EFFECTIVELY PROTECT SMALL BUSINESS INFORMATION?

THURSDAY, APRIL 6, 2017

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 10:00 a.m., in Room 2360, Rayburn House Office Building, Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Radewagen, Kelly, González-Colón, Bacon, Fitzpatrick, Marshall, Velázquez, Murphy, Lawson, Clarke, Espaillat, and Schneider.

Chairman CHABOT. The Committee will come to order.

We have votes we think approximately 15 to 20 minutes from now. So, and the ranking member will be here shortly. We both spoke on the floor and we understand that she will be here in a few minutes. So I am going to go ahead and give my opening statement now.

I cleared it with my colleagues on the other side of the aisle to make sure I took out all my attacks on Nydia in my opening statement because she was not here to defend herself. So, and I am just kidding, obviously, for those who may take that seriously.

So good morning. We thank everyone for being here. A special thanks to our witness, the Honorable J. Russell George, who is taking time away from his busy schedule to be here with us today.

As tax season heats up, so, too, does tax fraud season. In testimony before this Committee last year, IRS Commissioner John Koskinen reported that a cyber breach had exposed taxpayer data from over 700,000 accounts. Commissioner Koskinen also told us that IRS computer systems are under constant attack from would-be hackers to the tune of 1 million attempted cyberattacks per day. A million cyberattacks every single day. Criminals are becoming ever more sophisticated and ruthless in the ways that they can make attacks on identity theft and file fraudulent returns with ill-gotten personal information.

At a minimum, the goal of the IRS must be to make this crime harder, not easier, for identity thieves to commit. Identity theft is growing at a truly alarming rate. According to the most recent figures from the Bureau of Justice Statistics, more than 17.6 million Americans, including 2.6 million seniors, fell victim to this terrible crime in 2014. Seniors are attractive targets for identity thieves because they are more likely to have life savings, own their own home, and have good credit. All of us on this Committee have heard heartbreaking stories from our constituents, especially sen-

iors, who have been victimized by this crime. Identity theft does not just rob its victims of their money and their credit; it robs them of their sense of security and peace of mind.

As we have heard in previous hearings, most recently our series on small business cybersecurity, too often small businesses are targeted for this type of cybercrime because they often lack the resources to protect themselves. It has become clear that the IRS, like all agencies trusted with the American people's most sensitive personal information needs to step up its game. While the IRS may have taken a few limited steps in the right direction, there are countless additional steps that must be taken to ensure taxpayer information is adequately protected. To be clear, this is not an issue of funding at the IRS; it is an issue of priorities at the IRS. If the IRS can pay out big bonuses to its employees, some of whom were implicated in the targeting of Americans for their political views, it should be able to find the money to protect people's data from identity thieves. If the IRS can pay for its employees to travel to new training events and prioritize the enforcement of Obamacare over basic customer service, then there really is no excuse for failing to protect taxpayer information from thieves.

Our witness today is charged with periodically evaluating the IRS's efforts to safeguard taxpayers' personal information, including those of small businesses. It is my hope that he will shed light on the specific systems and procedures currently in place at the IRS and make recommendations for improvement going forward.

I look forward to hearing from our witness, Inspector General George, this morning, and I will yield to the ranking member when she gets here, which we understand will be very soon.

The ranking member is recognized for 5 minutes.

Ms. VELÁZQUEZ. Thank you, Chairman.

It is the first week of April and that means tax day is right around the corner. Over the next few weeks, millions of Americans will be trying to get their taxes filed on time. But this time of year also brings out criminals who target individual taxpayers, business owners, and tax preparers. In recent years, thousands of people have lost millions of dollars and their personal information to tax scams and fake IRS communication. The Association of certified 5 Fraud Examiners found that a typical organization loses an average of 5 percent of revenues each year due to fraud, translating to $3.7 trillion total. And although we typically hear of scams targeting individual taxpayers via phishing emails and phone calls, small businesses are actually more vulnerable. Whether it is a lack of awareness of cybercriminals, small firms and their tax preparers are increasingly becoming the focus of identity theft. Small business owners are already hampered by complying costs and the worry about data security adds an additional layer to that complexity.

Identity theft and the refunds claimed from it has become an increasing problem the IRS is battling to address. In fact, the agency said it rejected 1.8 million fraudulent returns filed in 2014 worth $22.5 billion in refunds. Unfortunately, the IRS also paid out approximately $3.1 billion in fraudulent returns.

Not only must the IRS protect itself from fraud; they are also tasked with alerting taxpayers to popular tax scams. Every year

the IRS releases its "daily dozen," a list of scams from phishing, phone scams, preparer fraud, and employer noncompliance schemes. In addition to publications, the IRS took steps to bring all stakeholders to the table for their Security Summit Initiative, a public-private partnership to amplify security risks and design new and innovative safeguards. The summit has led to a more active role by taxpayers to protecting their personal financial information.

While this is a step in the right direction, more must be done to address the needs of small business taxpayers and their battle against criminals.

Today's hearing will give us the chance to hear from the Treasury Inspector General for Tax Administration about how the IRS is educating, mitigating, and preventing scams for a small business customer. I hope we can take a lesson from the audience performed by TIGTA and develop multi-tiered approaches to combat identity theft and other scams harming our nation's small businesses.

With that, I welcome the gentleman for taking time to share his insights and help us seek solutions to this issue. Thank you.

Mr. Chairman, I yield back.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

It is a close call, but I am inclined since we have got a fair number of members here to let you testify now. If members have to leave to vote, you know, the first vote is open longer.

So, and I am going to forgo the explanation of your distinguished background. The gentleman before us today, of course, is Inspector General for Tax Administration, and you are recognized for 5 minutes, sir.

STATEMENT OF THE HONORABLE J. RUSSELL GEORGE, INSPECTOR GENERAL, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Mr. GEORGE. Thank you, Chairman Chabot, Ranking Member Velázquez, members of the Committee. Thank you for the opportunity to testify on scams and their impact on individuals and the business taxpayers.

Can the IRS protect taxpayer information? That is the primary premise of this hearing. Our ongoing work shows that the IRS is making progress. However, tax scams are constantly evolving, which will require the IRS to continually adapt its detection and prevention processes.

Since May 2012, my office has issued a number of reports that address the IRS's efforts to detect and prevent the filing of fraudulent individual and business tax returns by identity thieves, as well as the IRS's efforts to assist victims.

Identity theft refund fraud occurs when an individual uses another person's or our businesses name and taxpayer identification number to file a fraudulent tax return for the purpose of receiving a tax refund. For example, identity thieves file fraudulent business tax returns using the employee identification numbers of active or inactive businesses. Most recently, we reported in February 2017, that IRS efforts are resulting in improved detection of identity theft of individual tax returns before fraudulent tax refunds are released. Beginning with the 2017 filing season, the IRS now has

more timely access to third-party income and withholding information to compare against tax returns while processing these returns. Previously, the IRS did not have this information early enough in the filing season which had prevented it from making substantial improvements in its fraud detection efforts. Access to this information at the beginning of the filing season is the single most important tool to detect and prevent tax fraud related identity theft.

As I stated earlier, the IRS recognizes that new identity theft patterns are constantly evolving. As such, the IRS needs to continually adapt its fraud prevention processes. In September 2015, we reported that the IRS recognized a growing threat of business-related identity theft, and in response was implementing the processes to detect identity theft on business returns. However, TIGTA found that the IRS is not using data that it has readily available to proactively identify business identity theft. In response to TIGTA's recommendations, the IRS is expanding its detection filters to identify business identity theft. For the 2017 filing season, the IRS is using 25 filters to identify potentially fraudulent business tax returns and prevent the issue of fraudulent tax refunds.

Individuals can also be victims of employment-related identity theft which occurs when a taxpayer's stolen identity is used to gain employment. This can cause a significant burden due to the incorrect computation of taxes and Social Security benefits based on income that does not belong to the taxpayer. In August 2016, we reported that during the period February 2011 to December 2015, the IRS identified almost 1.1 million taxpayers who were victims of employment-related identity theft, but were not notified. In January 2017, the IRS began notifying victims. In addition, our ongoing audit found that the IRS's processes are not sufficient to identify all employment-related identity theft victims.

Finally, TIGTA has reported that the IRS is not effectively providing assistance to taxpayers who report that they have been victims of identity theft, resulting in an increased burden for those victims. In July 2015, the IRS created a centralized unit to combine the skills of employees working identity theft cases and multiple functions into one directorate. This has resulted in improvements in case closure timeframes and a reduction in case closing errors. To help protect identity theft victims and improve authentication, the IRS began using unique identification numbers for victims in fiscal year 2011. This number helps the IRS verify a victim's identity when their tax return is filed so that the processing of the return and the refund is not delayed. However, TIGTA has identified that victims of identity theft tax accounts were not always consistently updated to ensure that these identification numbers were generated as required.

Identity theft imposes significant financial and emotional hardship on individuals and businesses.

Chairman CHABOT. Excuse me, General, I am going to ask if you would suspend at this time. I think what we should do is go over and vote and then we will let you continue when we come back.

Mr. GEORGE. Mr. Chairman, that is fine. I am effectively done, so.

Chairman CHABOT. Okay. We will be back. We have two votes. Since this vote is almost through we should be back, I am guessing, in 20 minutes or so, 25 minutes at the most, I think.

Mr. GEORGE. Very good, sir.

Chairman CHABOT. So we are in recess until we come back after votes.

[Recess]

Chairman CHABOT. I note for the record that the ranking member did beat me back here today.

We will go ahead and continue. And General, if you had any concluding remarks there, or you could take up where you left off if you would like?

Mr. GEORGE. I have one additional paragraph, Mr. Chairman.

Chairman CHABOT. Okay.

Mr. GEORGE. And so suffice it to say, identify theft often imposes significant financial and emotional hardships on individuals and businesses. We at TIGTA remain concerned about these attempts to defraud taxpayers through identity theft and other scams. We will continue to review the IRS's efforts to prevent tax-related identity theft and investigate any instances of attempts to corrupt or otherwise interfere with the Nation's system of tax administration. Thank you.

Chairman CHABOT. Thank you very much. And now members will have 5 minutes. I am not sure how many members we will have actually come back because once votes are over for the week we tend to scurry to all parts of this great Nation.

Ms. VELAZQUEZ. And a storm.

Chairman CHABOT. Yeah, and there is a storm going on.

Mr. GEORGE. That is true, too.

Chairman CHABOT. So, you know, planes, and I think people are heading for the airport, including myself and the ranking member probably in the near future.

So I will recognize myself for 5 minutes.

First of all, you mentioned the State Suspicious Filer Exchange Initiative in both your September 2015 and February 2017 reports. How many States are now participating? And has this program been expanded to business filers as you recommended back in 2015?

Mr. GEORGE. As of January 1st, 43 States now participate in the program. IRS now includes business tax filings in the information shared with State tax agencies. Again, of the 43 States that participate, 33 have elected to receive confirmed business identity theft/fraud information from the Internal Revenue Service.

Chairman CHABOT. Thank you. In your testimony, you noted that the Consolidated Appropriations Act of 2014 requires the IRS to issue a notice to an employer requesting an address change to make employers aware in case the request was unauthorized. What process did the IRS use prior to that time to confirm that an address change request was authorized, if any?

Mr. GEORGE. Sir, it was surreal. First of all, we are not aware of any prior processes, formal processes that the IRS used prior, or at least proactively to confirm address changes, but the perverse part of all of this, sir, was that in many respects, the IRS was communicating with people who were, in effect, identity thieves. So if

someone used a legitimate taxpayer's address or name and taxpayer identification number and then used an address for themselves, in effect, a fake address, the IRS could communicate with the fraudster, the criminal. And the legitimate taxpayer was left in the dark.

Chairman CHABOT. Thank you very much.

With regard to the telephone impersonation scam, you mentioned the advise-and-disrupt strategy that you are using to flood reported telephone numbers with automated calls. However, you also noted that these scammers often generate a fake number for the caller ID. How effective is this program if most of the phone numbers the intended victims see are not the numbers from which the calls originate? And has this strategy ever resulted in calling some innocent person's phone line over and over again?

Mr. GEORGE. Yeah, this has been one of the biggest challenges to the IRS in this modern age, sir. A lot of the crooks are using VoiceOver internet protocols which allow them to fake ID caller ID information on people's telephone numbers. We have been effective in a number of ways in terms of addressing this.

One, we have put out the word, and that is something that I wanted to ask all members of this Committee and every member of Congress if they could help us in terms of your communications with your constituents, please put out the word about this. Knowledge is the most powerful, I think, tool that anyone can have in terms of addressing this overall issue so that people—my late mother used to, because this first occurred while she was still alive, she would say to me, "Russell, I got this call. I hung up on them." And she was so proud of that. I mean, she was emphatic about, "I hung up on them." And I said, "Mom, that is the right thing to do."

But what we have done, two things. We have established on the web a listing of telephone numbers that we are aware of where many of these calls are emanating from so that a taxpayer or someone who suspects that they were approached by criminals can input the telephone number and see that, yes, we have identified this as a false number. Two, we have called back a lot of these numbers and in effect said to the people who answered, "Hey, we are aware of what you are doing. Cease and desist." And three, we have also attempted to work with some of the telecommunications companies to help put these numbers out of service.

Chairman CHABOT. Thank you very much. My time is almost expired so rather than go into it and go over, I am going to go ahead at this time and recognize the ranking member for 5 minutes to ask questions.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Many small business taxpayers are not aware of identity theft until it is too late. What would you suggest is the best way for the IRS to reach out to businesses to educate them on identity theft and how to protect themselves?

Mr. GEORGE. Great question, Ranking Member Velázquez.

One, the IRS has taken efforts. They recently convened a group of private sector organizations to help, one, inform them of the problem, and two, to enlist their assistance in both becoming aware of the problem further, but to help educate once again those who are potentially the victims.

Ms. VELÁZQUEZ. Okay. So do you believe that the Small Business Administration has a role to play assisting the IRS? And are you aware if such collaboration exists?

Mr. GEORGE. You know, that is outside of my area of expertise, but yes, my thinking is and my recommendation is that the Small Business Administration should play an active role in this.

Ms. VELAZQUEZ. In fiscal year 2016, Congress appropriated an additional $290 million to the IRS for key areas that directly support taxpayers, including increasing telephone Level of Service, cybersecurity activities, and identity theft prevention and refund fraud mitigation activities. Do you believe this additional increase was sufficient for the IRS to carry out its duty to protect small businesses?

Mr. GEORGE. It was of assistance, yes. Now, the vast majority of that additional funding was used to increase the level of service that the Internal Revenue Service provides to taxpayers by way of its toll-free telephone number, which is extraordinarily important, especially during the tax filing season. But at the same time, if given additional resources, the IRS is able to do additional work.

Ms. VELÁZQUEZ. Thank you. We often hear about tax scams during this time of the year, but what we do not realize is that small businesses are considered good targets by the scam artists. In order to be adequately prepared, what is the best practice for a small business owner when they encounter such a scheme?

Mr. GEORGE. To, one, again, knowledge is power. You have heard that in various areas of your lives, but it is so true in this regard. Two, I mean, use common sense. I mean, just as you as an individual hopefully check your bank statements, businesses need to do so, also. Three, you cannot rely on the CFO necessarily alone, especially if you outsource. You have to be actively engaged here. And four, in all candor, I mean, there is too much reliance on assuming that electronic systems of accounting for your work will watch out for you and be in your best interest. You know, you have to be proactive. You have to ensure that you take the steps necessary to ensure that you safeguard your business and your employees.

Ms. VELÁZQUEZ. Okay, thank you. In your written testimony you indicate that the IRS uses 197 identity filters for individual returns and 25 filters for business tax returns, and these are used to identify potential fraudulent tax returns. I know business tax returns are different, but do you think 25 filters is enough for a business tax return?

Mr. GEORGE. You know, I hesitate, Ms. Velázquez, to elaborate too much on the number of filters and how the IRS is going about doing this only because I do not want to give a roadmap to the perpetrators of this.

Ms. VELÁZQUEZ. Sure. Okay.

Mr. GEORGE. The bottom line is the IRS, and I give them a lot of credit, they are being proactive in this regard to help produce processes to identify this area. In addition, it is important that we note, and I am not just wanting to give credit to my auditors and my investigators, you know, the IRS really did not have a great grasp of the magnitude of the problem. First of all, we brought it to their attention, and they did work on their own, also, I am not

taking anything away from them, of the individual tax fraud problems. And then we followed up with the business tax-related problems, fraud-related problems. So they really did not have their arms around this. We have outstanding work that we are doing that we hope to complete in the not too distant future which will assist them further in this regard.

Ms. VELAZQUEZ. Thank you.

Chairman CHABOT. Thank you.

Ms. VELAZQUEZ. I yield back.

Chairman CHABOT. Thank you. The gentlelady yields back. Her time is expired.

And the gentleman from Kansas is recognized for 5 minutes.

Mr. MARSHALL. Mr. Chairman, can you get back to me in 30 seconds, after the next person?

Chairman CHABOT. I would be happy to do that. We are going to go into a second round at this point, so I will go to myself if that is okay and give you a little time there.

General, the report you released earlier this week contained some very disturbing findings, particularly for small businesses. You mentioned that in October 2014, IRS Criminal Investigations, CI, instituted a policy that it would no longer pursue seizure and forfeiture of funds from legal sources that merely appeared to have been structured. However, you found that most of the seizures for structuring involved legally obtained funds while the intent of the statute is to pursue illegal activity. This is really important for small businesses because, based on their size, they are likely to make bank deposits in frequent intervals of less than $10,000. If CI is not following its own policy in this regard, what do you recommend to ensure that innocent small business owners are not unfairly targeted?

Mr. GEORGE. Thank you for that question, Mr. Chairman. This is the first time I have had a chance to speak publicly about this extraordinarily troubling situation. We discovered over 91 percent of the seizures were of a legal source of income. And again, just for the benefit of those who may not be familiar with the overall issue, there is a Federal statute that requires financial institutions to report transactions in excess of $10,000 to the appropriate government agency.

And what the Internal Revenue Service was doing in the meanwhile is a lot of bad people would structure, meaning transfer $7,000 and then $3,000, which if they had done the $10,000 transfer would have spurred the reporting requirement. But by breaking it up, otherwise saying structuring, they were able to avoid that. And so the IRS Criminal Investigation Division had a system established so that they spotted these unusual tactics.

Now, in an ideal world, perfect if it were to work that way because, in all candor, a lot of people who engage in illegal behavior do try to avoid the reporting requirement by doing that. But again, our report showed that of the vast majority of the people who were being caught up by the IRS's Criminal Investigations Division processes were not engaged in criminal behavior, and the most troubling aspect of this is they were having a very difficult time either getting their money back because the IRS was allowed to seize that money, to forfeit it. So then the burden of proof was shifted to the

innocent taxpayer, and in many instances that money was never returned to the innocent taxpayer. So the IRS has now stopped that practice. We hope through this report, and again, the actions of members of Congress, people will, one, seek to get their money back and, two, that the IRS never again engages in this type of behavior. This is very troubling, sir.

Chairman CHABOT. Thank you very much. I am glad you had the opportunity to clear that up because it is really unfair to a lot of small businesses that have been caught up in that.

In the short time I have remaining, let me ask you this. I had an opportunity during votes to talk with my Democratic colleague from Illinois, Brad Schneider, and he had a suggestion which I would like to raise at this point if I can. He said he is all the time getting notices that somebody has logged in under your name at such and such, and it is him, and I have had this happen to me. I am sure a lot of the folks in this room have as well. So in this area about somebody else filing a tax return and it is not you, and by the time you file yours you find out somebody else already fraudulently did that and got a return and then maybe you can get it cleared up. You ultimately get your money, but it is going to be slower and it is a hassle to go through this. Why not when a taxpayer files his or her return, why not have the IRS immediately send back a notice to them saying, hey, thanks, we just got your return? Because then you know that it happened. What about that?

Mr. GEORGE. Well, in theory that does occur, especially if you use some of those tax preparation software where literally they say to you the moment you file your return, check back within 24 hours to confirm that the IRS received your return and that everything is fine. So what was extraordinarily troubling, Mr. Chairman, is when the IRS would say, you know, our advice to you is to file early so that you beat the bad guy before he or she files a return in your name. So, but in terms of paper returns that was not the case in terms of paper returns. That, what you are suggesting, was not happening, and I do not believe it is happening.

Chairman CHABOT. I thought Mr. Schneider had a great idea so I am going to ask probably staff on both sides to maybe look into this and see if there is not some way we can put this into effect, maybe save a lot of people a lot of heartache.

My time is expired, so we will now recognize the gentlelady from Florida, Ms. Murphy, who is the Subcommittee ranking member on Contracting and Workforce, for 5 minutes.

Ms. MURPHY. Great. Thank you so much for being here and for your testimony.

Mr. GEORGE. Good morning.

Ms. MURPHY. Efiling has become more prevalent, but so has identity theft and refund fraud which we talked a little bit about here. TIGTA has been actively involved in working with the IRS to find solutions to combat this fraud. In your opinion, is the IRS doing enough with the stakeholder community to prevent that identity theft?

Mr. GEORGE. They are doing, candidly, as much as they can given the resources that they have. Over the last few years, as you may be aware, the IRS's budget has been cut dramatically and their responsibilities have been increased dramatically given the

ACA and the role that they have to play with that. Could they do more? Yes, but it is almost—I am trying to think of a right metaphor here, but the bottom line is if they do more in this area, they have to do less in this area.

Ms. MURPHY. So you are saying that they do not really prioritize protection against identity theft against the other responsibilities that they have?

Mr. GEORGE. Well, during the filing season their goal is, to the extent that they can, is to ensure that taxpayers who either reach them by phone, which again is an issue because of reduced resources, or who go to Taxpayer Assistance Centers, or have the ability to get questions answered. And yet, until they—and again, during my opening statement I made reference to a new directorate that the IRS created which is dedicated to helping victims of tax-fraud related identity.

Prior to that they used to have those same individuals who would normally handle those types of cases, one, answer the telephone for people who had basic tax questions and, two, those types of cases were assigned to random IRS officials. There was no dedicated person for the taxpayer to reach out to as you may find in the private sector where if you have a problem with a credit card, it is Ms. Jones or Mr. Jones whose extension is given to you and that is the person you would reach out to. So that is changing for the better, but again, the bottom line is more resources would help the IRS in this area.

And as I pointed out earlier, the tax cheaters, they are a very, you know, flexible sort. They change their means. They are located across the globe. This is truly a challenge for not only the IRS, but in this obvious instance we are referring to them.

Ms. MURPHY. And then to just dig into the part that you talked a little bit about, trying to streamline a bit of the processing of the fraudulent cases, you know, for small businesses it is really critical for them to have timely processing of their refunds, and they operate on such slim margins. What else do you think TIGTA can do to ensure that small firms are not hindered by the fraud prevention efforts?

Mr. GEORGE. Information. Getting the word out. Again, I mentioned that earlier. It is so important, and this is a group effort. At TIGTA, we have done it through television interviews and media releases. I do not know if you have this at your local pharmacy, but I saw at my pharmacy where the inspector general of the Department of Health and Human Services says—there was a sticker from him that said if you encounter fraud, if something suspicious is occurring, you know, call us. We have done the same at TIGTA now, and it is effective in that we get the word out. If you suspect someone is cheating you because of a telephone impersonation scam or any other type of criminal wrongdoing, call us at our 800 number, email us, and that is how we get a lot of the leads that we pursue.

Ms. MURPHY. Great. Thank you very much. And I will yield back the remainder of my time.

Chairman CHABOT. Thank you. The gentlelady yields back.

The gentleman from Kansas, Dr. Marshall, is recognized for 5 minutes.

Mr. MARSHALL. Thank you, Mr. Chairman.

I guess my first question has to do with cybersecurity in the sense of, in this case, identity theft. I think it is probably the same bucket of problems. I go to the Science and Space Technology Committee meeting and we talk about healthcare records being attacked, and I am sure if I was on a military committee we would be talking about it. What type of communications are we doing between the different agencies to work with each other? Is there one particular group of people that is really, really studying this problem hard and fast and trying to disseminate that information to let you do your job better, I guess?

Mr. GEORGE. You know, that is a very good question, Dr. Marshall. The problem that the IRS encounters is the Tax Code. Title 26, Section 6103 of the United States Code places severe restrictions on the type of information that the IRS can share with anyone, and these include criminal penalties. So literally, I cannot tell you about a particular constituent's tax information without—my lawyer is here—without risking prosecution. So being specific regarding that in terms of an individual's case, I mean, a taxpayer can sign a waiver to allow you as the congressman or representative or someone, a lawyer or an accountant, to represent them on their behalf. At last, there are efforts, government-wide, obviously, to look at cybersecurity threats. And in a couple of instances, again, as it related to the Affordable Care Act, where we and HHS-OIG were able to work together because of the overlapping role that we both played in that area.

Mr. MARSHALL. Yeah, and it seems like the privacy issues are backfiring. People give oversight to commodities. When one commodity system gets hacked, they are not allowed to share with their brethren that there has been a hack and prevent the next person. I do not have a solution, but at least I am trying to recognize the problem.

I think I am going to change the direction a little bit. If, indeed, we could get the majority of taxpayers to be able to file their income tax on a postcard, how would that help free up your life or make your life better or worse?

Mr. GEORGE. Candidly, I think you would have some of these scammers produce postcards or addresses and say send that information or that remittance or what have you to this address versus the official. It would help the taxpayer in terms of complying. That has been my position ever since holding this job, sir. Make the ability to comply with the tax burden as simple as possible and most likely you are going to get an increase in tax compliance and revenue owed to the U.S.

Now, technically, that is a tax policy question, and ever since the Reagan administration, sir, the Secretary of the Treasury has indicated that it is the assistant to the secretary for Tax Policy who speaks on it. But given the way you phrase it, I feel comfortable with the answer that I gave.

Mr. MARSHALL. Are you given a chance to make suggestions how to make it simpler?

Mr. GEORGE. That is tax policy, so. The short answer, though, is yes, if we say—and this was the case with the First-Time Homebuyers credit that you may recall from the Reinvestment Act, the

forms were such that people were able to bypass some legal requirements that they would otherwise be required to comply with. So when we identified the problems with the forms—and these were basic issues like how much money is a property worth, something along those lines, which ultimately affects how much money they would have to pay back every year—we were able to make the suggestion which the IRS did adopt, which made it more efficient.

Mr. MARSHALL. Okay. I will try to slip in one last question here. My constituents talk about wanting a kinder, gentler IRS, and I think of the fire marshal who comes by and he gives us a list of things to fix and if we get it fixed within 30 days we are okay. Do you feel like in the past several years you are kind of going in that direction? Is there more room to grow, or what are you doing from that standpoint?

Mr. GEORGE. Yes, I think there is. And again, and I did not bring, I normally keep it in my pocket, but third-party information. If a taxpayer knows that the money that he or she is being taxed on is reported by a third party, the compliance rate, meaning the amount of money in taxes that they pay, is in the upper 90 percent. And I am just going to cut to the other end. The same statistics, and they are somewhat dated, but the bottom line is people who engaged in all-cash transactions, the tax compliance rate was near 20 percent, you know, 20, 30 percent. So having third-party information, and thanks to Congress recently passing a law that requires the IRS to receive information prior to processing tax returns, that is extraordinarily helpful in terms of compliance.

Chairman CHABOT. The gentleman's time is expired.

Mr. MARSHALL. Thank you. I yield.

Chairman CHABOT. Thank you.

The gentleman from Florida, Mr. Lawson, who is the ranking member of the Subcommittee on Health and Technology, is recognized for 5 minutes.

Mr. LAWSON. Thank you very much, Mr. Chairman. And welcome to the Committee.

Mr. GEORGE. Good morning, sir.

Mr. LAWSON. For several years the IRS has been criticized for lack of efficiency. Can you speak to the budget issue that would probably make the IRS operate more efficient? I do not know whether you can speak to that issue or not, but early on I just heard you say cuts in the budget caused some restraints on what you could do.

Mr. GEORGE. You are correct on both accounts, sir. I am not in a position, because the President's budget has not been formally released, to address the impact of whatever the current administration is going to ultimately propose for the IRS formally. But the bottom line is with additional resources, the IRS could do more, there is no question. And again, many of the reports that my office has issued during my tenure did in the past show a waste on the part of the IRS with conferences and with videos and the like, and bonuses to people, which were not a good use of the taxpayers money.

But at the same time, for the most part, the IRS is really down. They used to be at least 100,000, an equivalent, you know, the FTE number of employees that they had, and they are now in the

80,000 range. Now, they have been able to automate a lot of things, and they have collected a record amount of tax revenue over the last few years, but in terms of the amount of customer service, in terms of the amount of time someone has to wait to speak to an IRS employee over the telephone, those numbers have also increased in a way that I think is unacceptable. But otherwise, I am going to have to stop there in terms of the impact of the current budget because we do not have the formal number.

Mr. LAWSON. Okay. I understand.

I hear commercials on the radio all the time, if your debt exceeds $10,000, give us a call and we will get the IRS, put them in place, and reduce this down. And people pay money to do that. How does that work? I mean, do they have a special inside track with the IRS than the average person that are running these commercials?

Mr. GEORGE. You know, sir, you really touched on something that is important, but, you know, I have got to be careful here because it also touches on tax policy, but also with Dr. Marshall, if you make it as easy as possible for people to comply with their tax obligations, they are going to do so. And there is an interesting statistic, but I want to get right to your point. That commercial is advertising a service that an individual could do by him or herself. So you can reach out. It is Offer in Compromise. You could call the IRS and do it yourself. However, as like a lawyer, sometimes it is better to have an expert who has experience to do it for you, whether it is for time reasons or just out of convenience.

So yes, I have seen that. I do not know how much they charge. I have not had a need to take advantage of that, fortunately, but the bottom line is, again, it is a matter of convenience. And there are some people who are in dire straits, but there is no question the IRS is willing to work with taxpayers. And so it is not criminal. It is not criminal for these businesses to engage in this, but, again, too many taxpayers do not realize they do not need to do that. They can do it themselves.

Mr. LAWSON. Another quick question I am going to try to get in. When people have gone delinquent for maybe 3 years and the interest rates that you all charge, do you all work with them on reducing the interest rate so that you all can get the amount of money that you need from the tax return?

Mr. GEORGE. No, that is the IRS. Just to make sure we are clear. The inspector general, we are separate. We are not part of the IRS. We are part of the Department of the Treasury overseeing the IRS.

Mr. LAWSON. Okay.

Mr. GEORGE. And so I am not very familiar with the amount of interest that they charge, but I do know, in all candor, the IRS is flexible as it relates to any past due debt. They would rather that people who owe money pay money than someone not pay it. And you are right, many times the interest can exceed the initial amount owed.

Chairman CHABOT. The gentleman's time——

Mr. LAWSON. I yield back, Mr. Chairman.

Chairman CHABOT. Thank you. The gentleman's time is expired. And I would compliment the gentleman on an excellent question on the $10,000. I have heard those ads many times. I sort of

wondered the same thing. Fortunately, as the general, I have not been in that position so I have not needed those services, but I thought about that. And I would assume that the $10,000 they are saying is because the company, they say if your debt is more than $10,000, because they do not want to mess around with folks that are below that so they are trying to make more money by hitting folks that have bigger debts. Would that be—there is no magic in $10,000?

Mr. GEORGE. There is no magic in $10,000, and again, I am guessing here, but I am almost certain that it depends on the amount of money that you owe and the amount of money that you ultimately pay will figure into their fee.

Chairman CHABOT. The IRS does negotiate with people on occasion if they think they are in tough financial straits and are not going to be able to pay and they are trying to work with them. Is that correct?

Mr. GEORGE. That is my understanding.

Chairman CHABOT. So if you ever want to use services, perhaps they do so much of it they sort of know how to, for lack of a better term, work the system, and maybe that benefits the person, and then again, maybe it does not.

Mr. GEORGE. That is my understanding, sir.

Chairman CHABOT. Okay, thank you. Excellent question.

Chairman CHABOT. The gentlelady from American Samoa, Mrs. Radewagen, who is the chairman of the Subcommittee on Health and Technology, is recognized for 5 minutes.

Mrs. RADEWAGEN. Thank you, Chairman Chabot, and Ranking Member Velázquez. Inspector General George, welcome. Thank you for testifying today.

American Samoa, like the other States, files taxes with the IRS. What resources do you believe that the U.S. Department of Treasury and the IRS can provide to U.S. territorial governments to protect the identities and information of their residents?

Mr. GEORGE. That crosses, you know, not only the territories, but every State and the District of Columbia. It has to make sure that the American people have the confidence that the information that they provide to the IRS is safeguarded. If people lose confidence that the information they provide is not going to be cared for, it could undermine the overall system of our Nation's tax administration system and that could be problematic.

This is not a direct response to your question, but this is something that I was averring to earlier when I was responding to an earlier question. A study done by the IRS Tax Oversight Board showed that most people would say, literally, again, almost approaching 100 percent, that they should pay the taxes that they owe when the question was posed to them. But when the question was varied slightly and they said, well, your neighbor down the block only pays 50 percent of what she owes, then they say, well—then what should your requirement be? And the number grows from near 100 percent closer to 50 or 60 percent. So when people know that everyone is paying what they owe and that the IRS is doing what it needs to do, they have confidence. They will comply. Again, it also goes to a simplicity of complying.

Mrs. RADEWAGEN. Thank you. Mr. Chairman, I yield back the balance of my time.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

The gentleman from Nebraska, Mr. Bacon, is recognized for 5 minutes.

Mr. BACON. I want to thank the inspector general for being here. As a 30-year Air Force veteran, I know the importance of the inspector general. And I would like to also say I have been a victim of credit card and fake identity, or a combination thereof, three different times. One time while deployed to the Middle East, a guy took my identity. He was living in a five-star hotel. My wife caught him and had to fight really hard to get him arrested and held accountable.

But I think Americans are tired of this because so many of us have been victims. I would like to ask you, how does the IRS work with law enforcement when they finally catch someone scamming?

Mr. GEORGE. Great question. Again, there are hoops that have to be jumped through. Again, I made mention of Title 26 of the United States Code, it is Section 6103, places severe restrictions on the type of information that the IRS can proactively share.

Mr. BACON. With law enforcement?

Mr. GEORGE. Even to law enforcement. But the individual can give the IRS license to release information, and that is normally how it is pursued. That is my understanding at least.

Mr. BACON. Can we pass a bill of some type or legislate, making it easier to hold these people accountable?

Mr. GEORGE. You know, I do not think it is a question of legislation in this instance, Congressman. I really do not. One, you do have to have a victim who is willing to cooperate with law enforcement, as most victims are unless they are engaged in somewhat——

Mr. BACON. Or you have some who have been dead for a while and they are using a deceased person. So it is hard to get their permission.

Mr. GEORGE. Well, again, you know, obviously, I would argue an estate, you know——

Mr. BACON. Right.

Mr. GEORGE.—or someone would on their behalf. So, but there is no question it is knowledge, sir.

Mr. BACON. Right.

Mr. GEORGE. And that is part of the problem. A lot of people, especially seniors, obviously deceased individuals, may not have an estate which is large enough to have an executor or someone or administrator or someone who is being proactive in that regard.

Mr. BACON. Right.

Mr. GEORGE. So this is an area, sir, where can you eliminate all types of crime?

Mr. BACON. No, but I would like to put a lot more of them in jail.

Mr. GEORGE. I am with you 100 percent, sir.

Mr. BACON. So I would love to work with—or us with you and as a team to figure out how do we put our brains together because I think this is way too rampant. People are getting off scot-free,

and I think if we put an effort on this—I believe in deterrence. Throw more people in jail, maybe less people will do it.

Maybe a parallel question. How do you tackle this when it is an overseas scam, say from Nigeria or wherever it may be?

Mr. GEORGE. Another great question. I am extraordinarily proud to give my colleagues, especially on the investigative side of my house at TIGTA, a pat on the back. We recently, working with the Department of Justice and a few others, announced the indictment of a number of firms in India, and these were firms—the irony is a lot of those call firms that are legitimate, if you call Xerox—not Xerox, but you know, one of these telephone or computer companies and you are transferred, you do not where they are; many of them are located in India. These small call centers where in the morning or night, depending on the time of day, you had a segment who were answering legitimate questions from consumers, and then we found that there was a small division over there who were engaged in these telephone scam things. I am calling from the IRS. You owe $10,000. You need to pay immediately. You need to use an iTunes card. You need to stay on the phone and do this while I am talking to you. And you would be surprised, sir, how many people fall prey to that, especially senior citizens and the like. So, by working with the Indian Government, as well as, obviously, Interpol and other law enforcement agencies, we were able to obtain indictments. And unfortunately, those indictments were here in the U.S., so while there were a number of people who were domestic who we were able to arrest, more were overseas, and unless they come into the United States—it is not just India, too, just to be clear. There are many other countries.

Mr. BACON. I really think your favorable status as an IRS would go way up if you start showing some convictions on people scamming and doing fake IDs and taking advantage of the taxpayers.

A related question or something that you were talking about and you may not be able to speak to it here, I realize when you have your funding cut it is very hard to do everything that you want to do and that is just a fact of life. And part of that was because of the targeting of the conservative and religious groups. Are there any investigations within the IG that are still working in that realm?

Mr. GEORGE. The short answer is yes, and we will be releasing shortly, in effect, a follow-up report to that initial. But I have to once again, Congressman, make it clear, I am not part of the IRS.

Mr. BACON. Okay. Part of the inspector general.

Mr. GEORGE. I am part of the Treasury. So, and we are the ones who identified that problem back in 2013.

Mr. BACON. Thank you.

Mr. GEORGE. No, thank you.

Chairman CHABOT. The gentleman's time is expired.

The chair is going to suggest that the gentleman, since you have had this experience a number of times, I am going to put at your disposal the resources of our staff here to see if we cannot move forward in conjunction with the witnesses we have here today and others to see if we cannot make some progress in this area, whether it is legislative or whether it is regulatory or whatever it is,

there are a lot of people getting ripped off for an awful lot of money and I commend the gentleman—would the gentleman accept that?

Mr. BACON. I would love to have that responsibility. Thank you, Mr. Chairman.

I think it is so widespread, Americans want to see accountability and people held responsible for doing this. And I do not think we see it, so we sense it has happened all around us and not enough is being done to counter it.

Chairman CHABOT. Thank you. And I would note for the record that the gentleman is literally a general, you know, a real general. You are a real general, too, but I mean a military general and is used to ordering people around. So I think he will get to the bottom of this.

Mr. BACON. I appreciate the inspector general in the Air Force not having to look my way too often, so.

Chairman CHABOT. The gentleman's time, as I say, has expired.

The gentleman from Pennsylvania, Mr. Fitzpatrick, is recognized for 5 minutes.

Mr. FITZPATRICK. Thank you, Mr. Chairman and the Ranking Member. Thank you, Mr. George, for your time.

Mr. GEORGE. Good morning.

Mr. FITZPATRICK. Two questions. Number one, in our region, I suspect we are not unique as well, there has been somewhat of an uptick in criminal prosecutions by the U.S. Attorney's Office surrounding the Earned Income Tax Credit. What we have seen in some of the cases are parents selling the tax credits for their children; in some cases, disabled children in homes having their identities being used for tax credit purposes. Do you think that that tax credit in particular is more susceptible to fraud than others? And if so, what can we do here in Congress to mitigate that risk?

Mr. GEORGE. That issue, sir, has been so pervasive. Over 20 years ago, I was a staffer here on Capitol Hill, and it was the Government Reform and Oversight Committee at that time. It was a Government Management, Information, and Technology Subcommittee, and we issued a report on improper payments, and the earned income tax—refundable credits in general, but the Earned Income Tax Credit in particular was one of the most—I do not want to use the word "wasteful" because it does have a beneficial impact on the part of taxpayers who need it, but it is so susceptible to fraud. It was back then in the billions of dollars. It is now 20-plus years later in the billions of dollars.

So it is a program that is not—I do not want to say effectively overseen, but because it is refundable, meaning that someone does not necessarily have to owe taxes in order to receive the benefits of it, it is abused. And it is something that Congress—we have brought it to Congress' attention many times. I have testified I cannot tell you the number of times about it and the additional child tax credit, the education tax credit. There are so many tax credits that the IRS has not effectively overseen in terms of its use. Are they reducing the number of improper payments? Yes. But is it to the extent that it should be? There should be none. There should be none, but there are.

Mr. FITZPATRICK. In the area of debt collections, it is my understanding that private debt collectors are being used now by the

Treasury Department. Is there a concern that that is going to create some confusion, particularly amongst the elder population who have been targeted by a lot of these scams?

Mr. GEORGE. Literally this week, the IRS will be formally rolling out this program. The short answer is yes, I think there will be confusion. It used to be, literally a week ago, my response to this question would have included the IRS will never reach out to you or a representative of the IRS would never reach out to you proactively. So if someone calls and claims to be calling on behalf of the IRS, it is a scam. Hang up. Now, that has changed. But the only thing that could possibly benefit the overall system is prior to that phone call the IRS is to send a letter indicating that their case, your tax obligation, has been assigned to a private debt collector and do expect a telephone call from someone who is trying to collect the amount of money that you owe.

Now, of course, again, as a former prosecutor, and again, having been in this job for a while, I can imagine the bad guys will soon catch on to this, and I hesitate to say this publicly, but it is what it is, will then now send a letter and find some logo and say we are going to call you. And then, of course, you know, give them some fake number to use or whatever the case might be.

But this is a challenge for the IRS, sir. There have been a couple of iterations of private debt collectors being used by the IRS dating back to the 1990s with very mixed success in terms of their effectiveness. But it is either this or, in all candor, having hundreds of billions of dollars sitting there uncollected by the IRS, accruing interest, but ultimately not paying, and there is a statute of limitations in effect on how long the IRS can avoid collecting money from taxpayers.

Mr. FITZPATRICK. Thank you. My time is expired. I just want to say that I think it goes without saying, but if the Treasury Department could just try to be vigilant in staying a step ahead because it does create a lot of angst, particularly amongst the senior population, and if there is a place that they could go, a hotline that people would actually answer questions that we could send to our constituents, it would be incredibly helpful.

Mr. GEORGE. And Mr. Chairman, with your indulgence——

Chairman CHABOT. Go right ahead.

Mr. GEORGE. Congressman, that is extraordinarily important, and I made this point. I do not know if you were in the room at the time, it is so important in your mailings to your constituents, you know, TIGTA—the Treasury Inspector General for Tax Administration, TIGTA—we have a hotline, we have websites, we have a telephone number. Please, if in doubt, even with the legitimate, call us, call the IRS to confirm. Do not fall prey. And too many people, and the amounts of money, especially amongst seniors that they are paying in false requests, it is troubling.

Chairman CHABOT. Thank you very much. The gentleman's time has expired.

And we want to thank the inspector general for participating today. The IRS faces truly a daunting challenge in combating tax identity theft, and this battle is one that we must win. It is essentially for the fair and efficient and effective functioning of our tax administrative system overall, and we appreciate the hard work of

General George in overseeing the IRS performance and progress in this area. And thank you for sharing that today.

Equally important to the objective evaluation of current conduct are your thoughtful recommendations for improvement going forward. You play an important role, and we want to thank you for being here today to share your insights with us, and we hope that we can continue to work together to improve the safety and security of our small businesses in particular, but individuals on their personal tax forms as well in the tax arena as we move forward.

I would ask unanimous consent that members have 5 legislative days to submit statements and supporting materials for the record. Without objection, so ordered.

And if there is no further business to come before the Committee, we are adjourned. Thank you very much.

Mr. GEORGE. Thank you, Mr. Chairman.

[Whereupon, at 11:28 a.m., the Committee was adjourned.]

APPENDIX

HEARING BEFORE THE
COMMITTEE ON SMALL BUSINESS
U.S. HOUSE OF REPRESENTATIVES

"Scam Spotting: Can the IRS Effectively Protect Small Business Information?"

Testimony of
The Honorable J. Russell George
Treasury Inspector General for Tax Administration

April 6, 2017

Washington, D.C.

TESTIMONY
OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON SMALL BUSINESS
U.S. HOUSE OF REPRESENTATIVES

"Scam Spotting: Can the IRS Effectively Protect Small Business Information?"
April 6, 2017

Chairman Chabot, Ranking Member Velazquez, and Members of the Committee, thank you for the opportunity to testify on identity theft and its impact on the Internal Revenue Service (IRS) and taxpayers.

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 and is mandated to ensure integrity in America's tax system. It provides independent audit and investigative services to improve the economy, efficiency, and effectiveness of IRS operations. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA plays the key role of ensuring that the approximately 83,000 IRS employees[1] who collected more than $3.3 trillion in tax revenue, processed more than 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2016,[2] have done so in an effective and efficient manner while minimizing the risk of waste, fraud, and abuse.

TIGTA has provided ongoing oversight and testimony on the issue of tax fraud-related identity theft because of the adverse effect on both the victims of this crime and the IRS. Identity theft continues to remain on the IRS's list of "Dirty Dozen" top tax scams. To address the scam, the IRS continues to take steps to more effectively detect and prevent the issuance of fraudulent refunds resulting from identity-theft tax return filings. Our ongoing audit work shows that the IRS is making progress in detecting and resolving identity-theft issues and providing victim assistance. However, our work also shows that improvements are still needed.

---

[1] Total IRS staffing as of January 7, 2017. Included in the total are approximately 16,200 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2016.*

Since May 2012, my office has issued numerous reports that address the IRS's efforts to detect and prevent the filing of fraudulent individual and business tax returns by identity thieves, as well as IRS efforts to assist victims. My comments today will focus on the results of those reports and on our ongoing work to assess the IRS's progress in detecting and resolving identity-theft issues related to tax administration.

DETECTION AND PREVENTION OF IDENTITY THEFT

Identity-theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number[3] to file a fraudulent tax return. Unscrupulous individuals steal identities for use in submitting tax returns with false income and withholding documents to the IRS for the sole purpose of receiving a fraudulent tax refund. Identity-theft tax refund fraud affects both individuals and businesses.

In July 2012,[4] TIGTA issued its first report on our assessment of IRS efforts to detect and prevent fraudulent tax refunds resulting from identity theft. We reported that the impact of identity theft on tax administration is significantly greater than the amount that the IRS detects and prevents. For example, our analysis of Tax Year (TY) 2010 tax returns identified approximately 1.5 million undetected individual tax returns that had the characteristics of identity theft confirmed by the IRS, with potentially fraudulent tax refunds totaling in excess of $5.2 billion.

We have continued to perform follow-up reviews evaluating the IRS's efforts to improve detection processes, including its implementation of TIGTA recommendations. Most recently, we reported in February 2017[5] that IRS efforts are resulting in improved detection of identity theft individual tax returns at the time returns are processed and before fraudulent tax refunds are released. For example, the IRS reported in its October 2016 Identity Theft Taxonomy Analysis that for TY 2014 it had detected and prevented approximately $12 billion in identity theft refund fraud.

For the 2017 Filing Season, the IRS is using 197 identity-theft filters to identify potentially fraudulent individual tax returns and prevent the issuance of fraudulent tax

---

[3] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the taxpayer, the number can be an Employer Identification Number, a Social Security Number (SSN), or an Individual Taxpayer Identification Number.

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

[5] TIGTA, Ref. No. 2017-40-017, *Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvements* (Feb. 2017).

refunds. These filters incorporate criteria based on characteristics of confirmed identity-theft tax returns, including characteristics such as amounts claimed for income and withholding, filing requirements, prisoner status, taxpayer age, and filing history. Tax returns identified by these filters are held during processing until the IRS can verify the taxpayer's identity. The IRS attempts to contact the individual who filed the tax return and, if the individual's identity cannot be confirmed, the IRS removes the tax return from processing. This prevents the issuance of many fraudulent tax refunds. As of March 2, 2017, the IRS reported that it had identified and confirmed 14,068 fraudulent tax returns and prevented the issuance of $91.9 million in fraudulent tax refunds as a result of the identity-theft filters.

Also, beginning with the 2017 Filing Season, the IRS has access to third-party income and withholding information to compare against tax returns during processing. In December 2015, Congress passed legislation to address TIGTA's ongoing concern about limitations in the IRS's ability to prevent the continued issuance of billions of dollars in fraudulent tax refunds.[6] We had previously reported that the IRS did not have timely access to third-party income and withholding information needed to make substantial improvements in its fraud detection efforts. Beginning in 2017, the enacted legislation now requires the annual filing of income and withholding information by January 31. Access to this information at the beginning of the filing season is the single most important tool to detect and prevent tax fraud-related identity theft. TIGTA will be reviewing the IRS's use of the income and withholding information returns as part of its FY 2017 assessment of the IRS's efforts to detect and prevent identity theft.

To prevent fraudulent tax returns from entering the tax processing system, the IRS continues to expand its processes to reject e-filed tax returns and prevent paper tax returns from posting. For example, as of March 13, 2017, the IRS locked approximately 33.2 million taxpayer accounts of deceased individuals. The locking of a tax account results in the rejection of an e-filed tax return and the prevention of a paper-filed tax return from posting to the Master File if the Social Security Number (SSN) associated with a locked tax account is used to file a tax return. According to the IRS, as of February 28, 2017, it had rejected approximately 10,954 fraudulent e-filed tax returns, and, as of March 16, 2017, it had stopped 2,317 paper-filed tax returns from posting to the Master File.

In addition, in response to concerns raised by TIGTA regarding multiple refunds going to the same address or bank account, the IRS now uses a clustering filter tool to group tax returns based on characteristics that include the address, zip code, and bank

---

[6] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. Q, § 201 (2015).

routing numbers. For the tax returns identified, the IRS uses criteria in an attempt to ensure that legitimate taxpayers are not included. Tax returns identified are withheld from processing until the IRS can verify the taxpayer's identity. As of March 2, 2017, the IRS reports that, using this tool, it has identified 72,622 tax returns and prevented the issuance of approximately $334.6 million in fraudulent tax refunds.

Beginning with the 2015 Filing Season, the IRS also implemented a systemic restriction to limit the number of deposits (three) to a single bank account. The IRS will convert the fourth and subsequent direct deposit refund requests to paper checks and send them to the taxpayers' addresses of record. In January 2017,[7] we reported that our analysis of direct deposit requests made as of May 5, 2016, identified 5,605 direct deposit attempts totaling approximately $9.2 million that did not convert to paper checks as required. We are evaluating IRS programming changes implemented to address the errors that we identified as part of our ongoing 2017 Filing Season review.

The IRS recognizes that new identity-theft patterns are constantly evolving and that, as a result, it needs to continuously adapt its detection and prevention processes. These evolving identity-theft patterns affect not only individuals, but also businesses. The IRS defines business identity theft as creating, using, or attempting to use a business's identifying information without authority, in order to claim tax benefits. For example, in order to obtain a fraudulent refund, an identity thief files a business tax return (*e.g.*, Form 1120, *U.S. Corporation Income Tax Return*, Form 720, *Quarterly Federal Excise Tax Return,* or Form 941, *Employer's QUARTERLY Federal Tax Return*) using the Employer Identification Number (EIN)[8] of an active or inactive business without the permission or knowledge of the EIN's owner. As another example, an identity thief applies for and obtains an EIN using the name and SSN of another individual as the responsible party (*i.e.*, fraudulently obtained EIN), without that individual's approval or knowledge, and uses it to create fictitious Forms W-2, *Wage and Income Statement* and bogus Forms 1040, *U.S. Individual Income Tax Return*, which the thief then files to claim a fraudulent refund.

In September 2015, we reported that the IRS recognized the growing threat of business related identity theft and, in response, was implementing processes to detect

---

[7] TIGTA, Ref. No. 2017-40-014, *Results of the 2016 Filing Season* (January 2017).
[8] An EIN is a Federal Tax Identification Number used to identify a taxpayer's business account. The EIN is a nine-digit number (in the format of xx-xxxxxxx) assigned by the IRS and used by employers, sole proprietors, corporations, partnerships, nonprofit associations, trusts and estates, government agencies, certain individuals, and other types of businesses.

identity theft on business returns at the time tax returns are processed.[9] These efforts included conducting a *Business Identity Theft Project* to detect potential business identity theft relating to the filing of Forms 1120 reporting overpayments and claiming refundable credits.

However, TIGTA also found that the IRS is not using data it has readily available to proactively identify potential business identity theft. For example, the IRS maintains a cumulative list of suspicious EINs that it has determined to be associated with fictitious businesses. As of March 24, 2015 the list included 6,176 suspicious EINs. Our analysis of business returns filed during Processing Year[10] 2014 identified 233 tax returns that were filed using a known suspicious EIN. Of these, 97 businesses claimed refunds totaling over $2.5 million. In response to TIGTA's recommendations, the IRS is expanding its filters to identify business identity theft. For the 2017 Filing Season, the IRS is using 25 identity theft filters to identify potentially fraudulent business tax returns and prevent the issuance of fraudulent tax refunds. TIGTA is planning a follow-up audit to assess the IRS's efforts to expand on its processes and procedures to detect business identity theft.

To further protect businesses that file employment tax returns, the Consolidated Appropriations Act of 2014[11] requires the IRS to issue a notice to these employers to confirm any address change. The intent of the notice is to make employers aware of address changes so they can contact the IRS if they did not authorize the address change. Address changes can occur for a variety of reasons, including the filing of a fraudulent employment tax return with a new address by an identity thief. The IRS is required to send a notice to both the employer's former and new address. The IRS implemented the required notice program in January 2015 and reports that for FY 2017 over 2 million sets of notices have been issued as of March 25, 2017. TIGTA is currently conducting a review to evaluate the effectiveness of this dual notification process.[12]

While the IRS's identification and detection strategies have led to many notable improvements, it recognizes the need to continue to explore other initiatives that would assist with its overall detection and prevention efforts. These initiatives include a collaborative effort among IRS officials, representatives from leading tax preparation

---

[9] TIGTA Ref. No. 2015-40-082, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* (Sept. 2015).
[10] The calendar year in which the tax return or document is processed by the IRS.
[11] Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, Div. E, § 106 (2014).
[12] TIGTA Audit 201640019, *Professional Employer Organization Certification Process*, report scheduled for August 2017.

firms, software developers, payroll and tax financial product processors, and representatives from the State Departments of Revenue to discuss common challenges and ways to leverage collective resources and efforts for identity theft detection and prevention. Additionally, the IRS obtains leads about potential identify theft tax returns from State tax agencies via its *State Suspicious Filer Exchange Initiative*, and is conducting a pilot initiative with select payroll providers to test the feasibility of using a verification code to authenticate Form W-2 data at the time tax returns are processed.

IRS ASSISTANCE TO VICTIMS OF IDENTITY THEFT

Tax-related identity theft adversely affects the ability of innocent taxpayers to file their tax returns and timely receive their tax refunds, often imposing significant financial and emotional hardships. Many taxpayers learn that they are a victim of tax-related identity theft when they attempt to file their electronic tax return and the IRS rejects it because someone else (an identity thief) has already filed a return using the same SSN. Individuals can also learn that they are victims of employment-related identity theft if they receive a notification from the IRS of an income discrepancy between the amounts reported on their tax returns and the amount employers reported to the IRS. This can occur when an innocent taxpayer's stolen identity is used by someone else to gain employment. It can cause a significant burden, due to the incorrect computation of taxes and Social Security benefits based on income that does not belong to the taxpayer.

TIGTA has reported that the IRS does not always effectively provide assistance to taxpayers who report that they have been victims of identity theft, resulting in an increased burden for those victims. Specifically, TIGTA reviews have identified long delays in case resolution and account errors, and have found that not all tax-related identity-theft victims receive Identity Protection Personal Identification Numbers (IP PIN).[13] For example, in March 2015,[14] we reported that victims continue to experience long delays while waiting for the IRS to resolve their cases and issue their refunds. Our review of a statistically valid sample of 100 identity-theft tax accounts resolved by the IRS between October 1, 2012, and September 30, 2013, revealed that the IRS took an average of 278 days to resolve the tax accounts. Our report also found that IRS employees did not correctly resolve 17 of the 100 tax accounts. We reported that an estimated 25,565 (10 percent) of the 267,692 taxpayers whose

---

[13] An IP PIN is a six-digit number assigned to taxpayers that allows their tax returns/refunds to be processed without delay and helps prevent the misuse of their SSNs to file fraudulent Federal income tax returns.

[14] TIGTA, Ref. No. 2015-40-024, *Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds* (Mar. 2015).

accounts were resolved may have been resolved incorrectly, resulting in a delayed issuance of refunds to some victims or in some victims receiving an incorrect refund amount.

In July 2015, the IRS created the Identity Theft Victim Assistance (IDTVA) Directorate to combine the skills of employees working tax-related identity-theft cases in multiple functions into one directorate. The goal is to improve the taxpayer's experience when working with the IRS to resolve his or her tax-related identity-theft case. Approximately 1,300 employees work in the IDTVA Directorate to resolve taxpayer-initiated identity-theft cases.[15] TIGTA's current review[16] of cases closed from August 1, 2015, through May 25, 2016, identified improvements in case closure timeframes and a reduction in case closing errors in comparison to our prior audit completed before the IDTVA Directorate was created. The IRS's efforts to centralize operations under a unified leadership, along with its enhanced procedures and processes, have contributed to the improvements identified since our prior audit. We plan to issue our final report in May 2017.

To provide relief to tax-related identity-theft victims, the IRS began issuing IP PINs to eligible taxpayers in FY 2011. For Processing Year 2016, the IRS issued more than 2.7 million IP PINs to taxpayers for use in filing their tax returns. In March 2017, TIGTA reported that some improvements are needed.[17] Specifically, TIGTA found that taxpayer accounts were not always consistently updated to ensure that IP PINs were generated for taxpayers as required. For example, the IRS did not generate IP PINs for more than 2 million taxpayers for whom the IRS resolved an identity-theft case by confirming that the taxpayer was a victim. This results from inconsistent processes and procedures when closing resolved identity-theft cases. Without the required marker on their account to generate an IP PIN, these taxpayers will experience delays when tax returns are subsequently filed.

In November 2016, TIGTA reported that additional actions can be taken to improve the accuracy and timeliness of processing tax return requests from victims of

---

[15] A taxpayer-initiated identity theft case is created when taxpayers contact the IRS to report that after filing their tax return they received a notice indicating the return was rejected because someone (an identity thief) already filed a return using the same SSN and name.
[16] TIGTA, Audit No. 201640015, *Identity Theft Victim Assistance Directorate*, report scheduled for April 2017.
[17] TIGTA, Ref. No. 2017-40-026, *Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers* (Mar. 2017).

tax-related identity theft.[18] In 2015, the IRS changed its policy to allow identity-theft victims to receive, upon request, redacted copies of fraudulent tax returns filed using their names and SSNs. To process taxpayer requests, the IRS established a new program called the Fraudulent Return Request Program. According to the IRS, it has received, as of December 31, 2016, more than 7,200 requests for copies of fraudulent returns since the program's inception in November 2015.

While the IRS took prompt action to establish this program, as of March 11, 2016, TIGTA's review of a statistically valid sample of 130 taxpayer requests, from a population of 1,962 taxpayer requests, identified 33 taxpayer requests with one or more processing errors. Based on the results of this sample, TIGTA projects that 498 taxpayers' requests could contain processing errors. The errors identified by TIGTA included not timely processing the request, not providing a copy of the fraudulent tax return, and not properly redacting all required information from the return, such as taxpayer names, street numbers, and telephone numbers.

In August 2016, we reported that during the period February 2011 to December 2015, the IRS identified almost 1.1 million taxpayers who were victims of employment-related identity theft, but who were not notified.[19] During this audit, the IRS announced it would begin notifying victims of employment identity theft starting in January 2017. The notification letter describes steps the taxpayers could take to prevent further misuse of their personal information, including reviewing their earnings with the Social Security Administration to ensure that their records are correct. TIGTA is currently conducting a review to assess IRS actions to notify victims, and we plan to issue our draft report in November 2017.[20]

We have an ongoing audit that is evaluating the IRS's processes to identify and mark victims' tax accounts and to notify the Social Security Administration to ensure that individuals' Social Security benefits are not affected by the misuse of their identities by imposters to gain employment.[21] TIGTA found that IRS processes are not sufficient to identify all employment identity-theft victims. In addition, IRS processes do not identify employment identity theft when processing paper tax returns, nor does the

---

[18] TIGTA, Ref. No. 2017-40-011, *Actions Can Be Taken to Improve Processes of a Newly Developed Program That Enables Victims of Identity Theft to Request Copies of Fraudulent Tax Returns* (Nov. 2016).
[19] TIGTA, Ref. No. 2016-40-065, *Processes Are Not Sufficient to Assist Victims of Employment-Related Identity Theft* (Aug. 2016).
[20] TIGTA, Audit No. 201740033, *Notification Letters to Victims of Employment Identity Theft.*
[21] TIGTA, Audit No. 201640028, *Employment Related Identity Theft – Returns Processing,* report scheduled for April 2017.

IRS have a process to notify the Social Security Administration of employment identity theft when both the victim's name and SSN are used by imposters to gain employment. TIGTA expects to issue its report in May 2017.

TELEPHONE IMPERSONATION SCAM

Since the fall of 2013, a significant amount of our Office of Investigations' workload has consisted of investigating a telephone impersonation scam in which more than 1.9 million intended victims have received unsolicited telephone calls from individuals falsely claiming to be IRS or Department of the Treasury employees. The callers demand money under the pretense that the victim owes unpaid taxes. To date, over 10,300 victims have purportedly paid more than $55 million to these criminals.

The telephone impersonation scam continues to be one of TIGTA's top priorities; it has also landed at the top of the IRS's "Dirty Dozen" tax scams. The numbers of complaints we have received about this scam have cemented its status as the largest, most pervasive impersonation scam in the history of our agency. It has claimed victims in every State.

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

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

According to the victims we have interviewed, these scammers then demanded that the victims immediately pay the money using Apple iTunes® gift cards, Target gift cards, prepaid debit cards, wire transfers, Western Union payments or MoneyGram® payments in order to avoid being immediately arrested. They are typically warned that if they hang up, local police will come to their homes to arrest them immediately. Sometimes the scammers also send bogus IRS e-mails to support their claims that

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

TIGTA has made several arrests in connection with this scam and has numerous investigations underway. In July 2015, in one of the largest prosecutions on this scam that we have had to date, an individual plead guilty to organizing an impersonation scam ring. He was sentenced to over 14 years of incarceration and ordered to forfeit $1 million. In October of 2016, after an extensive three-year investigation, TIGTA, the Department of Justice and the Department of Homeland Security announced the indictment of 56 individuals and five call centers located in India. Although the investigations and prosecutions have reduced the number of scam calls being placed by over 90 percent, we are still receiving reports that between 5,000 and 6,000 people are receiving calls each week.

In addition to the criminal prosecutions, to thwart scammers using robo-dialers, we have created and instituted an "Advise and Disrupt" strategy. The strategy involves cataloguing the telephone numbers that have been reported by intended victims. We then use our own automated call dialers to make calls to those telephone numbers to advise the scammers that their activity is criminal and to cease and desist their activity. Utilizing this technique, we have placed more than 142,000 automated calls back to the scammers. We are also working with the telephone companies to have the scammers' telephone numbers shut down as soon as possible. Of the 1,160 telephone numbers that have been reported by victims, we have successfully shut down 94 percent of them, some of them within one week of the number's being reported to us.

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

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

We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system. As such, we plan to provide continuing audit coverage of the IRS's efforts to identify and detect identity theft and provide assistance to victims.

Chairman Chabot, Ranking Member Velazquez, and Members of the Committee, thank you for the opportunity to share my views.

J. Russell George

Treasury Inspector General for Tax Administration

Following his nomination by President George W. Bush, the United States Senate confirmed J. Russell George in November 2004, as the Treasury Inspector General for Tax Administration. Prior to assuming this role, Mr. George served as the Inspector General of the Corporation for National and Community Service, having been nominated to that position by President Bush and confirmed by the Senate in 2002.

A native of New York City, where he attended public schools, including Brooklyn Technical High School, Mr. George received his Bachelor of Arts degree from Howard University in Washington, DC, and his Doctorate of Jurisprudence from Harvard University's School of Law in Cambridge, MA. After receiving his law degree, he returned to New York and served as a prosecutor in the Queens County District Attorney's Office.

Following his work as a prosecutor, Mr. George joined the Counsel's Office in the White House Office of Management and Budget, where he was Assistant General Counsel. In that capacity, he provided legal guidance on issues concerning presidential and executive branch authority. He was next invited to join the White House Staff as the Associate Director for Policy in the Office of National Service. It was there that he implemented the legislation establishing the Commission for National and Community Service, the precursor to the Corporation for National and Community Service. He then returned to New York and practiced law at Kramer, Levin, Naftalis, Nessen, Kamin & Frankel.

In 1995, Mr. George returned to Washington and joined the staff of the Committee on Government Reform and Oversight and served as the Staff Director and Chief Counsel of the Government Management, Information and Technology subcommittee (later renamed the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations), chaired by Representative Stephen Horn. There he directed a staff that conducted over 200 hearings on legislative and oversight issues pertaining to Federal Government management practices, including procurement policies, the disposition of Government-controlled information, the performance of chief financial officers and inspectors general, and the Government's use of technology. He continued in that position until his appointment by President Bush in 2002.

Mr. George also served as a member of the Integrity Committee of the Council of Inspectors General for Integrity and Efficiency (CIGIE). CIGIE is an independent entity within the executive branch, statutorily established by the Inspector General Act, as amended, to address integrity, economy, and effectiveness issues that transcend individual Government agencies and to increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General. The CIGIE Integrity Committee serves as an independent review and investigative mechanism for allegations of wrongdoing brought against Inspectors General.