WRITTEN STATEMENT OF

CHRISTOPHER J. LEE

SENIOR ATTORNEY-ADVISOR

TAXPAYER ADVOCATE SERVICE

HEARING ON

TAX-RELATED IDENTITY THEFT AND FRAUDULENT TAX RETURNS

BEFORE THE

COMMITTEE ON BUDGET

U.S. SENATE

AUGUST 26, 2015

Chairman Enzi, Ranking Member Sanders, and distinguished Members of the Committee:

Thank you for inviting me to testify today about the problems in tax administration stemming from the filing of fraudulent tax returns by identity thieves.[1]

When I joined the Taxpayer Advocate Service in 2004 as an attorney-advisor to the National Taxpayer Advocate, one of my first assignments was to look into how the IRS was dealing with the small, but growing, problem of identity theft. Since then, tax-related identity theft has become an epidemic, and the National Taxpayer Advocate has written about the problems it causes for its victims and for the IRS in nearly every Annual Report she has delivered to Congress.[2]

Identity theft cases account for approximately a quarter of all TAS case receipts.[3] One reason why so many identity theft cases end up in TAS is because of their complexity – these cases often require actions to be taken by employees from multiple IRS functional units. The vast majority of TAS identity theft cases involve more than one issue code, and about a third of them contain three or more issue codes,[4] as the figure below illustrates.

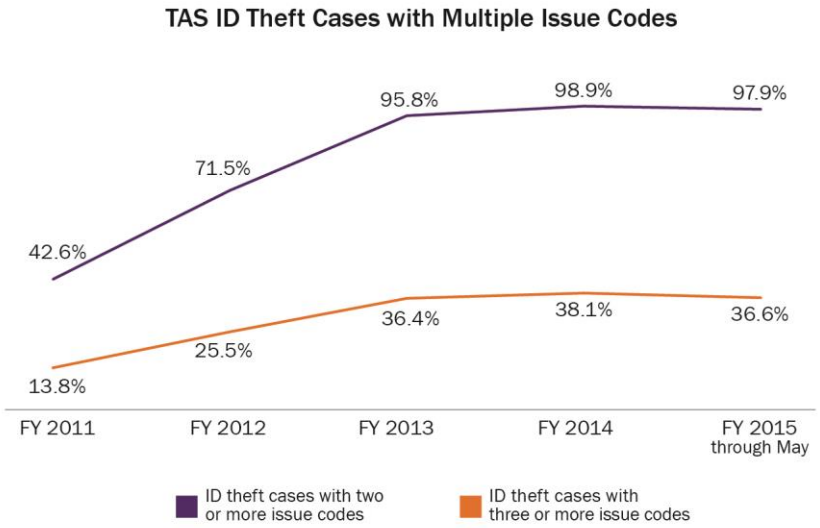
[1] The views expressed herein are those Christopher J. Lee, Senior Attorney-Advisor to the National Taxpayer Advocate, and do not necessarily reflect the position of the National Taxpayer Advocate, the IRS, or the Treasury Department.

[2] *See* National Taxpayer Advocate 2014 Annual Report to Congress vol. 2, 44-90 (*Identity Theft Case Review Report: A Statistical Analysis of Identity Theft Cases Closed in June 2014*); National Taxpayer Advocate 2013 Annual Report to Congress 75-83 (Most Serious Problem: *The IRS Should Adopt a New Approach to Identity Theft Victim Assistance that Minimizes Burden and Anxiety for Such Taxpayers*); National Taxpayer Advocate 2012 Annual Report to Congress 42-67 (Most Serious Problem: *The IRS Has Failed to Provide Effective and Timely Assistance to Victims of Identity Theft*); National Taxpayer Advocate 2011 Annual Report to Congress 48-73 (Most Serious Problem: *Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS*); National Taxpayer Advocate 2009 Annual Report to Congress 307-17 (Status Update: *IRS's Identity Theft Procedures Require Fine-Tuning*); National Taxpayer Advocate 2008 Annual Report to Congress 79-94 (Most Serious Problem: *IRS Process Improvements to Assist Victims of Identity Theft*); National Taxpayer Advocate 2007 Annual Report to Congress 96-115 (Most Serious Problem: *Identity Theft Procedures*); National Taxpayer Advocate 2005 Annual Report to Congress 180-91 (Most Serious Problem: *Identity Theft*); National Taxpayer Advocate 2004 Annual Report to Congress 133-36 (Most Serious Problem: *Inconsistence Campus Procedures*).

[3] During the first two quarters of fiscal year (FY) 2015, TAS received 23,657 identity theft cases (24 percent of all TAS receipts). TAS, *Business Performance Review* (2nd Quarter FY 2015).

[4] When TAS opens a case, it assigns a primary issue code based on the most significant issue, policy or process within the IRS that needs to be resolved. When a TAS case has multiple issues to resolve, a secondary issue code will be assigned. *See* Internal Revenue Manual (IRM) 13.1.16.13.1.1, *Taxpayer Issue Code* (Feb. 1, 2011).

Figure 1[5]



Even as complex as these cases have become, TAS Case Advocates have learned to resolve identity theft cases efficiently. In fiscal year (FY) 2015 (through May), TAS has taken an average of 66 days to close such cases, compared to 126 days over the same period five years ago.[6]

Before proceeding further, I would like to point out an important distinction between two common types of tax-related identity theft. In "refund-related" identity theft, a perpetrator uses the Social Security number (SSN) of another person to file a tax return with falsified information for the purpose of obtaining an improper refund, usually very early in the filing season. This scenario causes serious repercussions to the victim by delaying the processing of his or her legitimate return and the issuance of the legitimate refund, if any.

In "employment-related" identity theft, an individual files a tax return using his or her own taxpayer identifying number (sometimes using an Individual Taxpayer Identification Number, or ITIN), but uses someone else's SSN to obtain employment. The employer would then issue a Form W-2 reflecting the wages earned by this individual, but reported on the identity theft victim's SSN. When the SSN holder files a return with the IRS, the IRS Automated Underreporter program will notify the victim that additional tax is due on this unreported income. This may be the first time the SSN holder realizes he or she is a victim of identity theft.

[5] Data obtained from Taxpayer Advocate Management Information System (TAMIS) (Oct. 1, 2011; Oct. 1, 2012; Oct. 1, 2013; Oct. 1, 2014; June 1, 2015).

[6] Data obtained from TAMIS (June 1, 2010; June 1, 2015).

I. Refund-Related Identity Theft

For victims of refund-related identity theft, the consequences can be devastating. Apart from the time and frustration involved in dealing with the IRS to prove one's own identity, taxpayers generally do not receive their refunds until their cases are resolved. Among all taxpayers receiving refunds this filing season, the average refund amount was just over $2,700.[7] For low income taxpayers, a tax refund may constitute a significant percentage of their annual income. Lengthy case resolution times can translate to financial inconvenience and sometimes hardship, which is why we have been pushing the IRS to resolve identity theft cases promptly.

To get an accurate sense of how long the IRS takes to fully resolve an identity theft case, TAS conducted a study published in Volume 2 of the National Taxpayer Advocate's 2014 Annual Report to Congress.[8] Our 2014 case review showed that the average cycle time for identity theft cases worked by the IRS was 179 days.[9] The IRS can and should do better. To improve the victim experience and to shorten its identity theft case cycle time, the National Taxpayer Advocate recommended that for complex identity theft cases (ones that require the victim to deal with multiple IRS functions), the IRS designate a sole contact person with whom the victim can interact for the duration of the case.[10] We believe this would not only put the victim more at ease, but also avoid having an identity theft case fall through the cracks and adding to the cycle time.

Overall, about two-thirds (67 percent) of all identity theft cases in our sample were either (1) worked in more than one function, or (2) reassigned to another assistor within a function.[11] When a case is transferred or reassigned, it delays case resolution and adds to the frustration experienced by the victim. We found that 42 percent of the cases analyzed in our sample had periods of inactivity (*i.e.*, periods of time when no work was being performed on the case for more than 30 days).[12]

The IRS recently reorganized its identity theft victim assistance units, moving toward a more centralized approach for which our office has long advocated.[13] TAS will be involved with the IRS in its re-engineering of its identity theft victim assistance procedures this fall, and we will reiterate our recommendation that the IRS assign a

---

[7] IRS, *Filing Season Statistics for Week Ending April 17, 2015, available at* http://www.irs.gov/uac/Newsroom/Filing-Season-Statistics-for-Week-Ending-April-17-2015.

[8] *See* National Taxpayer Advocate 2014 Annual Report to Congress vol. 2 (*Identity Theft Case Report: A Statistical Analysis of Identity Theft Cases Closed in June 2014*).

[9] National Taxpayer Advocate 2014 Annual Report to Congress vol. 2, 53.

[10] National Taxpayer Advocate 2014 Annual Report to Congress vol. 2, 55.

[11] *See* National Taxpayer Advocate 2014 Annual Report to Congress vol. 2, 52.

[12] *See* National Taxpayer Advocate 2014 Annual Report to Congress vol. 2, 52.

[13] *See* National Taxpayer Advocate 2007 Annual Report to Congress 115.

sole contact person with whom the victim can interact for the duration of the identity theft case.

II. Employment-Related Identity Theft

Employment-related identity theft may occur when the perpetrator does not possess a valid SSN that authorizes him or her to work. As a result, he or she may steal, purchase, or borrow a valid SSN for purposes of obtaining employment. In other instances, the perpetrator of employment-related identity theft might have a valid SSN, but does not want wages reported under his or her SSN. For example, he may have a court-ordered obligation to pay spousal or child support, and thus have a strong desire to avoid earning income under his own SSN.

Victims of employment-related identity theft may receive an Automated Underreporter letter from the IRS. It may take months for the victim to demonstrate to the IRS that he or she did not actually earn the income on the Form W-2.

In situations where an individual files a tax return using an ITIN to report income from a Form W-2 with someone else's SSN, the IRS now has procedures in place to minimize the tax administration impact to the victims in these employment-related identity theft situations.[14] If the procedures work as intended, the victim will not experience any adverse tax consequences from an ITIN holder filing a tax return using the victim's SSN. Thus, as a practical matter, there is no tax administration impact to victims of this type of identity theft (where there is an ITIN/SSN mismatch).

In many instances, the IRS may be the first to learn that the victim's SSN has been compromised. In the 2011 Annual Report to Congress, the National Taxpayer Advocate recommended that the IRS "[p]romptly notify all victims of identity theft of the misuse of their SSN and provide information about what steps the taxpayer may take to further protect himself or herself."[15] When the IRS discovers that a taxpayer's SSN was used without authorization to file a tax return, it should immediately disclose to the SSN owner that the number has been used on another return and that he or she is an apparent victim of employment-related identity theft. That way, the victim may be able to make better decisions about how to minimize the impact of the identity theft.

For certain types of identity theft, the IRS does send a letter informing identity theft victims that their personal information has been compromised and providing suggestions about what the taxpayer may wish to do (*e.g.*, contact the credit reporting agencies).[16] However, the IRS does not currently send such letters to victims of employment-related identity theft.

---

[14] *See* IRM 4.19.3.3.3.4, *Other Transaction Codes and Math Error Codes* (July 22, 2015).

[15] National Taxpayer Advocate 2011 Annual Report to Congress 63.

[16] *See* IRM 21.9.2.5, *Responses to Identity Theft and Data Loss Notification Letters/Notices* (Oct. 1, 2014).

In July 2014, the IRS conducted a pilot and notified approximately 25,000 taxpayers that their SSN had been misused for employment tax purposes. The pilot targeted taxpayers between the ages of 25 and 65 who had filed a prior year return. The IRS sent these taxpayers a letter advising them of the misuse and suggesting ways they could protect themselves – contact credit bureaus, the Social Security Administration, etc. The IRS is currently exploring the following two recommendations from the pilot:

1) Should the IRS systemically issue letters to the taxpayer informing them the service identified their SSN as compromised?
2) Should the IRS allow those taxpayers the choice to opt-in to obtain an Identity Protection Personal Identification Number (IP PIN)?

III. Social Security Identity Defense Act of 2015[17]

In May of this year, Senators Ron Johnson (R-Wis.), Mark Warner (D-Va.), and Kelly Ayotte (R-N.H.) proposed legislation that would amend IRC § 6103(l)(23) to allow, among other things, the Secretary to disclose to the SSN holder:

- The belief that his or her SSN has been used fraudulently in the employment context;
- That the IRS had reported this identity theft to the Federal Bureau of Investigation (FBI) and Attorney General; and
- Any other information the IRS and the Federal Trade Commission deem helpful and appropriate to share with the identity theft victim.

The IRS is already able to disclose to identity theft victims that someone has misused their SSN to file an unauthorized tax return without this legislation. As mentioned earlier, the IRS completed a pilot program in 2014 and is currently considering whether to expand the use of systemically-generated letters to notify victims of employment-related identity theft, which our office has encouraged the IRS to do since 2011. Thus, while our office continues to urge the IRS to notify victims of employment-related identity theft that their SSN has been compromised, we do not believe this portion of the Social Security Identity Defense Act of 2015 is necessary.

The proposed bill would also allow the FBI and Attorney General to disclose information received from the IRS under this Act to federal, state, and local law enforcement authorities for purposes of carrying out criminal investigations or prosecutions. In a 2012 memorandum, the IRS Office of Chief Counsel noted that Internal Revenue Code (IRC) § 6103(i)(3)(A) allows the disclosure of the "bad return" to appropriate federal law enforcement agencies for purposes of enforcing federal non-tax crimes.[18] This 2012 Counsel memo further concluded that state and local

[17] S. 1323, 114th Cong. (2015).

[18] IRS Office of Chief Counsel Memorandum, *Disclosure Issues Related to Identity Theft*, PMTA 2012-05 (Jan. 18, 2012) ["2012 Counsel memo"], *available at* http://www.irs.gov/pub/lanoa/pmta_2012-05.pdf.

law enforcement agents appointed to the Department of Justice as part of grand jury investigations may access return information under IRC §§ 6103(h)(2) or (i)(1), (i)(2), and (i)(3)(A).

I believe the current framework of privacy and disclosure laws in IRC § 6103 allows the IRS to share sufficient information with federal, state, and local law enforcement. The continuing expansion of the exceptions to the privacy protections afforded by IRC § 6103 may erode taxpayers' confidence in the ability of the IRS to protect sensitive information, and may lead to reduced taxpayer compliance. Furthermore, although the bill specifies that state and local authorities must first enter into a Memorandum of Understanding with the IRS that covers confidentiality of returns/return information and prohibitions on re-disclosure, I remain concerned with how law enforcement agencies may use the information shared by the IRS. Even one incident where law enforcement officials violate taxpayer confidentiality may have a chilling effect on tax compliance among ITIN holders.

IV. Identity Theft Victims' Access to Tax Return Information

In 2009, the IRS Office of Chief Counsel provided guidance regarding whether the IRS could disclose to the victim information furnished by a perpetrator of the identity theft.[19] Counsel concluded that an identity theft victim's own return information may be disclosed to the taxpayer, and that the cause of the events on the taxpayer's account – suspected identity theft and use of the SSN on another return – would also be disclosable to the victim as the taxpayer's return information. However, any other information about the fictitious Form 1040 or the incorrect Form W-2 and any information about the IRS's investigation into the civil or criminal tax liability of the person who misused the SSN ***is not*** the return information of the victim. As such, it may not be disclosed to the victim because the Code provides no authority for disclosure of a third party's return information to that victim, including the perpetrator's identity.

In 2012, the IRS Office of Chief Counsel revisited this issue. Upon further reflection, Counsel revised how it analyzes ownership of tax return information filed by an identity thief. The 2012 Counsel memo concluded that the "bad return," upon its filing and receipt by the Service, is the return information of ***both*** the victim and the alleged identity thief, and thus the IRS may disclose an individual's return information, including a copy of the "bad return," to that individual so long as the disclosure would not impair federal tax administration. However, the Code provides no authority for disclosure of an identity thief's return information (including the identity of the person who filed the "bad return") to an identity theft victim.

[19] IRS Office of Chief Counsel Memorandum, *Identity Theft Returns and Disclosures Under Section 6103*, PMTA 2009-024 (June 8, 2008) ["2008 Counsel memo"], *available at* http://www.irs.gov/pub/lanoa/pmta2009-024.pdf.

Despite the Counsel guidance, the IRS continues to deny requests for copies of tax returns submitted by identity theft victims. IRM 21.3.6.4.3.2, *Return Copy Procedures and Identity Theft* (Aug. 5, 2015), instructs employees ***not*** to provide tax copies of tax returns when identity theft indicators are present on the requestor's account. In 2014, TAS received complaints (via our Systemic Advocacy Management System) from a practitioner who experienced difficulty obtaining transcripts for her clients who have been victimized by identity theft.[20]

On May 6, 2015, Senator Ayotte made a formal inquiry asking the Commissioner why the IRS has continued to deny access to account transcripts, despite the guidance from the 2012 Counsel memo. On May 28, 2015, Commissioner Koskinen responded to Senator Ayotte, stating that the IRS has decided to change its policy regarding the disclosure of fraudulently filed identity theft returns to the victims. The Commissioner explained that while some redaction may be necessary, the IRS would develop procedures to allow identity theft victims to request copies of tax returns filed under their SSN.[21] We support this decision and look forward to the adoption of the new procedures.

V. Fraud Detection

Thus far, I have focused on the victim assistance aspects of identity theft. Now I will share some thoughts on what the IRS has done to prevent identity theft from occurring in the first place. Through improved filters and screening, the IRS was able to detect and stop more than 3.8 million suspicious tax returns in the 2015 filing season (through May 31).[22] The largest component of these suspended returns was attributable to the Taxpayer Protection Program (TPP), where the IRS uses targeted filters to select and suspend the processing of tax returns it suspects were filed by identity thieves. When a TPP filter stops a return, the IRS sends the taxpayer a letter asking him or her to either call the TPP phone number or visit the out of wallet website to verify his or her identity.

This filing season, approximately one out of three returns suspended by the TPP were false positives, meaning that hundreds of thousands of taxpayers who filed legitimate returns had to spend time contacting the IRS to verify their identity.[23] This resulted in a severe backlog of calls to the TPP toll-free phone line. As shown in the figure below, the level of service (LOS) on the TPP line was particularly poor during

[20] *See* TAS, Systemic Advocacy Management System issues 32098 and 32098.

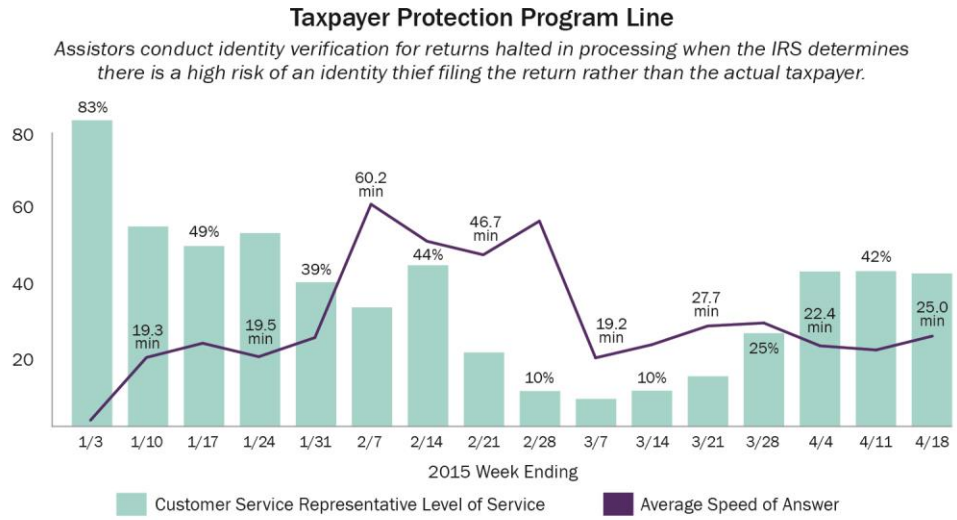
[21] IRM 21.2.3.5.8.1, *Transcripts and Identity Theft* (Aug. 19, 2015), provides that "if the taxpayer requests a transcript of a fraudulent tax return, advise the caller that procedures are currently being finalized."

[22] IRS, *Global Identity Theft Report* (May 31, 2015).

[23] IRS, *IRS Return Integrity & Compliance Services (RICS), Update of the Taxpayer Protection Program (TPP)* 9 (June 24, 2015).

the 2015 filing season, when the LOS dipped below ten percent for three consecutive weeks.[24]

Figure 2



The National Taxpayer Advocate supports the use of data-driven models to detect suspicious tax returns. However, the IRS has an obligation to sufficiently test these filters; a false positive rate of 34 percent is unacceptably high.[25] Furthermore, the IRS has a responsibility to ensure that the phone lines are sufficiently staffed to handle the volume of calls to the TPP. We cannot have a repeat of the 2015 filing season, when far too many legitimate filers were pulled into the TPP, and then were unable to reach an assistor when they called the number instructed.

VI. Conclusion

Identity theft causes significant problems for both the taxpayer and the IRS. As the IRS re-engineers its identity theft victim assistance procedures, it should look at its processes from the perspective of the identity theft victim. Given the multiple points of contact and resultant periods of inactivity, the IRS might find if it adopts our suggestions, that it would actually require **fewer** resources to do the same volume of work. I am confident that taxpayers – our customers – would be much more satisfied with their experience.

[24] For weeks ending February 28, 2015, March 7, 2015, and March 14, 2015, the level of service on the TPP line was 9.7 percent, 7.6 percent, and 9.8 percent, respectively. The IRS attributes the low LOS for the TPP line to a number of factors, including budget challenges that impacted all toll-free lines, problems with the Out-of-Wallet website, and multiple weather-related closures in TPP call sites. Additional staff for TPP were trained and added in late March to improve LOS.

[25] IRS, *IRS Return Integrity & Compliance Services (RICS), Update of the Taxpayer Protection Program (TPP)* 9 (June 24, 2015).

For victims of employment-related identity theft, we encourage the IRS to notify victims of the SSN misuse, as it already does in other types of identity theft. We also support the IRS's decision to release transcripts of tax returns filed under a taxpayer's SSN, with proper redactions to protect the identity of the perpetrator.

I thank the committee for its continued involvement and interest in this matter. I appreciate the opportunity to testify.