HEARING BEFORE THE
COMMITTEE ON FINANCE
UNITED STATES SENATE

"Tax Schemes and Scams During the 2015 Filing Season"

Testimony of
Timothy P. Camus
Deputy Inspector General for Investigations
Treasury Inspector General for Tax Administration

March 12, 2015

Washington, D.C

TESTIMONY OF
TIMOTHY P. CAMUS
DEPUTY INSPECTOR GENERAL for INVESTIGATIONS
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
Before the
COMMITTEE ON FINANCE
UNITED STATES SENATE

"Tax Schemes and Scams During the 2015 Filing Season"

March 12, 2015

Chairman Hatch, Ranking Member Wyden, and Members of the Committee, thank you for the opportunity to testify on the topic of Tax Schemes and Scams during the 2015 filing season.

I also want to thank you for holding a hearing on this topic, for by doing so, you are bringing attention to these schemes and scams, and thereby alerting your constituents and others across the country to their existence. By raising public awareness about such efforts to swindle people out of their money, we may prevent the next person from becoming a victim. And if we protect even one taxpayer from this type of theft, we have done a very good thing.

The Treasury Inspector General for Tax Administration, also known as "TIGTA," is statutorily mandated to provide independent audit and investigative services necessary to protect the integrity of Federal tax administration as well as to improve the economy, efficiency, and effectiveness of Internal Revenue Service (IRS) operations. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 91,000 IRS employees, who collected over $3.1 trillion in tax revenue, processed over 242 million tax returns and other forms, and issued $374 billion in tax refunds during Fiscal Year (FY) 2014, did so with the highest degree of integrity and in an effective and efficient manner while minimizing the risks of waste, fraud, or abuse. This includes investigating individuals who use the IRS as a means of furthering fraudulent, criminal activity that could call into question the integrity of the IRS, as well as investigating allegations of serious misconduct by IRS employees and investigating threats of violence against the IRS, its employees, and facilities. Over the past year, a significant part of our workload has been devoted to investigating scams that can negatively impact the integrity of tax administration.

Tax scams are nothing new. For at least the last decade, the IRS has provided the public with information about what it sees as the "Dirty Dozen" tax scams on its website. These scams range from offshore tax avoidance to fake charities and inflated refund claims. Compiled annually, the "Dirty Dozen" lists a variety of common scams that taxpayers may encounter. However, many of these scams peak during the filing season as people prepare their returns or utilize the services of paid preparers.

The 2015 filing season has unfortunately brought more of the same. However, there are two tax scams in particular that are among the most pernicious and dangerous. They have proven to be surprisingly effective and fast ways to steal taxpayers' money, and in this fast-paced electronic environment, the money can be gone before the victims ever realize they have been scammed.

PHONE IMPERSONATION SCAM

The phone impersonation scam has proven to be so large that it is one of my agency's top priorities**,** and it has also landed at the top of the IRS's **"**Dirty Dozen**"** tax scams this year. The number of complaints we have received about this scam make it the largest, most pervasive impersonation scam in the history of our agency. It has claimed thousands of victims, including victims in every State represented on this committee, with reported losses totaling more than $15.5 million dollars to date. Here is how it works:

The intended victim receives an unsolicited telephone call from a person claiming to be an IRS agent. The caller, using a fake name, tells the victim their "badge number," and claims that they owe taxes and are criminally liable for an amount owed. The callers may even know the last four digits of the victim's Social Security Number (SSN). They then threaten the victim by stating that if they fail to pay the amount immediately, the victim will be arrested, a suit will be filed, or some other form of adverse official action will be taken. These actions have been reported to include loss of a driver's license, deportation, or loss of a business license. They often leave "urgent" callback requests and call multiple times. Although these callers initially preyed on the most vulnerable people, such as the elderly, newly arrived immigrants and those whose first language is not English, they have expanded their scam to people from every walk of life. The continued number of people receiving these unsolicited calls from individuals who fraudulently claim to represent the IRS is alarming.

We first started seeing concentrated reporting of these calls in August, 2013. As the reporting continued through the fall, in October 2013, we started to specifically track this crime. To date, we have received hundreds of thousands of complaints about these calls. According to the victims, the scam artists made the threatening statements as described above, and then demanded that the victims immediately put money on prepaid debit cards in order to avoid being immediately arrested. The callers often warned the victims that if they hung up, local police would come to their homes to arrest them. The scammer may also send bogus IRS e-mails to support their scam. Those who fell for the scam withdrew thousands of dollars from their bank accounts and then purchased the prepaid debit cards as instructed by the callers. Once the prepaid debit cards were purchased, the criminals instructed the victims to call them back and to read the numbers off of the prepaid card. By the time the victims realized they had been scammed, the criminals had negotiated the prepaid cards and the money was long gone.

One particularly sad story was shared with TIGTA by a member of this Committee in a letter written on behalf of a constituent regarding the tragic death of the constituent's father as a result of receiving several threatening calls from a scammer claiming to be from the IRS and demanding money. This scam has cost thousands of taxpayers millions of dollars, but to my knowledge, this may be the most heartbreaking result. TIGTA continues to work with the IRS to strengthen its efforts to crack down on this type of abuse and try to prevent other vulnerable individuals from being victimized by this kind of fraud.

To date, TIGTA has received over 366,000 reports of these calls. We receive between 9,000 and 12,000 reports of these calls each week. As of March 9, 2015, 3,052 individuals have been victimized by this scam by paying a total of $15.5 million, averaging over $5,000 per victim. The highest reported loss by one individual was over $500,000. In addition, 296 of these victims also provided sensitive identity information to these scammers. The scam has claimed victims in almost every State in the country. For example, taxpayers in Utah have lost more than $276,000 to this scam, and taxpayers in Oregon have lost more than $180,000. As of February 28, 2015, the top five States for total dollar losses by victims are California ($3,840,000), New York ($1,352,732), Texas ($795,884), Florida ($760,000), and Virginia ($648,363).

The criminals do not discriminate; they are calling people everywhere, of all income levels and backgrounds. In fact, I myself received one of these calls on my home telephone on a Saturday, and you may also have received a call or know of a family member or constituent who has received one as well. Based on reviewing the complaints we have received, we believe the calls are now being placed from more than one source. This scam is the subject of an ongoing multi-agency investigation. For this reason, there is much that we are doing to apprehend the perpetrators, but I am not at liberty to disclose specifically what is being done as it may impede our ability to successfully bring these criminals to justice. I can tell you it is a matter of high priority for law enforcement. As I told the individual who called me on my home phone, "your day will come."

In the meantime, we are investigating some of the individuals who process the money, and most recently we arrested two individuals associated with this type of scam. The two individuals were arrested and prosecuted for their role in converting the prepaid money cards. When interviewed, one of the defendants estimated she had used prepaid debit cards to purchase approximately $5,000 in money orders per day, six days a week, since November 2013, or roughly $900,000 in money order purchases between November 2013 and July 2014.[1] In another case, in March 2014, an individual was indicted for using an impersonation scam. More specifically, he was indicted for extortion, false impersonation, and fraud.[2]

[1] S.D. Fla. Crim. Compl. filed Sept. 5, 2014.
[2] S.D.N.Y. Indict. filed Mar. 6, 2014.

However, there is much more that needs to be done, as these three examples are part of a broader ring of scam artists operating beyond our borders. This is unfortunately similar to most of the cybercrime we are seeing today – it is international in nature and committed using technology, *e.g.*, in the case of the phone fraud scam, the use of Voice over Internet Protocol technology, and much of it originates from a computer outside of the United States. To further deceive their intended victims, by using this technology, the criminals create false telephone numbers that show up on the victim's caller ID system. For example, the criminals make it appear as though the calls are originating from Washington, D.C., or elsewhere in the United States.

I am also concerned that these criminals and their copycats, like the bank robbers of old, will go where the money is, and will keep using this scam as long as people fall victim to it. For example, we have noted an increasing number of recent reports that the calls are coming in using robo-call technology. When the robo-calls are used, the scammers leave messages demanding that the victim immediately call back a telephone number and speak to a representative. Although the robo-calls are a different approach, the outcome is the same: once the criminal gets the victim on the phone, they demand immediate payment and threaten the victim with arrest for failing to comply with their demands.

Accordingly, we are reaching out aggressively by granting media interviews with all the major networks, and issuing warnings and multiple press releases to the media in conjunction with the IRS and the Federal Trade Commission (FTC), as well as providing this testimony to your Committee. Our message is simple: If someone calls unexpectedly claiming to be from the IRS with aggressive threats if you do not pay immediately, it is a scam artist calling. The IRS does not initiate contact with taxpayers by telephone. If you do owe money to the IRS, chances are you have already received some form of a notice or correspondence from the IRS in your mailbox.

To recap, the IRS will never:

- Call to demand immediate payment, nor will the IRS call about taxes owed without first having mailed you a notice;
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe;
- Require you to use a specific payment method for your taxes, such as a prepaid debit card;
- Ask for credit or debit card numbers over the phone; and
- Threaten to bring in local police or other law enforcement groups to have you arrested for not paying.

Remember, also, the IRS does not initially use e-mail, text messages, or any social media to discuss your personal tax issue involving taxes owed or refunds. For more information on reporting tax scams, go to www.irs.gov and type "scam" in the search box. If you have been targeted by this scam, report the incident to TIGTA at

www.tigta.gov by clicking on the IRS Impersonation Scam Reporting tab in the upper right corner, or call the TIGTA hotline at 1-800-366-4484. In addition, contact the FTC and use their "FTC Complaint Assistant" at www.ftc.gov. Please add "IRS Telephone Scam" to the comments of your complaint. If you know you owe taxes or think you might owe, call the IRS at 1-800-829-1040. They can help you with a payment issue.

LOTTERY WINNINGS

The lottery winnings scam we are seeing this filing season is a continuation of an older scam. It starts with an e-mail or telephone call stating that you have won the lottery and in order to collect the winnings, you need to send money to prepay the tax to the IRS. The lottery scam often, but not always, originates from outside of the United States, and continues because it capitalizes on a very common dream; getting rich quick and hitting the jackpot.

In one of the largest cases of this type, an individual and his co-conspirators operated a scheme to defraud numerous individuals through Internet solicitations, stealing more than $1 million as well as the identities of the victims. The criminals obtained and used massive e-mail distribution lists containing thousands of e-mail addresses to send unsolicited e-mails falsely informing victims that they had won a lottery or had inherited money from a distant relative. Follow-up e-mails instructed the victims to provide personal and bank account information to receive their lottery winnings or inheritance. Subsequent e-mails to victims falsely indicated that a Government or a quasi-governmental agency, such as the IRS or the United Nations, would not pay the money due to them because advance payment of taxes and other fees was required. The e-mails solicited the victims to wire money to pay the taxes and other fees to designated bank accounts controlled by the criminals.[3]

However, if the victims were unable to pay the taxes and fees, the criminals offered to loan them the money. The victims were then convinced to open online bank accounts and provide the necessary login information to the criminals. Using this information, the criminals stole money from various other bank accounts, transferred that stolen money to the victims' accounts, and then instructed the victims to wire the money to foreign bank accounts controlled by the criminals. In the end, the victims never received any lottery winnings, inheritance, or other money in connection with the scheme; however, they may have received much grief for unknowingly being placed in the middle of a money laundering scheme.

The lead defendant was sentenced to a total of 30-months of imprisonment and five-years of supervised release for Aggravated Identity Theft and Conspiracy to Commit Wire Fraud. He was also ordered to pay $1,741,822 restitution to his victims and a $200 assessment.[4]

[3] E.D.N.Y. Response to Defendant's Sentencing Letter filed Dec. 19, 2011 and E.D.N.Y. Superseding Info. Filed May 10, 2011.
[4] E.D.N.Y. Judgment filed Dec. 27, 2011.

OTHER FRAUDS IMPACTING TAX ADMINISTRATION

IDENTITY THEFT

The IRS continues to make improvements in its identification of identity theft tax returns at the time the returns are processed and before fraudulent tax refunds are released. The IRS has described identity theft as one of its "Dirty Dozen" and recognizes that new identity theft patterns are constantly evolving and, as such, it needs to adapt its detection and prevention processes.

Notwithstanding improvements in its detection efforts, the IRS still does not have timely access to third-party income and withholding information. Most of the third-party income and withholding information is not received by the IRS until well after taxpayers begin filing their tax returns. For example, the deadline for filing most third party information returns with the IRS is March 31, yet taxpayers began filing their tax returns for the 2015 Filing Season on January 20th. As of February 27, 2015, the IRS has received approximately 58.5 million individual tax returns. Legislation would be needed to accelerate the filing of the information returns.

The IRS has taken steps to more effectively prevent the filing of identity theft tax returns by locking the tax accounts of deceased individuals to prevent others from filing a tax return using their name and SSN. The IRS has locked approximately 26.3 million taxpayer accounts between January 2011 and December 31, 2014. These locks prevent fraudulent tax returns from entering the tax processing system. For Processing Year 2014,[5] the IRS rejected 338,807 e-filed tax returns and stopped 15,915 paper-filed tax returns through the use of these locks as of September 30, 2014.

Additionally, the IRS continues to take steps to more effectively detect and prevent the issuance of fraudulent refunds resulting from identity theft tax return filings. The IRS continues to expand identity theft filters to identify fraudulent tax returns at the time they are processed. It has expanded the number of identity theft filters used to identify potentially fraudulent tax returns and prevent the issuance of fraudulent tax refunds from 114 filters during Processing Year 2014 to 196 filters during Processing Year 2015. The identity theft filters incorporate criteria based on characteristics of confirmed identity theft tax returns.

Tax returns identified by these filters are held during processing until the IRS can verify the taxpayer's identity. As of January 31, 2015, just 11 days after the filing season began, the IRS reported that it identified and confirmed 264 fraudulent tax returns and prevented the issuance of more than $2 million in fraudulent tax refunds as a result of the identity theft filters.

[5] A processing year is the calendar year in which tax returns are processed by the Internal Revenue Service.

In addition to the above actions, the IRS developed and implemented a clustering filter in response to TIGTA's continued identification of large volumes of undetected potentially fraudulent tax returns with tax refunds issued to the same address or deposited into the same bank account. The clustering filter tool groups tax returns based on characteristics that include the address, zip code, and/or bank routing numbers. Using this tool, the IRS reports that as of October 9, 2014, it identified 517,316 tax returns and prevented the issuance of approximately $3.1 billion in fraudulent tax refunds.

PRISONER FRAUD

Refund fraud associated with prisoner SSNs remains a significant problem for tax administration. The number of fraudulent tax returns filed using a prisoner's SSN that were identified by the IRS increased from more than 37,000 tax returns in Calendar Year 2007 to more than 137,000 tax returns in Calendar Year 2012. The refunds claimed on these tax returns increased from $166 million to $1 billion. As of February 28, 2015, the IRS reports that it identified 24,011 potentially fraudulent tax returns filed by prisoners for screening.

In September 2014, TIGTA reported that the IRS has not yet shared fraudulent prisoner tax returns and return information with Federal or State prison officials.[6] As of June 2014, the IRS has yet to complete needed agreements to begin sharing information related to false prisoner tax returns and return information with Federal and State prison officials. This is despite the fact that the IRS was initially given the authority to share certain information with Federal prison officials in October 2008. The authority for the IRS to share information with prison officials is intended to enable prison officials to take action to punish prisoners for perpetrating fraud and to help stop this abuse of our tax system.

TIGTA also found that the required annual prisoner fraud reports to Congress are not timely and that the reports do not address the extent to which prisoners may be filing fraudulent tax returns using a different individual's SSN. In addition, we followed up on a condition identified in a past review and found that IRS processes still do not ensure that all tax returns filed using a prisoner SSN are assigned a prisoner indicator. Our analysis of tax returns filed during Calendar Year 2013 identified 43,030 tax returns that were filed using a prisoner SSN that were not assigned a prisoner indicator. When tax returns filed using a prisoner SSN are not assigned the required indicator, the tax return will not be subjected to the IRS's specialized prisoner fraud checks.

[6] TIGTA, Ref. No. 2014-40-091, *Prisoner Tax Refund Fraud: Delays Continue in Completing Agreements to Share Information With Prisons and Reports to Congress Are Not Timely or Complete* (Sept. 2014).

UNSCRUPULOUS TAX PREPARERS

Tax preparers who steal a client's identity information or their tax refunds can also cause great harm to the integrity of the Federal tax system. The following case highlights an example of this damage.

Last December, an Ohio accountant was sentenced for wire fraud, engaging in monetary transactions in property derived from specified unlawful activity, mail fraud, and attempting to interfere with administration of the internal revenue laws. The accountant was sentenced to 36 months in prison, followed by three years of supervised release, and was further ordered to pay $987,050.00 in restitution to victims.[7] From approximately 2009 through 2013, the accountant engaged in various schemes to defraud individuals to obtain money and property by means of false and fraudulent pretenses and representations, and to obstruct the due administration of the Internal Revenue laws.[8]

After the IRS issued a levy to a financial firm in the amount of $91,193.53 to collect taxes owed by one of his clients, the accountant transmitted, via e-mail, a falsified IRS Form 668-D, Release of Levy, which purported to remove the levy from the couple's account. The accountant did so knowing the IRS had not authorized the release of the levy from that account.[9]

Prior to this, around April 2011, the accountant devised a scheme to defraud another victim, a senior citizen with little experience managing financial matters. The accountant falsely represented to the victim that the victim owed the IRS a substantial amount of taxes, and directed the victim to send him multiple payments for taxes purportedly owed by the victim. The accountant kept all of the money received from the victim and used it for his own personal and business expenses, defrauding the victim of approximately $237,050.[10]

In a different case, a tax preparer used the means of identification of other people to file false income tax returns and obtain refunds from the IRS. The preparer obtained most of the means of identification from his previous employment as a tax preparer and from other employment positions he held. He provided this information to co-conspirators so they could also file false income tax returns and obtain refunds from the IRS. The preparer and his co-conspirators ultimately defrauded or attempted to defraud the IRS out of at least $560,000 in tax refunds.[11]

[7] E.D. Pa. Judg. filed Dec. 16, 2014.
[8] E.D. Pa. Indict. filed Jan. 9, 2014; E.D. Pa. Info. filed June 3, 2014.
[9] Id.
[10] E.D. Pa. Info. filed June 3, 2014.
[11] S.D. Cal. Superseding Indict. filed June 19, 2012.

PHISHING SCAMS

Phishing is a scam that has been around for several years and is typically carried out through the use of unsolicited e-mails or a fake website that poses as a legitimate site in order to lure potential victims in to either pay some sort of fee, or provide valuable personal and financial information. Armed with this information, a criminal can commit identity theft or financial theft. Phishing is often used as the technique to gather information to start other scams, such as the lottery scam identified earlier.

My investigators are alerted to hundreds of new phishing scams every year. For example, my agents can encounter numerous fake e-mails that lead to fraudulent websites appearing to be legitimate, but actually looking to steal taxpayers' personal information or to trick the victim into paying money. Also by clicking on any of the links in these e-mails or websites, innocent taxpayers have unknowingly invited the criminal into their computer where they can steal financial information, personal contact information, and even file more fraudulent documents. All the while, this activity is unknown to the victim.

The best thing taxpayers can do is to be alert and to stop and think before clicking on any link. The first contact a taxpayer receives from the IRS will not be made via e-mail. If they receive an unsolicited e-mail that appears to be from either the IRS or an organization closely linked to it, they should be leery and call the IRS to verify the contact and report it by sending it to www.phishing@irs.gov.

TIGTA and the IRS office of Online Fraud Detection and Prevention work closely together to protect innocent taxpayers from criminals who create fake websites that impersonate the IRS. In fact, since 2012, when the number of identified phishing sites peaked at almost 19,000, we have seen a reduction in the number of identified phishing sites over the past two years to 1,200 in 2014.

Chairman Hatch, Ranking Member Wyden, thank you for the opportunity to share my views. This concludes my testimony on some of the tax schemes and scams we have noted during the 2015 filing season. Much work is being done on multiple fronts to dismantle many of these schemes and scams, and our hope is that if we return to testify next year, these incidents will be greatly reduced or eliminated.

Timothy P. Camus
Deputy Inspector General for Investigations

Mr. Timothy P. Camus has served in the Treasury Inspector General for Tax Administration (TIGTA) and the Internal Revenue Service Inspection Service, TIGTA's predecessor organization, as a Special Agent, for over 23 years.

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

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