MSP #3 Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS

RESPONSIBLE OFFICIALS

Beth Tucker, Deputy Commissioner for Operations Support
Richard E. Byrd Jr., Commissioner, Wage and Investment Division

DEFINITION OF PROBLEM

Tax-related identity theft is a rapidly growing crime that often imposes enormous financial, emotional, and time-consuming burdens on its victims. It may take many forms, including the following:

- An identity thief files a false return early in the filing season that claims a refund and uses a victim's Social Security number (SSN). When the victim later tries to e-file her own return, it is blocked.[1] About 83 percent of all tax returns result in refunds, with the average amount over $3,000.[2] For many taxpayers, a significant delay in receiving a refund of this magnitude can impose financial hardship. Moreover, the victim may have to devote significant time and effort to proving to the IRS that she is the "real" taxpayer.
- An identity thief files a false return that claims a refund and uses the SSN of a disabled person in an assisted living facility. The false return shows fake self-employment (Schedule C and Schedule SE) income and refundable credits, resulting in a refund. The IRS reports the self-employment income to the Social Security Administration (SSA), which terminates the victim's Social Security benefits, potentially causing the facility to discharge the patient.
- An identity thief obtains data from the Social Security Death Master File via the Internet to find the names, SSNs, birth dates, and locations of recently deceased minor children and then claims them as dependents on a false tax return. When the parents subsequently try to electronically file a return claiming their child as a dependent during the year in which he or she died, they are unable to do so because the child was previously claimed by the identity thief. Instead, the grieving parents must file a paper return.

In recent years, the Taxpayer Advocate Service (TAS) has worked closely with the IRS to improve servicewide efforts to assist identity theft victims. Over the last few years, the IRS has made significant progress in this area and has adopted many of our recommendations, including the establishment of a dedicated unit to help the victims.

1 *See* Internal Revenue Manual (IRM) 21.3.4.32.1 (Nov. 8, 2010).

2 The average fiscal year (FY) 2010 refund amount was $3,048. FY 2010 IRS Data Book, table 8, footnote 3. The percent of returns with refunds is 82.9 percent (119.4 million refunds out of 144.1 million total individual tax returns). FY 2010 IRS Data Book, tables 2 and 7.

However, the crime of tax-related identify theft continues to grow, and notwithstanding the IRS's efforts, its resources and ability to resolve cases are stretched thin. In fiscal year (FY) 2011, the centralized Identity Protection Specialized Unit (IPSU) received more than 226,000 cases, a 20 percent increase over FY 2010.[3] Despite the establishment of the IPSU, TAS received over 34,000 identity theft cases in FY 2011, a 97-percent increase over FY 2010.[4] In reaction to this growing workload, the IRS is taking steps that may ensnare legitimate taxpayers without creating a pathway to quick resolution of their cases.

An IRS task force found that 28 different units within the IRS are involved in helping victims and discovered over 50 gaps in IRS procedures.[5] Among other deficiencies, the IRS does not have a mechanism to monitor how long it takes to resolve an identity theft case.[6] The task force recommended that the IRS adopt a specialized model for identity theft victim assistance and issue a personal identification number (PIN) to victims to use when filing returns so the IRS can properly distinguish the true taxpayer from the identity thief.

Even with a more specialized approach to victim assistance, the IRS will still require a "traffic cop" to ensure that the proper function handles each case in an acceptable timeframe. The IPSU has already been serving in this capacity for three years and should remain the single point of contact for taxpayers. In our view, however, this "traffic cop" needs greater authority. Although IPSU requests are supposed to receive priority treatment from other IRS organizations, some IPSU cases are not considered "aged" until after 180 days have passed.[7] Moreover, the IPSU has no way to ensure that the other functions adhere to the requested timeframes. Not surprisingly, identity theft cases controlled by the IPSU may languish for months.

The National Taxpayer Advocate has identified the following additional problems related to IRS handling of identity theft issues:

- The federal government facilitates tax-related identity theft by publicly releasing considerable personal information about recently deceased individuals, including a decedent's full name; SSN; date of birth; date of death; and the county, state, and zip code of the last address on record.
- When the IRS implements new filters to catch potentially fraudulent tax returns in identity theft cases, it does not always have effective strategies and sufficient resources

3 IRS, *IPSU Identity Theft Report* (Oct. 1, 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. It does not include 26,695 cases that meet TAS's "systemic burden" case criteria, which the IPSU tracks separately.

4 In FY 2010, TAS opened 17,291 stolen identity (primary issue code 425) cases. In FY 2011, the number jumped to 34,006. Taxpayer Advocate Management Information System (TAMIS), FY 2010, FY 2011 (Oct. 31, 2011).

5 IRS, Identity Theft Executive Steering Committee, *Identity Theft Program Enhancements, Challenges and Next Steps* 14 (Oct. 19, 2011).

6 TAS had an average cycle time of 107 days for identity theft cases, which sometimes involves multiple issues or multiple years, closed in FY 2011. TAS, Business Performance Management System.

7 IRM 21.9.2.1(6) (Oct. 1, 2011).

to adequately assist honest taxpayers whose returns and refund claims are held up by the filters in error.

- The IRS is not adequately protecting identity theft victims by quickly acting upon referrals of identity theft schemes from its Criminal Investigation (CI) division and other sources.
- The IRS has not developed consistent guidance for its employees to promptly remove fraudulent income and credits related to substantiated identity theft from the victims' accounts.
- The IRS is not fully utilizing its existing authority to share information about identity theft schemes and the impact on the victims with the heads of other federal agencies.
- Because TAS employees have the unique perspective of working identity theft cases from start to finish, the IRS should include TAS in all levels of identity theft program and procedural planning. This should include front-line teams, training development, guidance, and advisory and executive steering committees.

ANALYSIS OF PROBLEM

Background

In general, identity theft occurs in tax administration in two ways — when an individual intentionally uses the 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. In both situations, the victim is often sent on a journey through IRS processes and procedures that may take years to complete.

The IRS Has Improved Its Processes for Assisting Identity Theft Victims.

The National Taxpayer Advocate has discussed the problem of tax-related identity theft for over seven years in her Annual Reports to Congress and congressional testimony.[8] The IRS has accepted many of TAS's recommendations for improving identity theft procedures. At various times, we have advocated for the following improvements, each of which the IRS has adopted in some form:

- Allowing employees greater discretion to determine the true owner of an SSN in question without referring the matter to the SSA;

[8] *See* National Taxpayer Advocate 2009 Annual Report to Congress 307-317; National Taxpayer Advocate 2008 Annual Report to Congress 79-94; National Taxpayer Advocate 2007 Annual Report to Congress 96-115; National Taxpayer Advocate 2005 Annual Report to Congress 180-191; National Taxpayer Advocate 2004 Annual Report to Congress 133-136; *The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, a Drain on the Public Treasury*, Hearing Before the S. Comm. on Finance, Subcommittee on Fiscal Responsibility and Economic Growth, 112th Cong. (May 25, 2011) (statement of Nina E. Olson, National Taxpayer Advocate); *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).

- Developing an electronic indicator to mark the tax accounts of verified victims;[9]
- Creating an IRS identity theft affidavit form;
- Adopting a standardized list of acceptable documents to substantiate identity theft;
- Establishing a centralized unit to help identity theft victims;
- Providing for a global account review prior to closing an identity theft victim's case to ensure that all related issues have been resolved; and
- Issuing a PIN to verified victims of identity theft to enable them to file returns electronically and prevent others from filing under the victims' SSNs.

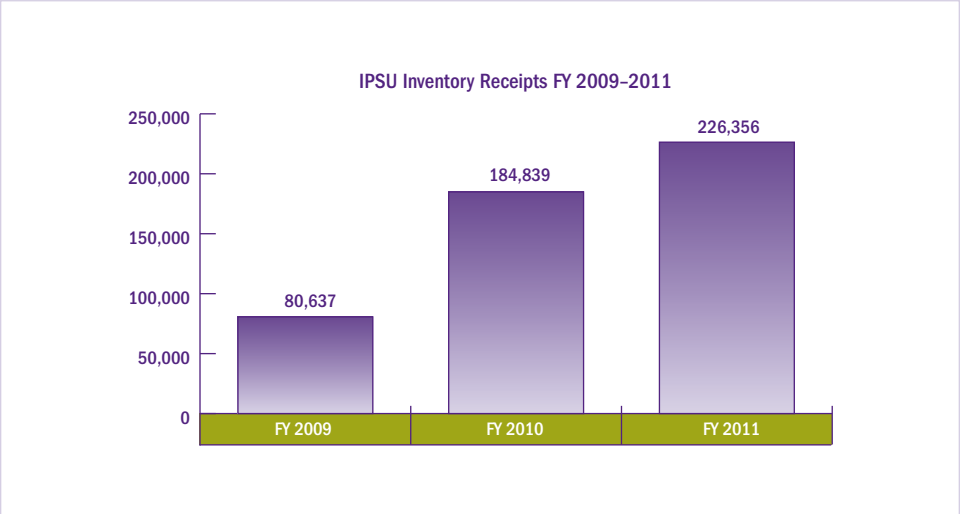
Without doubt, the IRS is in a better position to help identity theft victims today than when the National Taxpayer Advocate first identified identity theft as a Most Serious Problem facing taxpayers in her 2005 Annual Report. But despite the improvements that have taken place in the last few years, the IRS continues to struggle with identity theft and cannot proactively safeguard taxpayer accounts from this crime.

Despite Major Improvements, the IRS Is Receiving Unprecedented Volumes of Identity Theft Casework.

The IRS established the IPSU in 2008 because it wanted to have a centralized unit that would accept identity theft cases and, if necessary, monitor actions taken by the various functions. This centralized unit is receiving an unprecedented volume of cases. As the chart below shows, IPSU receipts in FY 2011 increased substantially over the two previous years. This inventory does not include the tens of thousands of potential victims linked to various ongoing investigations of organized identity theft operations.

9 Since the IRS started using an electronic indicator in 2009 to flag an account as being potentially compromised, it has tracked over 1.8 million incidents impacting over 1.1 million taxpayers. *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 September 30, 2011.

FIGURE 1.3.1, IPSU Inventory Receipts, FY 2009 to FY 2011[10]



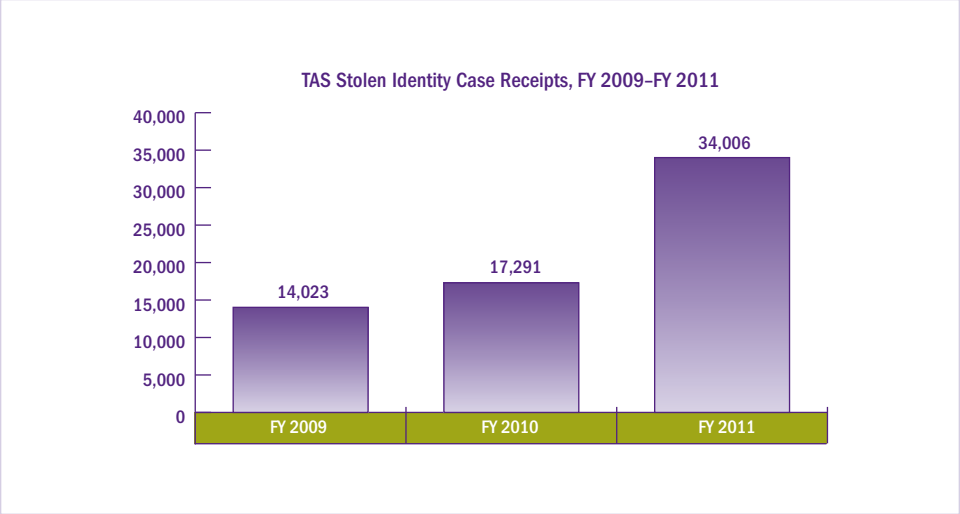
TAS casework reflects the impact of the IRS's inability to promptly address identity theft victims' tax issues. TAS received 34,006 stolen identity cases in FY 2011, compared to 17,291 in FY 2010 and 14,023 in FY 2009.[11] This translates to a 97 percent increase in identity theft receipts in FY 2011 over FY 2010, on top of a 23 percent gain from FY 2009 to FY 2010. Moreover, this increase does not include 26,695 cases that meet TAS's "systemic burden" case criteria and were referred to the IPSU for processing under the March 2010 Memorandum of Understanding between TAS and the Wage and Investment (W&I) division.[12]

10 IRS, *IPSU Identity Theft Report* (Oct. 1, 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. It does not include cases that meet TAS's "systemic burden" case criteria, which the IPSU tracks separately.

11 TAMIS, FY 2009, FY 2010, FY 2011 (Oct. 31, 2011).

12 IRS, *IPSU Identity Theft Report* (Oct. 1, 2011). *See Memorandum of Understanding Between the National Taxpayer Advocate and the Commissioner, Wage & Investment to Transition TAS Criteria 5-7 Identity Theft Cases to Wage & Investment Identity Protection Specialized Unit (IPSU)* (Mar. 31, 2010).

FIGURE 1.3.2, TAS Stolen Identity Case Receipts, FY 2009 to FY 2011[13]



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

Identity Thieves Have Become More Proficient.

Over the years, those who commit identity theft have become more adept at devising schemes to steal identities. Increasingly, these schemes target taxpayers who are not required to file returns, such as the elderly, disabled, and children. As a result, it may take years for a victim to find out that an identity thief has stolen his or her SSN. One of the more sinister schemes involves the misuse of a deceased taxpayer's SSN to obtain fraudulent refunds. Perpetrators have gone as far as using the SSNs of deceased children, leaving their grieving parents to deal with the aftermath of the identity theft.[14]

Tax-Related Identity Theft Remains a Growing Problem.

The rising IRS caseload may reflect an overall increase in *tax-related* identity theft as opposed to other types. The Federal Trade Commission (FTC) reports overall identity theft complaints have actually decreased in 2009 for the first time since 2006.[15] However, tax return-related identity theft has increased nearly six percentage points from 2006 to 2008.[16] The overall decline in incidents reported to the FTC may be attributable in part to the IRS's

13 Taxpayer Advocate Management Information System (TAMIS), FY 2009, FY 2010, FY 2011.

14 *See* CBS 3 News Report, *Deceased Riverside Child's Identity Stolen, Falsely Claimed on Taxes* (Mar. 1, 2011), *available at* http://philadelphia.cbslocal.com/2011/03/01/diseased-riverside-childs-identity-stolen-falsely-claimed-on-taxes; *The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, A Drain on the Public Treasury*, Hearing Before the S. Comm. on Finance, Subcommittee on Fiscal Responsibility and Economic Growth, 112th Cong. (May 25, 2011) (statement of Terry D. McGlung, Jr.).

15 *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.

16 *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.

creation of its own identity theft affidavit in 2009.[17] Additionally, the victims are sometimes deceased individuals, who cannot report the incidents to the FTC.

One example of alleged tax-related identity theft involves what media reports describe as a sophisticated ring based in the Tampa area. The media reported the individuals allegedly were using laptops, off-the-shelf tax preparation software, wireless hotspots, and easily obtainable personal information to file false returns and obtain refund checks or debit cards. Federal investigators estimate they have seized $100 million in questionable tax refunds from the operation, which authorities say adopted the name of the popular tax-filing software "Turbo Tax."[18]

The Public Is Increasingly Aware of Identity Theft.

The increase in identity theft cases may also be due to increased public awareness. Whether because of more effective outreach or just greater media coverage, people may be checking their credit reports more frequently and becoming better at detecting identity theft. If they see suspicious entries on their credit profiles, taxpayers may contact the IRS to make sure no one has used their SSNs to file returns.

The IPSU Is Struggling to Effectively Manage Identity Theft Cases.

The establishment of the Identity Protection Specialized Unit may have created a false sense of well-being in the IRS. Commissioner Shulman, in his written response to Senate Finance Committee Chairman Max Baucus's follow-up questions after 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."[19] While this description fits the model for which TAS advocated, it does not accurately reflect how the IPSU operates in practice.

The reality is that the IPSU does not work identity theft cases from beginning to end. Whether because of resource constraints or a policy decision, the IPSU is not staffed to work identity theft cases itself. Instead, it attempts to coordinate with up to 27 other functions within the IRS to obtain relief for the victim.[20] In some cases, the IPSU simply routes

17 *See* Form 14039, *Identity Theft Affidavit* (rev. Mar. 2010), *available at* http://www.irs.gov/pub/irs-pdf/f14039.pdf. Prior to 2009, identity theft victims could obtain an identity theft affidavit from the FTC and submit it to the IRS to receive assistance. *See* IRM 21.6.2.4.4.3(1) (Oct. 1, 2007) (superseded). The IRS still advises taxpayers, by telephone and notices, to file a complaint with the FTC. Filing a complaint to enter an incident in the FTC database is different from completing the FTC identity theft affidavit.

18 *See* Elaine Silvestrini & Lauren Mayk, *Police: Tampa Street Criminals Steal Millions Filing Fraudulent Returns*, Tampa Bay Tribune (Sept. 1, 2011), *available at* http://www2.tbo.com/news/politics/2011/sep/01/11/police-tampa-street-criminals-steal-millions-filin-ar-254724/.

19 *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.

20 IRS, Identity Theft Executive Steering Committee, *Identity Theft Program Enhancements, Challenges and Next Steps* 14 (Oct. 19, 2011).

the case to other IRS organizations and "monitors" the victim's account every 60 days.[21] In other cases (*e.g.*, those with a systemic burden issue), the unit uses Identity Theft Assistance Requests (ITARs) to ask other IRS functions to take specific actions.[22]

While the procedures call for the receiving functions to give ITARs priority treatment, there are no "teeth" to ensure that happens.[23] Unlike TAS, which can issue a Taxpayer Assistance Order[24] (TAO) if an operating division (OD) does not comply with its request for assistance in a timely manner, the IPSU procedures do not specify any consequences for functions that are unresponsive to a case referral or an ITAR. Moreover, TAS has negotiated agreements with the operating divisions that clearly define when and how the ODs will respond to a TAS request for action. The National Taxpayer Advocate urges the IPSU to enter into similar Service Level Agreements (SLAs) with other IRS divisions and functions that set forth the timeframes for taking the requested action and to develop tracking procedures to report to heads of office when functions regularly fail to meet these timeframes. For example, the SLAs may set forth a reporting mechanism that would notify the executives of other functions when their employees do not meet timeliness standards. The SLAs may also require the ODs to publish their identity theft case timeliness measures in their quarterly Business Performance Review reports.

IPSU procedures are a vast improvement over IRS processes in effect as recently as three years ago. Unless the IPSU is given adequate staffing and authority to oversee cases from start to finish, however, the benefits of these improvements will be inadequate for both taxpayers and the IRS.

Even with a Specialized Approach to Assisting Identity Theft Victims, the IPSU Should Continue to Play an Important Role.

Despite its "specialized" name, the IPSU actually operates as a hub in a centralized environment. One major recommendation from the identity theft working group was that the IRS create a specialized unit *within each function* to work on identity theft cases. Under this approach, each function would retain responsibility for individual aspects of a case, but would rely on employees who receive specialized training to help the victims.

The National Taxpayer Advocate believes the IPSU should continue to play an important role in this specialized environment. The IRS needs a "traffic cop" to work with the various functions, hold them to timeframes, and ensure that they do not neglect cases. The IPSU should remain the single point of contact for victims and should coordinate with the

21 IRM 21.9.2.4.3(7) (Oct. 31, 2011).

22 IRM 21.9.2.10.1 (Oct. 1, 2010).

23 IRM 21.9.2.1(4) (Oct. 1, 2011) provides:

> All cases involving identity theft will receive priority treatment. This includes... Form 14027-A *Identity Theft Case Monitoring*, and Form 14027-B, *Identity Theft Case Referral*...Identity Theft Assistance Request (ITAR) referrals are also included. IRM 21.9.2.10.1(1) (Oct. 1, 2011) provides that "Cases assigned as ITAR will be treated similar to Taxpayer Advocate Service (TAS) process including time frames."

24 *See* IRC § 7811.

specialists in the various functions. Each function should have a liaison with the IPSU and be held accountable for meeting established deadlines for taking requested actions (as set forth in the SLA).

The IRS Does Not Accurately Track Identity Theft Cases or Cycle Time.

The IRS does not yet have a centralized system to track identity theft cases and must pull data from multiple systems to estimate case receipts. Because identity theft often involves multiple tax issues that need to be worked by different functions, a case frequently appears on multiple systems. A task force determined that the IRS has 22 distinct systems and data sources that collect identity theft data.[25] Without conducting manual workarounds to manipulate the data, the IRS is susceptible to double- or triple-counting identity theft receipts if it simply adds up the case counts from the 22 systems.

Equally important, the IRS does not currently track any data about the cycle time for identity theft cases, although it recognizes the benefits of such a measure. The National Taxpayer Advocate believes that cycle time is useful as an indicator, but urges the IRS to focus more on *timeliness*. Because TAS routinely deals with complicated cases that may take months to fully resolve, TAS case advocates are measured on the timeliness of their actions rather than simply on how long it takes to close a case. For example, did the case advocate phone the taxpayer within one day of the initial contact? Did the case advocate follow up with the appropriate IRS function within three days of the negotiated completion date? Focusing on timeliness (1) requires the case advocate to come up with a detailed action plan to resolve the case and (2) alleviates the artificial pressure to prematurely close the case solely to reduce cycle time. Identity theft cases are similarly complicated and should be measured on timeliness, rather than strictly on cycle time.

Without the ability to compile meaningful identity theft case tracking data, it is difficult, if not impossible, for the IRS to determine whether identity theft cases are being treated with the urgency they demand.

The Federal Government Facilitates Tax-Related Identity Theft by Publicly Releasing Significant Personal Information of Deceased Individuals.

SSNs and other personal information are more accessible than ever. What is surprising and disturbing is that the federal government is the source of much of this personal information. Under a 1980 consent judgment resulting from a Freedom of Information Act (FOIA) lawsuit, the SSA was required to provide certain personally identifiable information about deceased individuals.[26] In response, the SSA created a "Death Master File" (DMF) containing the full name, SSN, date of birth, date of death, and the county, state, and ZIP

25 IRS, Identity Theft Assessment and Action Group, *IRS Identity Theft Program Future State Report* 8, 136 (Oct. 11, 2011).

26 *See Perholtz v. Ross*, Civil Action No. 78-2385 and 78-2386, U.S. District Court for the District of Columbia (Apr. 11, 1980).

code of the last address on record.[27] Today, anyone who conducts a quick web search can find a number of sites (including genealogy sites) that provide this information, for free or for a nominal fee.[28]

The National Taxpayer Advocate is appalled that the federal government is making sensitive personal information so readily available, when such information can easily be used to commit identity theft. Notably, the DMF contributes to tax-related identity theft by providing the date of birth, allowing thieves to determine which decedents are minors who can be claimed as dependents. While the Freedom of Information Act may require disclosure of this information, the IRS should work with the SSA to explore ways to minimize the potential harm associated with such information. For example, the SSA provides weekly updates to the DMF. Perhaps the DMF could be released once a year to the public, after the tax filing season. The IRS would continue to receive DMF data on a weekly basis, and thus would have time to load information onto its systems and be better positioned to scrutinize claims that include the SSNs listed in the DMF.

Alternatively, the SSA, perhaps in conjunction with the IRS, may propose to make public only the final four digits of decedents' SSNs, at least for several years after their deaths, to prevent the theft and misuse of their identities. If the federal government can show that the release of full SSNs is substantially furthering criminal conduct and that it reasonably believes the public benefits of partially redacting SSNs outweigh the public benefits of the release of full SSNs, we think a court would give such a request favorable consideration.

If neither of these approaches yield the desired result, the National Taxpayer Advocate is proposing that Congress pass legislation to restrict disclosure of certain personally identifiable information to the public.[29]

When the IRS Implements New Filters, It Should Have an Effective and Expedited Mitigation Strategy to Help Legitimate Taxpayers Obtain Their Refunds on a Timely Basis.

In the current environment, the IRS is under tremendous pressure to protect Treasury revenue from improper refund claims. The IRS is understandably deploying front-end verification procedures to prevent suspicious refunds from going out. For the 2012 filing season, the IRS plans to implement a set of identity theft filters it developed by analyzing a population of tax returns that included "verified" false returns along with known legitimate returns. Based on analysis of the differences between these "good" and "bad" returns, the IRS has developed a series of business rules that aim to filter out the verified false returns, while allowing the good returns to pass through processing. The IRS plans to notify

27 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).

28 See Scripps Howard News Service, *ID Thieves Cashing in on Dead Children's Information* (Nov. 3, 2011).

29 See Legislative Recommendation: *Restrict Access to the Death Master File, infra*. *See also* Identify Theft and Tax Fraud Prevention Act, S. 1534, 112th Cong. § 9 (1st Sess. 2011) (proposing restrictions on access to the Death Master File).

taxpayers whose returns it has flagged that it has questions about their returns and will not be able to process them until the taxpayers provide the requested information.

The National Taxpayer Advocate appreciates the need for the IRS to develop effective screening mechanisms to combat identity theft. However, she has several concerns about the planned filters. First, filters of this nature are inherently imprecise, so it is critical that the IRS employ reliable methods to determine whether a return flagged as questionable is valid or false. Indeed, IRS personnel generally do seek to "validate" or "verify" whether a flagged refund claim should be paid. However, this process often produces inaccurate results. According to a TAS review of approximately 20,000 TAS pre-refund wage verification cases in which refunds were denied, 80 percent of the taxpayers ultimately were found eligible for refunds, with 72 percent receiving the entire amounts they had claimed on their returns.[30] While TAS cases may not be representative of the overall population of taxpayers, the review raises questions about the accuracy of the IRS's processes and its claims concerning the number and percentage of "verified" false returns.

Second, the National Taxpayer Advocate is concerned that the IRS's mitigation strategy may not be effective. According to the plan, employees of the Submission Processing organization will be able to help taxpayers erroneously caught up in the identity theft filter. These employees are to retrieve the tax return information and make sure the return is treated as processed on the original date of filing. In the current budget environment, there is a significant risk that Submission Processing will not have sufficient staffing to aid the impacted taxpayers (a number which is unknown at this time).

Third, the National Taxpayer Advocate is concerned that procedural changes adopted through Servicewide Electronic Research Program (SERP) alerts or other staff instructions often have a significant impact on taxpayer mitigation strategies yet are not reviewed by TAS or other affected functions. To protect against that, we urge the IRS to require that any proposed modifications to its mitigation strategies be approved in advance by the Identity Theft Executive Steering Committee.

Fourth, the National Taxpayer Advocate is concerned that the IRS is underestimating the impact of these identity theft filters. During the 2011 filing season, when the IRS vastly underestimated the problems involved in processing repayments of the First-Time Homebuyer Credit, it had no communication strategy to inform the public about these issues. The IRS's silence drove taxpayers to vent their frustrations and share often inaccurate information on a Facebook page.[31] The IRS should learn from this experience and develop a national communication strategy now. It is important for the IRS to keep taxpayers better informed, especially if it becomes apparent that the identity theft filters will impact a significant number of taxpayers. Moreover, if the IRS's suspicions are correct and

30 *See* Most Serious Problem: *The IRS's Wage and Withholding Verification Procedures May Encroach on Taxpayer Rights and Delays Refund Processing*, *supra*.

31 *See* National Taxpayer Advocate Fiscal Year 2012 Objectives Report to Congress 28-32.

it receives an unprecedented number of returns involving identity theft in the 2012 filing season, it may have to slow down the processing of all returns to protect revenue. The IRS must have a nationwide communication plan in place if that happens.

The IRS Is Not Adequately Protecting Identity Theft Victims by Quickly Acting Upon Criminal Investigation and Other Identity Theft Referrals.

The Criminal Investigation division and other agencies sometimes investigate large-scale identity theft schemes and in the course of their investigations acquire lists of taxpayers whose identities have been or may be misused. When CI efforts or referrals from law enforcement agencies yield names and SSNs of impacted taxpayers, the IRS should not only try to protect revenue but should also help the victims. The IRS should promptly (1) place a civil freeze code on such accounts to prevent refunds from being processed without further scrutiny; (2) abate taxes, penalties, and interest from the impacted accounts, as appropriate; and (3) to the extent permitted by law, share this information with other agencies (such as the SSA) to reduce the effect of improperly inflated income.

The IRS Should Develop a Civil Freeze Code to Protect Revenue.

Historically, CI would input a TC 918 freeze code to flag accounts when it received leads from law enforcement agencies about SSN misuse. This code would protect revenue and control accounts. The downside of CI applying this code is that the civil functions of the IRS would no longer control the account and be unable to adjust the account or even discuss it with taxpayers. The IRS is considering the development of a civil freeze code that would allow Wage & Investment employees to talk with affected taxpayers and make adjustments while protecting revenue. However, the National Taxpayer Advocate is concerned that W&I employees will not have the expertise and experience to evaluate the merits of a referral from a law enforcement agency. With the mounting external pressure to protect revenue and limited resources to work cases, we are concerned that refund claims that are merely "suspicious" or "potentially fraudulent" may be permanently frozen. To address this concern, the National Taxpayer Advocate recommends that CI remain involved in the decision to implement a TC 918-equivalent freeze code. Only after CI personnel determine that a freeze code is warranted should W&I apply the TC 918-equivalent.

The IRS Has Not Developed Consistent Guidance for Its Employees to Promptly Remove Fraudulent Income and Credits Related to the Substantiated Identity Theft from the Victims' Accounts.

In June 2011, the National Taxpayer Advocate issued a Proposed Taxpayer Advocate Directive (TAD) ordering the Commissioner of W&I to establish procedures to adjust a taxpayer's account in instances where a tax return preparer altered the return without the taxpayer's knowledge or consent.[32] To date, the IRS has not issued this guidance to its employees. In August 2011, the National Taxpayer Advocate issued TAOs in four cases

32 *See* Proposed Taxpayer Advocate Directive (TAD) 2011-1 (June 13, 2011). This Proposed TAD is attached at the end of this Most Serious Problem.

ordering the Commissioner of W&I to adjust the accounts to remove all entries attributable to the purported returns. It was not until the National Taxpayer Advocate elevated the four TAOs to the Deputy Commissioner of Services and Enforcement in September 2011 (after W&I failed to respond) that the IRS took action in these particular cases. The Proposed TAD remains outstanding and unsatisfied, despite the W&I Commissioner's commitment to develop procedures.

The IRS Currently Has Sufficient Authority to Share Information Pertaining to Identity Theft with Other Federal Agencies and Should Do So Promptly to Minimize the Impact on Identity Theft Victims.

The IRS periodically receives referrals from law enforcement agencies that have uncovered an identity theft scheme. If a victim is receiving certain Social Security benefits, his or her benefits may be affected if the perpetrator reported inflated income using the victim's SSN. When the IRS receives such information, it has an obligation to notify both the victim and other agencies (such as the SSA) to minimize the impact to the victim. It should identify a liaison within the SSA and ensure that income information the SSA relies upon to process benefits is accurate.

Identity theft heightens historic concerns with security of return information. While the law generally makes return information confidential, there are various exceptions that allow the IRS to share certain information with the SSA.[33] When the IRS corrects an item of return information (by audit or otherwise), it incorporates updated data into the authorized release.[34] If the IRS corrects an item of return information due to identity theft, it likewise incorporates the correction into the authorized release for corresponding adjustment by the SSA.[35]

Conversely, law enforcement agencies that need return information can obtain it through proper procedures.[36] Federal officials can request return information for use in criminal investigation or proceedings, such as those relating to identity theft.[37] Effective use of existing authority can help stem identity theft.

33 *See, e.g.*, IRC § 6103(l)(1), (5), (7), (12), (21).

34 *See* IRM 11.3.29.3 (Sept. 1, 2009); *Agreement Between the Social Security Administration and the Internal Revenue Service* (Mar. 14, 2007).

35 Additionally, IRC § 6103(i)(3)(A) authorizes the IRS to apprise another federal agency charged with enforcement of a non-tax crime. To the extent that the Social Security Act criminalizes elements of identity theft (under 42 USC § 1307 or other provisions), this disclosure statute may apply to the agency charged with enforcement.

36 *See* IRC § 6103(i)(1), (i)(2); *see also* IRC § 6103(d) (permitting disclosure to state tax enforcement agencies).

37 *See* IRC § 6103(i)(2). In case of tax data provided by an individual that is classified as "taxpayer return information," a federal prosecutor may obtain a court order for release in criminal investigation or proceedings. *See* IRC § 6103(i)(1).

The IRS Issued Identity Protection PINs that Should Protect Some Victims from Refund Delays and Protect Revenue.

For the 2012 filing season, the IRS issued identity protection personal identification numbers (IP PINs) to over 200,000 victims whose identities and addresses have been verified.[38] In November 2011, the IRS sent out letters informing the victims that they must use the IP PIN to file their 2011 returns electronically. In December 2011, the IRS issued a second letter that actually contained the IP PIN. If the taxpayer attempts to e-file without that number, the IRS will not accept it and the taxpayer will need to file a paper return, which will delay processing.

The National Taxpayer Advocate supports the IP PIN in concept. However, we recognize that some taxpayers will not receive the notification letter, will lose the IP PIN, or will simply forget to use it when they try to e-file. The IRS must be prepared to respond to phone inquiries from these taxpayers and must be prepared, without the need for TAS involvement, to expedite return processing for those victims who demonstrate that identity theft has caused economic hardship. Absent such a mitigation strategy, this policy decision by the IRS may dramatically increase TAS's caseload.

The IRS Should Promptly Notify Victims of Identity Theft that Their SSNs Have Been Compromised in the Tax Context.

When the IRS discovers and confirms 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 identity theft. In many instances, the IRS is the first agency to learn of the theft. For example, a taxpayer's SSN may have been used by someone else for employment purposes. Where the IRS is able to verify without contacting the taxpayer that misuse has occurred, it can adjust the victim's account without notifying the taxpayer that his or her SSN has been compromised.

In 2008, the IRS Office of Chief Counsel advised that the IRS could notify taxpayers that they were the victims of identity theft without violating confidentiality laws.[39] Based on this advice, the IRS developed a letter informing the taxpayer that his or her personal information has been compromised and providing suggestions about what the taxpayer may wish to do (*e.g.*, contact the credit reporting agencies). However, the IRS does not send such notification in all known instances of identity theft. For example, the IRS does not send such letters to victims of employment-related identity theft.[40]

38 IRS, Identity Theft Executive Steering Committee, *Identity Theft Program Enhancements, Challenges and Next Steps* 6 (Oct. 19, 2011).

39 IRS Office of Chief Counsel Memorandum, *Identity Theft Returns and Disclosures Under Section 6103*, PMTA 2009-024 (June 8, 2008).

40 Email correspondence from Office of Privacy, Government Liaison, and Disclosure analyst (Nov. 2, 2011). The IRS does issue victim notification letters to CI-identified taxpayers. *See* IRM 10.5.3.2.2.4.3 (Dec. 23, 2010).

Taxpayers Should Be Allowed to Turn Off Their Ability to File Tax Returns Electronically.

Electronic filing has many benefits, including more accurate returns and faster processing. "IRS e-file is the best option for everyone, especially for people impacted by recent tax law changes," said Commissioner Shulman when IRS e-file approached the milestone of one billion returns processed in January 2011.[41] Twenty years after the IRS introduced e-file, nearly 70 percent of U.S. taxpayers use it.[42]

Unfortunately, the benefits of e-file also extend to perpetrators of identity theft. E-file allows the thieves to submit falsified returns early and repeatedly, in an attempt to beat the legitimate taxpayer to the IRS and claim improper refunds. The mandatory use of the IP PIN would go a long way toward alleviating recurring identity theft, but it would not help taxpayers who no longer have a filing obligation (or young children who do not need to file for many years to come). The IRS should allow taxpayers to voluntarily turn off the ability to e-file using their SSN and enable taxpayers to reacquire the e-file option later, upon proof of identity, if circumstances change. Such a feature would offer an additional level of protection to vulnerable taxpayers.

The IRS Should Include TAS Representatives in All Levels of Identity Theft Program and Procedural Planning.

As discussed, the IPSU functions as a traffic cop, coordinating with various IRS functions to address bits and pieces of an identity theft victim's tax issues. By contrast, TAS employees are the only IRS employees who work identity theft cases from start to finish. Their global perspective, along with the experience they have gained from working the significant volume of identity theft cases that TAS receives, qualifies some TAS employees as experts in identity theft processing. To ensure the IRS receives the benefit of TAS's broad experience in assisting identity theft victims, the IRS should include TAS in all levels of identity theft program and procedural planning, including front-line teams, training development, guidance, and advisory and executive steering committees.

CONCLUSION

In conclusion, the National Taxpayer Advocate preliminarily recommends that the IRS:

1. Implement Service Level Agreements between the Identity Protection Specialized Unit and the various functions that process case referrals and Identity Theft Assistance Requests.
2. Establish timeliness measures for identity theft case actions.
3. Before implementing identity theft filters, develop an effective and expedited mitigation strategy to help legitimate taxpayers obtain their refunds on a timely basis.

41 IRS, *IRS e-file Launches Today; Most Taxpayers Can File Immediately*, IR-2011-4 (Jan. 14, 2011).

42 *Id.*

4. Require any proposed modifications to its identity theft filters mitigation strategy be approved in advance by the Identity Theft Executive Steering Committee.
5. Create and implement a national communication strategy if the identity theft filters impact a significant number of legitimate taxpayers or cause excessive processing delays.
6. In conjunction with the Social Security Administration, seek a modification of the consent judgment requiring the SSA to release the SSNs of decedents, so that the SSA can begin to partially redact SSNs (*e.g.*, release only the last four digits).
7. If a civil freeze code is implemented for referrals from law enforcement agencies, require CI personnel to determine whether such a refund freeze is necessary before applying the civil freeze code.
8. Establish a point of contact in W&I so that Criminal Investigation or other IRS operations can supply lists of victims from their investigations of identity theft schemes and W&I can promptly mark the accounts accordingly.
9. Promptly 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.
10. Allow taxpayers to turn off the ability to file electronically.
11. Include TAS in all levels of identity theft program and procedural planning, including front-line teams, training development, guidance, and advisory and executive steering committees.

IRS COMMENTS

The IRS takes very seriously the issue of identity theft and its impact on the tax system, including the harm that it inflicts on innocent taxpayers. Over the past few years, the IRS has seen a significant increase in refund fraud schemes involving identity theft. The IRS has prioritized this issue and is committed to taking the necessary steps to be better prepared in both fraud prevention and victim assistance. In meeting this commitment, the IRS has substantially increased the resources devoted to both fraud prevention and victim assistance. Even in a declining budget environment, the IRS is taking a variety of steps to address the growing challenge of identity theft.

On the prevention side, the IRS is implementing new processes for handling returns, new filters to detect fraud, new initiatives to partner with stakeholders and a continued commitment to investigate the criminals who perpetrate these crimes. In implementing these processes the IRS must maintain the balance between the processing of refunds in a timely manner with the controls that are needed to minimize errors and fraud in returns that are submitted for processing.

The IRS launched a new program to enhance return processing and catch fraudulent refunds when they come in the door. A cross-functional group made up of IRS divisions developed processes and policies for the 2012 filing season to protect revenue by:

- Designing new identify theft screening filters;
- Developing new procedures to handle returns that are believed to be filed by identity thieves;
- Issuing special identification numbers to taxpayers whose identity has been stolen;
- Identifying mismatches in returns earlier in the process;
- Developing mechanisms to stop the growing trend of returns submitted with deceased taxpayers' information;
- Developing procedures for handling lists of personal information discovered by law enforcement officials;
- Expanding IRS' authority to better utilize the list of prisoners to stop fraudulent returns; and
- Collaborating with software developers and other industries to prevent theft.

In addition, the Criminal Investigation division is working closely with other IRS divisions to improve processes and procedures related to identify theft refund fraud prevention.

Along with prevention, the other key component of the IRS's efforts to combat identity theft involves providing assistance to taxpayers whose personal information has been stolen and used by a perpetrator in the tax filing process. This situation is complicated by the fact that identity theft victims' data has already been compromised outside the filing process by the time we detect and stop perpetrators from using their information.

The IRS agrees that integrated processes and procedures are needed to ensure that identity theft victims receive timely assistance. We recently initiated a focused effort to improve the overall end-to-end case resolution process. A servicewide group was formed to assess the current strategic and operational state of identity theft across the IRS. This effort identified several process and workflow enhancements that will significantly improve our victim assistance services. Because identity theft can manifest within multiple IRS functions, the IRS is establishing specialized groups within each function that encounters identity theft issues. The IRS is working to speed up case resolution, provide more training for employees who assist victims of identity theft, and step up outreach to and education of taxpayers so they can prevent and resolve tax-related identity theft issues quickly. The IRS is also capturing additional data about identity theft cases and integrating this with more robust management oversight processes. In combination, these processes, structural and oversight improvements are targeted to reduce the time required to resolve taxpayer issues and deliver a higher quality of taxpayer service.

Fighting identity theft will be an ongoing battle for the IRS, and one where we cannot afford to let up. The identity theft landscape is constantly changing, as identity thieves continue to create new ways of stealing personal information and using it for their gain. We must continually review our processes and policies to ensure that we are doing everything possible to minimize the incidence of identity theft and to help those who find themselves victimized by it.

As we continue our efforts in this area, we will continue to take into account the views of the National Taxpayer Advocate. With regard to the report's preliminary recommendations, we offer the following comments.

As discussed, the IRS recently has made a number of significant improvements and we continue to work to define our processes and procedures in this area. Due to the risk that specific information about these processes and procedures could be used to facilitate fraud, we are unable to publically disclose all of our improvements with specificity.

We have greatly improved our internal coordination throughout the operating divisions and criminal investigations in dealing with identity theft issues. We will consider whether implementing Service Level Agreements between the Identity Protection Specialized Unit and the various functions is necessary. The role of the IPSU will be reviewed and modified as the various operating units begin to stand up specialized teams. We will consider whether timelines are necessary, but recognize that given the complexity of the work required in the mitigation of identity theft issues and because multiple business operating divisions will have specialized units to address their unique issues, one standardized measure may not be applicable to all situations.

The IRS is making every effort to minimize the impact of identity theft filters on legitimate taxpayers. The growth in identity theft requires the IRS to put in place new methods to stop refund fraud. We recognize that these efforts could slow refunds for some taxpayers, but we are making every effort to minimize the impact. Our communication strategy will be implemented for the filing season as appropriate.

With respect to a mitigation strategy to help legitimate taxpayers obtain their refunds on a timely basis, the IRS plans to issue a letter to filers within days of their return being identified as having a potential issue. This new letter was shared with the National Taxpayer Advocate. IRS employees will be prepared to answer calls related to the letter and equipped with procedures to post the return and allow the refund when it is determined the return was filed by a legitimate taxpayer. The IRS is also testing the filters on returns prior to the filing season to assess their accuracy.

The IRS actively notifies victims and marks taxpayer accounts when we identify that a Social Security number has been misused. We have developed a specific indicator to note taxpayer accounts when the IRS first determines that there is a likelihood of identity theft. After these accounts are marked, taxpayers receive a notice that informs them of the SSN

misuse and that their tax accounts have been corrected and marked with the identity theft indicator. We also include information on steps that taxpayers should take to protect their identities. We have issued guidance through the IRM on how to apply the account indicator and when to send a notification letter to the victim. We have several additional initiatives underway to expand our processes to notify and assist identity theft victims.

The IRS supports efforts to prevent Social Security Administration death information from public availability as such information significantly contributes to identity theft in the tax system.

The electronic filing of tax returns creates multiple benefits for taxpayers including increased accuracy of filed returns, expedited refunds and ease of use. The IRS recognizes that these same benefits are sometimes exploited by those who choose to perpetrate fraud through identity theft. We have started to offer the Identity Protection Personal Identification Number to protect known identity theft victims and prevent subsequent fraudulent filings using their stolen identity. We are taking several additional steps in this regard.

The IRS looks forward to continued collaboration with the National Taxpayer Advocate on the servicewide tax related identity theft program.

Taxpayer Advocate Service Comments

The National Taxpayer Advocate applauds the IRS for bringing the IP PIN into service in advance of the 2012 filing season, one of the many process improvements the IRS has made over the years to assist victims of identity theft. However, despite even the best communication efforts, some taxpayers will inevitably need to contact the IRS because they either never received the IP PIN or have misplaced it. The National Taxpayer Advocate reiterates the need for the IRS to develop and implement mitigation strategies as part of its normal planning. In other words, not every taxpayer who loses the IP PIN should be referred to TAS, even if he or she meets TAS criteria.[43] Instead, the IRS's mitigation strategy should anticipate the need for taxpayers who require a replacement IP PIN. It should allocate sufficient staffing, develop adequate procedures, and conduct the necessary training to help these taxpayers, with minimal impact to TAS.

While the IRS recognizes the need for a time-tracking measure for identity theft cases, it states a standardized cycle time measure may not be desired, due to the complexity and uniqueness of such cases. The National Taxpayer Advocate agrees, and suggests that the

[43] *See* IRM 13.1.7.4 (Oct. 1, 2001) (providing that "Problems that meet TAS criteria do not necessarily need to be sent to TAS when they can be immediately resolved by an operating division or function...Cases that can be resolved on the "Same Day" should not be referred to TAS unless the taxpayer makes the request.").

IRS focus on *timeliness*, rather than cycle time, in developing measures for identity theft cases. By focusing on timeliness of actions, the IRS can give its employees an incentive to keep identity theft cases moving. Whether a case involves one issue for one tax year, or six issues spanning four tax years, a timeliness measure would allow the IRS to assess whether the case truly needed a long time to resolve, or whether the case was languishing in one IRS department with no action.

The National Taxpayer Advocate is pleased to report that some genealogy websites have voluntarily agreed to curtail the availability of Death Master File information. Ancestry.com recently announced it will no longer display SSNs for anyone who has passed away within the past ten years.[44] RootsWeb.com, another genealogy site affiliated with Ancestry.com, states that it will not share information from the DMF "due to sensitivities around the information in this database."[45] These changes appear to be in response to congressional and media pressure, and should make it more difficult for identity thieves to file false tax returns. It is our hope that other websites will follow suit, and that the SSA (or Congress, if necessary) will restrict access to the DMF to those with a legitimate need for such sensitive information. The National Taxpayer Advocate commends the IRS for its support of these efforts.

Finally, the National Taxpayer Advocate is pleased that the IRS has committed to working with and including TAS on servicewide teams to address identity theft issues and procedures. She urges the IRS to include TAS representatives at all levels of planning, given TAS's unique and extensive experience with identity theft cases.

44 *See* Ancestry.com, *Why Was the Social Security Death Index Recently Changed?* http://ancestry.custhelp.com/cgi-bin/ancestry.cfg/php/enduser/sab_answer.php?p_faqid=5420&p_created=1323809913&p_sid=utw11BLk&p_accessibility=&p_redirect=&p_lva=&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Byb2RzPSZwX2NhdHM9JnBfcHY9JnBfY3Y9JnBfcGFnZT0x&p_li=&p_topview=1 (last visited Dec. 19, 2011).

45 *See* About.com, *Genealogy Sites Pressured Into Removing SSDI*, http://genealogy.about.com/b/2011/12/16/genealogy-sites-pressured-into-removing-ssdi.htm (last visited Dec. 19, 2011); Ancestry.com, *Why Was the Social Security Death Index Recently Changed?* http://ancestry.custhelp.com/cgi-bin/ancestry.cfg/php/enduser/sab_answer.php?p_faqid=5420&p_created=1323809913&p_sid=utw11BLk&p_accessibility=&p_redirect=&p_lva=&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Byb2RzPSZwX2NhdHM9JnBfcHY9JnBfY3Y9JnBfcGFnZT0x&p_li=&p_topview=1 (last visited Dec. 19, 2011); Scripps Howard News Service, *Genealogy Sites Remove Social Security Numbers of Deceased* (Dec. 15, 2011), *available at* http://www.abcactionnews.com/dpp/news/national/genealogy-sites-remove-social-security-numbers-of-deceased.

Recommendations

The National Taxpayer Advocate recommends that the IRS:

1. Implement Service Level Agreements between the Identity Protection Specialized Unit and the various functions that process case referrals and Identity Theft Assistance Requests.
2. Establish timeliness measures for identity theft case actions.
3. Before implementing identity theft filters, develop an effective and expedited mitigation strategy to help legitimate taxpayers obtain their refunds on a timely basis.
4. Require any proposed modifications to its identity theft filters mitigation strategy be approved in advance by the Identity Theft Executive Steering Committee.
5. Create and implement a national communication strategy if the identity theft filters impact a significant number of legitimate taxpayers or cause excessive processing delays.
6. In conjunction with the Social Security Administration, seek a modification of the consent judgment requiring the SSA to release the SSNs of decedents, so that the SSA can begin to partially redact SSNs (*e.g.*, release only the last four digits).
7. If a civil freeze code is implemented for referrals from law enforcement agencies, require CI personnel to determine whether such a refund freeze is necessary before applying the civil freeze code.
8. Establish a point of contact in W&I so that Criminal Investigation or other IRS operations can supply lists of victims from their investigations of identity theft schemes and W&I can promptly mark the accounts accordingly.
9. Promptly 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.
10. Allow taxpayers to turn off the ability to file electronically.

June 13, 2011

MEMORANDUM FOR RICHARD E. BYRD, JR., COMMISSIONER
WAGE AND INVESTMENT DIVISION

FROM: Nina E. Olson
National Taxpayer Advocate

SUBJECT: *Proposed Taxpayer Advocate Directive 2011-1 (Establish procedures for adjusting the taxpayer's account in instances where a tax return preparer altered the return without the taxpayer's knowledge or consent, and the preparer obtained a fraudulent refund).*

PROPOSED TAXPAYER ADVOCATE DIRECTIVE

I am issuing this proposed Taxpayer Advocate Directive (TAD) to direct the Commissioner, Wage and Investment Division to:

1) within ten days of the date of this proposed TAD, cease any collection actions on liabilities assessed against taxpayers in connection with a refund or portion of a refund that the taxpayer never received due to return preparer fraud;
2) within 45 days of the date of this proposed TAD, in consultation with the National Taxpayer Advocate, issue interim guidance to establish procedures to abate assessments and correct refund amounts where the IRS is holding a taxpayer liable for repayment of a refund or portion of a refund that the taxpayer never received due to return preparer fraud; and
3) within 90 days of the date of this proposed TAD, in consultation with the National Taxpayer Advocate, revise the Internal Revenue Manual (IRM) to provide guidance on abating assessments or correcting refund amounts where the IRS is holding a taxpayer liable for repayment of a refund or portion of a refund that the taxpayer never received due to return preparer fraud.

Please provide a written response to this proposed TAD on or before June 23, 2011.

I. Authority

This directive is being issued pursuant to Delegation Order No. 13-3, which grants the National Taxpayer Advocate the authority to issue a TAD to mandate administrative or procedural changes to improve the operation of a functional process or to grant relief to groups of taxpayers (or all taxpayers) when implementation will protect the rights of taxpayers, prevent undue burden, ensure equitable treatment, or provide an essential service to taxpayers.[1] This authority may not be redelegated.

[1] Internal Revenue Manual (IRM) 1.2.50.4, Delegation Order 13-3 (formerly DO-250, Rev. 1), *Authority to Issue Taxpayer Advocate Directives* (Jan. 17, 2001). *See also* IRM 13.2.1.6, *Taxpayer Advocate Directives*, (July 16, 2009).

In June 2009, Systemic Advocacy Analysts convened a cross-functional team to develop procedures to handle cases where a return preparer defrauded the taxpayer. Since that time, TAS has been working unsuccessfully with the other IRS functions to establish procedures to protect the government's and taxpayers' interests in cases of preparer fraud. On March 23, 2011, Director Jane E. Looney, Accounts Management (AM), informed TAS that AM will not take any action on these accounts, because "investigating preparer fraud and determining if the taxpayer benefitted from the alleged fraud is outside the scope of AM."[2] She did not suggest who within the IRS does have the jurisdiction to implement procedures. Pursuant to IRM 13.2.1.6.1.2, a proposed TAD is an appropriate response to the IRS's failure to implement procedures that would protect the rights of taxpayers and prevent undue burden.

II. Background

TAS has at least 82 cases where preparers have defrauded the government and harmed taxpayers by filing fraudulent returns to obtain larger refunds than taxpayers expect and are entitled to. These preparers altered taxpayers' tax returns without their knowledge or consent by inflating income, deductions, credits, or withholding. The taxpayers generally received refunds from the preparers in the amount the preparer advised each taxpayer that he or she should receive; each taxpayer became aware of the preparer's fraudulent activity upon hearing from the IRS when it assessed or attempted to collect the erroneous excess refund amount. Here is a basic example to illustrate the actions of the preparer.

> Taxpayer A provides her tax return preparer with her W-2 and relevant information. The preparer completes Form 1040, reflecting a zero tax liability, and indicating Taxpayer A is eligible for a $350 refund. After providing Taxpayer A with a printed copy of that return, the preparer electronically files a different return with the IRS.
>
> Taxpayer A is not aware that the preparer altered the return before he electronically filed it by inflating income and the credit for income tax withholding; the preparer reported a tax liability of $500 and withholding of $3850, thereby increasing the refund to $3,350. Unbeknownst to Taxpayer A, the return preparer designated two bank accounts into which the $3,350.00 refund is split: $350.00 is direct-deposited into Taxpayer A's account and the balance of $3,000.00 is direct-deposited into the preparer's own account. Thus, Taxpayer A has received the refund to which she thought she was entitled, based on the copy of the return she approved and the preparer provided to her.
>
> The IRS selects Taxpayer A's return for examination the following year. The IRS disallows Taxpayer A's excess withholding and proposes a deficiency of $3,000.00 (plus penalty and interest).

[2] Jane E. Looney, Memorandum re: *Taxpayer Assistance Order* ***** (Mar. 23, 2011) (taxpayer name redacted).

In cases where a tax liability in excess of the taxpayer's true liability is assessed as a result of the preparer's actions, the IRS has refused to abate the excess tax as required by law and per advice from the Office of Chief Counsel, discussed below. In addition, even if the preparer's actions resulted in a larger refund than what the taxpayer was entitled to receive but did not result in an additional tax assessment, the IRS has refused to adjust the taxpayers' accounts for the erroneous balances due from the fraudulent portions of the refunds. Instead, the IRS holds taxpayers liable for any understatement of tax, penalties, and interest, as well as the amount of the refund that the IRS issued to the preparer. The IRS's failure to provide guidance to its employees about the proper handling of this type of case is evident by the following response received from Accounts Management in response to an Operations Assistance Request issued by TAS:

> The refund was traced and the financial institution indicates that the refund was deposited as requested and the funds are not available - per IRM 21-4.1.3.4 NOTE: If the taxpayer alleges preparer fraud as the reason for non-receipt of the refund, advise the taxpayer that while the IRS will conduct a trace to determine the deposition of the refund, the restoration of the refund to the taxpayer may become a civil matter.[3]

In that particular TAS case, the actions of the preparer resulted in the IRS offsetting the taxpayer's refunds in the following two tax years. Instead of offsetting the taxpayer's refunds, however, the IRS should have instituted procedures to adjust the taxpayer's account and not hold the taxpayer liable for the portion of the refund that the preparer received.

III. Reasons for Issuing this Proposed TAD

The IRS has failed to develop procedures that are consistent with the Internal Revenue Code and legal advice provided by the IRS Office of Chief Counsel. In this regard, Counsel has issued two memorandums (copies attached) that directly relate to this issue. The memorandum regarding *Horse's Tax Service* (Attachment 1) addresses whether an electronically filed tax return that was altered without the taxpayer's knowledge is a valid return.[4] Counsel analyzed the four-part test set forth in *Beard v. Commissioner,*[5] and concluded that when the taxpayer is unaware of the alterations to the return and the version that the taxpayer reviewed is not what the preparer filed with the IRS, the taxpayer did not sign that return under penalties of perjury. Consequently, the return filed by the preparer is a nullity and any assessment on the IRS's books and records relating to that return is invalid. Counsel further advised that the taxpayer should file an *original* return (not an amended return) so that the IRS can then adjust the taxpayer's Master File account to reflect the correct tax information. Thus, in situations where the taxpayer can prove that the version of

3 TAS, TAMIS Case File No. 4903292. IRS, OAR 1543701 Response (Jan. 28, 2011).

4 IRS Office of Chief Counsel, PMTA 2011-013 (May 12, 2003). The name of the preparer was changed to remove the identity of the preparer due to confidentiality concerns.

5 *Beard v. Commissioner*, 82 T.C. 766, 777 (1984), *aff'd per curiam*, 793 F.2d 139 (6th Cir. 1986). The test for a valid return is: (1) there must be sufficient data to calculate tax liability; (2) the document must purport to be a return; (3) there must be an honest and reasonable attempt to satisfy the requirements of the tax law; and (4) the taxpayer must execute the return under penalties of perjury.

the tax return that he or she reviewed is not the version the preparer filed with the IRS, the IRS should reverse the accounting entries on the taxpayer's module.

Even in situations where the taxpayer cannot produce a copy of a return from the preparer that is different than what the preparer filed with the IRS, Counsel has nonetheless advised that certain adjustments to the taxpayer's account are appropriate so that the taxpayer is not held liable for a refund (or portion thereof) fraudulently obtained by the preparer. In this regard, the memorandum entitled *Refunds Improperly Directed to a Preparer* (Attachment 2) specifically discusses the ability of the IRS to abate any improper amount of tax and withholding based on Internal Revenue Code (IRC) § 6404(a).[6] The memorandum specifically states:

> The portion of each refund that reflected the difference between the refund amount the client thought was being obtained and the amount that the Preparer included on the electronically filed return... deposited to the Preparer's account) should be attributed to the Preparer, and not to the client.

While abatement may not be appropriate in every case (*e.g.*, the preparer's actions resulted in a larger refund but did not result in an additional tax assessment, so there would be no tax to abate), the memorandum makes clear that the IRS "can and should adjust" each affected taxpayer's account for any refund (or portion thereof) illegally obtained by the preparer.

Moreover, part of the Wage and Investment Division's mission is "to protect the public interest by applying the tax law with integrity and fairness to all."[7] Requiring a taxpayer to repay a refund that he or she did not receive or have knowledge of is inequitable and unjust. The preparers defrauded the taxpayers by filing altered returns to illegally obtain refunds from the IRS. The IRS should take all available actions to protect taxpayers, to abate any improper assessments, and to expunge the refunds or portion of refunds from the taxpayers' accounts that the preparers received. Otherwise, the IRS itself is victimizing the disreputable preparer's victims.

IV. Conclusion

In light of the significant harm taxpayers are suffering as a result of the IRS's inability to develop a process for providing relief to these taxpayers over the last two years, I direct the IRS to:

- Cease any collection actions on liabilities assessed against taxpayers in connection with a refund or portion of a refund that the taxpayer never received due to return preparer fraud within ten days of this directive;

6 IRS Office of Chief Counsel, POSTN-145098-08 (Dec. 17, 2008).

7 *See* http://win.web.irs.gov/aboutus/aboutus_goals.htm#Mission (last viewed May 5, 2011).

- Issue an interim guidance memorandum (IGM), developed in consultation with the National Taxpayer Advocate, within 45 days of this directive; and
- Revise the IRM within 90 days of this directive to instruct IRS employees how to correct the taxpayers' accounts to reflect the removal of the inflated refund received by the return preparer.

I issued the attached interim guidance memorandum that the IRS can use as a model to identify accounts with preparer refund fraud issues and the documentation needed to ensure that taxpayers are only held liable for the actions of their preparer in appropriate circumstances.

Attachments:

(1) Office of Chief Counsel, PMTA 2011-13, *Horse's Tax Service* (May 12, 2003).

(2) Office of Chief Counsel, POSTN-145098-08, *Refunds Improperly Directed to a Preparer* (Dec. 17, 2008).

(3) National Taxpayer Advocate, *Interim Guidance on Recognizing and Assisting Victims of Refund Preparer Theft*, TAS-13.1.10-0311-004 (Mar. 14, 2011).

cc w/attachments: Steve Miller, Deputy Commissioner, Services and Enforcement