WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

IDENTITY THEFT-RELATED TAX FRAUD

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

U.S. HOUSE OF REPRESENTATIVES

AUGUST 2, 2013

TABLE OF CONTENTS

I. The IRS Combats Identity Theft by Utilizing Systemic Filters and Requiring Multiple Layers of Authentication. 2

II. Despite Its Efforts, the IRS Remains Inundated with Identity Theft Cases. 4

III. The IRS Should Revamp Its Approach to Assisting Identity Theft Victims, Which Currently Takes Much Too Long. 11

IV. Conclusion 19

Chairman Mica, Ranking Member Connolly, and distinguished Members of the Subcommittee:

Thank you for inviting me to testify today about the problems stemming from identity theft-related tax fraud.[1] I have appeared before this subcommittee several times regarding this matter and appreciate this subcommittee's continued interest.

As I have written in nearly every Annual Report I have delivered to Congress since 2004, tax-related identity theft is a serious problem – for its victims, for the IRS and, when Treasury funds are improperly paid to the perpetrators, for all taxpayers.[2] In general, tax-related identity theft occurs when an individual intentionally uses the Social Security number (SSN) of another person to file a false tax return to obtain an unauthorized refund.[3]

For victims, the consequences can be significant. Apart from the time and frustration involved in dealing with the IRS to prove one's own identity, taxpayers generally do not receive their refunds until their cases are resolved. This year, approximately 78 percent of all returns processed resulted in refunds, with the average amount approximately $2,650.[4] For low income taxpayers who qualify for the Earned Income

---

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

[2] *See* National Taxpayer Advocate 2012 Annual Report to Congress 42-67 (Most Serious Problem: *The IRS Has Failed to Provide Effective and Timely Assistance to Victims of Identity Theft*); National Taxpayer Advocate 2011 Annual Report to Congress 48-73 (Most Serious Problem: *Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS*); National Taxpayer Advocate 2009 Annual Report to Congress 307-317 (Status Update: *IRS's Identity Theft Procedures Require Fine-Tuning*); National Taxpayer Advocate 2008 Annual Report to Congress 79-94 (Most Serious Problem: *IRS Process Improvements to Assist Victims of Identity Theft*); National Taxpayer Advocate 2007 Annual Report to Congress 96-115 (Most Serious Problem: *Identity Theft Procedures*); National Taxpayer Advocate 2005 Annual Report to Congress 180-191 (Most Serious Problem: *Identity Theft*); National Taxpayer Advocate 2004 Annual Report to Congress 133-136 (Most Serious Problem: *Inconsistence Campus Procedures*).

[3] The IRS refers to this type of tax-related identity theft as "refund-related" identity theft. In "employment-related" identity theft, an individual files a tax return using his or her own taxpayer identifying number (usually an Individual Taxpayer Identification Number or ITIN), but uses someone else's SSN to obtain employment. Consequently, the wages are reported to the IRS under the SSN of the victim, potentially prompting the IRS to pursue the victim for additional tax on the apparent income. *See* IRM 10.5.3.2(4), *Identity Protection Program Servicewide Identity Theft Guidance* (Feb. 27, 2013). Unlike in 1993, when I first represented a client in an identity theft case, the IRS now has procedures in place to minimize the tax administration impact to the victim in these employment-related identity theft situations. Accordingly, I will focus on refund-related identity theft in this testimony.

[4] IRS, Filing Season Statistics for Week Ending May 10, 2013, *at* http://www.irs.gov/uac/Newsroom/Filing-Season-Statistics-May-10,-2013.

Tax Credit, a tax refund may constitute a significant percentage of their annual income. There is little doubt that longer case resolution times can translate to financial inconvenience and sometimes hardship. That is why it is crucial for the IRS to resolve cases promptly.

As requested, I will focus my statement on the impact of tax-related identity theft on the IRS and taxpayers. I will describe some of the actions being taken by the IRS to detect and prevent identity theft, as well as efforts to improve victim assistance. I will describe in detail the life cycle of an identity theft case, outlining the many steps needed to fully resolve the victim's account. This description makes clear that the IRS still has a long way to go to deliver adequate and timely assistance to victims of identity theft. Thus, I also offer recommendations to help the IRS improve its identity theft victim assistance.

I. The IRS Combats Identity Theft by Utilizing Systemic Filters and Requiring Multiple Layers of Authentication.

The IRS takes a multi-faceted approach to detecting tax returns filed by identity thieves and preventing the associated refunds from being processed. This includes using a series of filters to flag potentially fraudulent returns and adjusting the filters each year as the IRS learns more about how the thieves operate. In calendar year 2013 (through May), identity theft filters stopped nearly 850,000 returns, an increase of 135 percent from the same period in 2012.[5]

The IRS also works cooperatively with banks and other financial institutions to thwart attempts by identity thieves to defraud the government. Private businesses, which often have developed their own algorithms to detect fraud, alert the IRS of suspicious transactions. The IRS then investigates the taxpayers involved and recoups the funds from the financial institution if it verifies fraudulent activity. This "external leads" program has enabled the IRS to recover more than $293 million from over 122,000 accounts this year.[6]

The IRS also is using online tools to improve its employees' ability to conduct research in ID theft cases. Integrated Automated Technologies, or IAT, is a suite of software that allows employees to conduct research, adjust accounts, and prepare letters to send to the affected taxpayers. Several recent additions to the IAT suite should reduce the time employees spend working identity theft cases.

In an effort to provide a greater level of security to taxpayers who have previously been victimized by identity theft, the IRS has issued identity protection personal identification numbers (IP PINs) to victims whose identities and addresses it has verified. An IP PIN is a unique single-use code that the taxpayer must use, along

---

[5] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (June 27, 2013).

[6] *Id*.

with his or her taxpayer identification number, to file electronically.[7] If a return filer does not use a valid IP PIN, the return will be marked "unpostable" – meaning it will not be processed – and will be temporarily suspended while receiving additional scrutiny. These unpostable returns will be subjected to a series of filters (known as "business rules" in IRS parlance) that are designed to verify the identity of the filer.

For the 2013 filing season, the IRS issued more than 770,000 IP PINs.[8] For 2014, the IRS is exploring the use of "e-authentication" to expand the IP PIN program. Under this system, taxpayers would log onto a web portal, answer a series of "out-of-wallet" questions to establish and verify their identities, and then receive IP PINs electronically. Taxpayers could also use this e-authentication program to secure replacement IP PINs if they misplace the ones mailed to them.

As noted above, the IRS relies on a series of business rules to safeguard accounts from potential identity theft. When someone attempts to file using a taxpayer's SSN that has already been marked with an identity theft indicator, such a return must pass the business rules before it will be processed. Returns that fail the business rules will be marked unpostable. Initially marking a return as unpostable typically adds 39 to 44 days to the processing time of a legitimate tax return.[9]

I have serious reservations about the effectiveness of these business rules and the exceptionally high rate of legitimate returns they ensnare. Preliminary analysis suggests that an astonishing 80 percent of tax returns that the IRS flags as unpostable as a result of failed identity theft business rules or missing IP PINs are eventually deemed legitimate.[10] Of the 191,894 tax returns in this population of unpostable returns in the 2013 filing season, 152,951 (80 percent) eventually were found to be legitimate returns filed by the true owners of the SSNs. The IRS is aware of my concerns, as I have repeatedly asked the IRS to determine the cause of the spike in unpostable returns and adjust its business rules that are significantly over-inclusive. The IRS is harming too many taxpayers by unnecessarily rejecting and delaying the processing of their returns.

---

[7] *See* IRM 10.5.3.2.16, *Identity Protection Personal Identification Number (IP PIN)* (Jan. 11, 2013).

[8] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (June 27, 2013).

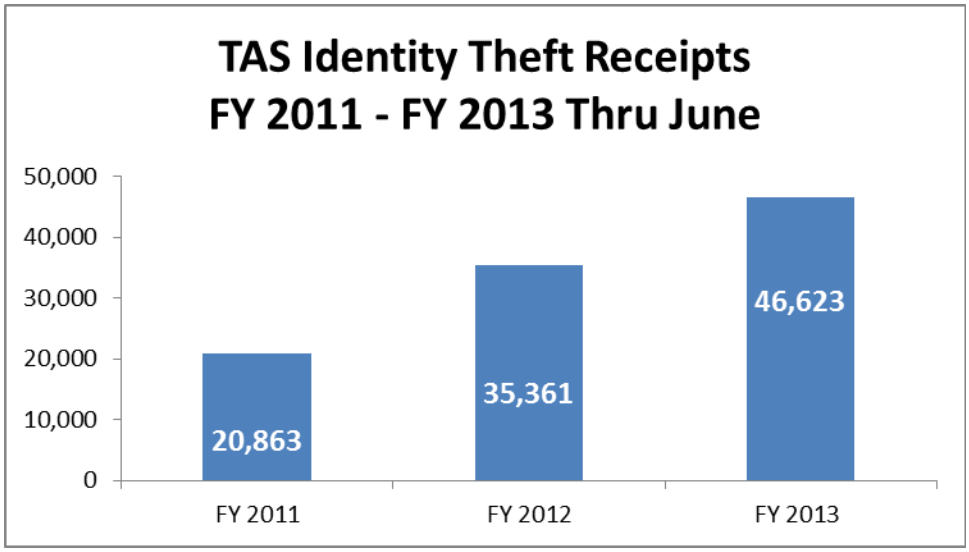
[9] The IRS Accounts Management (AM) function no longer works unpostable returns that failed business rules; this inventory was transferred to the Submission Processing identity theft specialized unit beginning in the 2013 filing season. *See* IRM 3.12.179.42.2; IRM 3.12.179.43. For this analysis of the average age of unpostable returns, we focused on Reason Code 0 (which is used when a return does not contain a matching IP PIN) and Reason Code 1 (which is used when a return "attempts to post to an account containing an unreversed TC (Transaction Code) 971 AC 501 or 506 and does not pass established identity theft business filters"). GUF 5740, through 6/27/2013.

[10] For this analysis of unpostable returns, we focused on Reason Code 0 and Reason Code 1, which are described more fully in the preceding footnote. *See* IRM 3.28.4.5, *Unpostable Code (UPC) 147 Reason Code (RC) 0 and Reason Code (RC) 1* (Feb. 14, 2013). IRS, GUF Reports 5540 and 5570 through 6/27/2013.

II. Despite Its Efforts, the IRS Remains Inundated with Identity Theft Cases.

Notwithstanding more stringent filters, improved cooperation with the private sector, and increased personnel resources dedicated to this problem,[11] the volume of identity theft returns continues to grow at a disturbing rate. The IRS had almost 690,000 identity theft cases in inventory at the end of May 2013, a substantial increase from a year ago, when the number was less than 500,000.[12]

Taxpayer Advocate Service (TAS) case receipts are a barometer of the effectiveness of IRS procedures. From fiscal year (FY) 2011 to FY 2012, TAS stolen identity cases rose by 61 percent,[13] and they are trending upward again this year. TAS received 46,623 identity theft cases during the first three quarters of FY 2013, a 32 percent increase over the same period in FY 2012 and a 123 percent increase from FY 2011.[14]



The growth in TAS's identity theft casework reflects both the increase in identity theft incidents and the IRS's inability to address the victims' tax issues promptly. Because identity theft cases generally encompass multiple issues (see chart below), these cases typically take longer to resolve than other types of cases.

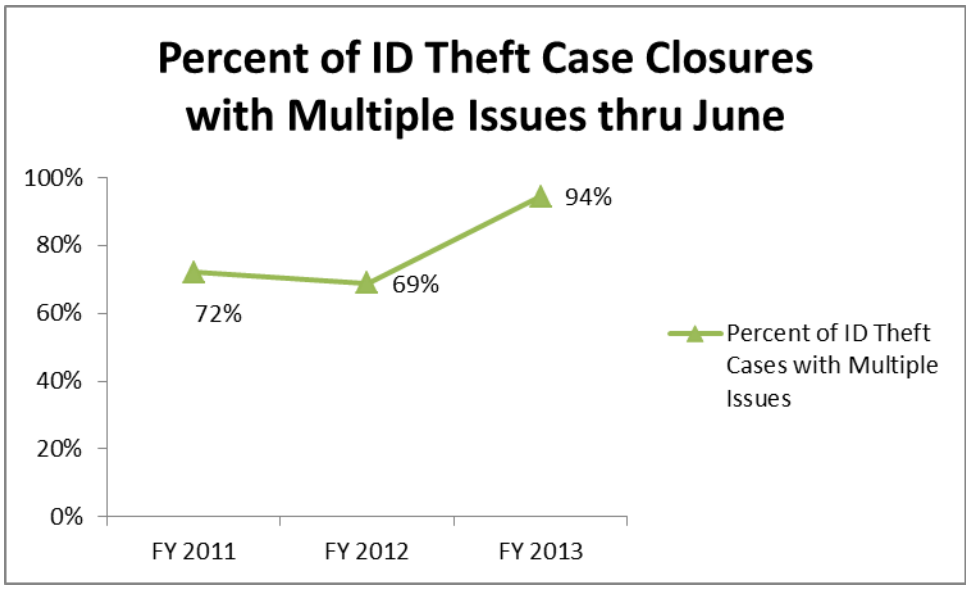
---

[11] As discussed later in this testimony, the IRS has increased the number of employees who work on identity theft cases to 3,000.

[12] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (June 27, 2013); IRS Identity Theft Advisory Council, *Identity Theft Status Update* (June 19, 2012).

[13] Data obtained from Business Performance Management System (BPMS) reports on October 3, 2012, showing TAS received 34,006 identity theft cases as of September 30, 2011, and 54,748 identity theft cases as of September 30, 2012.

[14] Data obtained from the Taxpayer Advocate Management Information System (TAMIS) (July 1, 2013, July, 1, 2012, July 1, 2011).



Accordingly, the cycle time for identity theft cases worked by TAS is approximately 88 days, compared with 77 days for TAS cases overall.[15] Despite the sharp increase in identity theft casework, TAS is working these cases more efficiently. Over the same period in FY 2012 and FY 2011, the cycle times for TAS identity theft cases were 106 days and 112 days, respectively. [16]

By contrast, the IRS's processing time for identity theft cases has been increasing. In 2008, former Commissioner Shulman made a commitment that the IRS would resolve identity theft victims' tax accounts "quickly and efficiently."[17] While some IRS functions can track the length of time a case is in their inventory (see chart below), the IRS still cannot provide a servicewide cycle time measure for resolving identity theft cases, nor does it track overall cycle time from the taxpayer's perspective. *Specifically, the chart below does not accurately reflect the cycle time from the taxpayer's perspective, since Accounts Management (like most specialized identity theft units in the IRS) measures cycle time solely from the date the case is received in the specific unit. Its cycle time measure does not reflect the time elapsed since the taxpayer filed his or her return or all of the interactions the victim had with the IRS prior to assignment to the function.* Thus, the IRS cannot determine how well it has done in meeting this commitment to resolve identity theft cases "quickly and efficiently."

---

[15] Data obtained from TAMIS (July 1, 2013).

[16] *Id*.

[17] *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), *at* http://finance.senate.gov/hearings/hearing/download/?id=f989b16e-5da3-452d-9675-b75d796fe2b4.

IRS Cycle Time for Various Categories of Identity Theft Cases Worked by Accounts Management (FY 2012)[18]

Business Operating Division	Function	Inventory Type	Case Type	Avg. Days Open from Receipt by Function to Closure by Function (as of 9/30/2012)
Wage & Investment (W&I)	Accounts Management (AM) Identity Protection Specialized Unit (IPSU)	IDTX	Monitoring tax-related identity theft cases that meet multiple functional criteria and do not meet TAS Criteria 5 – 7 (systemic burden cases); cases worked by appropriate function and monitored by the IPSU (every 165 days	196
W&I	AM IPSU	Identity Theft Assistance Request (ITAR)	Tax-related identity theft cases that meet Criteria 5 - 7. IPSU issues ITARs to appropriate functions and they receive priority treatment. Taxpayer may request IPSU or the case may be referred from another function.	133
W&I	AM	IDT1	Duplicate filing where the second return has a Form 14039 (ID theft affidavit) attached	230

[18] *See* IRS response to TAS information request (Nov. 5, 2012).

Business Operating Division	Function	Inventory Type	Case Type	Avg. Days Open from Receipt by Function to Closure by Function (as of 9/30/2012)
W&I	AM	IDT3	Mixed Entity cases - internally identified. Do not require a Form 14039. Duplicate filing research indicates identity theft that can be resolved internally without taxpayer contact.	323
W&I	AM	IDT4	Self-identified non tax-related identity theft (*e.g.*, stolen wallet)	131
W&I	AM	IDT6	Duplicate Filing Inventory subjected to the Electronic Fraud Detection System (EFDS) filters to identify the true SSN owner. There may already be an open IDT1/3 control on the module so the control will be updated to IDT6.	364
W&I	AM	IDT8	Duplicate filing condition with prior Integrity & Verification Operations (IVO) involvement.	Data not provided

Business Operating Division	Function	Inventory Type	Case Type	Avg. Days Open from Receipt by Function to Closure by Function (as of 9/30/2012)
W&I	AM	IDT9	An open IDT 1/3 is updated to IDT9 upon receipt of an ITAR referral from IPSU. There may be an open IDT1/3 already on the module so the control will be updated to IDT9. If not, a new IDT9 is created.	248

In a May 2012 audit report, the Treasury Inspector General for Tax Administration (TIGTA) found the average cycle time for the identity theft cases it reviewed was 414 days.[19] I am concerned that unless the IRS significantly changes its procedures, identity theft cycle time will continue to increase in the coming year as the IRS struggles to keep up with its burgeoning inventory.

IRS leadership has recognized identity theft as a serious problem and has dedicated more than 3,000 employees to work these cases. However, these employees are spread out among more than 20 different groups within the IRS (see chart below listing the various functions with a specialized identity theft unit). It seems that the IRS's strategy of throwing bodies at the problem, without addressing fundamental problems with its processes, is not achieving the goal of resolving ID theft cases and enabling victims to receive their refunds expeditiously. As the chart below demonstrates, a victim of identity theft must navigate an alphabet soup of IRS departments, forms, and notices before the IRS can fully unwind the harm caused by the identity theft.

[19] *See* TIGTA, Ref. No. 2012-40-050, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 3, 2012).

FUNCTIONS	Specialized Processes (Receipt, Roles, and Responsibilities)
Wage & Investment (W&I) Accounts Management (AM)	**Identity Protection Specialization Unit (IPSU)** is located in AM and is responsible for receiving Identity Theft Affidavits (Forms 14039) sent directly to IPSU for both tax-related and non-tax related identity theft. IPSU monitors IDT issues that cross multiple function lines as well as IDT cases that meet certain TAS criteria codes 5-7, called ITARs (Identity Theft Assistance Requests). **AM** also operates specialized groups that work ID theft taxpayer inquiries originating from duplicate-filed returns (fraudulent return posts to victim's account and victim also files) as well as IDT taxpayer correspondence.
W&I Compliance-Automated Underreporter (AUR)	The AUR program matches taxpayer income and deductions submitted by third parties against amounts reported on individual income tax returns. . Receipts mainly come from CP2000 (Request for Verification of Unreported Income, Payments, or Credits) responses. Unit works as specialized group.
W&I Compliance-Automated Collection Services (ACS)	Receipts come from taxpayers in the collection process, mainly responding to IRS balance due notices due to tax assessments caused by identity theft - works as specialized group.
W&I Compliance-Correspondence Examination	Receipts come from taxpayers who were selected for campus correspondence audits. The examination discovers that a fraudulent return was filed one*, i.e.,* one that does not belong to the SSN owner. Works as specialized group.
W&I Compliance – Campus Services Collection Organization (CSCO)	Campus compliance function includes Automated Substitute for Return (ASFR), Taxpayer Delinquent Investigations (TDI), Taxpayer Delinquent Accounts (TDA. As a result of multiple uses of the SSN's erroneous assessments result, causing incorrect account balances. Cases are received as a result of notices involving unfiled tax returns or returns filed by IRS on behalf of taxpayers. Works as specialized group.
W&I Compliance – Compliance Post Adjustment Team (CPAT)	Compliance Post Adjustment Team (CPAT) is a specialized group that works Wage &Investment (W&I) campus compliance back-end adjustments from all the W&I compliance specialized groups. The back end adjustments are completed and refunds are released to the victim. This group does the account clean-up work after other units have taken action.
W&I Compliance-Automated Substitute for Return (ASFR)	ASFR is a specialized group that prepares "substitute" returns based on third-party wage data for taxpayers who fail to file. Multiple or fraudulent use of the SSN generates wage data causing the substitute return to be incorrect and resulting in erroneous assessments on the victim's account. (See CSCO)
W&I Field Assistance (FA) – Taxpayer Assistance Centers (TACs)	TAC Field Assistors do not work IDT cases. However, because they are in the unique position of having the taxpayer in front of them, they have been trained to recognize possible ID theft, verify the taxpayer's identity while he or she is present, and capture all the necessary documentation, which they forward to the function responsible for fully resolving the case.
W&I Return Integrity and Correspondence Services (RICS) Taxpayer Protection Program (TPP)	RICS TPP is responsible for handling potential ID theft cases that are scored by a set of ID theft models (through Electronic Fraud Detection System (EFDS) and the Dependent Database (DDb). Returns pass through a set of "filters" designed to catch fraudulent returns this process also "snags" innocent taxpayers resulting in delayed refunds or requiring taxpayers to contact the IRS to get accounts corrected.
W&I RICS Integrity & Verification Operations (IVO)	RICS IVO handles identity theft account work filtered through EFDS and conducts research to verify the validity of tax return information using a variety of third party information.

FUNCTIONS	Specialized Processes (Receipt, Roles, and Responsibilities)
W&I Submission Processing – Identity Theft (SP-IDT)	The SP-IDT works IDT unpostable inventory – returns previously marked with identity theft markers that pass through a series of business rules. When the return fails these business rules, the return does not post but is sent to the SPIDT to determine if the return belongs to the fraudulent filer or the victim. SPIDT also works AM inventory of duplicate filed returns. SP Accounting will credit a victim's account for a refund lost due to an identity theft after the IDT is substantiated by another function.
Small Business/Self-Employed (SB/SE) Automated Underreporter (AUR)	The AUR program matches taxpayer income and deductions submitted by third parties against amounts reported on individual income tax returns. . Receipts mainly come from CP2000 (Request for Verification of Unreported Income, Payments, or Credits)
SB/SE Automated Collection Services (ACS)	Receipts come from taxpayers in the collection process, mainly responding to IRS balance due notices due to erroneous tax assessments caused by multiple uses of the SSN. Works as specialized group.
SB/SE Correspondence Examination (CORR Exam)	Receipts come from taxpayers who were selected for campus correspondence audits. The examination discovers that a fraudulent return was filed, *i.e.,* one that does not belong to the SSN owner. Works as specialized group.
SB/SE Campus Services Collection Organization (CSCO)	Campus compliance function includes Automated Substitute for Return (ASFR), Taxpayer Delinquent Investigations (TDI), Taxpayer Delinquent Accounts (TDA), etc. IDT may result in multiple uses of the SSNs, causing erroneous assessments and incorrect account balances. Cases are received as a result of balance due notices involving unfiled tax returns or returns filed by IRS on behalf of taxpayers. Works as specialized group.
SB/SE Automated Substitute for Return (ASFR)	ASFR is a specialized group that prepares "substitute" returns based on third-party wage data for taxpayers who fail to file. Identity theft occurs when the wage data is generated, causing the substitute return to be incorrect and resulting in erroneous assessments on the victim's account (See CSCO).
SB/SE Field Examination	Field examiners (revenue agents, tax compliance officers) have face-to-face contact with taxpayers. They are trained to recognize, address, and resolve ID theft cases that surface in examinations they conduct. Accounts needing "back-end" adjustments are sent to Designated Identity Theft Adjustment (DITA) to complete processing and issue refunds.
SB/SE Field Collection	Field revenue officers have face-to-face contact with taxpayers. They are trained to recognize, address, and resolve ID theft cases that surface in their collection case inventory. Accounts needing "back-end" adjustments are sent to DITA to complete processing and issue refunds.
SB/SE Designated Identity Theft Adjustment (DITA)	DITA is a specialized group that works SB/SE compliance "back end" adjustments from the SB/SE specialized groups and LB&I. The back end adjustments are completed and refunds are released to the victim.
Large Business & International (LB&I)	LB&I performs examinations on large businesses and international taxpayers. All employees in LB&I are trained to recognize, address, and resolve ID theft cases with new IDT specialized guidance. Back-end adjustments are sent to DITA to complete processing and issue refunds.
Appeals	All employees in Appeals are trained to recognize, address, and resolve ID theft cases that surface in their appeals work. They follow new IDT specialized guidance, and perform their own adjustments.

FUNCTIONS	Specialized Processes (Receipt, Roles, and Responsibilities)
Taxpayer Advocate Service (TAS)	TAS provides service to identity theft victims who are suffering hardship or are having problems getting their accounts resolved by the IRS. A TAS case advocate works cases from beginning to end and utilizes Operations Assistance Requests (OARs) to request account actions from the various IRS functions needed to resolve the case.

III. The IRS Should Revamp Its Approach to Assisting Identity Theft Victims, Which Currently Takes Much Too Long.

In FY 2013, the IRS changed its strategy for assisting identity theft victims, adopting a specialized approach under which each department (or "function") that deals with identity theft created a dedicated group of employees to work on those issues. Clearly, there are benefits in assigning identity theft cases to a small group of specially-trained employees who can quickly become experts in these types of cases.

However, the IRS is not adequately addressing another important element of the problem. Because identity theft cases are often complex, they often require adjustments by multiple functions.[20] Even in instances where there is just one issue at hand, a case may still require multiple "touches" from various specialized units. The IRS has drafted a complex "transfer matrix" outlining situations in which a case must be routed from one specialized function to another. I am concerned that routing cases among functions sequentially is inefficient and causing excessive delays. In addition, based on TAS's experience with identity theft cases over the years, I believe that transfers among functions will continue to be commonplace.

To illustrate the complexity of an identity theft case and how many "touches" the victim may have with various IRS functions, I want to walk through a hypothetical example of a typical identity theft case.

> On April 1, 2012, John Smith attempts to file his 2011 Form 1040 electronically to claim a refund. He receives an error message that the IRS cannot accept the filing because it has already processed a return under his SSN. Unbeknownst to Mr. Smith, another person had filed a return earlier in the filing season under his SSN (but using a fictitious address) and had also filed a return for the 2010 tax year. The IRS audited the return for the 2010 tax year filed by the thief and bearing Mr. Smith's SSN. Consequently, the IRS assessed additional tax, creating a balance due on Mr. Smith's account and a pending levy from the Collection unit. To fully resolve Mr. Smith's account, the

[20] 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).

Accounts Management (AM), Examination, and Collection functions all need to take actions to clear up his 2010 and 2011 tax year accounts.

On April 4, 2012, Mr. Smith calls the IRS toll-free line and reaches a Customer Service Representative (CSR). After researching Mr. Smith's account, the CSR alerts Mr. Smith of the pending Collection activity on his 2010 account. The CSR advises him to submit a paper return for 2011 with a completed Form 14039, *Identity Theft Affidavit*.[21]

On April 5, 2012, Mr. Smith downloads Form 14039 and completes the affidavit, noting that he believes that his 2010 and 2011 tax years are impacted. Mr. Smith submits a 2011 Form 1040 and an unsigned affidavit to the appropriate IRS campus. On April 15, 2012, a Submission Processing (SP) employee reviews the tax return, notes that an ID theft affidavit is attached, and generates a letter to Mr. Smith acknowledging receipt of the affidavit and providing a *180-day timeframe for resolution*. However, this letter does not provide contact information for the Identity Protection Specialized Unit (IPSU).[22] Thus, if Mr. Smith needs to provide additional information regarding his identity theft case, he could not reach the unit established to be the centralized point of contact with identity theft victims.

Because the fraudulent 2011 tax return had already been processed for this account, an internal transcript is generated, causing a duplicate filing condition for John Smith's SSN. On May 15, 2012, SP transfers the case to the Accounts Management (AM) Identity Theft specialized unit (IDT), which works internal transcript cases. The AM IDT unit works its inventory on a first-in, first-out (FIFO) basis and generally takes up to 180 days from the date it receives the taxpayer's complete and legible documentation. (Note that AM's cycle time is not calculated from the date the taxpayer first engaged with the IRS and submitted some documentation, so already there is at least a month's discrepancy between the taxpayer's 180-day expected resolution date and the AM IDT unit's 180-day resolution date.[23])

On September 15, 2012, the AM IDT employee performs preliminary research on John Smith's account and confirms that the first return posted was fraudulent and not submitted by Mr. Smith. However, the employee also notices that Mr. Smith did not sign the identity theft affidavit he submitted. The AM IDT employee contacts Mr. Smith and requests that he sign the affidavit. Mr. Smith complies, and returns the signed affidavit on September 30, 2012. Then, after performing more research, the AM IDT employee discovers that

---

[21] *See* IRM 21.9.2.3, *Identity Theft - Telephone Overview* (Jan. 7, 2013).

[22] *See* Letter 5073C; IRM 3.11.3-1, *Attachment Guide* (July 25, 2013).

[23] *See* IRM 10.5.3.2.4.1(1), *Multiple Function Criteria (MFC) Cases Requiring Referral to IPSU for Monitoring* (May 8, 2013). There is no correlation to the 180-day timeframe referenced in Letter 5073.

the prior-year return on Mr. Smith's account was also fraudulently filed, with an audit resulting in tax owed, and enforcement action (levy) imminent. [Note that had the CSR not mentioned the 2010 collection activity to Mr. Smith on the initial call, and had Mr. Smith not explicitly listed 2010 on his ID theft affidavit, the AM IDT employee would have looked solely at the 2011 tax year and not conducted research regarding 2010 or any other open tax year.[24] Mr. Smith would likely have to go through this same process with later-discovered issues. Even with an identity theft marker on the account, Mr. Smith would have to show the examination function that he was the "legitimate" Mr. Smith.]

The IPSU monitors taxpayer accounts through resolution when an SSN owner's account requires corrective actions by more than one function. Multiple Function Criteria are defined as "an identity theft case requiring resolution across functions,"[25] which in this case includes Accounts Management, Examination, and Collection. Therefore, after resolving the internal transcript issue and processing John Smith's correct return for tax year 2011 on November 15, 2012, the AM CSR completes the referral paperwork (Form 14027A) and faxes it to the IPSU. At this point – more than seven months after filing his return on paper – Mr. Smith still has not been told when he can expect to receive his refund, nor has he received any communication from the IRS regarding the processing of his 2011 tax return.

Upon receipt of the paperwork from AM on November 15, 2012, IPSU will:

- Open a control for the purpose of monitoring;
- Research to identify all functions needing to take corrective actions;
- Email a completed referral form (Form 14027B) to the various ID theft functional liaisons, notifying them that the taxpayer's account needs corrective actions, including:
    - Collection to halt the impending levy;
    - Exam to review and correct the prior-year account; and
    - AM to review and correct the current-year account.
- Monitor for account actions by all functions on the 165th day from receipt of referral. *Thus, the first "monitoring" action by the IPSU centralized function occurs more than one year after Mr. Smith filed his return on paper*.

[24] *See* IRM 21.6.2.4.2.3, *Preliminary Research* (June 18, 2013).

[25] *See* IRM 10.5.3.2.4.1, *Multiple Function Criteria (MFC) Cases Requiring Referral to IPSU for Monitoring* (May 8, 2013).

On December 15, 2012, the IPSU sends referral forms to Collection, Exam, and AM. The referral form to Collection requests that the pending levy be stopped. Unfortunately, John Smith's current year refund, which was finally processed now that his return was processed, was applied to the prior-year balance due and not paid to him. On January 15, 2013, the Collection employee temporarily suspends the levy while the account is under review for identity theft and notifies the IPSU.

On April 1, 2013, the Examination employee is assigned Mr. Smith's case on a FIFO (first in, first out) basis as calculated from the date of receipt of the IPSU referral in the Exam unit (not the date when Mr. Smith first raised the issue of identity theft to the IRS). The employee concurs with the identity theft determination and agrees to remove the fraudulent return and additional tax assessment from John Smith's 2011 tax year. However, a different processing function in Compliance must remove the fraudulent return and additional assessment from the prior year account to complete the adjustments (in this case, the Compliance Post Adjustment Team, or CPAT). The CPAT, in contrast to other specialized identity theft units, works cases based on the age of the case from the date the IRS first received documentation from the identity theft victim.[26]

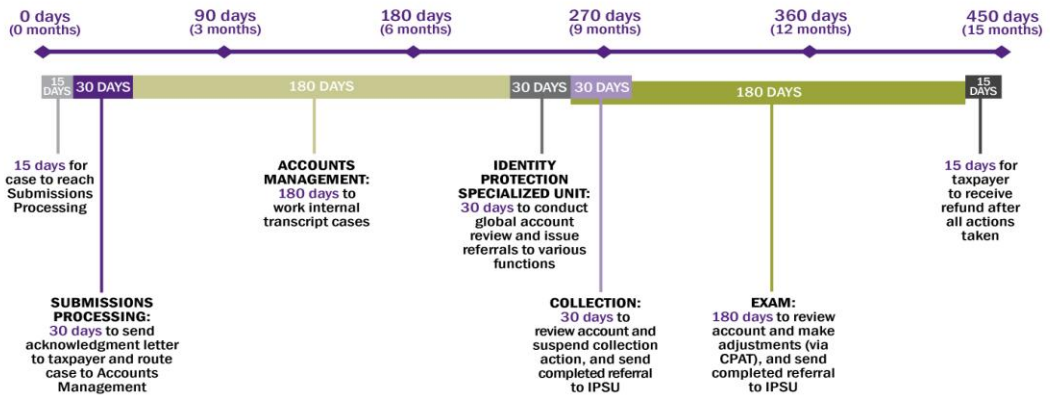
On April 30, 2013 (165 days after the IPSU established control of the case and more than a year after Mr. Smith filed his 2011 return on paper), the IPSU CSR reviews the account and notices that no action was taken on John Smith's 2010 account. On May 7, 2013, the IPSU CSR sends a secure email to Examination asking about the status of the account and reminding Exam that the 180th day for resolution is approaching. Examination must either resolve and close its case or send an interim letter to provide the taxpayer with a status update and extend case resolution period by another 60 days (13 months after Mr. Smith filed his 2011 return on paper).[27]

On June 15, 2013, a CPAT employee adjusts the prior-year account and sends a completed referral form back to the IPSU. On July 1, 2013, John Smith finally receives his refund, 15 months after he initially filed his 2011 return.

[26] *See* IRM 4.19.13.25.11, *Referrals to CPAT/DITA* (Sept. 11, 2012).

[27] *See* IRM 21.9.2.4.2, *Tax-Related Identity Theft (Andover and Fresno IPSU Only)* (May 29, 2013).

Cycle time from the taxpayer's perspective in the ID theft example



TAXPAYER ADVOCATE SERVICE
YOUR VOICE AT THE IRS

This convoluted example may seem contrived, but it is, unfortunately, a very typical identity theft case. Identity theft victims routinely must deal with three or four IRS functions to resolve all of their account issues. Most specialized units treat the identity theft as a separate case and work its inventory on a FIFO basis from the perspective of that specialized unit. Under this "silo-FIFO" approach, a taxpayer who reported the identity theft incident two weeks ago may be placed in the queue ahead of a victim who has been trying to obtain a refund for 20 months, if the latter taxpayer had the misfortune of dealing with other IRS departments to resolve related issues. By having the IRS work identity theft cases as FIFO from the perspective of each "silo," rather than holistically from the taxpayer perspective, we not only harm taxpayers (the victims) but also give a distorted picture of IRS efficiency and productivity.

The Treasury Inspector General for Tax Administration has confirmed that identity theft cases are complex and easy for the IRS to lose in the shuffle. In its May 2012 report on IRS identity theft victim assistance, TIGTA selected a sample of 17 identity theft cases and found the IRS had opened 58 separate cases to resolve the accounts of those 17 victims – an average of nearly three and a half cases for each person.[28] The average cycle time for those cases was 414 days, which included an average of 86 days of inactivity.[29]

[28] *See* IRM 21.9.2.4.2, *Tax-Related Identity Theft (Andover and Fresno IPSU Only)* (May 29, 2013).

[29] *Id.*

I have long advocated for the creation of a "traffic cop" to guide cases through the bureaucracy and serve as the single point of contact for the victim. By assigning ownership of an identity theft case to a central unit, or even a single employee within that unit, the IRS can move the case forward in the most efficient manner and reduce delays and taxpayer frustration. Without this single point of contact to facilitate case transfers from one function to another and to ensure timeliness of actions, there is greater risk that cases will get "stuck" or lost in the process.

In contrast, when TAS works a case, we assign one case advocate to the taxpayer. After speaking with him or her and reviewing documentation, the case advocate:

- Determines what actions are needed;
- Develops an action plan that prioritizes the actions; and
- Works with the appropriate functions to see that the actions are taken in a timely manner.

This includes frequent follow-up with the functions and regular communication with the taxpayer. Each taxpayer who has a case accepted into TAS is assigned a single case advocate whose toll-free phone number is given to the taxpayer, and every Local Taxpayer Advocate office has a toll-free fax number, eliminating barriers to communication. I believe, and the data support me in saying, that this is the reason TAS can resolve identity theft cases in 88 days, while cases worked under normal IRS procedures can languish for more than a year. Although identity theft cases are complex, TAS case advocates have achieved a relief rate of 88.5 percent in identity theft cases in FY 2013 (compared to 78.9 percent for TAS cases overall). An overwhelming 94 percent of identity theft victims that come to TAS in FY 2013 (through March) have expressed satisfaction (compared to a customer satisfaction score of 90 percent for TAS cases overall in that time period).[30]

The IRS needs to approach its processes from a completely different perspective than it has to date. I have repeatedly proposed that the IPSU, the centralized IRS organization established in 2008 to assist identity theft victims, be designated to fulfill this key "ownership" role. I believe that the IRS should follow TAS's approach to case resolution, and allow the IPSU to "own" identity theft cases rather than simply "monitor" them. I had the pleasure of consulting with IPSU front-line managers and analysts earlier this summer in the Andover campus. I was pleasantly surprised at how open they were about their frustrations and suggestions for relieving those frustrations. Based on those conversations and on my observations over the years, I have formulated some specific recommendations that I believe will greatly benefit victims of identity theft and help the IRS operate more efficiently.

1. **Designate the IPSU as the centralized function that controls *all* identity theft cases.** Currently, the IPSU monitors identity theft cases only when

[30] Analysis conducted by TAS Business Assessment of customer satisfaction scores reported for FY 2013 (through March 2013); data obtained from TAMIS (July 1, 2013).

multiple functions are involved. *This is misleading, because the IRS treats all Compliance functions (such as ACS, ASFR, AUR, and Correspondence Exam) as "one function" for purposes of IPSU monitoring*. To avoid having identity theft cases bounce around from one Compliance function to another, with no function responsible for overall resolution of the case, the IRS should designate the IPSU as the responsible function for all identity theft cases, and staff it accordingly. (The IRS will be able to shift resources to the IPSU because our proposed approach will reduce rework and wasted, repetitive efforts in other identity theft-related areas, including answering and referring phone calls from frustrated victims experiencing endless delays and runaround.) Taxpayers who believe they are victims of identity theft should be directed to the IPSU from the beginning. The IPSU should collect all documentation and review it as soon as it is received, so the taxpayer can cure any defects immediately.

2. **Allow IPSU employees to make simple account adjustments.** Many IPSU employees have experience in adjusting taxpayer accounts from their prior positions in AM. When I met with IPSU employees this summer, some of them expressed frustration at not being able to make simple adjustments themselves. Instead, they must transfer control to a different function, request that account adjustments be made, and follow up periodically. It would be simpler (and more beneficial to the taxpayer) if IPSU employees had the delegated authority to make account adjustments.[31]

3. **Give "teeth" to the IPSU to make its involvement in cases more meaningful.** As stated above, the IPSU must rely on various functions to take certain actions, but has no authority to hold these functions accountable. When TAS works an identity theft case, we issue Operations Assistance Requests asking that a function complete an action within, for example, three days. If the function does not comply, we can follow up by issuing a Taxpayer Assistance Order *requiring* the IRS to take an action (or cease taking an action).[32] The IPSU has no similar tools at its disposal. I suggest that the IPSU enter into Memoranda of Understanding with all of the specialized identity theft units that specify the timeframes within which actions will occur and provides for regular reporting to IRS leadership to identify the frequency with which a function fails to meet those timeframes. Otherwise, involvement by the IPSU adds little value and is very frustrating for the IPSU employees.

4. **Implement "timeliness" measures to ensure cases do not languish.** TIGTA's report noted that the identity theft cases it reviewed showed an

[31] For example, the Deputy Commissioner for Services and Enforcement delegated to the National Taxpayer Advocate the authority to perform routine customer service functions, including making certain account adjustments. *See* IRM 1.2.50.3, *Delegation Order 13-2 (Rev. 1)* (Mar. 3, 2008). (The National Taxpayer Advocate then re-delegated these authorities to case advocates.)

[32] *See* Internal Revenue Code § 7811.

average of 86 days of inactivity. In TAS cases, we institute "timeliness" goals that are intended to help our case advocates move cases along. The IRS should adopt a similar approach so its cases do not languish in one function. For example, an IPSU employee could have a goal to contact the taxpayer within two days of case receipt, develop a case action plan within three days of contact with the taxpayer, issue a request to a function within three days of developing the case action plan, follow up with the function within three days of the requested completion date, etc. The goal of these "timeliness" measures is to keep cases moving, which in turn will reduce cycle time in an organic way – not by artificially or arbitrarily setting a cycle time goal. Moreover, by centralizing cases in the IPSU, the IRS's cycle time measure will reflect the taxpayer's experience more closely, and the IPSU can designate certain taxpayer cases for expedited treatment in one function based on the overall cycle time of the case.

5. **Utilize Field Assistance employees in Taxpayer Assistance Centers more effectively.** I recognize that the IRS is trying to achieve efficiencies through specialization. But the IRS should not ignore the advantages of having geographically-dispersed Taxpayer Assistance Centers (TACs). For example, when a taxpayer comes to the TAC to present evidence of his or her identity, the Field Assistance (FA) employee may collect documentation, verify the SSN owner, temporarily suspend Collection action, and submit a referral to Exam. However, in order for the return to be processed, the FA employee must forward the case to SP. The resolution of the taxpayer's issue would still need to be handled by the three separate functions – Submission Processing, Collection, and Exam. A victim of identity theft should also be able to make an appointment to bring in all required documentation to a TAC so the return can be processed and account adjustments made as soon as the initial determination is made. From a taxpayer perspective, this would be a far better solution than waiting in various queues. Alternatively, the IRS should consider allowing victims of identity theft to make an appointment at a TAC and use virtual service delivery to connect the taxpayer with the appropriate unit for an immediate decision.

6. **Develop an identity theft database or system accessible to all functions working on identity theft cases.** As I discussed above, the IRS does not track cycle time from the identity theft victim's perspective; rather, each specialized function tracks the cycle time of the particular aspect of an identity theft case within its silo. With the vast majority of identity theft cases requiring action by multiple functions (even if not deemed to meet "multiple function criteria" under the IRS's misleading definition), the IRS does not have the capability to accurately track identity theft cases. By developing and utilizing a servicewide platform for tracking and monitoring its cases, the IRS could accurately assess the inventory at a given time and measure cycle time from the date the taxpayer identities himself or herself as a victim of identity theft. Such a system would also allow seamless transfers of cases from one function

to another. Additionally, a single identity theft database would allow for the sharing of information amongst functions. They could see if the taxpayer submitted documentation and what actions the other functions have taken, thereby helping to reduce duplicative actions by multiple functions. We recognize that the start date may differ depending on the facts and circumstances of the case, but the IRS should be able to develop guidance about when to start counting cycle time that more closely reflects the taxpayer's experience and more accurately flags over-aged cases. Currently, as the case example above shows, an identity theft case might not be considered over-aged until the victim has been in the system for over a full year.

IV. Conclusion

Identity theft causes significant problems for both the taxpayer and the IRS. IRS leadership has responded to this challenge not only by assigning more employees to work on identity theft but also by spending significant resources re-engineering its victim assistance processes over the years.[33] Certainly, some improvements have been made. Yet I think we can all agree that the IRS is not where it needs to be in terms of victim assistance.

Identity theft is a discrete problem, even if it has multiple parts. As such, it lends itself to developing a centralized unit staffed with experts whose work is given high priority by all the other units that handle aspects of the cases. That is what I expected from the IPSU when the Commissioner authorized the establishment of this unit in 2008. Yet five years later, it is clear that is not what the IRS has achieved. In fact, the IRS has gone in the opposite direction and has adopted a decentralized approach to identity theft victim assistance, one that imposes undue burden on the victims and creates procedures that would make Rube Goldberg proud.

The IRS needs to look at its processes from the perspective of the identity theft victim. Given the multiple points of contact, multiple inactive periods, and FIFO processing for each unit, the IRS might find, if it adopts our suggestions, that it would actually require **fewer** resources to do the same volume of work. I am confident that taxpayers – our customers – would be much more satisfied with their experience.

In my testimony, I have tried to identify a number of positive, practical, and achievable steps the IRS can take to improve its assistance to victims of identity theft. I thank the committee for its continued involvement and interest in this matter. I stand ready to help and appreciate the opportunity to testify.

[33] TAS had representatives on many of these task forces and re-engineering teams, yet I never got the sense that our voice was heard.