WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

IDENTITY THEFT AND TAX FRAUD

BEFORE THE

SUBCOMMITTEES ON OVERSIGHT

AND SOCIAL SECURITY

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES

MAY 8, 2012

TABLE OF CONTENTS

Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, and distinguished Members of the respective subcommittees:

Thank you for inviting me to testify today about the subject of tax-related identity theft.[1] I have written extensively about the impact of identity theft on taxpayers and tax administration and have addressed identity theft in two other congressional hearings this spring.[2] While the IRS has made significant progress in this area in recent years, I believe the IRS can do more. Identity theft is not a problem the IRS can fully solve, but I have significant concerns about certain aspects of the IRS's approach.

I first raised concerns about the IRS's processing of identity theft cases in 2004 and included identity theft as a Most Serious Problem in my 2005 Annual Report to Congress, even before the IRS acknowledged identity theft as a problem worthy of a dedicated program office.[3] The Taxpayer Advocate Service (TAS) is unique in that we work identity theft cases from beginning to end, and many TAS employees have developed expertise in this issue over the years. To its credit, the IRS has adopted many of my office's recommendations to help victims of identity theft. Indeed, a number of former TAS employees have moved to the IRS's Office of Privacy, Governmental

---

[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*); *Hearing on Tax Compliance and Tax-Fraud Prevention Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency, and Financial Management*, 112th Cong. (Apr. 19, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Tax Fraud by Identity Theft Part 2: Status, Progress, and Potential Solutions: Hearing Before the S. Comm. on Finance, Subcomm. on Fiscal Responsibility and Economic Growth*, 112th Cong. (Mar. 20, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *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, Subcomm. 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).

[3] 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*).

Liaison, and Disclosure (PGLD), the organization in charge of coordinating identity theft efforts servicewide.

Today, I am concerned that the IRS is proceeding with certain efforts to assist identity theft victims without seeking my office's involvement. TAS has an important perspective to offer in that we are the "voice of the taxpayer" within the IRS, yet we are not being given the opportunity to weigh in at the early stages when the IRS develops new procedures in this area.

For example, the IRS recently decided to adopt a specialized approach to assisting identity theft victims. As I understand it, each affected IRS function will create its own specialized unit whose employees will work solely on identity theft cases and will be trained to resolve related account problems. These specialized, embedded employees will adjust the taxpayers' accounts themselves, rather than sending them to the servicewide Accounts Management (AM) unit. Because TAS will continue to receive and resolve identity theft cases that meet our case criteria, TAS employees will work closely with these units.

In general, I support the concept of a specialized unit approach, but "the devil is in the details." Thus, I would like my staff to have an opportunity to review the procedures being developed by the various functions. Our review would serve two purposes: (1) to ensure that the rights of identity theft victims are adequately protected and (2) to allow the Taxpayer Advocate Service to update its internal procedures so that our requests for help in resolving identity theft cases reach the appropriate contacts throughout the IRS. When we asked to be a part of the review process, we were initially told that it was not our role to comment on procedures being created by other functions. Only when we recently raised this issue with the Director of PGLD were we permitted to participate in the review process. Just in the past week or so, my staff was given access to the procedures developed by the specialized units. Including TAS at such a late stage severely limits the opportunity for the IRS to adequately consider our suggestions. In the meantime, my office continues to receive identity theft cases at a record pace, and our case advocates are uncertain about where to send their identity theft-related Operations Assistance Requests (OARs).[4] In fact, I hear reports from my offices that the IRS functions are improperly rejecting our OARs. With all this confusion, taxpayers are being harmed. This is simply unacceptable.

The IRS's track record in assisting victims of return preparer fraud does not bode well for victims of identity theft.

I am concerned at the moment about the IRS's ability to develop procedures to promptly assist taxpayers who are victimized by identity theft, in part because of how the IRS has handled a related issue involving fraud by tax return preparers. The IRS has struggled

[4] An OAR (Form 12412) is used by TAS case advocates to request assistance from the IRS when TAS does not have the statutory or delegated authority to take the required action(s) on a taxpayer's case. *See* Internal Revenue Manual *(*IRM) 13.1.19.1, *TAS OAR Process* (Feb. 1, 2011).

to unwind the harm done to victims – even when it had plenty of time to develop procedures.

More specifically, TAS has received a significant number of cases involving preparer refund fraud. These preparers alter taxpayers' returns by inflating income, deductions, credits, or withholding without their clients' knowledge or consent, and pocket the difference between the revised refund amount and the amount expected by the taxpayer. The IRS ultimately discovers that the taxpayer's return is incorrect and attempts to recover the excess refund from the taxpayer through levies, liens, and other enforcement actions. In one egregious instance involving several returns prepared by the same tax return preparer – and despite the IRS's concurrence that the returns it processed were not the returns signed by the taxpayers – our Local Taxpayer Advocate could not persuade the IRS Accounts Management function (AM) to adjust the taxpayers' accounts to remove the fabricated income or credits.

In these cases, the Local Taxpayer Advocate issued Taxpayer Assistance Orders (TAOs)[5] to AM in December 2010. After AM refused to comply, I elevated these TAOs 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 correct the victims' accounts. It was not until the end of March 2012 that the IRS finally made the adjustments.

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.[6] 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. The Proposed TAD pointed out that the IRS has been aware of the issue of unscrupulous tax return preparers altering returns in this manner for at least eight years. In particular, in March of 2003, the Refund Crimes section of the IRS's Criminal Investigation (CI) division had identified a scheme in which a particular tax return preparer had altered several hundred of his clients' returns without their knowledge in order to increase the total amount of each refund, and he then diverted the excess refund into his bank account. CI sought advice from the IRS Office of Chief Counsel, which issued an opinion

[5] Internal Revenue Code (IRC) § 7811 authorizes the National Taxpayer Advocate to issue a Taxpayer Assistance Order upon a determination that a taxpayer is suffering or about to suffer a significant hardship as a result of the manner in which the internal revenue laws are being administered by the Secretary. *See* IRC § 7811.

[6] 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).

concluding that a return altered by a tax return preparer *after* the taxpayer has verified the accuracy of the return is a nullity (*i.e.*, not a valid return).[7] Counsel also advised that the taxpayer's account should be corrected by having the taxpayer file an accurate return and then adjusting the account to reflect the correct information reported on that return.[8] The Office of Chief Counsel issued an additional opinion in 2008, concluding that the IRS *can and should* adjust each taxpayer's account to remove any entries attributable to the invalid return filed by the preparer.[9] And in 2011, shortly after I issued the Proposed TAD, Counsel reaffirmed the conclusion that such altered returns were not valid.[10]

After receiving an unsatisfactory response to concerns raised about this matter in the Proposed TAD and my 2011 Annual Report to Congress,[11] I issued a TAD to the W&I Commissioner and the Small Business/Self-Employed (SB/SE) division Commissioner on January 12, 2012.[12] While both have acknowledged their intent to comply with the substance of the TAD, they appealed the TAD solely in an effort to extend the time allowed to comply with the actions, notwithstanding that they already had over eight years to develop procedures to assist these victims of fraud.

It has been almost a year and a half since TAS first raised this issue with Accounts Management. In this time, I have issued a Proposed TAD and a TAD directing the IRS to develop procedures, and have discussed this concern in my 2011 Annual Report to Congress. I and my employees have issued Taxpayer Assistance Orders in specific cases. I find it entirely unacceptable that the IRS needs more time to develop guidance for its employees about a type of return preparer fraud that it has known about for more than eight years, is growing, is closely related to identity theft, and 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.

Because of experiences like this, I believe it is critical that TAS be included in pre-decisional meetings at which changes in IRS identity theft procedures are discussed in order to ensure that the victims' perspective is adequately considered.

In my testimony today, I will make the following points with respect to identity theft:

---

[7] *See* IRS Office of Chief Counsel Memorandum, *Horse's Tax Service*, PMTA 2011-13 (May 12, 2003).

[8] *Id*.

[9] IRS Office of Chief Counsel Memorandum, *Refunds Improperly Directed to a Preparer*, POSTN-145098-08 (Dec. 17, 2008).

[10] IRS Office of Chief Counsel Memorandum, *Tax Return Preparer's Alteration of a Return*, PMTA 2011-20 (June 27, 2011).

[11] *See* National Taxpayer Advocate 2011 Annual Report to Congress 59-60.

[12] *See* 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).

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

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

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

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

5. The Taxpayer Protection Unit needs significantly more staffing to increase its level of service.

6. The IRS should clarify the purpose and impact of identity theft indicators.

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

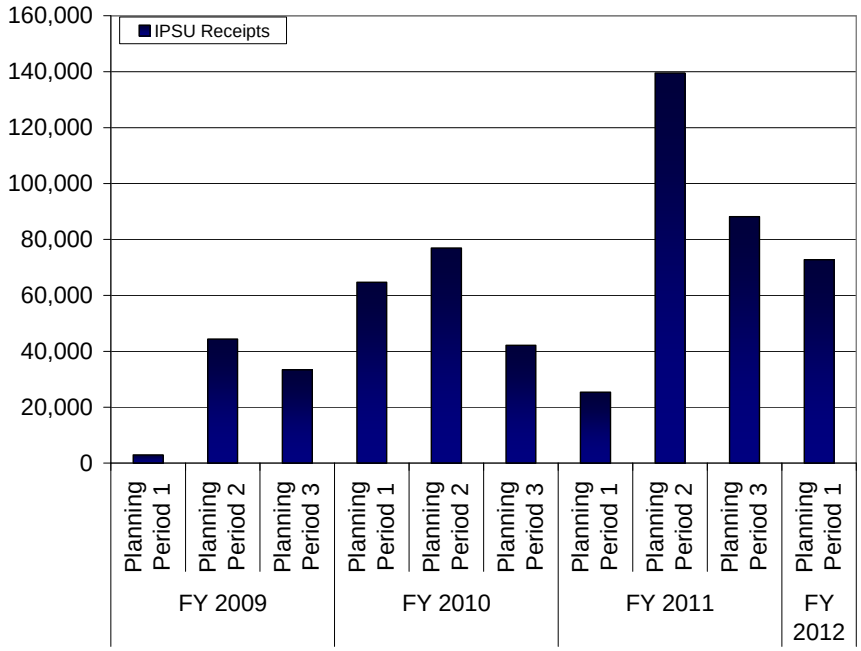
I. The IRS and TAS Continue to See Unprecedented Levels of Identity Theft Casework.

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. 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.[13] Identity theft wreaks havoc on our tax system in many ways. Victims not only must deal with the aftermath of an emotionally draining crime, but may also have to deal with the IRS for years to untangle the resulting tax account problems. Identity theft also impacts the public fisc, as Treasury funds are diverted to pay out improper tax refunds claimed by opportunistic perpetrators. In addition, identity theft takes a significant toll on the IRS, tying up limited resources that the IRS could otherwise shift to taxpayer service or compliance initiatives.

[13] 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 taxpayer identifying 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 in this testimony.

Today, identity theft can be an organized, large-scale operation. Indeed, the most recent IRS data show more than 450,000 identity theft cases servicewide.[14] The Identity Protection Specialized Unit (IPSU), the centralized IRS organization established in 2008 that assists identity theft victims, is experiencing unprecedented levels of case receipts.[15] As this chart shows, IPSU receipts increased substantially over the two previous years.

Chart 1: IPSU Paper Inventory Receipts, FY 2009 to FY 2012 by Planning Period[16]



The Taxpayer Advocate Service has experienced a similar surge in cases, as TAS identity theft receipts rose 97 percent in fiscal year (FY) 2011 over FY 2010. The upward trend has continued in the current fiscal year. In the first two quarters of FY 2012, TAS received 9,988 identity theft cases, a 43 percent increase over the same period in FY 2011.[17] The growth in casework reflects the both the increase in identity theft incidents and the IRS's inability to address the victims' tax issues promptly.

[14] Data provided by the IRS Office of Privacy, Governmental Liaison, and Disclosure (e-mail dated Apr. 17, 2012).

[15] With the IRS moving to a specialized approach to identity theft victim assistance, it is unclear what role the IPSU will play in the future. The National Taxpayer Advocate believes it is important for the IPSU to continue to serve as the "traffic cop" and serving as the single point of contact with the identity theft victim, as discussed later in this testimony.

[16] 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.

[17] There were 6,999 stolen identity (Primary Issue Code 425) cases in TAS during the same period in FY 2011. Data provided by TAS Technical Analysis and Guidance (Apr. 16, 2012).

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

I am concerned that the federal government continues to facilitate tax-related identity theft by making public the Death Master File (DMF), a list of recently deceased individuals that includes their full name, Social Security number (SSN), date of birth, date of death, and the county, state, and ZIP code of the last address on record.[18] The SSA characterizes release of this information as "legally mandated,"[19] but the extent to which courts currently would require dissemination of death data under the Freedom of Information Act (FOIA)[20] has not been tested. To eliminate uncertainty, I have recommended that Congress pass legislation to clarify that public access to the DMF can and should be limited.[21]

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

In light of the practical difficulties of passing legislation, however, I also urge the Social Security Administration to reevaluate whether it has the legal authority to place limits on the disclosure of DMF information administratively. In 1980, the SSA created the DMF, now issued weekly, after an individual filed suit in the U.S. District Court for the District of Columbia seeking certain data fields pursuant to FOIA and the court entered a consent judgment in the case pursuant to an agreement reached by the parties.[22] While the 1980 consent judgment may have seemed reasonable at the time, the factual and legal landscape has changed considerably over the past three decades.

---

[18] *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).

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

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

[21] *See* National Taxpayer Advocate 2011 Annual Report to Congress 519-23 (Legislative Recommendation: *Restrict Access to the Death Master File*).

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

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

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

In general, agencies receiving FOIA requests for personal information must balance (1) the public interest served by release of the requested information against (2) the privacy interests of individuals to whom the information pertains.[23]

In 1989, the Supreme Court reiterated that the public's FOIA interest lies in learning "what their government is up to."[24] The Court continued:

> Official information that sheds light on an agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct.[25]

Following the Supreme Court's reasoning, the Court of Appeals for the D.C. Circuit rejected a request for a list of names and addresses of retired or disabled federal employees, concluding that the release of the information could "subject the listed annuitants 'to an unwanted barrage of mailings and personal solicitations,'" and that such a "fusillade" was more than a *de minimis* assault on privacy.[26]

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

> the death of the subject of personal information does diminish to some extent the

---

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

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

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

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

> privacy interest in that information, though it by no means extinguishes that interest; one's own and one's relations' interests in privacy ordinarily extend beyond one's death.[27]

The courts have reiterated that decedents and their surviving relatives possess privacy rights in numerous cases.[28] In the decided cases, the privacy interest at issue generally has consisted exclusively of emotional trauma. Where there is tax-related identity theft, the privacy interest is much stronger because there is a financial as well as an emotional impact. For example, a parent who has lost a child to Sudden Infant Death Syndrome and then discovers an identity thief has used the DMF to claim his child as a dependent must not only devote time trying to prove to the IRS that he was the legitimate parent, but he must also deal with the financial burden of having his tax return (and refund) frozen.

Consider two legitimate uses of DMF information. One is by pension funds that use the information to terminate benefits as of the date of a beneficiary's death. The other is by genealogists who use DMF information to help them build a family tree. While both uses are reasonable, neither fits within the core purpose of FOIA of alerting the citizenry about "what their government is up to." The D.C. Circuit has held that where disclosure does not serve the core purpose of FOIA, no public interest exists, and any personal privacy interest, however modest, is sufficient to tip the balance in favor of nondisclosure.[29] Even if a court were to decide that the DMF does serve a core FOIA purpose, it would balance the public and privacy interests and could easily conclude that the privacy interests predominate.

Thus, if legislation is not forthcoming, I hope the SSA will reconsider its legal analysis and decide to take steps to restrict access to the DMF.[30]

---

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

[28] *See, e.g., National Archives & Records Administration v. Favish*, 541 U.S. at 170 ("FOIA recognizes surviving family members' right to personal privacy with respect to their close relative's death-scene images."); *Accuracy in Media, Inc. v. National Park Service*, 194 F.3d 120, 123 (D.C. Cir. 1999) (noting that the D.C. Circuit "has squarely rejected the proposition that FOIA's protection of personal privacy ends upon the death of the individual depicted"); *Campbell v. Department of Justice,* 164 F.3d 20, 33 (D.C. Cir. 1998) ("The court must also account for the fact that certain reputational interests and family-related privacy expectations survive death."); *New York Times v. National Aeronautics & Space Administration,* 920 F.2d 1002, 1005 (D.C. Cir. 1990) (*en banc*) (concluding that NASA was not required to release audio tapes of the final minutes aboard the Challenger space shuttle).

[29] *National Association of Retired Federal Employees v. Horner*, 879 F.2d 873, 879 (D.C. Cir. 1989).

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

III. 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.[31]

The Internal Revenue Code (IRC) contains significant protections for the confidentiality of returns and return information. IRC § 6103 generally provides that returns and return information shall be confidential and then delineates a number of exceptions to this general rule. "Return information" is defined broadly and includes a taxpayer's identity; the nature, source, or amount of income; payments; receipts; deductions; exemptions; credits; and similar items.[32] For example, information furnished on a Form W-2 constitutes return information.

Section 6103(i)(2) authorizes the disclosure of return information (other than "taxpayer return information"[33]) in response to requests from federal law enforcement agencies for use in criminal investigations. The head of the federal agency (or the inspector general of that agency)[34] 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 which the United States or such agency is or may be a party.[35] Section 6103(i)(3)(A) authorizes the IRS to disclose return information (other than "taxpayer return information"[36]), 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.

---

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

[32] IRC § 6103(b)(2).

[33] "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).

[34] If the request is being made by the Department of Justice, multiple specifically named high level officials can make the written request for the information. *See* IRC § 6103(i)(2)(A).

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

[36] *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). "Return information" that is not "taxpayer return information" may include a taxpayer's identity, amount of income, deductions, etc., that is not filed with (or furnished to) the IRS by the taxpayer to whom the return information relates. IRC § 6103(b)(2) & (3). In the typical "bad return" case, the thief's identity, if discovered, will almost always come from other than taxpayer return information.

There is no corresponding exception in IRC § 6103 that allows for the release of identity theft information to *state or local* agencies.[37] 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 has developed a pilot that would facilitate a consent-based 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 have significant concerns about loosening taxpayer privacy protections and I do not believe that such an expansion of this statute is appropriate at this time. I believe the current framework of IRC § 6103 includes sufficient exceptions to allow the IRS to share information about identity thieves.

The IRS Office of Chief Counsel has advised that under IRC § 6103(i)(3)(A), the IRS may share the "bad return" and other return information of an identity thief with other federal law enforcement agencies investigating the identity theft. In addition, the Office of Chief Counsel has advised that because a "bad return" filed by an identity thief may be considered return information of the victim, an identity theft victim can 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 has developed a pilot in which tax data related to the "bad return" may be shared with state and local law enforcement agencies based on the victim's written consent. I believe this approach strikes an appropriate balance – protecting taxpayer return information while simultaneously giving state and local law enforcement authorities more information to help them investigate and combat identity theft. However, I am concerned that once the information is in the hands of state and local law enforcement, there is no prohibition in the tax code against redisclosure. Therefore, I suggest that Congress consider modifying IRC § 6103(c) to explicitly limit the use of tax return information to the purpose agreed upon by the taxpayer (*i.e.*, to allow state or local law enforcement to use the information solely to enforce state or local laws) and to prohibit the redisclosure of such information.[38]

---

[37] 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.

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

IV. 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 specialized unit (IPSU) 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."[39] 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 coordinates with up to 27 other functions within the IRS to obtain relief for the victim.[40] 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 are not stuck in one function or another. 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 account every 60 days.[41] In other cases, the unit uses Identity Theft Assistance Requests (ITARs) to ask other IRS functions to take specific actions.[42]

While the procedures call for the receiving functions to give ITARs priority treatment, there are no "teeth" to ensure that this happens.[43] Unlike TAS, which can issue a Taxpayer Assistance Order 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.

---

[39] *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.

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

[41] IRM 21.9.2.4.3(7) (Oct. 1, 2011).

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

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

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

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

Although the IRS has now shifted gears and plans to take a specialized approach to assisting identity theft victims, I firmly believe 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 without a coordinator, there is a high risk that these cases will get "stuck" or fall through the cracks. The IPSU should continue to play a central role in this process by conducting a global account review and then tracking each identity theft case from start to finish, from one specialized function to another.

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

For the 2012 filing season, the IRS designed and implemented several identity theft filters intended to weed out suspicious returns. Through data mining, programmers can detect trends based on a variety of factors and develop customized filters to isolate suspicious claims for refunds.

When the IRS proposed these filters, I was consulted and I said I could support them on the condition that the IRS also expeditiously address legitimate returns that happen to have the characteristics of a fabricated return. Significantly, the IRS must be able to answer phone calls from legitimate taxpayers who are caught up in the filters. I was assured there would be a mechanism for filtered tax returns to be retrieved and quickly processed, and a dedicated unit would be sufficiently staffed to take taxpayers' calls.

The IRS now notifies affected taxpayers by letter that it had a problem processing the return and instructs them to call the new Taxpayer Protection Unit (TPU) to provide more information.[44] Unfortunately, this unit is woefully understaffed to handle the volume of calls from taxpayers trying to figure out why their returns are not being processed. For the week ending March 10, the level of service on this unit's phone line was 11.7 percent, meaning that only about one out of every nine calls was answered.[45] And callers who did get through had to wait on hold an average of an hour and six minutes![46]

---

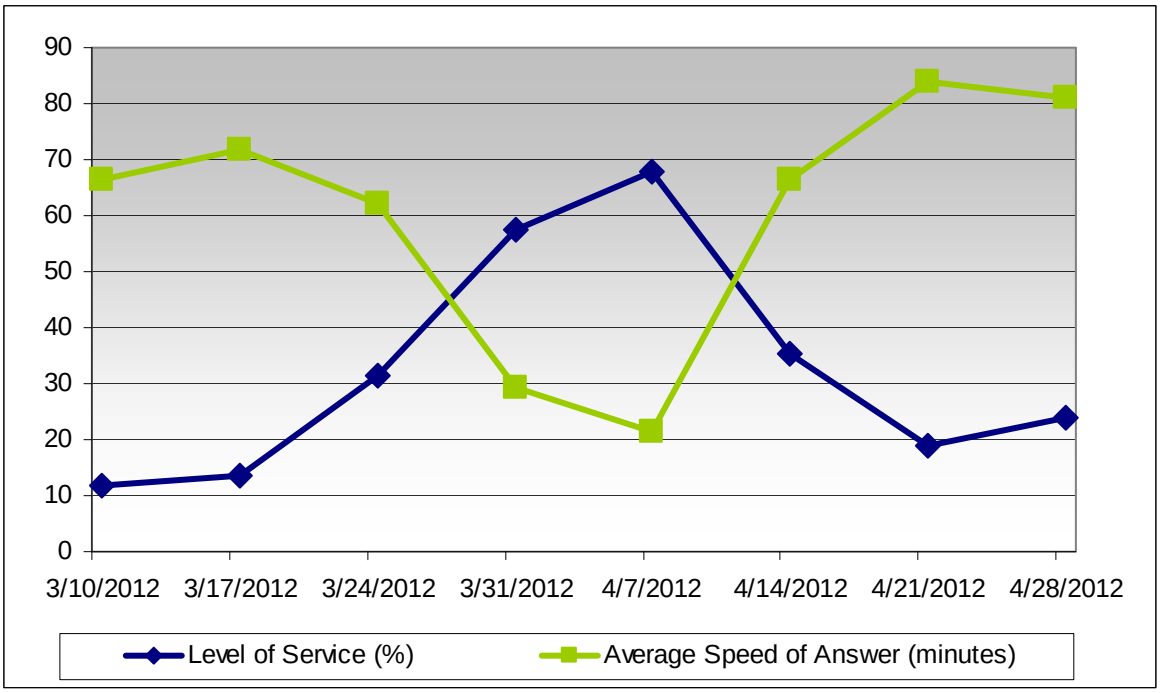
[44] The Taxpayer Protection Unit should not be confused with the Identity Protection Specialized Unit, which assists victims of identity theft. The number to the TPU phone line is provided to taxpayers who receive a letter as a result of the identity theft filters implemented in the 2012 filing season. Victims of identity theft are still instructed to call the toll-free line operated by IPSU.

[45] 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 2009 Data Dictionary (Aug. 4, 2009).

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

In the following weeks, the IRS provided additional staffing for the TPU, yet the level of service for this line has not risen to an acceptable level. For the week ending April 28, the TPU achieved a 24.0 percent level of service, with the average wait time increasing to one hour and 21 minutes.[47] This performance is simply unacceptable. The TPU clearly requires more support. I note, however, that in a zero-sum budget environment, providing more resources for this unit means another IRS unit will have less. The table below shows the level of service and average wait time for this "Taxpayer Protection" toll-free line for the past two months.

Chart 2: Taxpayer Protection Unit Toll-Free Line Data



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

The IRS leadership has assured me this problem has been identified and resolved, and additional resources have been allocated to TPU staffing. Yet the actual LOS data cast doubt on these assurances. Accordingly, 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. From this point on, I will be less

[47] The average speed of answer was 4,868 seconds for this period. IRS, Joint Operations Center Executive Level Summary Report (Apr. 28, 2012).

willing to lend my support to additional filters until I see actual staffing plans and commitments, beyond mere verbal assurances, that the IRS will address the needs of legitimate taxpayers ensnared by the 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 an alleged identity thief's laptop. 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. With the current level of service on the phones at 24 percent, can we realistically expect that this unit will be able to devote much attention to referral lists?

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

The IRS is making efforts to improve its tracking and reporting of identity theft cases.[48] Each function that works a case is required to input an identity theft marker on the purported 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 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 IRS has simply flagged the account as a potential identity theft account.

I have asked 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.

---

[48] The National Taxpayer Advocate first recommended that the IRS develop an electronic indicator to mark the accounts of identity theft victims in 2005, an idea the IRS ignored in its response. *See* National Taxpayer Advocate 2005 Annual Report to Congress 185, 191. It was not until 2008 that the IRS developed such an indicator. *See* National Taxpayer Advocate 2007 Annual Report to Congress 110 ("In collaboration with the TAS and representatives from IRS business and operating divisions, the IRS has developed a process for using a universal identity theft indicator that will be placed on a taxpayer's account, beginning in 2008, when the taxpayer self-identifies as an identity theft victim.").

In addition to applying an identity theft marker to a victim's account, the IRS should also notify victims in writing that their personal information has been misused. I made this recommendation in my 2007 Annual Report to Congress.[49] While such a letter would not directly stop identity theft, it would alert innocent taxpayers that their personal information has been compromised and allow them an opportunity to take measures to protect themselves from further harm. Only recently has the IRS developed such a letter, and my understanding is that over 16,000 letters have gone out thus far in the 2012 filing season.[50] However, not every function appears to be issuing these notification letters.[51] The fact that it took over four years to develop such a simple and helpful letter suggests the IRS has not placed adequate emphasis on victim assistance. The fact that not all appropriate functions currently issue these letters reveals the need for a stronger identity theft program office that does not rely on individual functions to develop their own procedures without sufficient oversight.

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

I want to take a moment to provide much-needed 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.[52] 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.[53]

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

---

[49] National Taxpayer Advocate 2007 Annual Report to Congress 112.

[50] Data obtained from the Notice Gatekeeper intranet site (May 3, 2012).

[51] For example, there is no guidance in the IRM for the Automated Underreporter function to issue Letter 4310c to taxpayers whose SSNs have been misused.

[52] 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).

[53] 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.

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. 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.[54] While it is important for the IRS 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 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 the IRS can process most refund requests within a week or two of filing.[55] 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 seeks to implement automated filters to screen out as many suspicious refund claims as possible, it is unrealistic to expect the IRS to detect and deny all such claims. 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 certain 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 nearly the full arsenal of information reporting databases – including complete data on wages and withholding, interest income, dividends, and capital gains – and could better detect and resolve discrepancies and questionable returns before refunds are issued.

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 or two of electronically filing their returns. 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. Many taxpayers have grown accustomed to the existing cycle and make financial decisions based on the assumption they will receive their refunds 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

[54] 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.

[55] 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 can now manage, then Congress should authorize significantly more funding for the IRS so it can expeditiously work cases where returns and associated refunds have been flagged but may be legitimate. 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.[56] 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 for the necessary wage and withholding verification. Absent one of these steps, honest taxpayers will continue to be harmed and overall taxpayer service and compliance will suffer as the IRS directs resources from other IRS activities to combat fraud and identity theft.

Recently, the IRS started exploring the feasibility of using an e-authentication system. The White House is promoting the development of an "Identity Ecosystem" – essentially a marketplace of trusted credential providers that individuals could choose to use in order to better authenticate and protect themselves online.[57] The IRS is in discussions with the National Strategy for Trusted Identities in Cyberspace (NSTIC) to see how this e-authentication system can both make it more difficult for individuals to commit identity theft and offer increased convenience to taxpayers.[58] The IRS will conduct a cost-benefit analysis of participation in this NSTIC program.

VIII. Conclusion

Identity theft poses significant challenges for the IRS. Opportunistic thieves will always try to game the system. From their perspective, the potential rewards of committing tax-related identity theft may be worth the risk. We can do more both to reduce the rewards (by continuing to implement targeted filters) and to increase the risk (by actively pursuing criminal penalties against those who are caught). In making the tax system less attractive to such criminal activity, we cannot impose significant burden on

---

[56] 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.

[57] *See* The White House, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy* (Apr. 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf; The White House Blog, *The National Strategy for Trusted Identities in Cyberspace*, http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace (last visited May 3, 2012).

[58] For more information about the NSTIC program, see http://www.nist.gov/nstic.

taxpayers, including those who are identity theft victims. Moreover, identity theft 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. Under current circumstances, it is simply not possible for the IRS both to process legitimate returns rapidly and to combat identity theft effectively.