WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

THE SPREAD OF TAX FRAUD BY IDENTITY THEFT: A THREAT TO TAXPAYERS, A DRAIN ON THE PUBLIC TREASURY

BEFORE THE

SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH

COMMITTEE ON FINANCE

UNITED STATES SENATE

MAY 25, 2011

TABLE OF CONTENTS

I. The IRS Has Made a Number of Process Improvements to Assist Identity Theft Victims. 2

II. Despite Major Improvements, the IRS Is Seeing Unprecedented Levels of Identity Theft Casework. 3

III. There Are Multiple Likely Explanations for the Increase in Identity Theft Cases. . 4

IV. The IPSU Is Struggling to Effectively Manage Identity Theft Cases. 6

V. The Population of Taxpayer Accounts with an Identity Theft Indicator Has Grown Significantly, Subjecting Almost One Million Accounts to Business Rules. 8

VI. The IRS Does Not Track Identity Theft Case Cycle Time. 9

VII. Recommendations 9

VIII. Conclusion 12

Chairman Nelson, Ranking Member Crapo, and distinguished Members of the Subcommittee:

Thank you for inviting me to testify today about the subject of identity theft.[1] I have written extensively about the impact of identity theft on taxpayers and tax administration and have worked closely with the IRS to improve its efforts to assist taxpayers who are identity theft victims. Over the last three years, the IRS has made significant progress in this area, including adopting many of my recommendations, and it continues to engage my office as it works through new issues. Notwithstanding these efforts and the fact that the IRS has been put in the unenviable position of sorting through the aftermath of a devastating crime, it is clear that the current approach to identity theft is not working as intended.

In my testimony today, I will make the following points:

1. The IRS has made a number of improvements to assist identity theft victims over the past several years.

2. Despite these changes, we are seeing unprecedented levels of identity theft casework.

3. There are several likely explanations for the increase in identity theft cases. Among them: there has been a continued increase in tax-related identity theft; there is increased public awareness of identity theft; identity thieves have become more proficient; and personal information has become more readily accessible.

4. The IRS Identity Theft Protection Specialized Unit (IPSU) is struggling to effectively manage identity theft cases.

5. The population of taxpayer accounts with an identity theft indicator has grown significantly, subjecting almost a million accounts to business rules.

6. The IRS does not track identity theft case cycle time.

7. TAS has made numerous recommendations to address tax-related identity theft. These include allowing taxpayers the option to turn off the ability to file electronically; systematically retiring expired Social Security numbers; utilizing

[1] The views expressed herein are solely those of the National Taxpayer Advocate. The National Taxpayer Advocate is appointed by the Secretary of the Treasury and reports to the Commissioner of Internal Revenue. However, the National Taxpayer Advocate presents an independent taxpayer perspective that does not necessarily reflect the position of the IRS, the Treasury Department, or the Office of Management and Budget. Congressional testimony requested from the National Taxpayer Advocate is not submitted to the IRS, the Treasury Department, or the Office of Management and Budget for prior approval. However, we have provided courtesy copies of this statement to both the IRS and the Treasury Department in advance of this hearing.

information reporting earlier in the filing season; notifying taxpayers of potential identity theft; and working with the Social Security Administration to keep Social Security numbers out of the public domain.

I. The IRS Has Made a Number of Process Improvements to Assist Identity Theft Victims.

In general, identity theft occurs in tax administration in one of two ways – when an individual intentionally uses the Social Security number (SSN) of another person to (1) file a false tax return with the intention of obtaining an unauthorized refund or (2) gain employment under false pretenses. When these types of identity theft occur, the victim often begins a journey through IRS processes and procedures that may take years to complete.

I have written about the growing problem of identity theft in tax administration for many years in my Annual Reports to Congress and in my testimony for various congressional hearings.[2] While it may not have happened as quickly as I would have liked, I am happy to report that the IRS has accepted many of my office's recommendations for improving identity theft procedures. At various times, I have advocated for the following improvements, each of which has been adopted in some capacity:

- Allowance of greater discretion for IRS employees to determine the true owner of an SSN in question without referring the matter to the Social Security Administration (SSA);
- Development of an electronic indicator to mark accounts of verified identity theft victims;
- Creation of an IRS identity theft affidavit form;
- Adoption of a standardized list of acceptable documents to substantiate identity theft;
- Establishment of a centralized unit to provide assistance to identity theft victims;

[2] *See* National Taxpayer Advocate 2009 Annual Report to Congress 307-317 (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 180-191 (Most Serious Problem: *Identity Theft*); National Taxpayer Advocate 2004 Annual Report to Congress 133-136 (Most Serious Problem: *Inconsistence Campus Procedures*); *Filing Season Update: Current IRS Issues, Hearing Before the S. Comm. on Finance*, 111th Cong. (Apr. 15, 2010) (statement of Nina E. Olson, National Taxpayer Advocate); *Identity Theft: Who's Got Your Number, Hearing Before the S. Comm. on Finance*, 110th Cong. (Apr. 10, 2008) (statement of Nina E. Olson, National Taxpayer Advocate).

- Provision for a global account review prior to closing an identity theft victim's account to ensure that all related issues have been resolved; and

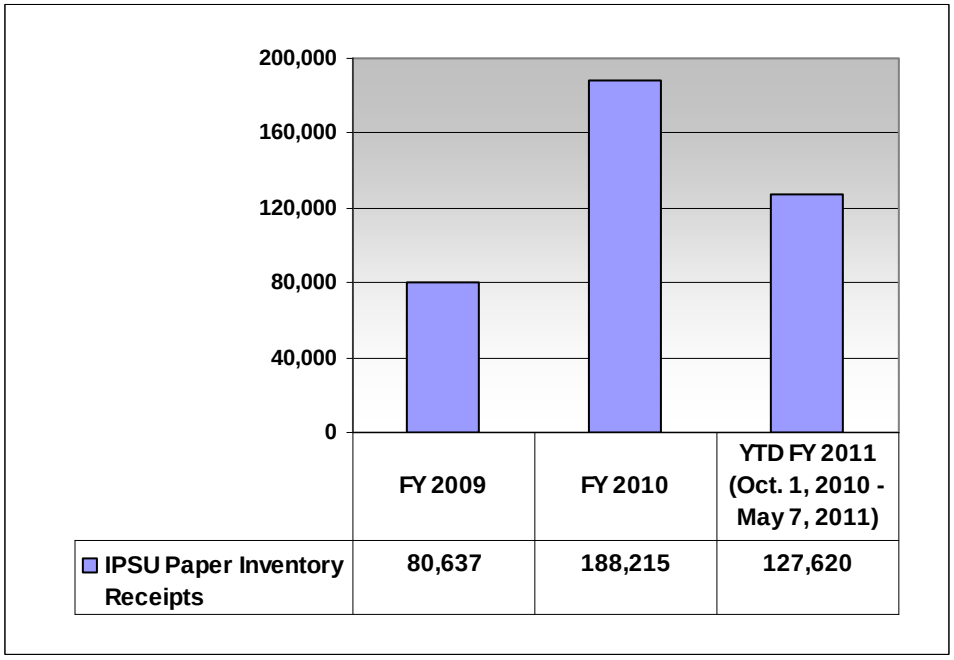
- Issuance of a PIN to verified taxpayers that would enable them to file tax returns electronically.

I can say that the IRS is in a much better position to help identity theft victims today than when I first included identity theft as a Most Serious Problem facing taxpayers in my 2005 Annual Report to Congress. However, there is still room for improvement.

II. Despite Major Improvements, the IRS Is Seeing Unprecedented Levels of Identity Theft Casework.

Despite the sweeping changes made in the last few years, the IRS continues to struggle with identity theft. The Identity Protection Specialized Unit (IPSU), the centralized unit that helps identity theft victims, is experiencing unprecedented levels of case receipts.

Chart 1: IPSU Paper Inventory Receipts, FY 2009 to FY 2011 (thru May 7)[3]



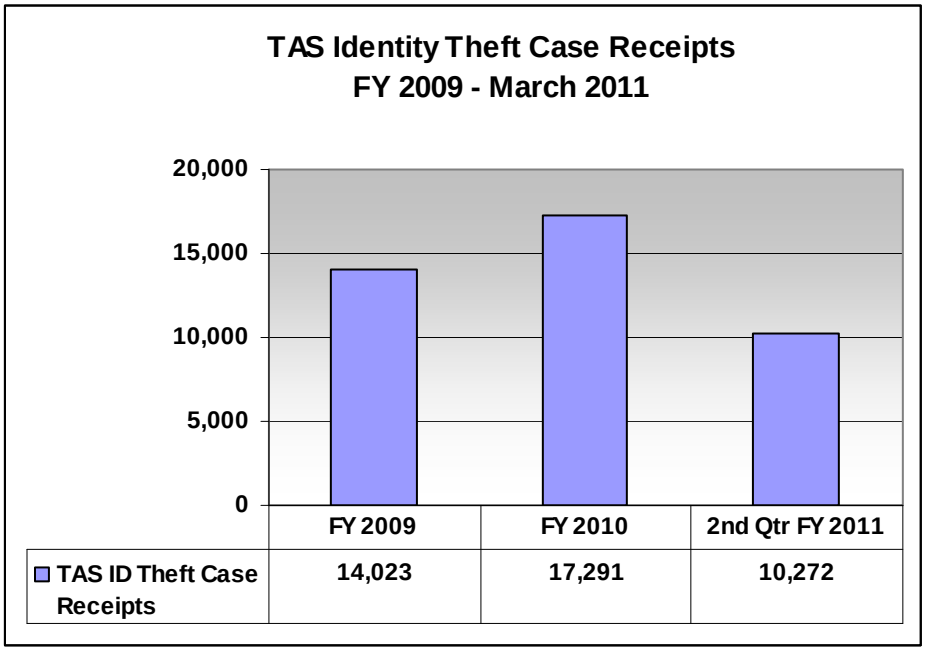
As this chart shows, identity theft cases will be substantially higher in fiscal year (FY) 2011 than they were last year if the trend through May 7 continues. Moreover, in FY 2010, the IPSU worked nearly 3,400 cases that would have otherwise been referred

[3] IRS, *IPSU Identity Theft Report* (May 7, 2011); IRS, *IPSU Identity Theft Report* (Oct. 2, 2010); IRS, *IPSU Identity Theft Report* (Oct. 3, 2009). This inventory includes all identity theft cases controlled by the IPSU paper unit, including self-reported non-tax-related identity theft cases, cases the IPSU monitors, and cases undergoing global account review.

to the Taxpayer Advocate Service (TAS). Through May 7, 2011, this number has already more than doubled, increasing to 7,742 cases so far this year.[4]

The Taxpayer Advocate Service has experienced similar increases in identity theft cases. Through the first two quarters of FY 2011, TAS has received 10,272 identity theft cases, compared to 6,427 cases during the same period in FY 2010 and 5,760 for that period in FY 2009.[5] This translates to a 60 percent increase in identity theft case receipts through the second quarter in FY 2011 over the same period in FY 2010, on top of an almost 12 percent increase in identity theft receipts for that period from FY 2009 to FY 2010. Accordingly, the Taxpayer Advocate Service is also feeling the impact of the IRS's inability to promptly address identity theft victims' tax issues.

Chart 2: TAS Identity Theft Case Receipts, FY 2009 to FY 2011 (thru March 31)



III. There Are Multiple Likely Explanations for the Increase in Identity Theft Cases.

While it is difficult to pinpoint exactly the reasons for the increase in IRS identity theft cases, I can share some possible explanations.

[4] IRS, *IPSU Identity Theft Report* (Oct. 2, 2010); IRS, *IPSU Identity Theft Report* (May 7, 2011). In addition to handling taxpayer cases that would have been designated TAS Criteria 5 – 7 (systemic burden) cases, the IPSU is responsible for identity theft monitoring, taxpayers who self-identify non-tax related identity theft, unpostable cases (*i.e.*, returns that will not be processed until it is manually reviewed), and global account reviews.

[5] TAS Business Performance Management System (Apr. 1, 2011).

a. There Has Been a Continued Increase in Tax-Related Identity Theft.

The increase of such cases in the IRS could simply reflect an overall increase in *tax-related* identity theft as opposed to other kinds of identity theft. Although the Federal Trade Commission (FTC) reports that overall identity theft complaints to its office have actually decreased for the first time since 2006,[6] tax return-related identity theft has increased nearly six percentage points since 2006.[7] The overall decline in incidents reported to the FTC may be attributable in part to the IRS's creation of its own identity theft affidavit in 2009.[8] Prior to 2009, the IRS required identity theft victims to obtain an identity theft affidavit from the FTC and submit it to the IRS to receive assistance.[9]

b. There Is Increased Public Awareness of Identity Theft.

The increase in identity cases may be due to increased public awareness of the issue as a result of more effective outreach. People may be checking their credit reports more frequently and may be more adept in detecting identity theft. If they see suspicious entries in their credit profile, they may contact the IRS to make sure no one has used their SSNs to file a return.

c. Identity Thieves Have Become More Proficient.

Criminals have become more proficient in devising schemes to steal identities. It is apparent that identity thieves are targeting populations that have no filing requirements, such as the elderly and children. Because these individuals often do not file tax returns, it can take years to discover that an identity thief has usurped their SSN. One of the more sinister schemes involves the misuse of a deceased taxpayer's SSN to obtain fraudulent refunds. Thus far in 2011, the IRS has received 660,000 decedent returns.[10] Effective April 17, 2011, the IRS instituted business rules to filter out some of these "decedent scheme" returns; within one month, it stopped 42,441 decedent-related returns claiming questionable refunds estimated at $194 million.[11] The IRS estimates that an additional 221,000 returns claiming $700 million in refunds would have been stopped had the business rules been in place at the beginning of the filing season.[12]

---

[6] *See* Federal Trade Commission, *Consumer Sentinel Data Book* 5 (Feb. 2010), *available at* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf.

[7] *See* Federal Trade Commission, *Consumer Sentinel Data Book* 3 (Feb. 2009), *available at* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf.

[8] *See* Form 14039, *Identity Theft Affidavit* (rev. Mar. 2010), *available at* http://www.irs.gov/pub/irs-pdf/f14039.pdf.

[9] *See* Internal Revenue Manual (IRM) 21.6.2.4.4.3(1) (Oct. 1, 2007) (superseded).

[10] TAS notes from IRS Decedent Schemes conference call (Apr. 25, 2011).

[11] TAS notes from IRS Decedent Schemes conference call (May 12, 2011, and Apr. 21, 2011).

[12] TAS notes from IRS Decedent Schemes conference call (May 12, 2011).

d. Personal Information Has Become Readily-Accessible.

There has been a proliferation of readily-accessible SSNs and other personal information. As I discuss later in the testimony, the Social Security Administration is required to make available certain information about deceased individuals, including their name and SSN. Anyone who conducts a quick web search can find a number of sites that provide this information, often free of charge.

IV. The IPSU Is Struggling to Effectively Manage Identity Theft Cases.

I believe the establishment of the IPSU may have created a false sense of well-being in the IRS with respect to identity theft issues. Commissioner Shulman, in his written response to Senator Baucus's follow-up questions stemming from an April 2008 hearing, described the unit as providing "a central point of contact for the resolution of tax issues caused by identity theft." His response further stated: "This unit will provide end-to-end case resolution. Victims will be able to communicate with one customer service representative to have their questions answered and issues resolved quickly and efficiently."[13] While this description fits the model for which my office advocated, it does not accurately reflect how the IPSU works in practice.

The reality is that the IPSU does not "work" an identity theft case from beginning to end; it simply "monitors" a victim's account every 60 days.[14] Whether because of resource constraints or a policy decision, the IPSU is not staffed to handle cases itself. Rather, it attempts to coordinate with up to 16 different functions within the IRS to obtain the necessary relief for the identity theft victim. The IPSU utilizes Identity Theft Assistance Requests (ITARs) to coordinate with other IRS functions.[15]

While the procedures call for the receiving functions to treat ITARs as a priority, there are no "teeth" to ensure this priority designation is followed. Unlike TAS, which can issue a Taxpayer Assistance Order[16] if another IRS organization does not respond to an Operations Assistance Request,[17] the IPSU procedures do not specify any consequences for functions that are unresponsive to an ITAR.

---

[13] *Identity Theft: Who's Got Your Number, Hearing Before the S. Comm. on Finance*, 110th Cong. (Apr. 10, 2008) (response of IRS Commissioner Douglas H. Shulman to questions from Chairman Max Baucus), *available at* http://finance.senate.gov/hearings/hearing/download/?id=f989b16e-5da3-452d-9675-b75d796fe2b4.

[14] IRM 21.9.2.4.2(4) (Oct. 1, 2010).

[15] IRM 21.9.2.10.1 (Oct. 1, 2010).

[16] *See* IRC § 7811.

[17] An Operations Assistance Request (Form 12412) is the form that TAS employees use when requesting that the IRS complete an action on a TAS case when TAS lacks the authority to take that action.

To illustrate the IPSU's role in the identity theft resolution process, the following example describes the multiple steps necessary to assist a hypothetical identity theft victim who calls the IRS:

1. Taxpayer receives a notice that he has underreported his income for tax year 2008. He calls the number on the notice and learns that the income in question is from a Florida-based company.

2. Because the taxpayer lives in California and has never worked for this company, he suspects he might be a victim of identity theft. He locates the toll-free number for the IPSU telephone unit and explains the situation to the Customer Service Representative (CSR).

3. The IPSU representative verifies that the taxpayer has an open case in the IRS Automated Underreporter (AUR) function.[18] The CSR asks the taxpayer to send documentation substantiating the identity theft to the address on the notice, along with an explanation of why the tax is not owed.[19]

4. The CSR advises the taxpayer that there will be processing delays while the situation is resolved and that he may receive correspondence requesting additional information.[20]

5. The CSR advises the taxpayer that the IPSU will monitor the case and sends a letter to the taxpayer providing him with the name of the person who will be monitoring the account.

6. The IPSU CSR completes the form for monitoring, faxes the monitoring sheet for scanning, makes an account entry documenting the conversation, and refers the case to the IPSU paper unit.[21]

7. The CSR in the IPSU paper unit sends an Identity Theft Assistance Request to the IRS's AUR function to resolve the taxpayer's problem and make the appropriate account adjustments.

8. The IPSU CSR then waits for the account to be resolved and contacts the ID Theft Functional Liaison by e-mail if the function does not contact the taxpayer every 60 days.[22]

---

[18] The AUR Program is a compliance initiative that uses third-party information returns (such as Forms W-2 and Forms 1099) to identify income that was not reported on tax returns.

[19] IRM 21.9.2.3.2(1) (June 11, 2010).

[20] *Id.*

[21] *Id*

[22] IRM 21.9.2.4.2(4) (Oct. 1, 2010).

9. The AUR function eventually agrees that the wages should be removed from the California taxpayer's account, and an identity theft indicator will be applied to his account. For the next three years, any tax return filed with his SSN will have to pass through "business rules," a series of filters designed to kick out questionable returns, before being processed.[23]

10. The following year, the taxpayer is mailed a six-digit Identity Theft PIN.[24] He can use this one-time PIN in conjunction with his paper or electronic return to bypass the business rules. If anyone files a tax return using his SSN without this PIN, that return will be subject to the business rules.

These procedures are a vast improvement over IRS processes in effect as recently as three years ago. However, without adequate staffing in the IPSU and the related functions that make the adjustments on identity theft victims' accounts or that deal with the returns filed by the identity thieves, the benefits of these process improvements will be minimal for both taxpayers and the IRS.

V. The Population of Taxpayer Accounts with an Identity Theft Indicator Has Grown Significantly, Subjecting Almost One Million Accounts to Business Rules.

The IRS may have become a victim of its own success. Since the IRS started using an electronic indicator in 2009 to flag an account as being potentially compromised, it has tracked over 980,000 incidents impacting over 600,000 taxpayers.[25] Each tax return associated with an account marked with an indicator must go through business rules. If a return does not pass these business rules, it will be considered "unpostable" – meaning that it will not be processed until it is manually reviewed, which means longer processing time and refund delays.[26]

Sometimes, it is easy to tell if the wages do not belong to the taxpayer. For example, if the taxpayer is a five-year-old, it is fairly obvious that the income is probably not his. However, if the Unpostable unit cannot quickly determine whether the SSN owner or an unauthorized user filed the return, it will refer the case to the IPSU to conduct research on various databases.[27]

---

[23] *See* IRM 10.5.3.2.2.1.1 (Dec. 10, 2010); IRS Notice CP 01.

[24] IRS Notice CP 01A.

[25] *See* IRS Office of Privacy, Information Protection, and Data Security (PIPDS) Incident Tracking Statistics Reports for calendar years ending 2009 and 2010 and for the period of January 1, 2011, through March 31, 2011.

[26] IRM 21.9.2.5 (Mar. 30, 2010).

[27] IRM 21.9.2.5(2) (Mar. 30, 2010).

If the IPSU determines that the return belongs to the true taxpayer, it instructs the Unpostable unit to process the return. If the IPSU is unable to make a determination, it sends a letter to the "good" taxpayer's address of record seeking additional information and then suspends the case for 45 days.[28]

VI. The IRS Does Not Track Identity Theft Case Cycle Time.

Although the IRS purports to treat ITARs as a "priority," it allows 60 days for the IPSU to follow up with a function to see if the requested action was taken. It is telling that the IPSU does not consider a case "aged" until after 180 days have passed.[29] Unsurprisingly, identity theft cases controlled by the IPSU routinely languish for months without resolution. However, the IRS does not currently track any data about the cycle time for identity theft cases.

The IRS Office of Privacy, Information Protection, and Data Security (PIPDS) recognizes the need for a measure that tracks the length of time it takes the IRS to resolve a taxpayer's identity theft issue. PIPDS has engaged in dialogue with the various functions and with TAS to develop such a measure, but it has yet to implement any meaningful cycle time tracking and analysis. Without the ability to capture this data, it is difficult, if not impossible, for the IRS to determine whether identity theft cases are being treated with the urgency it intends.

VII. Recommendations

Employees from the Wage and Investment division and TAS have formed a team to review a sample of identity theft cases closed between January 1, 2011, and March 31, 2011. It will take a while to review the cases, but the goal is to identify both the underlying source of casework (*e.g.*, Automated Underreporter, Examination, Collection, etc.) and any procedural gaps that contribute to increased receipts. This team expects to report its findings in July of this year.

In advance of these findings, we offer several recommendations that will improve the IRS's approach to identity theft, better protect victims, and prevent revenue loss.

a. Allow taxpayers the option to turn off the ability to file electronically.

The IRS should allow taxpayers to turn off the ability to file electronically. While there are undoubtedly many benefits to e-filing, we must recognize that it also provides more opportunity for identity thieves to "ping" the system with multiple attempts to file fraudulent returns at little cost. For taxpayers (including parents of minor children) who

[28] IRM 21.9.2.5(11) (Mar. 30, 2010).

[29] IRM 21.9.2.1(6) (Oct. 1, 2010).

are victims of identity theft and thus do not wish to e-file, the IRS should allow them to disable e-filing with their SSNs.

b. Utilize information reporting earlier in the filing season.

The IRS should explore ways to utilize information reporting earlier in the filing season. One of the tools it uses to verify wage withholding on questionable returns is the Information Returns Processing Transcript Requests (IRPTR) command code.[30] However, the IRPTR is not available until mid-May. If this resource were available even a month earlier, it would alleviate a great deal of burden for the thousands of taxpayers whose refunds are held up while the IRS undergoes its wage withholding verification process. I have previously recommended that the IRS study how to receive and utilize real-time information reporting data,[31] and I plan to include a more comprehensive analysis of this issue in my 2011 Annual Report to Congress.

c. Work with the Social Security Administration to keep Social Security numbers out of the public domain.

In 1980, the Social Security Administration created a Death Master File (DMF) as a result of a consent judgment reached in a Freedom of Information Act lawsuit brought by a private citizen. In essence, the individual had argued that SSN files are government records and that a deceased individual does not retain a privacy interest in his SSN and related information.

The SSA now makes public significant personal information upon a person's death, including the decedent's full name; SSN; date of birth; date of death; and the county, state, and zip code of the last address on record. This information is now regularly obtained and used by government agencies, credit reporting agencies, financial firms, and genealogists. Unfortunately, it is also used by identity thieves to commit tax fraud.

For tax filing purposes, the SSN of an individual may be used even after his or her death. For example, the surviving spouse of an individual who died in January of 2011 generally may file a joint return for 2011, which would require the decedent's SSN. The due date for the 2011 return, with an extension, would be October 15, 2012 – 20 months after the death occurred. For that reason, the IRS cannot immediately block the use of the decedent's SSN. In the interim, however, identity thieves may troll the DMF to obtain the decedent's SSN and then use it to file a fraudulent return claiming a refund.

---

[30] The IRPTR command code allows IRS employees to request either online or hardcopy Information Returns Processing transcripts from the Information Returns Master File. IRM 2.3.35.1 (Aug. 1, 2003).

[31] National Taxpayer Advocate 2009 Annual Report to Congress 338-345 (Legislative Recommendation: *Direct the Treasury Department to Develop a Plan to Reverse the "Pay Refunds First, Verify Eligibility Later" Approach to Tax Return Processing*).

A similar type of tax fraud arises with respect to dependency claims for minor children. In one recent TAS case that the taxpayers authorized me to discuss publicly, the taxpayers (husband and wife) had a child who died of sudden infant death syndrome (SIDS) in 2009.[32] By law, the couple was entitled to claim the child as a dependent on their 2009 tax return. But by the time they filed their 2009 tax return in 2010, an identity thief had already filed a return claiming their child, so their claim was initially denied.

While I understand the competing policy concerns, the government's provision of all of this information in unredacted form aids and abets identity theft and tax fraud, and it is frankly appalling. It provides identity thieves with the opportunity to steal potentially billions of dollars of federal funds through fraud. It also has the effect of imposing untold burden on the innocent victims of identity theft, who often must spend hundreds of hours to prove who they are and straighten out their finances. Not insignificantly, there is also a compelling personal and emotional consequence to all this. One can only imagine how a taxpayer must feel first to lose a spouse or a child and then find out that his sense of privacy was violated by routine government release of information that allowed someone else to profit from the death and requires him to prove to an initially skeptical government agency that his spouse or child was indeed his relative and not the identity thief's.

I urge Congress and the SSA to address this problem immediately. The most comprehensive solution would be for Congress to pass legislation for the SSA similar to Internal Revenue Code (IRC) § 6103, which prohibits the IRS from releasing taxpayer return information (including SSNs and addresses), absent explicit statutory exceptions or taxpayer consent. (If Congress proceeds along these lines, I recommend that it create a statutory exception for sharing the DMF with the IRS, so the IRS may screen for and ultimately "retire" SSNs of deceased taxpayers from its own databases.) A less comprehensive but quicker solution is for the SSA simply to truncate SSNs in the DMF and make public only the last four digits of the number.[33] If that requires the SSA to ask the court to modify its 1980 consent judgment, it should do so.

d. Systematically retire expired SSNs.

The IRS should systematically retire expired SSNs. The IRS should use the DMF database provided by the SSA to retire the SSNs of decedents, perhaps three years after their death (which should allow sufficient time for the administrator of the decedent's estate to wind down his or her affairs). It is absolutely vital that the SSA continue to provide the IRS with access to the DMF database. Without this resource, the IRS will be unable to systemically and proactively identify questionable returns.

[32] Consent to Disclosure of Tax Return Information (signed May 20, 2011).

[33] In response to an audit conducted by the Office of the Inspector General, the SSA replied "We are considering limiting the information included in the DMF version sold to the public to the absolute minimum required. We will also explore alternatives to the use of the full SSN." Social Security Administration Office of Inspector General, Audit Report A-06-08-18042, *Personally Identifiable Information Made Available to the General Public via the Death Master File* D-4 (June 2008).

Early access to this database will enable the IRS to better proactively and systemically screen out improper returns as they are filed.

e. Notify taxpayers of potential identity theft.

In my 2007 Annual Report to Congress, I recommended that the IRS notify victims if their personal information has been misused.[34] In its response, the IRS committed to work with TAS to develop "a notification process for taxpayers who have been identified by the IRS as identity theft victims related to a refund scheme." While it would do little to stop identity theft, such a letter would alert innocent taxpayers that their personal information may have been compromised. It is my understanding that the IRS received clearance from the IRS Office of Chief Counsel that such a letter, notifying a taxpayer that his or her SSN may have been used by an identity thief, does not violate IRC § 6103 and that draft language has been developed. Yet for reasons unknown to me, the IRS still has not begun to issue such a letter. I urge the IRS to implement its commitment to sending out this notification expeditiously.

VIII. Conclusion

Next month, the IRS Office of Privacy, Information Protection, and Data Security will host a cross-functional Identity Theft Assessment and Action Group kickoff meeting to engage in a servicewide assessment of the identity theft program. The Taxpayer Advocate Service will participate in this working group and will continue to provide assistance and recommendations regarding IRS improvements to its processes to meet taxpayer expectations.

I urge the IRS to re-think its identity theft victim assistance strategy. In 2009, I expressed my desire that the IPSU be structured after the TAS model, where a case advocate works with a taxpayer from beginning to end, ensuring that all of the taxpayer's issues are resolved in a timely manner.[35] As discussed above, the IRS has used a different approach with the IPSU. The IPSU refers identity theft cases to various functions, but it does not have the tools to ensure that these cases receive priority treatment.

I firmly believe that the IRS needs a specialized unit that works solely on identity theft cases from start to finish. Identity theft cases are too complex to be worked any other way. This centralized unit should be staffed appropriately, both in terms of numbers and experience, to deal with the increasingly complex identity theft cases we are seeing. Due to the large volume of identity theft cases, the IRS may need to centralize such a unit in two or more of its campuses. I realize that such an overhaul of the

---

[34] National Taxpayer Advocate 2007 Annual Report to Congress 112 (Most Serious Problem: *Identity Theft Procedures*).

[35] National Taxpayer Advocate 2009 Annual Report to Congress 316 (Status Update: *IRS's Identity Theft Procedures Require Fine-Tuning*).

system will require a substantial investment of resources, and I ask Congress to address this need when it establishes the IRS’s budget.