MSP #4 The IRS Has Failed to Provide Effective and Timely Assistance to Victims of Identity Theft

RESPONSIBLE OFFICIALS

Peggy Bogadi, Commissioner, Wage and Investment Division
Becky Chiaramida, Director, Office of Privacy, Governmental Liaison, and Disclosure

DEFINITION OF PROBLEM

In general, tax-related identity theft occurs when an individual intentionally uses the personal identifying information of another person to file a false tax return with the intention of obtaining an unauthorized refund.[1] 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 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. In addition, identity theft takes a significant toll on the IRS, tying up limited resources that the IRS could shift to taxpayer service or compliance initiatives.

In April 2008, former Commissioner Shulman appeared before Congress and stated, "My overall goal as the IRS Commissioner is that when a taxpayer contacts us with an issue or concern, we have in place a seamless process that gets the issue resolved promptly."[2] In October 2008, the IRS established the Identity Protection Specialized Unit (IPSU), a unit dedicated to assisting victims of identity theft. However, the Commissioner's vision has yet to be realized. The help the IRS has offered to the victims of this crime has been anything but seamless and prompt.

The National Taxpayer Advocate has written and testified extensively about the impact of identity theft on taxpayers and tax administration, and has made many specific, concrete recommendations to improve IRS efforts to assist taxpayers who become identity theft victims.[3] While the IRS has adopted several of TAS's recommendations, it has not responded with the urgency that the identity theft crisis demands. Despite the proclamation of the Commissioner to Congress that identity theft is a top priority, victims who come to the IRS for assistance today will routinely need to speak with multiple employees and wait more

1 This type of tax-related identity theft is referred to as "refund-related" identity theft. In "employment-related" identity theft, an individual files a tax return using his or her own tax identification number, but uses another individual's Social Security number (SSN) to obtain employment, and consequently, the wages are reported to the IRS under the SSN. The IRS has procedures in place to minimize the tax administration impact to the victim in these employment-related identity theft situations. Accordingly, we will focus on refund-related identity theft in this report.

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

3 *See, e.g.*, 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*); *Identity Theft and Income Tax Preparation Fraud*, Hearing Before the H. Comm. on the Judiciary, Subcomm. on Crime, Terrorism, and Homeland Security, 112th Cong. (statement of Nina E. Olson, National Taxpayer Advocate) (June 28, 2012).

than six months to have their issues resolved. In fact, the IRS has now established 21 different units to address identity theft cases,[4] many with their own rules and procedures — a far cry from the initial vision of the centralized "traffic cop" function the National Taxpayer Advocate recommended and the Commissioner committed to in 2008.

Meanwhile, tax-related identify theft continues to grow at an alarming pace. In fiscal year (FY) 2012, the IPSU received nearly 450,000 cases, a 78 percent increase over FY 2011.[5] TAS has experienced a similar increase in stolen identity case receipts; an increase of over 60 percent from FY 2011 to FY 2012, and an increase of more than *650 percent* from FY 2008.[6] Identity theft cases comprise 25 percent of TAS's FY 2012 case receipts and were the number one issue in TAS case receipts for the last two fiscal years.[7]

Identity theft cases are complex, often encompassing multiple issues and tax years.[8] TAS case advocates are unique in that they both serve as a single point-of-contact for taxpayers and work to resolve all of the taxpayer's related issues completely before closing cases. Despite TAS's extensive experience working complex identity theft cases, TAS was not afforded an opportunity to review the IRS's procedures before some of the specialized identity theft units became operational. The National Taxpayer Advocate believes the IRS's failure to draw upon the collective expertise of TAS and its employees is a significant oversight that will result in less effective case-resolution procedures.

As of September 30, 2012, the IRS had almost 650,000 identity theft cases in inventory servicewide.[9] Much of the IRS's focus in the past few years has been on revenue protection (that is, developing filters designed to prevent the payout of questionable refund claims). The National Taxpayer Advocate urges the IRS to expend as much effort as necessary to reduce the time it takes to fully resolve an identity theft victim's case.

The National Taxpayer Advocate is concerned that:

- The IRS is moving backward — away from a centralized approach to assisting identity theft victims — and is increasing the risk that taxpayer-victims may fall through the cracks;
- After years of ineffective efforts to reengineer its processes, the IRS still takes too long to fully resolve the accounts of victims;

4 *See* IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Oct. 24, 2012).

5 IRS, *IPSU Identity Theft Report* (Sept. 29, 2012). 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. Total IRS FY 2012 ID Theft receipts were 449,809 compared to 253,051 in FY 2011, an increase of 77.8 percent.

6 TAS analysis of Taxpayer Advocate Management Information System (TAMIS) data. TAS received 54,748 ID theft cases in FY 2012, compared with 34,006 in FY 2011, and 7,147 in FY 2008 for an increase of 666.0 percent

7 *Id.* TAS received 54,748 ID theft cases in FY 2012, or 24.9 percent of its 219,666 total cases.

8 *Id.* TAS received 54,748 ID theft cases in FY 2012, of which 37,307 (68.1 percent) included more than one issue code per case.

9 *See* IRS Identity Theft Advisory Council, Identity *Theft Status Update* (Oct. 24, 2012). Actual number is 646,950.

- While the Identity Protection Personal Identification Number (IP PIN) that the IRS has developed provides additional security, it does not cover all victims;
- The Taxpayer Protection Unit may not be sufficiently staffed to handle the volume of calls from impacted taxpayers;
- Congress may unnecessarily create additional exceptions to taxpayer privacy protections; and
- The Social Security Administration still makes the Death Master File available to the public, creating an opportunity for identity thieves to steal and then misuse personal information.

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 National Taxpayer Advocate has consistently urged the IRS to improve its strategy for assisting identity theft victims. Since 2004, the National Taxpayer Advocate included identity theft as a Most Serious Problem six times in her Annual Report to Congress.[10] In just the past year, the National Taxpayer Advocate has testified about this topic before Congress in five separate hearings.[11]

10 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.

11 *See Identity-Theft Related Tax Fraud*, Hearing Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency and Financial Management, 112th Cong. (Nov. 29, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *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).

In addition, former Commissioner Shulman (or his designee) has discussed the problem in at least five hearings before Congress.[12] The IRS has established numerous task forces and Lean Six Sigma teams focused on improving identity theft processes. Despite all of this attention, victims who need their tax accounts corrected quickly and effectively still face many of the same issues they did five years ago — a labyrinth of procedures and drawn-out timeframes for resolution.[13]

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

In former Commissioner Shulman's first month in office, 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.[14]

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. As discussed below, 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 — hardly the single point of contact envisioned.

In 2011, the IRS convened yet another task force to look at its victim assistance strategy. In the view of many participants, the external consulting firm leading this task force came

12 *See 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 Steven T. Miller, IRS Deputy Commissioner for Services and Enforcement); *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 Steven T. Miller, IRS Deputy Commissioner for Services and Enforcement); *Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service*, Hearing Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency, and Financial Management, 112th Cong. (Nov. 4, 2011) (statement of Steven T. Miller, IRS Deputy Commissioner for Services and Enforcement); *IRS E-File and Identity Theft*, Hearing Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency, and Financial Management, 112th Cong. (June 2, 2011) (statement of Doug Shulman, IRS Commissioner); *Identity Theft in Tax Administration*, Hearing Before the Senate Committee on Finance, 110th Cong. (Apr. 10, 2008) (statement of Doug Shulman, IRS Commissioner).

13 Unfortunately, the IRS did not track cycle time on identity theft cases until this year, so we have no empirical data on ID theft case cycle time to analyze.

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

in with the pre-conceived notion that the IRS should move away from centralized victim assistance and toward a specialized approach. Based upon a recommendation from this task force, IRS leadership decided to create a specialized unit *within each of its 21 individual departments* (or functions) to work on identity theft cases.[15] 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).[16] The IRS maintains that transfers of cases between functions 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.

In 2012, each function was asked to develop procedures for its embedded identity theft unit. The IRS-wide Office of Privacy, Governmental Liaisons, and Disclosure (PGLD) was tasked with compiling and reviewing such procedures to ensure some level of consistency. Although TAS has asked to review these procedures before these embedded units became operational in October 2012, we were not afforded this opportunity in all cases. At least three of these embedded specialized units began work without having their procedures reviewed by TAS.[17]

In addition, PGLD is coordinating the development of employee guidance that spells out how and when a taxpayer's case will be moved from one embedded unit to another. Although the National Taxpayer Advocate and Taxpayer Advocate Service staff have asked to review such procedures to ensure that they do not increase taxpayer burden or impair taxpayer rights, as of October 26, 2012, PGLD has not shared a final transfer matrix with TAS for review.

The National Taxpayer Advocate firmly believes that the IRS needs a centralized body (such as the IPSU) to serve as the "traffic cop." Identity theft cases are often complex, requiring adjustments by multiple IRS departments.[18] 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 our view, the IPSU 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 or memorandum

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

16 If a function contemplates a scenario in which it would not work all aspects of the case, it would submit a request for exception to the office of Privacy, Governmental Liaison, and Disclosure (PGLD). PGLD is currently developing a transfer matrix to facilitate such transfer requests.

17 The Compliance Post-Adjustment Team and Designated Identity Theft Adjustment 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 sharing its procedures with PGLD or TAS prior to stand up.

18 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).

of understanding with the IPSU and be held accountable for meeting established deadlines for taking actions.[19]

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.[20]

Identity Theft Cases Now Comprise 25 Percent of TAS Case Receipts and Clearly Show That Many Identity Theft Cases Involve More Than One Issue.

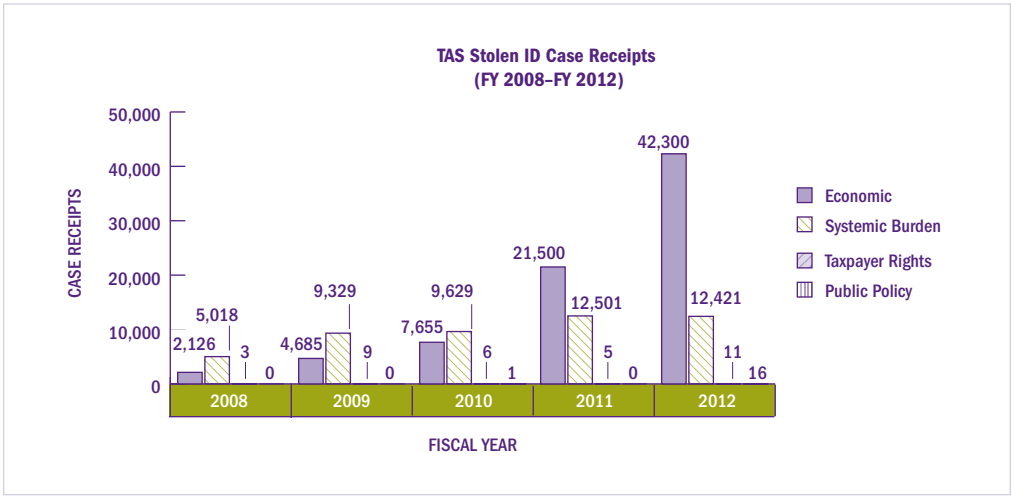
When established IRS procedures do not work as intended, taxpayers turn to the Taxpayer Advocate Service for assistance. The volume of identity theft cases in TAS has risen each year since the IRS established the IPSU, from about 7,100 in FY 2008 to nearly 55,000 in FY 2012, an increase of more than 650 percent.[21]

19 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.

20 From the outset, the National Taxpayer Advocate has inquired about the role of the IPSU in the new specialized environment. After months of what appeared to be stonewalling, 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 appeared to have no real decision-making authority with respect to the IPSU's interaction with the embedded specialized units.

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

FIGURE 1.4.1, TAS Stolen Identity Case Receipts, FY 2008 to FY 2012[22]



In FY 2012, identity theft cases constituted 25 percent of TAS's case receipts, more than any other issue in TAS case inventory. Moreover, identity theft has been the top issue in TAS case receipts for the last two fiscal 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 in the case and, by inference, what functions TAS must work with to resolve all the tax issues completely before closing the case. In fact, identity theft cases are complex, often encompassing multiple issues and tax years. The table below shows the various secondary issues associated with TAS identity theft cases closed in FY 2012.

22 *Id.* TAS received 54,748 identity theft cases in FY 2012, out of 219,666 total cases (24.9 percent).

TABLE 1.4.2, FY 2012 TAS Identity Theft Closures by Secondary Issue[23]

Top Ten Secondary Issues	Closed Cases	Avg. Case Age (Days)
Unspecified [24]	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**

For example, if there is a problem with an unpostable return, TAS would need to interact with the Submission Processing function. If there are issues related to wage or withholding verification, TAS would coordinate with the Accounts Management Taxpayer Assurance Program (AMTAP) function. With levy or offset issues, TAS may need to deal with the Collection function. Any given case could involve several tax years with any combination of these issues. It is highly unlikely that 21 separate units will be able to resolve complex cases involving multiple units without a "traffic cop" that owns the case, serves as the taxpayer's single point-of-contact, and is ultimately held responsible for its timely and correct resolution.

The IRS Still Takes Much Too Long to Fully Resolve the Accounts of Identity Theft Victims.

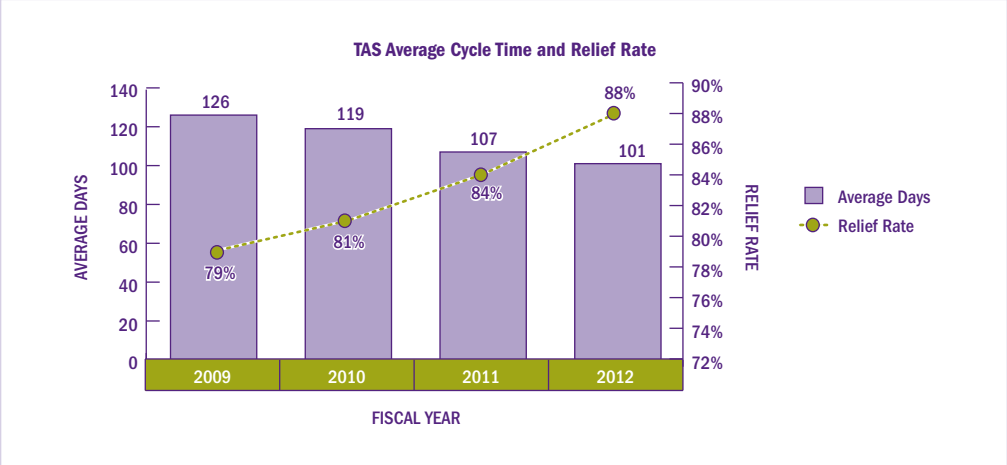
As discussed above, the National Taxpayer Advocate and TAS understand all too well that identity theft cases can be very complex, and, it takes time to work through all related issues. When TAS accepts a case, TAS case advocates must work with the appropriate IRS function to get them to make the necessary decisions and take the appropriate steps to resolve issues. Case advocates set specific timeframes within which those actions must be completed by the IRS functions. Thus, TAS case cycle time represents the "best case" for identity theft victims – there is someone watching over the IRS and making sure that it takes actions timely and correctly, and that cases don't languish or disappear between functions.

23 Data obtained from TAMIS on October 16, 2012.

24 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.

The chart below shows the average number of days it took TAS to close a stolen identity case from FY 2009 to FY 2012, along with the relief rate obtained in those cases. As the chart shows, since FY 2009, TAS's identity theft case cycle time decreased by 20 percent, even as its relief rate rose from 79 percent to 88 percent.[25] In other words, in 88 percent of the cases, taxpayers who came to TAS were the victims of identity theft and entitled to relief.

FIGURE 1.4.3, TAS Stolen Identity Case Cycle Time and Relief Rate, FY 2009 to FY 2012[26]



In 2008, former Commissioner Shulman made a commitment that the IRS would resolve identity theft victims' tax accounts "promptly." The IRS cannot determine how well it has done in meeting this commitment, because until this year, the IRS had no ability to track identity theft case inventory, much less monitor how long it takes to resolve cases. Even today, while some IRS functions track the length of time a case is in its inventory, the IRS cannot provide an overall average cycle time for its identity theft cases. For one prominent category of identity theft work, the IRS reports an average closure time of 196 days.[27]

We are by no means attempting to minimize the complexity of identity theft cases, but taking well over six months to close an identity theft case is simply not acceptable for the hundreds of thousands of victims. Remarkably, rather than acknowledging the need to

25 Analysis of TAMIS data conducted on October 17, 2012. One reason for the decrease in cycle time is a favorable change in IRS procedures. When we first started writing about identity theft, the IRS had no procedures that would allow its employees to determine the rightful owner of an SSN in question. Instead, the IRS would send the case to the Social Security Administration (SSA) for resolution, which would routinely take two years. *See* IRM 21.6.2.4.4.2 (Oct. 1, 2012). In the 2005 Annual Report, the National Taxpayer Advocate recommended that the IRS train and empower its employees to make such determinations without involving the SSA. *See* National Taxpayer Advocate 2005 Annual Report to Congress 183. Today, the IRS not only allows its employees to determine SSN ownership based on documentation, but uses data mining to speed up the process even more. We view this as a significant advance and applaud the IRS for this change.

26 Analysis of TAMIS data conducted on October 16, 2012.

27 *See* IRS response to information request (Nov. 5, 2012). IDTX (monitoring tax-related identity theft cases) cases were open an average of 196 days.

work identity theft cases faster and streamlining its procedures, the initial IRS response has been to lower taxpayers' expectations. In September 2012, the IRS instructed employees to advise identity theft victims that *it would take 180 days to resolve their cases.*[28] (These instructions were rescinded shortly thereafter when the National Taxpayer Advocate objected to its release.)

One consequence of the IRS taking so long to resolve an identity theft case is that many victims will enter the following filing season with unresolved account issues. Because the IRS will generally issue identity protection personal identification numbers (discussed later) only to taxpayers with fully resolved identity theft issues, many victims will still be at risk of having a perpetrator steal their refund again the following year, and will require further assistance later on. To avoid such consequences, the IRS must ensure that identity theft cases do not languish and must strive to resolve them completely in well under six months.

The National Taxpayer Advocate believes the IPSU, in its role as the "traffic cop," needs more effective tools to achieve this goal. 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.[29] The IPSU has no way to ensure that the other functions adhere to the requested timeframes. The IPSU should enter into agreements with each of the specialized units working identity theft cases to specify timeframes for action, along with consequences for not meeting the timeframes.

While the Identity Protection Personal Identification Number 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 (IP PINs) to about 250,000 victims whose identities and addresses it has verified.[30] 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 it 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 600,000 participants. We 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 resolved. Contrary to IRS practice, the

28 SERP Alert 12A0535, *Identity Theft Timeframe - 180 Days* (Sept. 4, 2012).

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

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

protection of the taxpayer should begin as soon as the SSN owner and address is verified. Tying the IP PINs to *closing* of the identity theft case unnecessarily delays this protection.

From the inception of the program, TAS has advocated for immediate delivery of the IP PIN to victims whose identities and addresses the IRS has verified. The IRS advised that it could not do this systemically for the 2012 filing season, but would be open to it for the following year. Yet the IRS still does not allow identity theft victims to be assigned IP PINs throughout the year, increasing the risk of delay and economic hardship to taxpayers who have already been victimized at least once.

We note that many of the nearly 650,000 victims with cases in inventory will not be afforded the protection of the IP PIN because their cases will not be fully resolved by the time IP PINs are mailed out, which means their accounts will be unprotected from fraudulent filings.[31] This is another reason why it is imperative that the IRS work through identity theft cases as soon as it can. To this end, the IRS has diverted personnel from Taxpayer Assistance Centers and other departments to assist with the backlog of identity theft cases, and continue working on them during the 2013 filing season.[32]

In October 2012, the National Taxpayer Advocate expressed concern to W&I management that the nearly 22,000 taxpayers with stolen identity cases in TAS inventory would not receive the benefit of the protections afforded by the IP PIN for the 2013 filing season.[33] The Accounts Management (AM) unit shared this concern and worked feverishly to develop a work-around solution. For identity theft cases that have been through the Electronic Fraud Detection System, the IRS would place an "S" indicator on the account to signify the true SSN owner and an "N" indicator on the account to signify the non-SSN owner. (At the National Taxpayer Advocate's suggestion, the IRS refrained from using the typical "good"/"bad" designation.) We are 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. However, 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.

It is inevitable that a certain percentage of taxpayers will misplace or forget to use the IP PIN. Despite the IRS's attempts to verify the taxpayers' addresses, over 9,000 letters

31 The inventory of identity theft cases at the end of FY 2012 was 646,950. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Oct. 24, 2012).

32 To assist with the backlog of identity theft cases in Accounts Management, the IRS temporarily moved 170 employees from Taxpayer Assistance Centers (TACs). Diverting these TAC employees to work identity theft issues reduces their availability to assist taxpayers in other matters. *See* Most Serious Problem: *The IRS Lacks a Servicewide Strategy that Identifies Effective and Efficient Means of Delivering Face-to-Face Taxpayer Services, infra.*

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

containing the IP PINs were returned undeliverable in 2012.[34] In addition, the IRS received almost 23,000 (about nine percent) requests for replacement IP PINs in 2012.[35]

Without replacement numbers, these taxpayers will need to file paper returns and be subject to additional scrutiny and delay. The IRS says that for the 2013 filing season, it will be easier and quicker to obtain a replacement, as taxpayers can request a new PIN by phone from any IRS customer service representative after validating their identity.

The Taxpayer Protection Unit Requires Sufficient Staffing to Handle the Volume of Calls from Impacted Taxpayers.

In the current environment, the IRS is under tremendous pressure to protect Treasury revenue from improper refund claims. During the 2012 filing season, the IRS designed and implemented several identity theft filters to weed out suspicious returns. Through data mining, programmers attempted to detect trends based on a variety of factors and develop customized filters to isolate suspicious claims for refunds.

The IRS notified affected taxpayers by letter that it had a problem processing their returns and instructed them to call the new Taxpayer Protection Unit (TPU) to provide more information.[36] Initially, this unit was woefully understaffed to handle the volume of calls from taxpayers trying to figure out why their returns were not being processed. For the week ending March 10, 2012, the level of service (LOS) on this unit's phone line was a dismal 11.7 percent. This means the IRS failed to answer eight of every nine calls — and taxpayers who got through had to wait on hold an average of an hour and six minutes![37]

The chart below shows the level of service and average wait time for the TPU toll-free line for March and April 2012, at the height of the filing season.

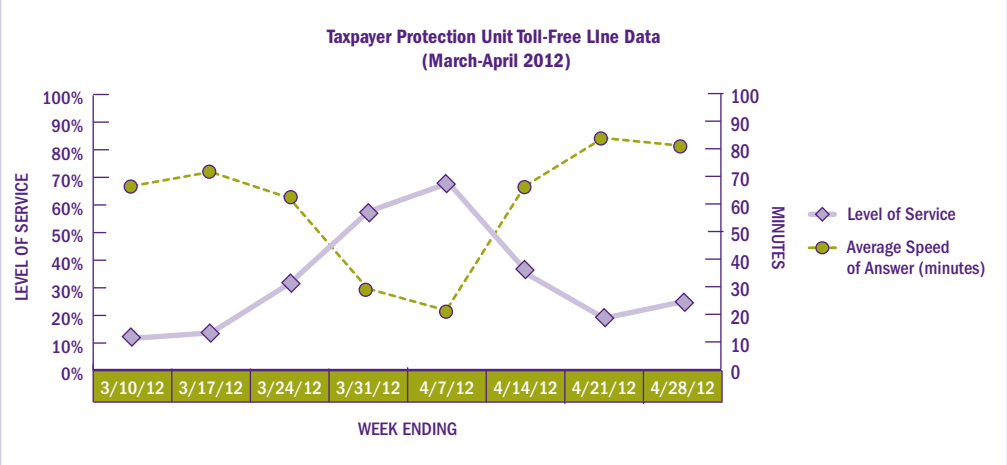
34 9,137 letters containing IP PINs were undeliverable through September 30, 2012. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Aug. 23, 2012).

35 The IRS received 22,814 requests for replacement IP PINs during 2012 (January through September 30, 2012). IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Aug. 23, 2012). The actual number of taxpayers who requested a replacement IP PIN was 20,848. *See* IRS, *IP PIN Replacement Program* (Apr. 5, 2012).

36 The Taxpayer Protection Unit should not be confused with the IPSU, which assists victims of identity theft. The number to the TPU phone line was provided to taxpayers who received a letter due to the identity theft filters implemented in the 2012 filing season. Victims of identity theft are still instructed to call the toll-free line operated by IPSU.

37 The average speed of answer was 3,991 seconds. IRS, Joint Operations Center Executive Level Summary Report (Mar. 10, 2012).

FIGURE 1.4.4, Taxpayer Protection Unit Toll-Free Line Data (Mar. and Apr. 2012)[38]



In the following weeks, the IRS provided additional staffing for the TPU in an attempt to boost the level of service. During FY 2012, the TPU had achieved an overall LOS of 45.5 percent, about half the 85 percent goal.[39]

It seems not only that the IRS misjudged the number of customer service representatives needed to staff this line, but also that the identity theft filters have picked up more returns than anticipated. *With such a low level of service, it is impossible to assign legitimacy to any IRS estimate of the filters' accuracy.* If fewer than half of the attempts at calling the number listed in the notice get through to the TPU, how can the IRS accurately assess the success of the identity theft filters?

Creating New Exceptions to Taxpayer Privacy Protections Poses Risks and Should Be Approached Carefully, If at All.

In the 2011 Annual Report to Congress, the National Taxpayer Advocate recommended that Congress enact a comprehensive Taxpayer Bill of Rights, and suggested that the right to confidentiality is one of those core taxpayer rights.[40] Taxpayers have the right to expect that any information they provide to the IRS will not be used or disclosed by the IRS unless authorized by the taxpayer or other provision of law.

The Internal Revenue Code (IRC) contains significant protections for the confidentiality of returns and return information. IRC § 6103 generally provides that returns and return information shall be confidential and then delineates a number of exceptions to this general rule. Section 6103(i)(2) authorizes the disclosure of return information in response to requests from federal law enforcement agencies for use in criminal investigations. There

38 IRS, Joint Operations Center, Executive Level Summary Reports (Mar. 10 - Apr. 28, 2012).

39 *See* IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Oct. 24, 2012).

40 National Taxpayer Advocate 2011 Annual Report to Congress 505.

is no corresponding exception in IRC § 6103 that allows for the release of identity theft information to *state or local* agencies.[41] However, IRC § 6103(c) provides that a taxpayer may consent to disclosure of returns and return information to any person designated by the taxpayer.

Some have called for the expansion of exceptions to IRC § 6103, ostensibly to help state and local law enforcement combat identity theft. The National Taxpayer Advocate has significant concerns about loosening taxpayer privacy protections and does not believe that such an expansion of the statute is appropriate at this time. The current framework of IRC § 6103 includes sufficient exceptions to allow the IRS to share information about identity thieves.

The IRS Office of Chief Counsel has advised that the IRS may share the "bad return" and other return information of an identity thief with other federal law enforcement agencies investigating the identity theft.[42] In light of this advice, the IRS has implemented a pilot program in the state of Florida to facilitate a consent-based sharing of identity theft information with state and local law enforcement agencies.[43] Through August 23, 2012, the IRS received 664 requests from identity theft victims to share information.[44] The IRS stated that it is aware of press articles covering a couple of indictment/arrest type scenarios related to information provided under the pilot program. It should be noted there is no requirement for state and local agencies to provide data regarding the outcome of cases related to the waiver pilot.

We believe this approach strikes an appropriate balance — protecting taxpayer return information while simultaneously giving state and local law enforcement authorities more information to help them investigate and combat identity theft. However, we are concerned that once the information is in the hands of state and local law enforcement, there is no prohibition in the tax code against redisclosure. Therefore, the National Taxpayer Advocate suggests that Congress consider modifying IRC § 6103(c) to explicitly limit the use of tax return information to the purpose agreed upon by the taxpayer (*i.e.*, to allow state or local law enforcement to use the information solely to enforce state or local laws) and to prohibit the redisclosure of such information.[45]

41 Note, however, that certain disclosures to state law enforcement are permissible. *See* IRC § 6103(i)(3)(B)(i) (disclosure of return information, including taxpayer return information, can be made to the extent necessary to advise appropriate officers or employees of any state law enforcement agency of the imminent danger of death or physical injury to any individual; disclosure cannot be made to local law enforcement agencies). While identity theft may cause emotional and economic injury, the typical identity theft situation does not pose an imminent danger of death or physical injury.

42 IRS Office of Chief Counsel Memorandum, *Disclosure Issues Related to Identity Theft*, PMTA 2012-05 (Jan. 18, 2012).

43 The IRS has expanded the pilot program to work with law enforcement in eight additional states: Alabama, California, Georgia, New Jersey, New York, Oklahoma, Pennsylvania, and Texas. *See* http://www.irs.gov/uac/Law-Enforcement-Assistance-Pilot-Program-on-Identity-Theft-Activity-Involving-the-IRS (last visited Nov. 9, 2012).

44 E-mail from Senior Advisor, Criminal Investigation Division, Refund Crimes (Aug. 27, 2012).

45 *See* National Taxpayer Advocate 2011 Annual Report to Congress 505.

In the meantime, the IRS should insert into every agreement with state and local agencies an explicit clause that says this information may only be used for prosecution of identity theft-related crimes. Any other disclosure or use should void the agreement.

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

The federal government unwittingly facilitates 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.[46] The SSA characterizes release of this information as "legally mandated" under the Freedom of Information Act,[47] but this position has not been tested.[48] To eliminate uncertainty, the National Taxpayer Advocate recommended in 2011 that Congress pass legislation to clarify that public access to the DMF can and should be limited.[49]

The National Taxpayer Advocate has raised this issue at every opportunity over the past two years.[50] Although some genealogy websites have voluntarily agreed to curtail the availability of DMF information, not much has been done by either Congress or the executive branch. In the meantime, taxpayers continue to face harm due to the inaction of the government.[51] Thus, while waiting for legislative action, the National Taxpayer Advocate urges the SSA to reconsider its legal analysis and take steps to restrict access to the DMF.

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

TAS employees work each case they receive until all related issues are resolved. TAS employees also interact with every IRS function during the course of working cases. Their global perspective, along with the experience 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 consider TAS as equal partners and include TAS representatives in all levels of identity theft program and procedural planning, including front-line teams, training development, guidance, and advisory and executive steering committees.

---

46 *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).

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

48 *Social Security and Death Information*, Hearing Before H. Comm. on Ways & Means, Subcomm. on Soc. Security, 112th Cong. (statement of Michael J. Astrue, Commissioner of Social Security) (Feb. 2, 2012).

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

50 *See* National Taxpayer Advocate FY 2012 Objectives Report to Congress xxvii (June 2011); National Taxpayer Advocate 2011 Annual Report to Congress 9, 519; *Identity Theft and Tax Fraud*, Hearing Before the Subcomm. on Oversight and Social Security, H. Comm. on Ways and Means, 112th Cong. (statement of Nina E. Olson, National Taxpayer Advocate) (May 8, 2012); National Taxpayer Advocate FY 2013 Objective Report to Congress 12 (June 2012).

51 For a detailed analysis of the government's obligation to release personal information of decedents, see *Identity Theft and Tax Fraud*, Hearing Before the Subcomm. on Oversight and Social Security, H. Comm. on Ways and Means, 112th Cong. (statement of Nina E. Olson, National Taxpayer Advocate) (May 8, 2012).

CONCLUSION

When former Commissioner Shulman took office in 2008, he expressed to Congress a specific plan of action to address identity theft victim assistance. Almost five years later, it is evident that the IRS has not accomplished its goals of providing seamless account resolution in a timely fashion.

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

1. Issue IP PINs throughout the year, as soon as the identities and addresses of the rightful SSN owner are verified. The issuance of IP PINs should not be tied to the final resolution of an identity theft case.
2. Retain the Identity Protection Specialized Unit as the single point of contact with identity theft victims throughout the duration of their cases.
3. Move the Identity Protection Specialized Unit out of the Accounts Management function, to afford it greater autonomy as it acts as the face of the IRS to identity theft victims.
4. Expand the Identity Protection Specialized Unit's role in managing identity theft case resolution, such as conducting initial and final global account reviews on all identity theft cases.
5. Provide sufficient staffing for the Identity Protection Specialized Unit to take on this expanded role.
6. Implement agreements between the Identity Protection Specialized Unit and the various functions that work identity theft cases to set forth acceptable timeframes for completing the required actions and consequences for not meeting the timeframes.
7. Strive for a Level of Service within the Taxpayer Protection Unit equal to or greater than the Level of Service goal set for the main toll-free phone line.
8. Insert into every agreement with state and local agencies an explicit clause that says that return information of an identity thief may be used only for prosecution of identity theft-related crimes (with no redisclosure to third parties).
9. Together with the Social Security Administration, seek modification of the consent judgment requiring the release of personal identifying information of decedents.
10. Include TAS at all levels of identity theft program and procedural planning, including front-line teams, training development, guidance, and advisory and executive steering committees.

IRS COMMENTS

Combating identity theft and providing victim assistance are top priorities of the IRS. The IRS is committed to helping the victims of identity theft and, while more work remains, we have made significant progress this year. As the report recognizes, identity theft cases are complex, often encompassing multiple issues and tax years. Although we cannot stop all identity theft, our efforts in filing season 2012 provide a solid foundation upon which we will continue to build and improve. During the first ten months of this calendar year, the IRS protected more than $20 billion of revenue related to fraudulent returns, including identity theft. We strengthened our preventative measures to catch identity theft before erroneous refunds are issued and increased our investigative efforts to detect and prosecute perpetrators of refund fraud.

We continually review our policies and procedures to ensure we are doing everything possible to minimize the incidence of identity theft, help victims, and investigate perpetrators. Once a legitimate taxpayer's account is identified, marked, adjusted, and closed, it is the IRS's intent to ensure that future filings of returns by these taxpayers are protected from further harm or burden. Business rules are implemented to identify unique characteristics of fraudulent returns submitted by identity thieves, and used as a basis for rejecting them if these characteristics surface. We have also implemented new procedures to resolve cases more efficiently and accurately, as well as found additional ways to reduce customer burden. These efforts include, but are not limited to the following:

- Implementing programming to identify returns with ID theft documentation;
- Revising procedures to utilize Information Returns Processing Transcript data to identify the SSN owner and reduce processing time;
- Implementing a tool to review multiple accounts quickly and identify accounts that have high potential for ID theft;
- Initiating programming changes to systemically identify and send cases with ID theft markers directly to ID theft specialized groups for processing; and
- Expanding the IP PIN program from 53,000 IP PINs in 2010, to more than 250,000 in TY 2011 and more than 600,000 TY 2012.

We strongly disagree that the IRS "has not responded with the urgency that the identity theft crisis demands." The IRS's comprehensive identity theft strategy squarely focuses on both fraud prevention and victim assistance. We acknowledge that fighting identity theft will continue to be an ongoing battle for the IRS, but we take great pride in the advancement of our efforts and the noteworthy successes we have attained over the past year.

Contrary to the assertion in the report, the IRS's streamlined approach closely aligns itself with the vision of having the point of contact be a person knowledgeable of the specific identity theft issue and authorized to execute the actions necessary to resolve the problem. Accordingly, we believe it is a mischaracterization to state that the IRS is heading toward a

decentralized approach in light of how the specialized groups function. The specialization process allows the IRS to utilize the unique skill sets and experience of dedicated employees, who work in strict accordance of service-wide policy, procedures, and processing timeframes that instill consistency and efficiency. Specialization not only provides a single point of contact for the taxpayer, but it also affords the taxpayer with the expertise needed to handle all aspects of their case. It should be noted that the Identity Theft Assessment and Action Group was a servicewide team represented by all organizations impacted by identity theft, including TAS. We continue to believe that the decision to implement specialized groups was a sound one and is beginning to pay significant dividends.

As stated in the report, IRS functions were asked to develop procedures for their embedded identity theft units; however, the IRS established consistent and mandatory requirements for developing these procedures. For example, these requirements set specific guidelines regarding prioritization, documentation, communications, and adjustments. An essential aspect of these requirements and capabilities is making the taxpayer whole while minimizing instances where accounts are transferred between functions. The IRS's Office of Privacy, Governmental Liaison and Disclosure has overseen the development of a "transfer matrix" which accounts for all identity theft processing scenarios to minimize case transfers and provide taxpayers a seamless customer service experience. As new scenarios are identified, PGLD will work with the other IRS functions and incorporate as necessary. The IRS is currently finalizing the "transfer matrix" and will share this guidance with all identity theft stakeholders, including TAS.

Additionally, in July 2012, PGLD revised its IRM 10.5.3, to serve as the "hub" IRM for the IRS's servicewide identity theft guidance and establish a reference point for all identity theft work. PGLD worked closely with the specialized groups to develop any remaining procedures necessary to account for the intricacies of their respective functions. It should be noted that all identity theft guidance is reviewed by PGLD using the IRS's Internal Management Document (IMD) process in which TAS is also included. Job aids from these functions were posted to the IRS's Servicewide Electronic Research Program (SERP), where they are readily available for review and comment. The functions worked with TAS to provide updates to the TAS Service Level Agreement Addendums for TAS Operations Assistance Request (OAR) routing, and PGLD has met regularly with TAS staff to provide updates on the specialized teams.

In light of the specialized approach and additional reengineering efforts and advancements made by the IRS, the IRS recently convened a multi-functional team, including TAS, to explore the future state of the Identity Protection Specialized Unit. In an effort to ensure efficient processing of IDT cases and the avoidance of duplicate work, the IRS is investigating IPSU activities such as third-party monitoring to determine if IPSU work overlaps with that of the specialized teams. The reengineering team will analyze and evaluate IDT work processes and develop strategic changes to ensure a balance between service to customers and available resources.

The IRS acknowledges that many taxpayers continue to seek TAS assistance on identity theft issues, as evidenced by the increase in case receipts over the past four years. However, it should be noted that the largest number of TAS receipts reflect Economic Burden cases which by their very nature are routed directly to TAS without allowing the IRS an opportunity to take actions to resolve the taxpayer's issue. Additionally, it should be noted that the information in TAS's summary of Secondary Issues (table and subsequent example cited in the Most Serious Problem) supports the need for the IRS's specialized group process. In the example, the taxpayer's account has more than one issue, which, under the "traffic cop" proposal, would require additional coordination between the appropriate functions. Under the specialized process, both issues can be worked by the same function unless a complexity issue required another's involvement. Thus, we believe that the specialized process would prove beneficial to TAS and the taxpayers who come to it for assistance. We will, however, continue to monitor to ensure that the process works as intended.

We disagree that IRS cannot adequately track how many identity theft cases it has in inventory and how much time it takes to work an identity theft case. Since February 2012, all functions report their inventory to PGLD on a monthly basis while working towards the development of servicewide system, and this data is shared monthly with TAS during the Identity Theft Executive Steering Committee and Advisory Council meetings. Additionally, in June 2012, the IRS developed a comprehensive "global report" that tracks servicewide refund fraud and identity theft metrics. The IRS continues to make strides in developing processes to track the time it takes to resolve an identity theft case from receipt to closure. At the present time, only those functions with relatively small amounts of inventory are unable to do so, whereas Accounts Management (which historically works over 90 percent of all identity theft cases) has been providing these data since early 2012.

Similarly, we disagree that the IRS has lowered taxpayer expectations regarding the time it takes to work a case. The IRS has taken numerous steps to quickly identify and streamline its identity theft processes through a variety of reengineering initiatives. New procedures are in place to identify the legitimate taxpayer's return, correct taxpayer account data and initiate refunds to identity theft victims more quickly. One such procedure added the use of Electronic Fraud Detection System data as a tool to determine the true SSN owner, thus eliminating numerous research steps and improving efficiencies. Additionally, new programming to identify returns with identity theft documentation attached was implemented. Cases are now generated directly to the specialized groups, reducing the amount of cases that pass through several areas.

The IRS is dedicating a significant number of additional resources to identity theft. The IRS has nearly tripled the number of employees working identity theft cases. The IRS also initiated the Taxpayer Protection Unit in FY 2012 to provide a centralized staff to assist taxpayers in processing their returns. The overwhelming response to the TPU necessitated additional staffing and the IRS is increasing staffing in this area in FY 2013 to achieve an appropriate level of service. Moreover, the IRS improved its identity theft training efforts

in 2011 (and again in 2012) to ensure that all public contact employees had the tools they needed to respond appropriately to those who have been victimized by identity theft. We developed a new training course that includes sensitivity training as well as training on the proper tools and techniques for handling identity theft cases. In all, 35,000 IRS employees received this training in preparation for filing season 2012 and even more have taken (or are scheduled to complete this training) for filing season 2013.

The IRS appreciates the acknowledgement in the report of the work in the Identity Protection PIN program. The IP PIN is issued to select ID theft victims whose identities have been validated by the IRS, allows legitimate returns to be processed, and prevents processing of fraudulent returns, thereby mitigating processing delays in ID theft victims' federal tax return processing. Generally, the IP PIN is mailed out once the taxpayer's account has been resolved. Current programming allows one IP PIN to be generated each year. The IRS is exploring the feasibility of being able to provide IP PINs *on demand* though current programming limits IP PIN generation to once annually. This limitation is attributable to various factors that include the posting of identity theft markers, the IRS's year-end IT conversion process, and taxpayer correspondence issuance. The inclusion of cases within the IP PIN universe, only after an account was finally resolved, provided an added layer of taxpayer protection through the use of business rules if the taxpayer chose to file their return without an IP PIN. Additionally, for the 2013 filing season, the IRS expanded the IP PIN population by applying a temporary marker to accounts for which the legitimate taxpayer was determined and the correct address verified, even though the account had not been completely resolved. Temporary markers were input on approximately 100,000 accounts. This innovative and collaborative approach to working active ID theft inventory provides added protection and reduces burden on taxpayers in the event the perpetrator attempts to misuse the TP's identity before the account is resolved.

Taxpayers who misplace their IP PIN can contact the IRS by calling the IPSU, the 1-800 assistance line, or visit any taxpayer assistance walk in center. Taxpayers will be asked to validate their identities by answering a series of basic questions mandated by the IRM for disclosure level authentication.[52] Once the taxpayer's identification is validated through this process, they will be provided with a replacement IP PIN for use on their TY 2012 return. The replacement IP PIN will allow the taxpayer to e-file their return and, subject to standard validation checks, be accepted. The return will be subjected to a manual validation process prior to being allowed to post.

With respect to the IPSU, this unit will continue operations as it has since its inception in October 2008. The cross-functional IPSU Reengineering Team is studying the future role of IPSU. We are awaiting the team's final analysis and recommendations before making any changes to IPSU operations. The IRS will consider the recommendations of the National Taxpayer Advocate regarding the IPSU.

52 IRM 21.1.3.2.3 (Nov. 13, 2012); IRM 21.1.3.2.4 (Dec. 12, 2011).

The IRS agrees that the practice of public release of the Death Master File should be changed. The IRS continues to work with SSA and the Administration on a legislative solution that would limit public release of the DMF.

The IRS views TAS as a valued partner in the discussion and development of identity theft procedures and processes and looks forward to continued collaborations in the future. TAS is already included in all identity theft governance meetings (Advisory Council and Executive Steering Committee) and is a team member on numerous other identity theft-related initiatives such as the Accounts Management Reengineering and IPSU future state teams. The IRS will continue to seek the input and participation of TAS on future endeavors.

Taxpayer Advocate Service Comments

The National Taxpayer Advocate appreciates the difficulty the IRS faces in serving as both the protector of the federal fisc and as the tax administrator responsible for delivering refunds to millions of taxpayers. With the volume of fraudulent refund claims, many of which involve identity theft, increasing significantly over the years, IRS resources are understandably stretched thin. To its credit, the IRS is exploring ways to more effectively detect and stop fraudulent claims. It is also moving to a specialized approach to victim assistance.

In its response, the IRS states that its "streamlined approach closely aligns itself with the vision of having the point of contact be a person knowledgeable of the specific identity theft issue and authorized to execute the actions necessary to resolve the problem." The National Taxpayer Advocate does not oppose the IRS's decision to create specialized identity theft units in each function, and recognizes there will be some efficiencies gained in having a small group of employees focus solely on identity theft cases. However, she also notes that these employees will often not have the capability to address all related issues presented in their cases.

As the National Taxpayer Advocate has consistently and frequently pointed out to senior IRS officials, the IRS does not know the full scope of issues presented in any given identity theft case because, unlike TAS, it does not track this information. The IRS works the vast majority of its identity theft cases as "single issue" cases. For example, if a case is in the Accounts Management (AM) function because the processing of taxpayer's current year's return is blocked by the IRS's acceptance of a return filed by an identity thief (known in IRS parlance as a "duplicate return"), AM employees only work that issue. They do not undertake a global account review to identify any prior returns that may be affected or whether there is impending audit or collection action with respect to impacted prior year returns.

Thus, the IRS does not know enough about the make-up or complexity of identity theft cases in its inventory to project how many cases will require the involvement of multiple units. The only comprehensive source of information about the composition of identity theft casework is TAS. Since our inception, we have tracked identity theft cases in our inventory, and until 2012, TAS was the only function in the IRS that could reliably report how many identity theft cases it was working at any one time and over time. While TAS's case inventory may not be identical to the IRS's, TAS is the *sole* reliable source of historic and current information about the scope of issues and complexity presented in identity theft cases. As noted earlier, identity theft is now the number one issue in TAS casework, constituting over a quarter of our case receipts. This has made us experts on identity theft work.

It is this experience that leads to the National Taxpayer Advocate's sense of urgency. In our view, the IRS still does not understand the full scope of the problem and is developing procedures that will continue to harm identity theft victims. The National Taxpayer Advocate does not want to be in the situation, several years from now, of saying "I told you so." She wants the IRS to address her concerns in a comprehensive way *now*.

As noted earlier, the vast majority of TAS identity theft cases involve multiple issues. The IRS states that "[u]nder the specialized process, both issues can be worked by the same function unless a complexity issue required another's involvement." The National Taxpayer Advocate disagrees strongly with the IRS's complacent assessment. Our analysis of TAS casework shows that the *vast majority* of identity theft cases involve multiple issues, often requiring actions by employees from different functions and with different skills. Unless the IRS is going to reproduce each of those functions within each of the 21 embedded units, cases will need to be transferred from one function to another regularly — and with much greater frequency than the IRS anticipates. And once the case is transferred, it is unclear whether the original employee working the case will continue to be the point of contact for the taxpayer or whether the taxpayer will be given a new contact employee in the new function. As anyone who has ever sought to resolve an issue with the IRS knows, the IRS is not exactly a model of ease and transparency in terms of the taxpayer's ability to communicate with specific employees. It is only TAS that assigns one case advocate to work a case from start to finish, addressing all issues. Without a traffic cop to ensure that the victim's case is properly and timely transferred between functions, the risk is too great that the case will get lost among the 21 different specialized units.

Since writing the initial discussion for this Most Serious Problem, the National Taxpayer Advocate has had in-depth discussions with both the Acting Commissioner and the Commissioner of the Wage and Investment Division, laying out her concerns about the operation of the specialized units. She has proposed what is an extremely reasonable alternative approach. Identity theft cases come to the IRS from multiple sources. Where the IRS receives calls on its toll-free assistance line, cases that appear to present only one issue can be routed to the appropriate specialized unit, as currently planned. The assigned

employee in that specialized unit would be required to conduct a global account review on that taxpayer's identification number. If the global account review shows that there are other issues or other years impacted by identity theft, the specialized unit would continue to work its narrow portion of the case, but oversight of the case would be transferred immediately to the IPSU, which would serve as the "traffic cop" for the case and ensure that all units do their part to ensure that the issues are timely and effectively resolved. Where the IPSU receives calls directly, the IPSU would conduct its own global account review and direct cases to the appropriate specialized unit(s). If the global account review shows that there is only a single issue in the case, the IPSU would transfer oversight of the case to the specialized unit.

The National Taxpayer Advocate's proposed approach combines the benefits of having dedicated experts in each specialized unit with the reality of the complexity and number of issues and years presented in the majority of identity theft cases. The IRS's approach, on the other hand, does not address taxpayers' needs and will further burden and harm the victims.

In addition, the IPSU must be strengthened and adequately staffed for either approach to work. Although the IPSU has existed since 2008, it does not appear to us that the IRS has used it optimally. In our view, the IPSU not only should serve as the traffic cop that routes the case to the appropriate function(s), but also should perform triage to prioritize which actions should be taken first to minimize harm. The IPSU re-engineering team made a number of recommendations that TAS concurs with, but it also suggested reducing the monitoring function of the IPSU — an idea we strongly oppose. As we have stated, we believe the IPSU should have increased ability to monitor ID theft cases.

The National Taxpayer Advocate acknowledges the recent improvements PGLD has made in tracking the inventory of identity theft cases and the case cycle time, but believes it should perform much more data analysis. As noted above, we did not claim that the IRS cannot currently track the number of identity theft cases or its cycle time; rather, we stated that *until this year*, the IRS could not "track identity theft case inventory, much less monitor how long it takes to resolve cases." We maintain that although many IRS functions now track the time an ID theft case is in its inventory, the IRS cannot provide an overall average cycle time. Furthermore, the IRS starts tracking the age of an identity theft case from the date it processes identity theft documentation, not the date the taxpayer provides the documentation. This means the cycle time reported by the IRS may be significantly shorter than the actual time a victim must wait for his or her account to be resolved.

In its comments, the IRS notes that it has taken steps to streamline its identity theft case resolution processes through a number of reengineering initiatives and by dedicating additional staffing resources. While we applaud these actions, we are disappointed that the IRS has not committed to a firm goal of reducing case cycle time. As we noted, the average

closure time for one prominent category of identity theft work was 196 days in FY 2012.[53] This does not include the time the IRS spent reviewing and processing the documentation (such as the identity theft affidavit) provided by the taxpayer to substantiate his or her identity, so in reality, the case cycle time is much longer than six months.

As this report goes to press, the IRS is yet again seeking to send letters to identity theft victims asking that they wait 180 days while the IRS works their cases. The National Taxpayer Advocate is concerned that this letter will send a message to IRS employees that it is acceptable to make identity theft victims wait six months. She notes that despite all the improvements to processing that the IRS says it has made over the years, the cycle time for identity theft victim assistance remains as long as it was years ago.

As of September 30, 2012, the IRS had almost 650,000 identity theft cases in inventory servicewide.[54] The victims of tax-related identity theft suffer extraordinary inconveniences and, in many cases, hardships. In general, more than 75 percent of U.S. taxpayers receive refunds, with the amount averaging about $3,000.[55] Identity theft victims generally cannot receive their significant and sometimes urgently needed tax refunds until the IRS resolves their cases, which is now taking six months or longer. The IRS's failure to provide timely relief to these identity theft victims is simply unacceptable.

If the IRS prioritizes identity-theft victim assistance to the extent its response suggests, it would set firm goals for its employees to provide prompt and comprehensive relief to victims. Reasonable goals include:

- Conducting a global account review upon receipt of a taxpayer's claim of identity theft in whichever IRS function serves as the taxpayer's first point of contact so that the case is appropriately routed;
- Determining who is the legitimate taxpayer within 45 to 60 days from date of the taxpayer's documentation submission; and
- Taking all closing actions with respect to processing the impacted return, including issuing any refunds in the quickest manner possible and marking the identity theft victim's account as eligible for an IP PIN, within 30 days from the date of making the identity determination.

These goals address the taxpayer's immediate anxiety and needs with respect to recognition of his or her identity and financial distress by requiring employees to meet accelerated timeframes for the return-processing component of the case, while affording the IRS the time it needs to resolve more complex and downstream issues. Importantly, they would halve the current cycle time experience to 90 days.

53 *See* IRS response to information request (Nov. 5, 2012). IDTX (monitoring tax-related identity theft cases) cases were open an average of 196 days.

54 *See* IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Oct. 24, 2012).

55 *See* IRS Filing Season Statistics – Dec. 31, 2011, *available at* http://www.irs.gov/uac/Filing-Season-Statistics----Dec.-31,-2011 (last visited Dec. 28, 2012).

In conclusion, the National Taxpayer Advocate reiterates that TAS's experience in working thousands of identity theft cases each year from beginning to end affords us a unique perspective on how to improve the process. Since 2004, the National Taxpayer Advocate has made numerous recommendations in her Annual Reports to Congress to strengthen the ways the IRS helps victims. As the table below shows, the IRS ultimately adopted many of TAS's recommendations — often after initially opposing them. The National Taxpayer Advocate urges the IRS to use the knowledge gained from TAS's vast experience to improve its identity theft victim assistance procedures, and thoughtfully consider all of our recommendations.

TABLE 1.4.5, TAS RECOMMENDATIONS FOR HELPING ID THEFT VICTIMS ADOPTED BY THE IRS

MSP Year	Rec. #	TAS Recommendation	Year First Recommended	Year IRS Adopted
2004	9-A2	Revise the IRM to provide that scrambled procedures be used only after phone contact is attempted with the SSN users and only in those cases where available information clearly supports use of the SSN by both taxpayers.	2004	2009
2004	9-A3	Standardize procedures for information required from taxpayers.	2004	2009
2005	9-1	Conduct appropriate training for employees who determine whether to send cases to the SSA.	2005	2009
2005	9-2	Integrate awareness of identity theft into various training modules throughout the operating divisions and functions, so all employees are sensitive to this issue and can refer taxpayers to the appropriate IRS function.	2005	2011
2005	9-3	Use an electronic indicator on its master files to mark the accounts of taxpayers who have verified that they have been victims of identity theft.	2005	2008
2007	6-2	Develop a form that taxpayers can file when they believe they have been victims of identity theft. The instructions on the form should explain which steps the IRS will take and which steps the taxpayer should take (*e.g.*, obtaining an FTC affidavit) to restore the integrity of the taxpayer's account.	2007	2009
2007	6-7	Create a prefix for IRS numbers (IRSNs) or some other system so that it does not deny tax benefits to the rightful owner of the Social Security number (SSN). While assignment of IRSNs may be the only way to isolate the fraud taking place under an SSN, it is inequitable to assign the IRSN to identity theft victims and then deny tax benefits that depend on the SSN.	2007	2012
2011	3-10	Allow taxpayers to turn off the ability to file electronically.	2007	2012

Recommendations

The National Taxpayer Advocate recommends that the IRS:

1. Mark identity theft victims' accounts as eligible for IP PINs as soon as the identities and addresses of the rightful SSN owner are verified, rather than after final resolution of the identity theft case.
2. Conduct a global account review upon receipt of a taxpayer's claim of identity theft in whichever IRS function serves as the taxpayer's first point of contact to ensure the case is appropriately routed and the all identity-theft issues are comprehensively resolved.
3. Retain the IPSU as the single point of contact with identity theft victims throughout the duration of their cases, unless the global account review indicates that there is only a single issue or tax year present in the case.
4. Move the IPSU out of the AM function, to afford it greater autonomy as it acts as the face of the IRS to identity theft victims.
5. Require the IPSU (or in the case of a single-issue case, the specialized function) to conduct final global account reviews on all identity theft cases.
6. Implement agreements between the IPSU and the various functions that work identity theft cases to set acceptable timeframes for completing the required actions and consequences for not meeting the timeframes.
7. Set a Level of Service goal for the Taxpayer Protection Unit equal to or greater than the Level of Service goal set for the main toll-free phone line.
8. Establish procedures that meet accelerated 90-day timeframes for determination of the true SSN owner and resolution of return-processing issues.
9. Insert into every agreement with state and local agencies an explicit clause that says that return information of an identity thief may be used only for prosecution of identity theft-related crimes (with no redisclosure to third parties).
10. Work with the Social Security Administration, the Office of Management and Budget, and the Justice Department to develop guidance that withholds the Death Master File from public release under a FOIA exemption for the limited period required to prevent the DMF's use in committing tax-related identity theft (which we believe to be two years).
11. Include TAS at all levels of identity theft program and procedural planning, including front-line teams, training development, guidance, and advisory and executive steering committees.