WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

IDENTITY THEFT-RELATED TAX FRAUD

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY, AND FINANCIAL MANAGEMENT

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

NOVEMBER 29, 2012

TABLE OF CONTENTS

Chairman Platts, Ranking Member Towns, and distinguished Members of the Subcommittee:

Thank you for inviting me to testify today about the subject of identity theft-related tax fraud.[1] I have had the opportunity to address the impact of this subject on taxpayers and to tax administration in four other congressional hearings this year.[2] A month from now, I will submit my 2012 Annual Report to Congress, where I will again discuss identity theft and refund fraud, and describe in detail my continuing concerns with the IRS's approach to victim assistance.

My first of many experiences with identity theft took place when I was the founder and Executive Director of The Community Tax Law Project (CTLP), the first independent nonprofit low income taxpayer clinic in the country.[3] CTLP provides *pro bono* legal representation to low income taxpayers throughout Virginia.[4] In 1993, a legally resident agricultural worker came to CTLP with Internal Revenue Service (IRS) assessments for additional tax purportedly attributable to unreported wages. My client and I spent the next four years proving to the IRS that it was impossible for him to be working and physically present at three different locations at the same instant. Because the identity thieves – several co-workers on a job from years before – continued to work under my client's name and Social Security number (SSN), we had to prove *each year* to the IRS that my client did not earn the unreported income. At that time, the IRS did not have

---

[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.

[2] *See Identity Theft and Income Tax Preparation Fraud*, Hearing Before the H. Comm. on the Judiciary, Subcomm. on Crime, Terrorism, and Homeland Security, 112th Cong. (June 28, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Identity Theft and Tax Fraud*, Hearing Before the H. Comm. on Ways and Means, Subcomm. on Oversight and Social Security, 112th Cong. (May 8, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Tax Compliance and Tax-Fraud Prevention*, Hearing Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency, and Financial Management, 112th Cong. (Apr. 19, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Tax Fraud by Identity Theft Part 2: Status, Progress, and Potential Solutions*, Hearing Before the S. Comm. on Finance, Subcomm. on Fiscal Responsibility and Economic Growth, 112th Cong. (Mar. 20, 2012) (statement of Nina E. Olson, National Taxpayer Advocate).

[3] S*ee generally* Internal Revenue Code (IRC) § 7526. The Low Income Taxpayer Clinic (LITC) program serves individuals whose incomes are below a certain level and require assistance in dealing with the IRS. LITCs are independent from the IRS and most LITCs can provide representation before the IRS or in court on audits, tax collection disputes, and other issues for free or for a nominal fee. IRC § 7526 authorizes the IRS to award matching grants of up to $100,000 per year to qualifying clinics that represent low income taxpayers involved in controversies with the IRS, or that provide education and outreach on the rights and responsibilities of U.S. taxpayers who speak English as a second language.

[4] *See* www.ctlp.org.

any system to flag my client's account and avoid tormenting and burdening him each year.

My experiences as a tax lawyer representing clients in identity theft and other cases have served as a guide in my role as the National Taxpayer Advocate, the "voice of the taxpayer" inside the IRS. The Taxpayer Advocate Service (TAS) is unique in the IRS in that we work our taxpayers' cases from beginning to end. We are also charged, by statute, to make administrative and legislative recommendations to mitigate the problems taxpayers experience with the IRS.[5] As a result, many TAS employees have developed expertise in identity theft over the years.

To its credit, the IRS has adopted many of my office's recommendations to help victims of identity theft and refund fraud. Certainly, identity theft-related tax fraud is not a problem the IRS can fully solve. But I believe that the IRS can do considerably more to assist victims of identity theft.

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

1. The IRS has made significant improvements in its identity theft procedures over the years, but significant challenges remain.

2. The IRS and TAS continue to see unprecedented levels of identity theft casework.

3. Identity theft cases are quite complex, often involving multiple issues and impacting multiple tax years.

4. With the IRS moving away from a centralized approach to identity-theft victim assistance, more taxpayers may fall through the cracks.

5. Even after determining the legitimate owner of an SSN, the IRS does not promptly update the address on the account in question with the address of the identity theft victim, leaving the victim susceptible to further victimization and increasing the likelihood that the victim will not receive legally significant notices.

6. While the identity protection personal identification number (IP PIN) program provides additional security, it covers only part of the identity theft victim population.

7. TAS works closely with the Criminal Investigation division to ensure that identity theft victims receive the attention and assistance they require.

8. The Social Security Administration should restrict access to the Death Master File.

[5] *See* IRC § 7803(c)(2)(A)(iii) & (iv).

I. The IRS Has Made Significant Improvements in Its Identity Theft Procedures Over the Years, but Significant Challenges Remain

When I first started writing about tax-related identity theft in 2004, the IRS literally had no procedures for its employees to follow when taxpayers claimed to be victims of identity theft. Since then, the IRS has established a program office in charge of developing procedures to assist victims of identity theft (now known as the Office of Privacy, Governmental Liaison, and Disclosure, or PGLD). PGLD has adopted many of the recommendations my office has made over the years, some of which I describe below. While the IRS needs to do more, I want to acknowledge the significant progress it has made over the past few years.

Determination of SSN ownership

Just a few years ago, if a taxpayer claimed that another person had used his or her SSN to file a tax return, the IRS would send the case to the Social Security Administration (SSA) to determine the true owner of the SSN, a process that would routinely take two years.[6] In my 2005 Annual Report, I recommended that the IRS train and empower its employees to make determinations of the true SSN owner without involving the SSA. Today, the IRS not only allows its employees to determine SSN ownership based on documentation, but it uses data mining to speed up the process even more. I view this as a significant advance and applaud the IRS for this change.

"Fencing off" of wages

When someone who is not authorized to work in this country seeks employment, he or she must still generally provide a valid SSN to the employer. Often, the undocumented worker will provide to the employer an SSN belonging to another individual. Because the tax code requires taxpayers to report all income "from whatever source derived," these undocumented workers are required to obtain an individual taxpayer identification number (ITIN) and file a tax return using that number.[7] The problem is that the wages are reported on a Form W-2 with someone else's SSN. In the past, a mismatch between an ITIN on a tax return and an SSN on a Form W-2 created problems for the unsuspecting owner of the SSN, who would receive a notice from the IRS that he or she underreported income. I have urged the IRS to develop procedures that will protect victims of identity theft from having to spend unnecessary time and effort proving that they did not earn the wages reported under their SSNs.[8] Today, the IRS has

[6] *See* IRM 21.6.2.4.4.2 (Oct. 1, 2012).

[7] *See* IRC § 61(a).

[8] *See* National Taxpayer Advocate 2005 Annual Report to Congress 185.

procedures to dissociate the wages from the SSN and associate the wages with the ITIN holder's account.[9]

Identity theft affidavit

Initially, the IRS did not have its own identity theft affidavit, and it required victims to complete and submit the Federal Trade Commission (FTC) identity theft affidavit. However, the FTC affidavit contained this statement emblazoned in red ink and capital letters: "DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY." Faced with contradictory instructions from the IRS and FTC, identity theft victims were understandably confused about the purpose and use of the affidavit. In 2007, I recommended that the IRS create its own identity theft affidavit.[10] The IRS has now developed its own ID theft affidavit (Form 14039), which the victim signs under penalty of perjury.

Standardized documentation requirements

An identity theft case frequently involves more than one IRS function. In the past, identity theft victims were required to present different sets of documents to establish their identity with a particular IRS function. It was a burdensome requirement for identity theft victims, who would often correspond with multiple IRS functions during the course of their case resolution. In 2005, I recommended that the IRS establish standardized documentation requirements for taxpayers to substantiate their claim of identity theft and for taxpayers to provide this documentation just once.[11] In 2007, the IRS adopted this recommendation, and procedures are now detailed in the Internal Revenue Manual.[12]

Electronic indicator

In my 2005 Annual Report, I recommended that the IRS consider using an electronic indicator on its master files to mark the accounts of taxpayers who have verified that they have been victims of identity theft. Such an indicator would alert IRS personnel in other departments that this taxpayer might have special needs based on the circumstances and relieve the taxpayer of the burden of proving again that he or she was a victim of identity theft. Use of an indicator would also raise awareness that this taxpayer may have identity theft-related issues in future filing seasons. Today, the IRS uses a transaction code to mark the accounts of taxpayers who have established that they are victims of identity theft. Such an indicator not only enables the IRS to protect the victims' accounts from future identity theft, but it also allows the IRS to track the number of identity theft cases and the amount of time it takes to close them.

---

[9] *See* IRM 4.19.3.15.1.3, *Withholding and ITIN Filers* (Oct. 2, 2012).

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

[11] *See* National Taxpayer Advocate 2005 Annual Report to Congress 185.

[12] *See* IRM 10.5.3.2.7 (July 9, 2012).

Centralized ID theft unit

In 2007, I recommended that the IRS develop a dedicated, centralized unit to handle all identity theft cases. In 2008, the IRS established the Identity Protection Specialized Unit (IPSU) to assist identity theft victims. As I describe more fully later in this testimony, I have concerns about the limited role of the IPSU. I believe the IPSU should serve as the single point of contact with the identity theft victim and serve as the "traffic cop" to help the taxpayer navigate the various IRS functions that may touch the identity theft case.

Despite these improvements, the IRS still faces significant challenges in handling identity theft cases. The increasing levels of identity theft cases have driven the IRS to move away from a central overseer of this casework, increasing the risk that more taxpayers will fall through the cracks or come to TAS for help. The IRS still does not provide adequate taxpayer service to victims of identity theft, waiting too long to update the address of the legitimate owner of the SSN, and unnecessarily increasing the risk of continued harm to the victim and revenue loss to the government. The federal government, through the release of the Death Master File, still makes available to the public at large, including identity thieves, taxpayers' personally identifying information.

II. The IRS and TAS Continue to See Unprecedented Levels of Identity Theft Casework

As I have written in my Annual Reports to Congress since 2004, tax-related identity theft is a serious problem – for its victims, for the IRS and, when Treasury funds are improperly paid to the perpetrators, for all taxpayers.[13] In general, tax-related identity theft occurs when an individual intentionally uses the SSN of another person to file a false tax return with the intention of obtaining an unauthorized refund.[14] Identity theft wreaks havoc on our tax system in many ways. Victims not only must deal with the aftermath of an emotionally draining crime, but may also have to deal with the IRS for

[13] *See* 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 307-317 (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*).

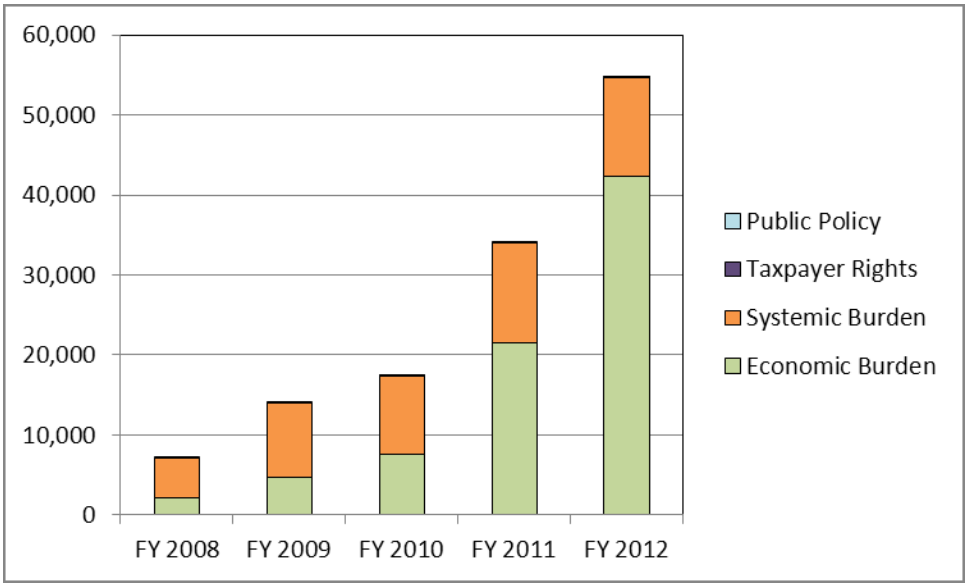
[14] We refer to this type of tax-related identity theft as "refund-related" identity theft. In "employment-related" identity theft, an individual files a tax return reporting his actual wages using his or her own taxpayer identifying number (usually an Individual Taxpayer Identification Number or ITIN), but uses another individual's SSN in order to obtain employment, and consequently, the wages are reported to the IRS under the SSN. Unlike in 1993, when I first represented a client in an identity theft case, the IRS now has procedures in place to minimize the tax administration impact to the victim in these employment-related identity theft situations. Accordingly, I will focus on refund-related identity theft in this testimony.

years to untangle the resulting tax account problems. Identity theft also impacts the public fisc, as Treasury funds are diverted to pay out improper refunds claimed by opportunistic perpetrators. In addition, identity theft takes a significant toll on the IRS, tying up limited resources that could otherwise go toward improving taxpayer service or compliance initiatives.

Today, identity theft can be an organized, large-scale criminal operation. The most recent IRS data show nearly 650,000 identity theft cases in inventory servicewide.[15] I would love to be able to report on the upward trend of identity theft cases IRS-wide from the past several years, but the IRS does not have this data. Until this year, the IRS had no ability to track identity theft case inventory, much less monitor the time it takes to resolve such cases.

I firmly believe that the failure of the IRS to take prompt action on my office's recommendations in the early years – when the volume of identity theft cases was relatively modest – has led to the crisis we have today. When established IRS procedures do not work as intended, taxpayers turn to the Taxpayer Advocate Service for assistance. The volume of identity theft cases in TAS has risen each year since the IRS established the IPSU, from about 7,100 in FY 2008 to nearly 55,000 in FY 2012, an increase of more than 650 percent.[16]

FIGURE 1, TAS Stolen Identity Case Receipts, FY 2008 to FY 2012[17]



[15] IRS, Identity Theft Advisory Council, *Identity Theft Status Update* (Oct. 24, 2012). As of September 30, 2012, there were 646,950 identity theft cases servicewide.

[16] Data obtained from TAMIS on Oct. 16, 2012. TAS received 7,147 identity theft cases in FY 2008, compared to 54,748 in FY 2012, a 666.0 percent increase.

[17] Data obtained from TAMIS on Oct. 16, 2012. TAS received 54,748 identity theft cases in FY 2012, out of 219,666 cases overall (24.9 percent).

In FY 2012, identity theft cases constituted 25 percent of TAS's receipts, more than any other issue in our inventory. Moreover, identity theft has been the top issue in TAS case receipts for the last two fiscal years.

III. Identity Theft Cases Are Quite Complex, Often Involving Multiple Issues and Impacting Multiple Tax Years

When TAS case advocates receive a case, they assign Primary and (one or more) Secondary Issue Codes to the case, indicating what issues are involved and, by inference, what other IRS functions TAS must work with to resolve all the tax issues completely before closing the case. The vast majority of TAS identity theft cases encompass multiple issues and tax years, as shown in the table below.

FIGURE 2, FY 2012 TAS Identity Theft Closures by Secondary Issue[18]

Top Ten Secondary Issues	Closed Cases	Avg. Case Age (Days)
Unspecified[19]	13,306	95
020 - Expedite Refund Requests	9,216	98
310 - Processing Original Returns	5,582	109
045 - Pre-Refund Wage Verify Hold	5,529	86
315 - Unpostable/Reject	3,190	74
330 - Processing Amended Returns	1,046	112
090 - Other Refund Inquiries	974	115
040 - Returned/Stopped Refunds	848	92
410 - Multiple/Mixed TIN	813	132
060 - IRS Offset	669	139
670 - Closed Automated Underreporter	603	133
All Other Secondary Issues	4,846	132
Total	**46,622**	**101**

Each case that comes in to TAS is assigned to a case advocate, who identifies potential related issues and keeps the case open until all related issues are resolved. For example, if a taxpayer has a problem with an unpostable return, TAS would need to interact with the Submission Processing function. If the case issues relate to wage or withholding verification, TAS would coordinate with the Accounts Management Taxpayer Assurance Program function. With levy or offset issues, TAS may need to

[18] Data obtained from TAMIS on Oct. 16, 2012.

[19] Pursuant to TAS guidance, identity theft cases, by definition, have at least one secondary issue. However, a portion of TAS identity theft cases did not specify a secondary issue code, which is an error.

deal with the Collection function. Any given case could involve several tax years with any combination of these issues.

In contrast, the vast majority of the IRS's identity theft cases are being worked by Accounts Management (AM). AM does not look back at the taxpayer's filing history to conduct a global account review and address all related issues, but focuses on the issue before it. I believe that because the IRS does not take the holistic approach to case resolution that TAS employs, the IRS vastly underestimates the complexity of the typical identity theft case. I am concerned that the IRS is making strategic decisions based on a distorted view of how difficult it can be to fully unwind an identity theft case.

IV. With the IRS Moving Away from a Centralized Approach to Identity Theft Victim Assistance, More Taxpayers May Fall Through the Cracks

In former Commissioner Shulman's first month in office in 2008, he testified before the Senate Finance Committee on identity theft. At this hearing and through his responses to follow-up questions, the Commissioner described his vision for addressing the issue. In describing the IPSU, the Commissioner 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…. We have found that over time, identity theft cases can be handled by approximately 24 functional areas of the IRS, including customer service, tax return processing, and compliance, and we believe this unit will assist taxpayers whenever the need arises in dealing with identity theft.[20]

The National Taxpayer Advocate generally agrees with the approach outlined by the Commissioner in 2008 – a single point of contact, seamless assistance, and prompt resolution. However, it is clear that the promises made by the Commissioner are not being fulfilled. Not only has the IRS failed to achieve the goals expressed by the Commissioner in 2008, but it is moving backward. The IRS is heading toward a *decentralized* approach to aiding identity theft victims, who are unlikely to describe the assistance they receive as "quick" or "efficient." In short, it is replacing the 24 units the Commissioner identified as a problem in 2008 with 21 units today – a far cry from the single point of contact envisioned by the Commissioner.

In 2011, the IRS convened a task force to evaluate its victim assistance strategy. In the view of many participants, the external consulting firm leading this task force came in with the pre-conceived notion that the IRS should move away from centralized victim assistance and toward a specialized approach. It was based on a recommendation from this task force that the IRS leadership decided to create a specialized unit within each of its 21

[20] *See Identity Theft in Tax Administration*, Hearing Before the Senate Committee on Finance, 110th Cong. (Apr. 10, 2008) (statement of Doug Shulman, IRS Commissioner).

individual departments (or functions) to work on identity theft cases.[21] Under this approach, identity theft cases would be assigned to specially trained employees in each function. If an identity theft case involves multiple issues, the case may be transferred to a specialized unit in a different function to address the additional issue(s).[22]

The IRS maintains that transfers will be the exception rather than the rule, but based upon TAS's experience with identity theft cases over the years, it is foreseeable that transfers between functions will become commonplace. Since the IRS does not track all issues raised in an identity theft case and instead takes a piecemeal approach to victim assistance, and because no one employee has been responsible for all aspects of the case, the IRS has no data on the complexity of the cases. Thus, the IRS is designing its procedures based on flawed assumptions.

In 2012, each function was asked to develop procedures for its embedded identity theft unit. PGLD has been compiling and reviewing such procedures to ensure some level of consistency. Although TAS asked to review these procedures – and the procedures for when a taxpayer's case should be moved from one embedded unit to another – before these embedded units became operational in October 2012, we were not afforded this opportunity in all instances. At least three of these embedded specialized units began work without having their procedures reviewed by TAS.[23]

I agree that, when properly designed, specialized units within various IRS functions staffed with employees who are familiar and skilled with identity theft issues should improve the speed and quality of identity theft case handling. However, I also firmly believe that the IRS needs a centralized body (such as the IPSU) to serve as the "traffic cop." As noted earlier, identity theft cases are often complex, requiring adjustments by multiple IRS departments.[24] Without a case coordinator, the risk that cases requiring involvement from multiple functions will get "stuck" or fall through the cracks is high. The IPSU has already been serving in this capacity for four years. Under the new, specialized approach to identity theft victim assistance, it is unclear what the role of the IPSU will be. In my view, the IPSU

---

[21] IRS, *Identity Theft Assessment and Action Group (ITAAG) Future State Vision and Supporting Recommendations* 44 (Oct.11, 2011).

[22] To transfer a case to another unit, the function must submit a transfer request to the office of Privacy, Governmental Liaison, and Disclosure, which is currently developing a transfer matrix to facilitate such transfer requests.

[23] Two centralized compliance teams were created to complete the identity theft post-function adjustment work; Examination no longer refers identity theft post-function adjustment work to Accounts Management. All Large Business & International (LB&I) and Small Business/Self-Employed (SB/SE) compliance referrals will be routed to the Designated Identity Theft Adjustment (DITA) team located in Philadelphia. All Wage and Investment (W&I) referrals will be routed to the Compliance Post Adjustment Teams (CPAT) located in Austin and Fresno. The CPAT and DITA units stood up in April 2012, but TAS did not receive procedures until October 2012. Submission Processing's embedded unit became operational in October 2012, without first sharing its procedures with TAS.

[24] An IRS task force found that up to 28 different functions may touch an identity theft case. IRS, *Identity Theft Assessment and Action Group (ITAAG) Future State Vision and Supporting Recommendations* 7 (Oct. 11, 2011).

should remain the single point of contact for victims, tracking each case from start to finish as it moves from one specialized unit to another. Each function should have a liaison and service level agreement with the IPSU and be held accountable for meeting established deadlines for taking actions.[25]

In addition, the IPSU should continue to serve an important role in this process by conducting a global account review on all identity theft cases. To provide the best service, the IPSU should conduct two global account reviews – an initial one to identify all related issues prior to transferring the case to the appropriate specialized units, and a final global review to ensure that all issues have been resolved prior to closing any identity theft case. Despite its "specialized" moniker, the IPSU should actually operate as a hub in a centralized environment to ensure a "seamless" experience for the victim.[26]

V. Even After Determining the Legitimate Owner of an SSN, the IRS Does Not Promptly Update the Address on the Account in Question with the Address of the Identity Theft Victim, Leaving the Victim Susceptible to Further Victimization and Increasing the Likelihood That the Victim Will Not Receive Legally Significant Notices

Identity thieves typically file early in the tax filing season, well in advance of the true owner of the SSN. The IRS often has no way of knowing that the first return received is from an identity thief. As a result, the IRS will process the return and its systems will automatically update the last known address on the taxpayer's account with the address provided by the perpetrator. This address becomes the address of record where notices are sent for all open years, including years for which the identity theft has not filed returns.[27]

When the true owner of the SSN contacts the IRS, he or she will be asked to provide several documents to substantiate his or her identity and address. While the IRS takes this information and corroborates the identity and address of the identity theft victim, it

[25] A service level agreement (SLA) outlines the procedures and responsibilities for the processing of casework when the authority to complete certain case actions rests outside of one organization, operating division, or function. The SLA defines roles and responsibilities, and includes procedures for elevating disagreements. TAS established SLAs with each OD/function for the processing of TAS Operations Assistance Requests (OARs). The SLAs identify timeframes for acknowledging and assigning OARs, procedures for handling disagreements over actions requested or timeframes for completing actions.

[26] From the outset, the National Taxpayer Advocate has inquired about the role of the IPSU in the new specialized environment. After months of nonresponsiveness, the IRS finally created a team to look at the IPSU and invited TAS to participate. However, the "IPSU re-engineering" team that TAS was invited to join appears to have no real decision-making authority with respect to the IPSU's interaction with the embedded specialized units.

[27] Treas. Reg. § 301.6212–2(a) generally provides that a taxpayer's last known address is the one that appears on the taxpayer's most recently filed and properly processed return.

does not update the address on the account until after the case is fully resolved.[28] This decision to delay updating the address has a detrimental impact on taxpayer rights, as the identity theft victim may not receive IRS notices with legal significance – such as a statutory notice of deficiency or a collection due process notice.[29] The fact that the IRS has had the correct address of the taxpayer from the beginning of the case, yet chooses not to update the address until the close of the case (typically in excess of six months[30]) illustrates how difficult it is for the IRS to keep taxpayer rights in the forefront.

VI. While the Identity Protection Personal Identification Number (IP PIN) Program Provides Additional Security, It Covers Only Part of the Identity Theft Victim Population

For the 2012 filing season, the IRS introduced a number of identity theft-related process improvements. For example, to provide a greater level of security for taxpayers, the IRS issued identity protection personal identification numbers or IP PINs to about 250,000 victims whose identities and addresses it has verified.[31] An IP PIN is a unique code that the taxpayer must use, along with his or her taxpayer identification number, to file electronically and bypass certain filters. Letters went out in December 2011, instructing the victims to use the IP PINs to file their 2011 returns. If the taxpayer attempts to e-file without that number, the IRS will not accept the e-filed return and the taxpayer will need to file a paper return, which will delay processing.

For the 2013 filing season, the IRS plans to expand the IP PIN program to more than 500,000 participants. I support expansion to as many verified identity theft victims as possible, provided the IRS can validate their current addresses. In general, the IRS does not issue IP PINs until after the victim's account is fully resolved. I have pushed the IRS to begin protecting the identity theft victim as soon as the SSN owner and address are verified. Tying the IP PINs to the *closing* of the identity theft case unnecessarily delays this protection.

Last month, I expressed concern to the Wage & Investment Division (W&I) management that the nearly 22,000 taxpayers with stolen identity cases in TAS

---

[28] *See, e.g.*, IRM 10.5.3.2.9, *Closing Identity Theft Issues* (July 9, 2012). *See also* e-mail dated Nov. 14, 2012, from a tax practitioner (alerting me of this harmful IRS practice).

[29] Rev. Proc. 2010-16, 2010-19 I.R.B. 664, explaining how the IRS is informed of a change of address, identifies 20 Code sections that require notices and documents to be sent to the taxpayer's last known address, including the IRC § 6212(b) notice of deficiency, the IRC § 6320(a)(2)(C) notice and opportunity for hearing upon filing of notice of lien, and the IRC § 6330(a)(2)(C) notice and opportunity for hearing before levy. If the taxpayer does not respond to a valid statutory notice of deficiency, IRC § 6213(c) requires the IRS to assess the tax. The taxpayer can no longer obtain judicial review without first paying the tax. A taxpayer who does not respond to a valid IRC § 6330 or § 6320 notice loses not only the right to an administrative hearing, but also the right to pre-enforcement judicial review.

[30] The IRS monitored tax-related identity theft cases for an average of 196 days.

[31] The IRS issued 251,568 IP PINs. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Aug. 23, 2012).

inventory would not receive the benefit of the protections afforded by the IP PIN for the 2013 filing season, which means their accounts would be unprotected from fraudulent filings and they would be forced to file their legitimate returns on paper.[32] The W&I Accounts Management unit shared this concern and worked quickly with TAS to develop a work-around solution. For identity theft cases that have been through the Electronic Fraud Detection System, the IRS will place one indicator on the account to signify the true SSN owner and a different indicator on the account to signify the non-SSN owner.

While I am pleased to report that these taxpayers will be eligible to receive the IP PIN for use in the 2013 filing season and appreciate AM working with us, I am disappointed that it took a last-minute fire drill to accomplish this result. The IRS had ample opportunity to verify the taxpayer addresses and input a marker making the verified taxpayer eligible to receive an IP PIN. Until the IRS changes its procedures to place the IP PIN marker on accounts upon verification rather than closure, the IRS will continue to waste resources on one-off adjustments and work-arounds.

VII. TAS Works Closely with the Criminal Investigation Division to Ensure Identity Theft Victims Receive the Attention and Assistance They Require

For many perpetrators, tax return fraud may be viewed as a low-risk, high-reward venture. News reports suggest some very organized groups have chosen tax-related identity theft as the crime du jour.[33] Identity theft has become a large-scale operation, with "boiler room" operations involving the theft of massive lists of SSNs. Apparently, there are networks of criminals who not only share stolen personal information, but even present seminars about how to use this information to file bogus returns.[34] Such brazen behavior suggests that identity thieves are not worried about criminal prosecution.

I am pleased to report that the IRS's Criminal Investigation division (CI) doubled the number of convictions against identity thieves in FY 2011. CI initiated 276 fraud cases related to identity theft, with 81 convictions – up from 224 investigations and 40 convictions in FY 2010.[35] To respond more nimbly to identity theft situations, CI now

---

[32] As of October 16, 2012, there were 21,908 open stolen identity cases in TAS.

[33] According to one report, suspects are teaching classes of 50 to 100 people at a time on how to file fraudulent returns. *See* Tampa Bay Times, "49 Accused of Tax Fraud and Identity Theft" (Sept. 2, 2011), *available at* http://www.tampabay.com/news/publicsafety/crime/49-accused-of-tax-fraud-and-identity-theft/1189406; Tampa Bay Online, "Police: Tampa Street Criminals Steal Millions Filing Fraudulent Tax Returns," *at* http://www2.tbo.com/news/politics/2011/sep/01/11/police-tampa-street-criminals-steal-millions-filin-ar-254724/.

[34] *See, e.g.*, Tampa Bay Times, "49 Accused of Tax Fraud and Identity Theft," (Sept. 2, 2011), *available at* http://www.tampabay.com/news/publicsafety/crime/49-accused-of-tax-fraud-and-identity-theft/1189406; Tampa Bay Online, "Police: Tampa Street Criminals Steal Millions Filing Fraudulent Tax Returns," *at* http://www2.tbo.com/news/politics/2011/sep/01/11/police-tampa-street-criminals-steal-millions-filin-ar-254724/.

[35] Data obtained from the IRS Criminal Investigation division's research function (Mar. 13, 2012).

has a designated liaison for identity theft in each of its major offices, but more action is required.

My office has worked closely with CI over the last few years to make sure that where CI has identified a scheme and has lists of victims' SSNs, this information is quickly transferred to the civil side of the IRS so the victims are notified and identity theft markers are placed on their accounts. We have coordinated with CI and the Department of Justice on certain cases to ensure victims receive notification and are informed about avenues for assistance at the IRS. Only through detection, prosecution, and victim assistance will we be able to comprehensively address the rise of tax-related identity theft.

VIII. The Social Security Administration (SSA) Should Restrict Access to the Death Master File

I am concerned that the federal government continues to facilitate tax-related identity theft by making public the Death Master File (DMF), a list of recently deceased individuals that includes their full name, SSN, date of birth, date of death, and the county, state, and ZIP code of the last address on record.[36] The SSA characterizes release of this information as "legally mandated,"[37] but the extent to which courts currently would require dissemination of death data under the Freedom of Information Act (FOIA)[38] has not been tested. To eliminate uncertainty, I have recommended that Congress pass legislation to clarify that public access to the DMF can and should be limited.[39]

The public availability of the DMF facilitates tax-related identity theft in a variety of ways. For example, a parent generally is entitled to claim a deceased minor child as a dependent on the tax return that covers the child's year of death. If an identity thief obtains information about the child from the DMF and uses it to claim the dependent on a fraudulent return before the legitimate taxpayer files, the IRS will stop the second (legitimate taxpayer's) return and freeze the refund. The legitimate taxpayer then may face an extended delay in obtaining the refund, potentially causing an economic hardship, and will bear the emotionally laden burden of persuading the IRS that the deceased child was really his or hers.[40] Legislation could relieve survivors of this burden by simply delaying release of the information for several years.

---

[36] *See* Office of the Inspector General, SSA, *Personally Identifiable Information Made Available to the General Public via the Death Master File*, A-06-08-18042 (June 2008).

[37] *Social Security and Death Information* 1, Hearing Before H. Comm. on Ways & Means, Subcomm. on Soc. Security (statement of Michael J. Astrue, Commissioner of Social Security) (Feb. 2, 2012).

[38] FOIA generally provides that any person has a right to obtain access to certain federal agency records. *See* 5 U.S.C. § 552.

[39] *See* National Taxpayer Advocate 2011 Annual Report to Congress 519-523 (Legislative Recommendation: *Restrict Access to the Death Master File*).

[40] The full impact to families is demonstrated by a recent case described by a Low Income Taxpayer Clinic (LITC) to TAS in its interim grant report. A young woman was murdered, leaving her young children

In light of the practical difficulties of passing legislation, however, I also urge the SSA to reevaluate whether it has the legal authority to place limits on the disclosure of DMF information administratively. In the 1980s, the SSA created the DMF, now issued weekly, after an individual filed suit in the U.S. District Court for the District of Columbia seeking certain data fields pursuant to FOIA and the court entered a consent judgment in the case pursuant to an agreement reached by the parties.[41] While the 1980 consent judgment may have seemed reasonable at the time, the factual and legal landscape has changed considerably over the past three decades.

From a factual standpoint, DMF information was sought in 1980 as a way to prevent fraud by enabling pension funds to identify when a beneficiary died so they could stop the payment of benefits. Today, DMF information is used to commit tax fraud, so there is a factual basis for keeping the information out of the public domain.

From a legal standpoint, judicial interpretations of FOIA and its privacy exceptions have evolved in several important respects, including the recognition of privacy rights for decedents and their surviving relatives.

In general, agencies receiving FOIA requests for personal information must balance (1) the public interest served by release of the requested information against (2) the privacy interests of individuals to whom the information pertains.[42]

In 1989, the Supreme Court reiterated that the public's FOIA interest lies in learning "what their government is up to."[43] The Court continued:

---

to be raised by their grandmother. The deceased woman was a wage earner and entitled to a sizeable refund for the tax year in which she was murdered. The grandmother sought assistance from the LITC after the daughter's income tax return for that tax year was returned to her by the IRS with a request for Form 56, *Notice Concerning Fiduciary Relationship*. After obtaining an order from Probate Court naming the grandmother as personal representative of the estate, the return was resubmitted. The LITC then discovered that an earlier return had been e-filed by an identity thief using the deceased woman's name and SSN and claiming a refund based on fictitious income. The LITC assisted the grandmother in filing an identity theft affidavit. The case was referred to the IRS's IPSU to which the LITC was required to submit additional evidence of the grandmother's identity and claims. The grandmother finally received her daughter's refund more than a year after the original return was due.

[41] *See Perholtz v. Ross*, Civil Action Nos. 78-2385, 78-2386 (D.D.C. Apr. 11, 1980).

[42] *See, e.g.*, *Department of Defense v. Federal Labor Relations Authority*, 510 U.S. 487, 497 (1994); *Department of Justice v. Reporter's Committee for Freedom of the Press*, 489 U.S. 749, 773 (1989). This balancing applies to information described in FOIA Exemption 6, 5 U.S.C. § 552(b)(6) ("personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"), which would encompass files like the DMF. *See Department of State v. Washington Post Co*., 456 U.S. 595, 599-603 (1982); *see also Judicial Watch, Inc. v. Food & Drug Administration*, 449 F.3d 141, 152 (D.C. Cir. 2006).

[43] *Department of Justice v. Reporter's Committee for Freedom of the Press*, 489 U.S. at 773 (quotation omitted).

> Official information that sheds light on an agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct.[44]

Following the Supreme Court's reasoning, the Court of Appeals for the D.C. Circuit rejected a request for a list of names and addresses of retired or disabled federal employees, concluding that release of the information could "subject the listed annuitants 'to an unwanted barrage of mailings and personal solicitations,'" and that such a "fusillade" was more than a *de minimis* assault on privacy.[45]

The courts have increasingly found that privacy rights do not belong only to living persons. In 2001, the D.C. Circuit stated that:

> the death of the subject of personal information does diminish to some extent the privacy interest in that information, though it by no means extinguishes that interest; one's own and one's relations' interests in privacy ordinarily extend beyond one's death.[46]

The courts have reiterated that decedents and their surviving relatives possess privacy rights in numerous cases.[47] In the decided cases, the privacy interest at issue generally has consisted exclusively of emotional trauma. Where there is tax-related identity theft, the privacy interest is much stronger because there is a financial as well as an emotional impact. For example, a parent who has lost a child to Sudden Infant Death Syndrome and then discovers an identity thief has used the DMF to claim his child as a dependent must not only devote time trying to prove to the IRS that he was the legitimate parent, but he must also deal with the financial burden of having his tax return (and refund) frozen.

---

[44] *Id. See also National Archives & Records Administration v. Favish*, 541 U.S. 157, 171 (2004) (quotation omitted) ("FOIA is often explained as a means for citizens to know 'what the Government is up to'").

[45] *National Association of Retired Federal Employees v. Horner*, 879 F.2d 873, 876 (D.C. Cir. 1989) (quotation omitted), *cert. denied*, 494 U.S. 1078 (1990).

[46] *Schrecker v. Department of Justice*, 254 F.3d 162, 166 (D.C. Cir. 2001) (citations omitted), *reiterated on appeal following remand*, 349 F.3d 657, 661 (D.C. Cir. 2003).

[47] *See, e.g., National Archives & Records Administration v. Favish*, 541 U.S. at 170 ("FOIA recognizes surviving family members' right to personal privacy with respect to their close relative's death-scene images."); *Accuracy in Media, Inc. v. National Park Service*, 194 F.3d 120, 123 (D.C. Cir. 1999) (noting that the D.C. Circuit "has squarely rejected the proposition that FOIA's protection of personal privacy ends upon the death of the individual depicted"); *Campbell v. Department of Justice,* 164 F.3d 20, 33 (D.C. Cir. 1998) ("The court must also account for the fact that certain reputational interests and family-related privacy expectations survive death."); *New York Times v. National Aeronautics & Space Administration,* 782 F. Supp. 628 (D.D.C. 1991) (concluding that NASA was not required to release audio tapes of the final minutes aboard the Challenger space shuttle).

Consider two legitimate uses of DMF information. One is by pension funds that use the information to terminate benefits as of the date of a beneficiary's death. The other is by genealogists who use DMF information to help them build a family tree. While both uses are reasonable, neither fits within the core purpose of FOIA of alerting the citizenry about "what their government is up to." The D.C. Circuit has held that where disclosure does not serve the core purpose of FOIA, no public interest exists, and any personal privacy interest, however modest, is sufficient to tip the balance in favor of nondisclosure.[48] Even if a court were to decide that the DMF does serve a core FOIA purpose, it would balance the public and privacy interests and could easily conclude that the privacy interests predominate.

Thus, if legislation is not forthcoming, I urge the SSA to reconsider its legal analysis and take steps to restrict access to the DMF.[49]

IX. Conclusion

As I have stated, my office is unique in that my case advocates work every case from beginning to end, allowing us to make observations about the complexity of identity theft cases and pinpoint areas where IRS procedures are insufficient to fully resolve the problems. Each year, my office makes numerous recommendations to improve IRS identity theft victim assistance procedures. We have seen the IRS adopt many of our recommendations, often after initially resisting them. I first started focusing on this issue in 2004, when the IRS's identity theft caseload was at a more manageable level. By waiting years to adopt our recommendations, the IRS has put itself in a difficult position today, when the volume of cases is overwhelming. I urge the IRS to take advantage of TAS's vast experience dealing with identity theft cases and work together with TAS in developing its identity theft victim assistance strategy.

That said, identity theft-related tax fraud will continue to pose significant challenges for the IRS, as opportunistic thieves will always try to game the system. From their perspective, the potential rewards of committing tax-related identity theft may be worth the risk. We can do more both to reduce the rewards (by continuing to implement targeted filters) and to increase the risk (by actively pursuing criminal penalties against those who are caught). But in making the tax system less attractive to such criminal activity, we must do our best to avoid imposing additional burdens on legitimate taxpayers.

---

[48] *National Association of Retired Federal Employees v. Horner*, 879 F.2d at 879.

[49] The SSA may be able to restrict access to the DMF without even asking the court to modify its consent judgment in *Perholtz v. Ross*, Civil Action Nos. 78-2385, 78-2386 (D.D.C. Apr. 11, 1980). By its terms, the consent judgment applies only to requests for updated information submitted by Mr. Perholtz himself, is limited to one request per year, and covers only a decedent's "social security number, surname and (as available) date of death." Our understanding is that Mr. Perholtz has not submitted requests for updated information in recent years, that the SSA is now making DMF information available weekly, and that the SSA is making public considerably more information than the three data fields described.

At a fundamental level, we need to make some choices about what we want most from our tax system. If our goal is to process tax returns and deliver tax refunds as quickly as possible, the IRS can continue to operate as it currently does – but that means some perpetrators will get away with refund fraud and some honest taxpayers will suffer harm. If we place a greater value on protecting taxpayers against identity theft and the Treasury against fraudulent refund claims, we may need to make a substantial shift in the way the IRS does business. Specifically, we may need to ask all taxpayers to wait longer to receive their tax refunds, or we may need to increase IRS staffing significantly. Under current circumstances, I have come to the conclusion that it is simply not possible for the IRS both to process legitimate returns rapidly and to combat refund fraud effectively at the same time.