WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

TAX FRAUD BY IDENTITY THEFT, PART 2: STATUS, PROGRESS, AND POTENTIAL SOLUTIONS

BEFORE THE

SUBCOMMITTEE ON FISCAL RESPONSIBILITY

AND ECONOMIC GROWTH

COMMITTEE ON FINANCE

UNITED STATES SENATE

MARCH 20, 2012

TABLE OF CONTENTS

I. The IRS Continues to See Unprecedented Levels of Identity Theft Casework. 2

II. When Analyzing the Impact of Identity Theft, a Broad Perspective Is Necessary. 7

III. The IRS Should Continue Working with the Social Security Administration to Restrict Access to the Death Master File. 9

IV. Creating New Exceptions to Taxpayer Privacy Protections Poses Risks and Should Be Approached Carefully, if at All. 12

V. There Is a Continuing Need for the IRS's Identity Protection Specialized Unit to Play a Centralized Role in Managing Identity Theft Cases. 14

VI. Recent Identity Theft Process Improvements Require Fine-Tuning. 15

VII. The IRS Has Had Ample Time to Develop Procedures to Assist Victims of Return Preparer Fraud and Should Finalize Procedures Promptly. 18

VIII. Conclusion. 19

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

Thank you for inviting me to testify today about the subject of identity theft.[1] 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. Since 2004, I have written extensively about the impact of identity theft on taxpayers and tax administration and have worked closely with the IRS to improve its efforts to assist taxpayers who are identity theft victims.[2] The IRS has made significant progress in this area in recent years, including adopting many of my office's recommendations. Notwithstanding these efforts, it is clear that combating identity theft continues to pose significant challenges for the IRS.

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

1. The IRS continues to see unprecedented levels of identity theft casework.

2. When analyzing the impact of identity theft, a broad perspective is necessary.

3. The IRS should continue working with the Social Security Administration to restrict access to the Death Master File.

4. Creating new exceptions to taxpayer privacy protections poses risks and should be approached carefully, if at all.

---

[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 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*); *The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, a Drain on the Public Treasury*, Hearing Before the S. Comm. on Finance, Subcommittee on Fiscal Responsibility and Economic Growth, 112th Cong. (May 25, 2011) (statement of Nina E. Olson, National Taxpayer Advocate); *Filing Season Update: Current IRS Issues, Hearing Before the S. Comm. on Finance*, 111th Cong. (Apr. 15, 2010) (statement of Nina E. Olson, National Taxpayer Advocate); *Identity Theft: Who's Got Your Number, Hearing Before the S. Comm. on Finance*, 110th Cong. (Apr. 10, 2008) (statement of Nina E. Olson, National Taxpayer Advocate).

5. There is a continuing need for the IRS's identity protection specialized unit to play a centralized role in managing identity theft cases.

6. Recent identity theft process improvements require fine-tuning.

7. The IRS has had ample time to develop procedures to assist victims of return preparer fraud and should finalize procedures promptly.

I. The IRS Continues to See Unprecedented Levels of Identity Theft Casework.

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 with the intention of obtaining an unauthorized refund.[3] Identity theft wreaks havoc on our tax system in many different ways. Victims of identity theft 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 tax refunds claimed by opportunistic perpetrators. In addition, identity theft takes a significant toll on the IRS, tying up limited resources that could otherwise be shifted to taxpayer service or compliance initiatives.

The IRS has begun to utilize data analysis to develop automated identity theft filters. Programmers can perform data mining to detect trends based on a variety of factors and develop customized filters to isolate suspicious claims for refunds. While such tools make it easier for the IRS to identify such schemes, the IRS is fighting an uphill battle. It seems that new schemes are hatched each week, and while the IRS can scramble to adjust its filters, it will generally be in a reactive mode.

News reports suggest some very organized groups have chosen tax-related identity theft as the crime du jour.[4] Identity theft has become a large-scale operation – it is no longer just the work of one person stealing a few numbers and trying to get refunds, nor

[3] 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 SSN in order 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, I will focus on refund-related identity theft for this testimony.

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

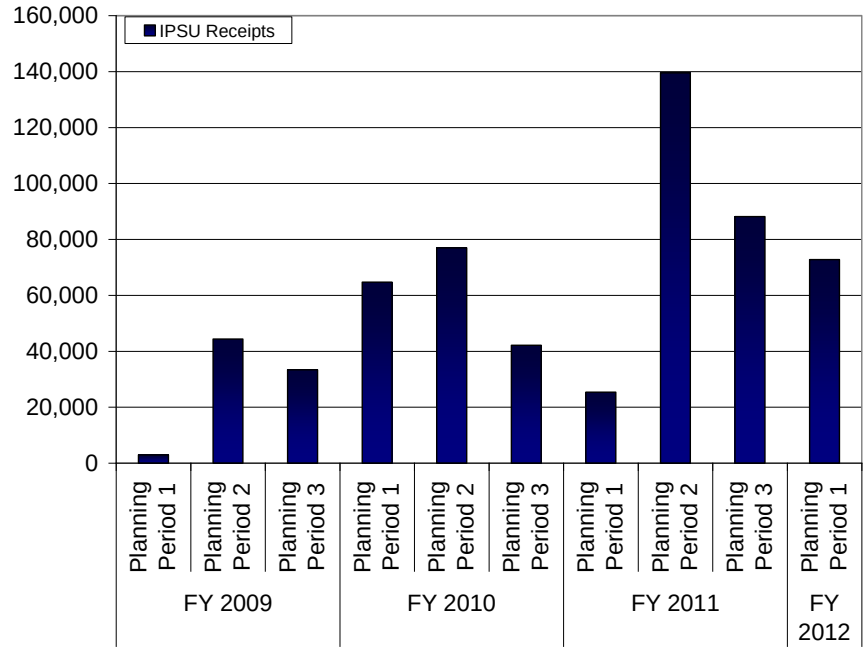
is it just someone trying to work under someone else's number. The greatest source of harm today is with "boiler room" operations involving the theft of massive lists of numbers. Apparently, there are networks of criminals who not only share stolen personal information, but also present seminars about how to use this information to file bogus returns.[5] In response to the increase in criminal activity in this area, the IRS's Criminal Investigation division (CI) in fiscal year (FY) 2011 initiated 276 fraud cases related to identity theft, with 81 convictions – up from 224 investigations and 40 convictions in FY 2010.[6]

The Identity Protection Specialized Unit (IPSU), the centralized IRS organization that assists identity theft victims, is also experiencing unprecedented levels of case receipts. As the chart below shows, IPSU receipts increased substantially over the two previous years.

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

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

Chart 1: IPSU Paper Inventory Receipts, FY 2009 to FY 2012 by Planning Period[7]

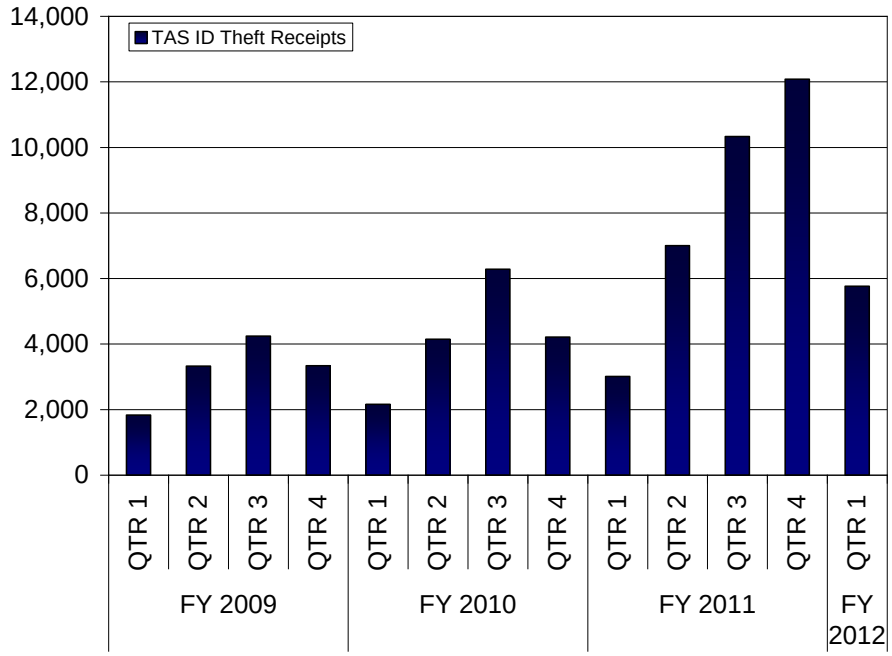


The Taxpayer Advocate Service (TAS) has experienced similar increases in identity theft cases. TAS had a 97 percent increase in identity theft receipts in FY 2011 over FY 2010, on top of a 23 percent rise from FY 2009 to FY 2010. The upward trend in identity theft receipts has continued in FY 2012. In the first quarter of FY 2012, TAS received 5,762 identity theft cases, a 91 percent increase over the same period in FY 2011.[8] The increase in TAS identity theft casework reflects the impact of both the increase in identity theft incidents and the IRS's inability to address the victims' tax issues promptly.

[7] Data obtained from IRS Identity Protection Specialized Unit (Mar. 13, 2012). The IPSU tracks cases by "planning period." Planning Period 1 covers Oct. 1 to Dec. 31, Planning Period 2 covers Jan. 1 to June 30, and Planning Period 3 covers July 1 to Sept. 30.

[8] Data provided by TAS Technical Analysis and Guidance (Mar. 12, 2012).

Chart 2: TAS Stolen Identity Case Receipts, FY 2009 to FY 2012 by Quarter[9]



The IRS has more identity theft cases than those that show up in IPSU inventory and TAS Stolen Identity receipts. The most recent IRS data show nearly 300,000 identity theft cases servicewide.[10] In addition, there will be fallout from the newly implemented identity theft filters, which stopped approximately 140,000 tax refunds from going out in the 2012 filing season (just through February 22).[11] The IRS notifies the impacted taxpayers by letter that there was a problem processing the return and instructs them to call the new Taxpayer Protection Unit (TPU) to provide more information to have their returns processed. These cases are not included in the IPSU or TAS counts. The TPU will also handle lists of SSNs involved in identity theft schemes referred by the Criminal Investigation division and other law enforcement agencies. Once the TPU reviews these lists, verified identity theft victims will receive the appropriate identity theft marker on their accounts.

Notwithstanding the IRS's verification of the identity of the victim, the fact that the SSN was misused once means it could be misused again. Thus, the taxpayer will be required to include a special personal identification number (PIN) when e-filing in future years. For verified identify theft accounts, the IRS undertakes certain protective measures, including processing future tax returns associated with a marked account through a

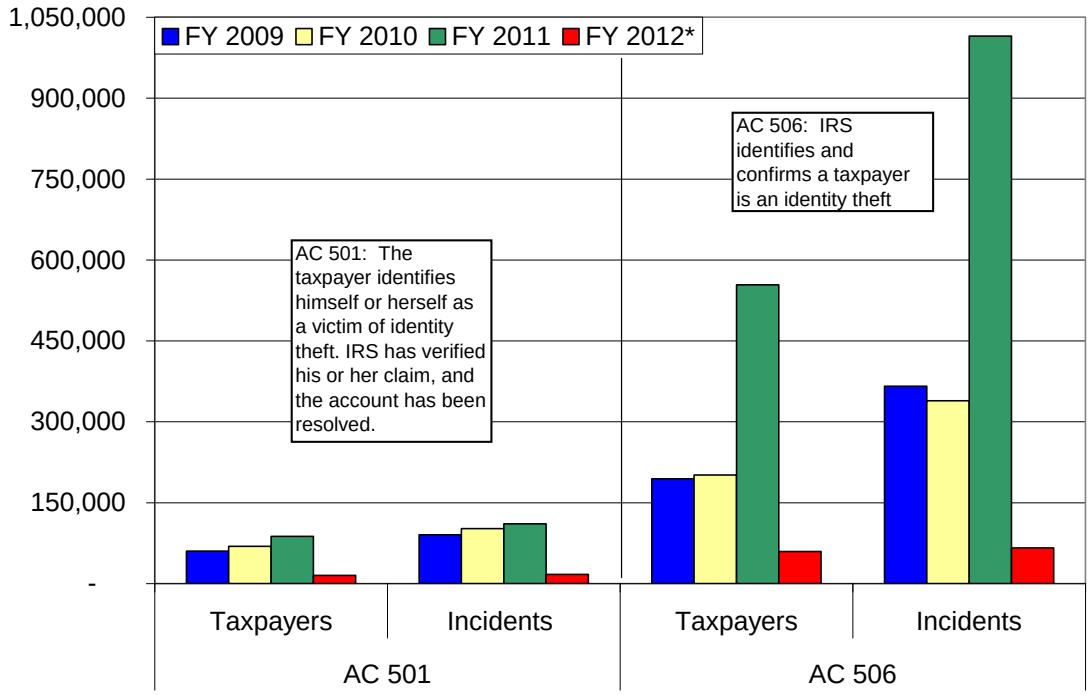
[9] Taxpayer Advocate Management Information System (TAMIS), FY 2009, FY 2010, FY 2011.

[10] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[11] Through Feb. 22, 2012. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

series of business rules designed to filter out suspicious returns. Consequently, not only does the IRS face a growing number of new identity theft cases each year, but the overall number of taxpayers impacted by identity theft continues to rise as well.

Chart 3: Accounts with Identity Theft Indicators, FY 2009 to FY 2012 Q1[12]



I am pleased to report that the IRS has accepted many of my office's recommendations for improving identity theft procedures. At various times, I have advocated for the following improvements, each of which has been adopted in some capacity:

- Development of an electronic indicator to mark accounts of verified identity theft victims;
- Creation of an IRS identity theft affidavit form;
- Adoption of a standardized list of acceptable documents to substantiate identity theft;
- Establishment of a centralized unit to provide assistance to identity theft victims;
- Provision for a global account review prior to closing an identity theft victim's account to ensure that all related issues have been resolved; and

[12] Office of Privacy, Government Liaison, and Disclosure, Incident Tracking Reports.

- Issuance of an identity protection PIN to verified taxpayers that would enable their electronically filed returns to bypass the identity theft business rules.

Despite these significant improvements, more can be done to combat, or even prevent, identity theft and other refund fraud.

II. When Analyzing the Impact of Identity Theft, a Broad Perspective Is Necessary.

Before I discuss possible process improvements, I want to take a moment to provide perspective on the IRS's overall mission and the challenges and trade-offs that addressing tax-related identity theft presents.

As the nation's tax collection agency, the IRS is responsible for processing over 145 million individual income tax returns annually, including more than 109 million requests for refunds.[13] In 2011, the average refund amount was approximately $2,913, representing a significant lump-sum payment for those taxpayers with incomes below the median adjusted gross income of $31,494 for individual taxpayers.[14]

During the filing season and throughout the year, the IRS must protect the public fisc from illegitimate refund requests while expeditiously processing legitimate tax returns and paying out legitimate refund claims. The dual tasks of fraud prevention and timely processing of returns present challenges even in simple tax systems, and ours is far from simple. The recent trend of running social programs through the tax code that require the IRS to make payments to taxpayers, combined with a reduction in IRS funding, has made the IRS's job much harder.

To better protect the public fisc from a surge of new refund schemes, the IRS has expanded its use of sophisticated fraud detection models based on data mining to filter out questionable refund claims. In FY 2011, the IRS's Electronic Fraud Detection System (EFDS) selected over one million questionable returns for screening, a 72 percent increase from the previous year.[15] The IRS estimates that EFDS has an 89 percent accuracy rate, meaning that upwards of 100,000 legitimate taxpayers are

[13] In calendar year 2011, the IRS processed 145,320,000 individual tax returns, with 109,337,000 requests for refunds. IRS, *Filing Season Statistics – Dec. 31, 2011*, *at* http://www.irs.gov/newsroom/article/0,,id=252176,00.html (last visited Mar. 12, 2012).

[14] IRS, *Filing Season Statistics – Dec. 31, 2011*, *at* http://www.irs.gov/newsroom/article/0,,id=252176,00.html (last visited Mar. 12, 2012); Compliance Data Warehouse, Individual Returns Transaction File for CY 2011.

[15] The volume of returns selected to be screened rose from 611,845 in CY 2010 to 1,054,704 in CY 2011 (through Oct. 15, 2011), a 72 percent increase. *See* National Taxpayer Advocate 2011 Annual Report to Congress 28.

expected to be caught up in these filters.[16] In my 2011 Annual Report to Congress, I discuss in depth my concerns with the IRS's delay in processing the refunds of such legitimate taxpayers.[17]

While it is important for the IRS to develop procedures to address the one million questionable returns, we should not lose sight of the fact that the IRS also has a duty to the other 144 million individual taxpayers in this country. Taxpayers have become accustomed to filing their tax returns shortly after they receive their Forms W-2 or Forms 1099 (reporting wages and interest, respectively, and available to taxpayers by January 31). Approximately 77 percent of U.S. taxpayers file electronically, meaning that the majority of refund requests can be processed within days of filing.[18] With the introduction of e-filing, combined with the increasing number of refundable credits run through the tax code, our tax system has shifted, for better or worse, to one of instant gratification.

The benefit of enjoying such a tax system is somewhat offset by the increased ability of perpetrators to defraud the government. While the IRS can develop automated filters to try to screen out as many suspicious refund claims as possible, it is unrealistic to expect the IRS to detect and deny all such claims given its resource and time constraints. Because the fraud detection algorithms are constantly evolving in response to new patterns, there will always be a lag in the filters.

If we wanted to be absolutely sure that no improper refunds are paid out to identity thieves or other individuals filing bogus returns, we could keep the April 15 filing deadline, but push the date on which the IRS will issue refunds a few months into the summer, after the return filing due date, as some other tax systems do. Such a shift would allow the IRS sufficient time to review every suspicious return. More importantly, the IRS would have at its disposal the full arsenal of information reporting databases – including complete data on wages and withholding, interest income, dividends, capital gains, and partnership income – and could better detect and resolve discrepancies and questionable returns.

However, this would be an extreme shift and it would take considerable effort to change a culture in which taxpayers have become accustomed to receiving their refunds within a week of filing their return. Delaying the delivery of a $3,000 refund to a family that is relying on these funds to meet basic living expenses may inflict severe financial hardships. Such a population may have made substantive decisions depending upon the availability of cash in February or March.

There would be other costs associated with such a drastic shift as well. Third-party lenders may welcome the opportunity to provide bridge loans to taxpayers who feel they

[16] National Taxpayer Advocate 2011 Annual Report to Congress 28.

[17] *Id*. at 28-47.

[18] IRS, *IRS e-file Launches Today; Most Taxpayers Can File Immediately*, IR-2012-7 (Jan. 17, 2012).

cannot wait six months for a refund. Because experience has shown that such lenders will be tempted to charge predatory interest rates, we would need to be prepared to further regulate this industry.

Alternatively, if we prefer not to delay the processing of refunds for six months but still insist on greater fraud detection than the IRS is currently able to manage, then Congress would need to authorize significantly more funding for the IRS. In my 2011 Annual Report, I noted that while questionable returns selected by EFDS increased by 72 percent, the staffing of the IRS unit conducting the manual wage and withholding verification grew by less than nine percent.[19] It is unrealistic to expect the IRS to keep up with its increasing workload without either allocating a corresponding increase in resources or extending the timeframe in which to conduct the necessary wage and withholding verification. Absent that, overall taxpayer service and compliance will suffer as the IRS directs resources from other IRS activities to combat identity theft.

III. The IRS Should Continue Working with the Social Security Administration to Restrict Access to the Death Master File.

In a relatively new tactic, some identity thieves are filing tax returns that claim the personal or dependency exemption and various tax credits for deceased individuals. Identity thieves have found that SSNs and other personal information of the deceased are easily accessible. Perhaps surprisingly, the federal government itself is one source of this information. The Social Security Administration (SSA) maintains a "Death Master File" (DMF) containing the full name, SSN, date of birth, date of death, and the county, state, and ZIP code of the last address on record of decedents.[20] DMF data is updated weekly and made available to the public. Today, anyone can quickly find a number of websites (including genealogy sites) that publish DMF information free or for a nominal fee.[21]

The SSA created the DMF database in 1980 in the aftermath of a consent judgment it entered into with an individual who had sought some of this information under the

---

[19] The Accounts Management Taxpayer Assurance Program (AMTAP) staff increased from 336 in FY 2010 to 366 in FY 2011, a gain of nearly nine percent. *See* National Taxpayer Advocate 2011 Annual Report to Congress 29.

[20] *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).

[21] *See* Boston Herald, *Sandwich Parents Are Twice Robbed* (Nov. 27, 2011); Scripps Howard News Service, *ID Thieves Cashing in on Dead Children's Information* (Nov. 3, 2011). Recently, several genealogy websites have voluntarily agreed to curtail the availability of DMF information. Ancestry.com announced in December 2011 that it will no longer display SSNs for anyone who has passed away within the past ten years, and RootsWeb.com, a genealogy site affiliated with Ancestry.com, states that it will not share information from the DMF "due to sensitivities around the information in this database." *See* Scripps Howard News Service, *Genealogy Sites Remove Social Security Numbers of Deceased* (Dec. 15, 2011), *available at* http://www.abcactionnews.com/dpp/news/national/genealogy-sites-remove-social-security-numbers-of-deceased.

Freedom of Information Act (FOIA).[22] FOIA generally provides that any person has a right to obtain access to certain federal agency records.[23] In crafting FOIA, Congress recognized the importance of allowing citizen access to government information. The core purpose of FOIA is to allow the public to learn what the government is up to.[24] Congress also understood the government's need to keep some information confidential, including private information about individuals who might be mentioned in federal files, and it thus included nine exemptions in the law.[25]

Personal privacy interests are protected by two exemptions within FOIA. Section 552(b)(6) protects information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." Section 552(b)(7)(C) relates to information compiled for law enforcement purposes and protects personal information when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

The challenge for the courts has been balancing the public's interest in the release of records in question against the privacy interest of the individuals involved. In 1989, the Supreme Court reiterated that the purpose of FOIA is to enable citizens to find out "what their government is up to" and clarified that this purpose "is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct."[26] The DMF contains personal records of more than 80 million deceased individuals, but these records do not reveal much, if anything, about the SSA's own conduct.[27]

An additional challenge for the courts has been assessing the privacy interest of the deceased. FOIA contains an exemption for records or information compiled for law enforcement purposes, but only to the extent production could reasonably be expected to constitute an unwarranted invasion of personal privacy (hereinafter referred to as "Exemption 7(C)").[28] While the death of the subject of personal information diminishes

---

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

[23] *See* 5 USC § 552.

[24] *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978) (citations omitted). In contrast, see *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 773 (1989) (withholding criminal "rap sheets" compiled by the FBI; they reveal nothing about agency operations); *NARA v. Favish*, 541 U.S. 157, 169, *reh'g denied*, 541 U.S. 1057 (2004) (withholding photographs of body of publicly notable individual; they reveal nothing about agency operations).

[25] *See* 5 USC § 552(b).

[26] *Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 772-73 (1989).

[27] We acknowledge that there may be some value in accessing the DMF to gain insight into the SSA. For example, an individual may suspect that the SSA's death records are grossly inaccurate. By accessing the DMF, an individual could attempt to show that the SSA's method of recordkeeping is seriously flawed. However, one could make such a finding with only partial access to the DMF or if access was delayed a couple of years.

[28] 5 U.S.C. § 552(b)(7)(C).

to some extent the privacy interest in that information, courts have held that it does not extinguish that interest.[29] In *Accuracy in Media, Inc. v. Nat'l Park Service*, the U.S. Court of Appeals for the District of Columbia "squarely rejected the proposition that FOIA's protection of personal privacy ends upon the death of the individual depicted."[30]

In 2004, the Supreme Court recognized that surviving family members also enjoy a privacy interest that must be considered when analyzing the release of agency records as it relates to Exemption 7(C). It unanimously held that the surviving family members of former Deputy White House Counsel Vince Foster had a protectable privacy interest in his death-scene photographs.[31] Other courts have also applied FOIA exemptions to withhold decedent information on the basis of survivor privacy.[32]

It is my understanding the SSA has determined there are no exemptions from FOIA that support the nondisclosure of the DMF, and it may seek a legislative remedy. I strongly support legislation to limit public access to the DMF. At the same time, I recognize the difficulty of passing legislation, and if Congress does not act, I believe the SSA has sufficient legal authority to limit public access to the DMF even without a statutory change.

Since the 1980 *Perholtz* consent judgment, significant FOIA case law has developed that articulates strong arguments, and may be relied upon, to withhold the DMF under existing FOIA exemptions.[33] Given that (1) the type of information the DMF holds does not reveal much about "what the government is up to," (2) there is significant risk identity thieves can misuse the information contained in the DMF to claim improper tax benefits, and (3) the victims' families may suffer emotional and financial harm as they deal with the aftermath of identity theft and a death in the family, I believe that a court, after conducting the requisite balancing test under FOIA, might well allow the SSA to shield some DMF information from disclosure.

---

[29] *Schrecker v. Dep't of Justice*, 254 F.3d 162, 166 (D.C. Cir. 2001) (citations omitted), *reiterated on appeal following remand*, 349 F.3d 657, 661 (D.C. Cir. 2003).

[30] *See, e.g., Accuracy in Media, Inc. v. Nat'l Park Serv.*, 194 F.3d 120, 123 (D.C. Cir. 1999) (relating to photos of the death scene of White House official Vince Foster).

[31] *National Archives & Records Admin. v. Favish*, 541 U.S. 157, 168 (2004) (finding that "well-established cultural tradition acknowledging a family's control over the body and death images of the deceased has long been recognized at common law").

[32] *Hale v. DOJ*, 973 F.2d 894 (10th Cir. 1992) (families have a privacy interest in the photographs of a deceased victim under FOIA Exemption 7(C)); *Badhwar v. U.S. Dept. of the Air Force*, 829 F.2d 182, 185-86 (D.C. Cir. 1987) (observing privacy interest of families of deceased pilots in withholding autopsy reports "of a kind that would shock the sensibilities of surviving kin"); *New York Times v. NASA*., 920 F.2d 1002, 1005 (D.C. Cir. 1990) (*en banc*) (audio tapes of the foundering of the space shuttle Challenger withheld).

[33] We recognize that, in light of the consent judgment, SSA may not be in a position to unilaterally change its position. Rather, we believe the changes in facts and law may merit the filing of a motion to alter the consent judgment to allow SSNs to be released in truncated form.

I recognize that there are many legitimate users of DMF information, and we should not restrict access any more than necessary to thwart tax-related identity theft. Perhaps the SSA can explore whether DMF data could be released with partial redaction of the SSN. Alternatively, the SSA may consider releasing unredacted DMF data on a delayed basis. Withholding DMF data for three years, for example, would frustrate the ability of identity thieves to file a purported tax return before the IRS locks down the SSN. (Because there may be legitimate tax filings with a decedent's SSN in the year of death and the year or two following death, the IRS is not able to "retire" an SSN immediately.) In my view, the damage to tax administration and the federal fisc caused by identity theft outweighs the incremental value of prompt release.

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

In my most recent Annual Report to Congress, I recommended that Congress enact a comprehensive Taxpayer Bill of Rights, and I suggested that the right to confidentiality is one of those core taxpayer rights. 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.[34]

The Internal Revenue Code (IRC) contains significant protections for the confidentiality of tax 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. "Return information" is defined broadly and includes a taxpayer's identity; the nature, source, or amount of income; payments; receipts; deductions; exemptions; credits; etc.[35] For example, information furnished to the IRS on a Form W-2 constitutes return information.

Section 6103(i)(2) authorizes the disclosure of return information (other than "taxpayer return information"[36]) in response to requests from federal agencies for use in criminal investigations. The head of the federal agency (or the Inspector General thereof)[37] must request the information in writing and can only disclose it to officers and employees of that agency who are personally/directly engaged in: (1) the preparation of a judicial or administrative proceeding regarding enforcement of a nontax federal criminal statute, (2) an investigation which may result in such a proceeding, or (3) a grand jury proceeding relating to enforcement of a nontax federal criminal statute to

[34] National Taxpayer Advocate 2011 Annual Report to Congress 505.

[35] IRC § 6103(b)(2).

[36] "Taxpayer return information," is defined as return information "which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates." IRC § 6103(b)(3).

[37] If the request is being made by the Department of Justice, multiple individuals can make the written request for the information. *See* IRC § 6103(i)(2)(A).

which the United States or such agency is or may be a party.[38] Section 6103(i)(3)(A) authorizes the IRS to disclose return information (other than "taxpayer return information"[39]), if the information may constitute evidence of a violation of a *nontax* federal criminal law, to apprise the head of the appropriate federal agency charged with responsibility for enforcing that law.

There is no corresponding exception in IRC § 6103 that allows for the release of identity theft information to *state or local* agencies.[40] However, IRC § 6103(c) provides that a taxpayer may consent to disclosure of returns and return information to any person designated by the taxpayer. Under this exception, the IRS may develop procedures that would facilitate sharing of identity theft information with state and local law enforcement agencies.

It is my understanding that some have called for the expansion of exceptions to IRC § 6103, ostensibly to help state and local law enforcement combat identity theft. I do not believe that such an expansion of this statute is appropriate. I believe that 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 recently advised that under IRC § 6103(i)(3), the IRS may share the "bad return" and other return information of an identity thief with other federal agencies. In addition, the Office of Chief Counsel has advised that because a return filed by an identity thief may be considered return information of the victim, an identity theft victim may obtain from the IRS a copy of the "bad return" and other return information associated with the processing of the "bad return" filed by the alleged thief. Further, the Office of Chief Counsel has concluded that under IRC § 6103(c)[41], an identity theft victim may consent to the disclosure of the "bad return" filed by the alleged identity thief to state and local law enforcement agencies in connection with state and local law enforcement investigations related to the identity theft.

In light of this advice, the IRS is working to develop procedures regarding how this information related to the "bad return" may be shared. For example, the IRS could

---

[38] *See* IRC § 6103(i)(2)(A)(i)-(iii).

[39] *See* IRC § 6103(b)(3). The information disclosed can include the taxpayer's identity only if there is information other than taxpayer return information that may constitute evidence of a taxpayer's violation of a nontax federal criminal law. IRC § 6103(i)(3)(A)(ii). In the typical "bad return" case, however, the thief's identity, if discovered, will almost always come from other than taxpayer return information.

[40] 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.

[41] IRC § 6103(c) provides that the IRS can disclose returns and return information to any person or persons the taxpayer designates in a request for, or consent to, such disclosure. Treas. Reg. § 301.6103(c)-1 contains the requirements for such disclosures.

request taxpayer consent to release tax return information directly to state and local law enforcement. However, I am concerned that once the information is in the hands of state and local law enforcement, there is no restriction on redisclosure under the current law. I propose that Congress modify 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 redisclosure of such information.[42]

V. There Is a Continuing Need for the IRS's Identity Protection Specialized Unit to Play a Centralized Role in Managing Identity Theft Cases.

Commissioner Shulman, in his written response to Senator Baucus's follow-up questions stemming from an April 2008 hearing, described the IPSU unit as providing "a central point of contact for the resolution of tax issues caused by identity theft." His response further stated: "This unit will provide end-to-end case resolution. Victims will be able to communicate with one customer service representative to have their questions answered and issues resolved quickly and efficiently."[43] While this description fits the model for which my office advocated, it does not accurately reflect how the IPSU works in practice.

The IPSU does not "work" an identity theft case from beginning to end. Instead, it attempts to coordinate with up to 27 other functions within the IRS to obtain relief for the victim.[44] That is, the IPSU is designed to act as the "traffic cop" for identity theft cases, ensuring that cases move along smoothly and timely and don't get stuck in one function or another along the way. In some cases (such as when the victim faces no immediate tax impact), the IPSU simply routes the case to other IRS organizations and "monitors" the victim's account every 60 days.[45] In other cases, the unit uses Identity Theft Assistance Requests (ITARs) to ask other IRS functions to take specific actions.[46]

While the procedures call for the receiving functions to give ITARs priority treatment, there are no "teeth" to ensure that this happens.[47] Unlike TAS, which can issue a Taxpayer

---

[42] *See* National Taxpayer Advocate 2011 Annual Report to Congress 505.

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

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

[45] Internal Revenue Manual (IRM) 21.9.2.4.3(7) (Oct. 1, 2011).

[46] IRM 21.9.2.10.1 (Oct. 1, 2011).

[47] IRM 21.9.2.1(4) (Oct. 1, 2011) provides:

> All cases involving identity theft will receive priority treatment. This includes…Form 14027-A *Identity Theft Case Monitoring*, and Form 14027-B, *Identity Theft Case Referral*….Identity Theft Assistance Request (ITAR) referrals are also included.

Assistance Order (TAO)[48] if an operating division (OD) does not comply with its request for assistance in a timely manner, the IPSU procedures do not specify any consequences for functions that are unresponsive to a case referral or an ITAR. Moreover, TAS has negotiated agreements with the ODs that clearly define when and how the ODs will respond to a TAS request for action. I have urged the IPSU to enter into similar agreements with other IRS ODs and functions that set forth the timeframes for taking the requested actions and to develop tracking procedures to report to heads of office when functions regularly fail to meet these timeframes.

In 2011, the IRS made a decision to adopt a specialized approach to assisting identity theft victims. Under this approach, each impacted IRS function will create a specialized unit that will be trained on identity theft account resolution and work solely on identity theft cases. Because these specialized employees will see a lot of identity theft cases, they will quickly become familiar with patterns and recognize the needs of victims.

While I agree that this approach will have benefits, I firmly believe that there remains a need for a centralized body such as the IPSU to serve as the "traffic cop." Identity theft cases are often complex, requiring adjustments by multiple IRS functions, and the risk that cases requiring involvement from multiple IRS functions will get "stuck" or fall through the cracks is high without a case coordinator. The IPSU should continue to serve an important role in this process by conducting a global account review and by then tracking each identity theft case from start to finish as it moves from one specialized function to another.

VI. Recent Identity Theft Process Improvements Require Fine-Tuning.

Identity Theft Personal Identification Numbers Rolled Out with Mixed Results

For the 2012 filing season, the IRS introduced a number of identity theft-related process improvements. Some were designed to provide greater protection for previously verified identity theft victims. Others were intended to help the IRS detect identity theft patterns using advanced data analysis. I believe these initiatives were well intentioned, but I have some concerns about their implementation.

In order 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 have been verified.[49] Letters went out in December 2011, instructing the victims that they must use the IP PIN 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.

IRM 21.9.2.10.1(1) (Oct. 1, 2011) provides that "Cases assigned as ITAR will be treated similar to Taxpayer Advocate Service (TAS) process including time frames."

[48] *See* IRC § 7811.

[49] The IRS issued 251,568 IP PINs. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

It is my understanding that over 9,000 letters containing the IP PINs were returned undeliverable, meaning that these taxpayers are unaware they cannot file their returns electronically.[50] In addition, as of February 23, approximately 15,000 taxpayers have contacted the IRS to request replacement IP PINs.[51] Through March 6, only 69 taxpayers have come to TAS for assistance with obtaining replacement IP PINs, but I anticipate that more taxpayers will be coming to TAS in the coming weeks, as they begin to realize they will not be able to electronically file without this six-digit code.

The Taxpayer Protection Unit Needs Significantly More Staffing to Increase Its Level of Service

The IRS also designed and implemented several identity theft filters this filing season that are intended to weed out suspicious returns based on a variety of factors. The good news is that the IRS can identify these patterns relatively quickly and adjust the filters accordingly. The bad news is that there is a lot of work involved to resolve the downstream consequences of these actions. Significantly, the IRS must be able to answer phone calls from legitimate taxpayers who have been caught up in these filters.

When the IRS proposed these filters, I was consulted and I consented to them on the condition that the IRS develop procedures to address legitimate returns that happen to have the characteristics of a fabricated return. I was assured there would be a mechanism for filtered tax returns to be retrieved and quickly processed, and that a dedicated Taxpayer Protection Unit would take calls from taxpayers who receive notices after being caught by the identity theft filters.

Although the IRS has established this TPU, I am disheartened to learn that the level of service on the phone line for the TPU was 11.7 percent for the week ending March 9, with an average speed of answer exceeding 3,990 seconds.[52] Let me repeat this in layman's terms – about nine out of ten calls to the "Taxpayer Protection" line did not get through, and those that did get through had to wait on hold an average of an hour and six minutes! It seems not only that the IRS misjudged the number of customer service representatives that are needed to staff this line, but also that the identity theft filters have picked up more

[50] 9,137 letters containing IP PINs were undeliverable. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[51] 15,011 taxpayers have requested replacement IP PINs as of February 23, 2012. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[52] IRS, Joint Operations Center Executive Level Summary Report (Mar. 13, 2012). Level of service (LOS) measures the relative success rate of taxpayers that call for toll-free services seeking assistance from customer service representatives (CSRs). LOS is calculated by dividing the number of calls answered by the total number of callers attempting to reach the CSR queue. *See* IRS Performance Measures Data Dictionary, *available at* http://cfo.fin.irs.gov/AssistReview/docs/FY%202009%20MD&A%20Data%20Dictionary%2008-04-09.doc (last visited Mar. 12, 2012).

returns than were anticipated. The IRS leadership has assured me this problem has been identified and resolved, and that additional resources have been allocated to ramp up TPU staffing. My staff and I will monitor the situation and continue to have conversations with the IRS concerning how we can better serve the honest taxpayers caught up in the identity theft filters.

The IRS often receives lists of compromised identities from its Criminal Investigation function, law enforcement agencies, and other third parties. Information that can identity a taxpayer comes in various forms, such as a series of debit cards, Treasury checks, or personally identifiable information retrieved from a laptop. As noted earlier, the TPU will be responsible for the review, verification, and resolution of potential identity theft cases referred to the IRS. This process includes checking and verifying returns, determining refund status, and taking appropriate action based on verification results. By identifying and preventing these schemes, the TPU should help protect taxpayers against identity theft-related fraud and enhance IRS revenue protection capabilities.

I am pleased that there is now a process in place to work these referrals, but I am concerned they will be worked by the same TPU employees who are now inundated with identity theft filter calls. If the current level of service on the phones is at 11.7 percent, can we realistically expect this unit to devote much attention to referral lists?

The IRS Should Clarify the Purpose and Impact of Identity Theft Indicators

As I mentioned earlier, the IRS is making efforts to improve its tracking and reporting of identity theft cases. Each function that works an identity theft case will be required to input an identity theft marker on a purported identity theft victim's account. This initial indicator simply marks the account as belonging to a potential identity theft victim. For any filing or refund protections to be activated, a second identity theft marker must be placed on the account after the identity theft has been verified.

With the backlog of identity theft cases, it often takes months to determine which filer is the rightful owner of the SSN where there have been duplicate filings. By this time, the next filing season may already be underway. When the identity theft victim files the following year's tax return, he or she may assume, mistakenly, that the IRS has taken steps to protect the account from would-be identity thieves, when in reality the only thing the IRS has done is to flag the account as a potential identity theft account.

I have requested that additional training be provided to remind IRS employees (including TAS employees) that the initial identity theft marker provides no protection to the victim's account and is used solely for tracking purposes. It is imperative that we quickly resolve the account problem and apply the subsequent identity theft marker, both to protect revenue and to protect the legitimate taxpayer.

VII. The IRS Has Had Ample Time to Develop Procedures to Assist Victims of Return Preparer Fraud and Should Finalize Procedures Promptly.

TAS has received a significant number of cases involving tax return preparer refund fraud. These preparers alter taxpayers' tax returns by inflating income, deductions, credits, or withholding without their clients' knowledge or consent. In one egregious instance involving several returns prepared by one person – and despite agreement by the IRS that the returns it processed were not the returns signed by the taxpayers – the Local Taxpayer Advocate could not persuade the IRS Accounts Management function to make the proper account adjustments to remove the fabricated income or credits.

The Local Taxpayer Advocate issued four Taxpayer Assistance Orders to Accounts Management in December 2010. After Accounts Management refused to comply, these TAOs were elevated to the Commissioner of the Wage and Investment (W&I) division in July 2011. After receiving no response, I further elevated the TAOs in August 2011 to the Deputy Commissioner for Services and Enforcement, who agreed that the IRS needed to make appropriate adjustments to the victims' accounts. It was not until last week that the IRS finally made the requested adjustments to the taxpayers' accounts.

Because this was a systemic issue that required guidance to W&I employees, I issued a Proposed Taxpayer Advocate Directive (TAD) to the Commissioner of W&I on June 13, 2011.[53] This Proposed TAD directed W&I to establish procedures for adjusting the taxpayer accounts in instances where a tax return preparer alters the return without the taxpayer's knowledge or consent in order to obtain a fraudulent refund. In this Proposed TAD, I cited two published opinions from the IRS Office of Chief Counsel which conclude that a return altered by a preparer *after* the taxpayer has verified the accuracy of the return is a nullity (*i.e.*, not a valid return).[54]

After receiving an unsatisfactory IRS response to concerns raised about this matter in the Proposed TAD and my 2011 Annual Report to Congress, I issued a TAD to the W&I Commissioner and the Small Business/Self-Employed Commissioner on January 12, 2012.[55] While both have acknowledged their intent to comply with the substance of the

---

[53] Pursuant to Delegation Order No. 13-3, the National Taxpayer Advocate has the authority to issue a TAD to mandate administrative or procedural changes to improve the operation of a functional process or to grant relief to groups of taxpayers (or all taxpayers) when implementation will protect the rights of taxpayers, prevent undue burden, ensure equitable treatment, or provide an essential service to taxpayers. IRM 1.2.50.4, Delegation Order 13-3 (formerly DO-250, Rev. 1), *Authority to Issue Taxpayer Advocate Directives* (Jan. 17, 2001). *See also* IRM 13.2.1.6, *Taxpayer Advocate Directives* (July 16, 2009).

[54] *See* IRS Office of Chief Counsel Memorandum, *Tax Return Preparer's Alteration of a Return*, PMTA 2011-20 (June 27, 2011); IRS Office of Chief Counsel Memorandum, *Horse's Tax Service*, PMTA 2011-13 (May 12, 2003).

[55] *See* National Taxpayer Advocate 2011 Annual Report to Congress 59-60; Taxpayer Advocate Directive 2012-1 (*Establish procedures for adjusting the taxpayer's account in instances where a tax return preparer altered the return without the taxpayer's knowledge or consent, and the preparer obtained a fraudulent refund*) (Jan. 12, 2012) (attached).

TAD, they appealed the TAD solely in an effort to extend the timeframes within which to comply with the directed actions.

It has been 15 months since TAS first raised this issue in a series of TAOs issued to Accounts Management. I have no idea why the IRS needs more time to develop guidance to its employees with respect to an area of return preparer fraud that is growing, that is closely related to identity theft, and that is potentially very harmful to the impacted taxpayers. The taxpayers are the victims here, and the IRS should act with all due haste to correct their accounts and eliminate the risk of unlawful collection.

VIII. Conclusion.

Identity theft poses significant challenges for the IRS. There will always be opportunistic thieves who try to game the system. From their perspective, the potential rewards of committing tax-related identity theft may be worth the risk. We can do more both to reduce the rewards (by continuing to implement targeted filters) and to increase the risk (by actively pursuing criminal penalties against those who are caught). But it is not a problem the IRS can solve on its own.

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