

**KENNETH H. RYESKY, ESQ., STATEMENT FOR THE RECORD, UNITED STATES  
HOUSE OF REPRESENTATIVES COMMITTEE WAYS & MEANS,  
SUBCOMMITTEES ON SOCIAL SECURITY AND ON OVERSIGHT, JOINT  
HEARING ON IDENTITY THEFT AND TAX FRAUD:**

**I. INTRODUCTION:**

The House Ways & Means Committee, Subcommittees on Social Security and on Oversight, held a Hearing on 8 May 2012, regarding the use of identity theft by tax fraudsters. Public comments were solicited. This Commentary is accordingly submitted.

**II. COMMENTATOR'S BACKGROUND & CONTACT INFORMATION:**

Background: The Commentator, Kenneth H. Ryesky, Esq., is a member of the Bars of New York, New Jersey and Pennsylvania, and is an Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York, where he teaches Business Law courses and Taxation courses. Prior to entering into the private practice of law, Mr. Ryesky served as an Attorney with the Internal Revenue Service ("IRS"), Manhattan District. In addition to his law degree, Mr. Ryesky holds BBA and MBA degrees in Management, and a MLS degree. He has authored several scholarly articles and commentaries on taxation, including one made part of the printed record of a previous hearing before the full Senate Finance Committee<sup>1</sup> and also cited in a report by Her Majesty's Treasury's Office of Tax Simplification.<sup>2</sup>

As explained in greater detail in commentaries to previous related Hearings, the Commentator has a personal and sometime professional interest in genealogy.

Contact Information: Kenneth H. Ryesky, Esq., Department of Accounting & Information Systems, 215 Powdermaker Hall, Queens College CUNY, 65-30 Kissena Boulevard, Flushing, NY 11367. Telephone 718/997-5070; E-mail: khresq@sprintmail.com.

Disclaimer: Notwithstanding various consultations between the Commentator and other interested individuals and organizations, this Commentary reflects the Commentator's personal views, is not written or submitted on behalf of any other person or entity, and does not necessarily represent the official position of any person, entity, organization or institution with which the Commentator is or has been associated, employed or retained.

---

<sup>1</sup> *Tax: Fundamentals in Advance of Reform*, Hearing before the Committee on Finance, U.S. Senate, 110th Congress, 2nd Session, April 15, 2008, S. Hrg. 110-1037, pp. 113 - 150  
<<http://finance.senate.gov/library/hearings/download/?id=fead52be-a791-4105-96da-0010264cd7ed>>.

<sup>2</sup> Her Majesty's Treasury, Office of Tax Simplification, *Review of Tax Reliefs, Interim Report*, pp 9 - 10 (December 2010) <[http://www.hm-treasury.gov.uk/d/ots\\_review\\_tax\\_reliefs\\_interim\\_report.pdf](http://www.hm-treasury.gov.uk/d/ots_review_tax_reliefs_interim_report.pdf)>.

### III. COMMENTARY ON THE ISSUES:

#### A. Previous Hearings:

The instant proceeding of 8 May 2012 is not written on a blank slate. The Social Security Subcommittee already held a hearing on the issue on 2 February 2012, and the Fiscal Responsibility & Economic Growth Subcommittee of the Senate Finance Committee also held hearings on 25 May 2011 and on 20 March 2012.

The Commentator submitted Statements for the Record for the 2 February 2012<sup>3</sup> and 20 March 2012<sup>4</sup> Hearings. These previous Statements are incorporated by reference into this instant Statement.

#### B. Of Mice and SSNs:

The Subcommittees would do well to take to heart the Talmudic dictum to not blame the mouse, but to blame the hole.<sup>5</sup> If indeed the Social Security Death Master File (DMF)<sup>6</sup> is the "mouse," then cutting off all public access to it will not close the "mousehole." Enterprising fraudsters have a plethora of other available sources for Social Security Numbers (SSNs) with which to commit tax fraud through identity theft.

SSNs have been inadvertently posted on websites.<sup>7</sup> SSNs are to be found in trash cans and dumpsters,<sup>8</sup> including those of such entities as hospitals,<sup>9</sup> law firms,<sup>10</sup> schools,<sup>11</sup> banking

---

<sup>3</sup> Posted on the internet at <<http://www.fgs.org/rpac/wp-content/uploads/2012/02/wm-ssdmf-comments-2012.pdf>>, also available at 2012 TNT 25-32.

<sup>4</sup> Posted on the internet at <<http://www.fgs.org/rpac/wp-content/uploads/2012/04/senfincomm-taxfraud-20120320-corrected2.pdf>>, also available at 2012 TNT 56-30.

<sup>5</sup> TALMUD, GITTIN 45a.

In using the mouse and mousehole metaphor, the Commentator does not in any way intend to insult or denigrate rodents by equating them to the depraved reprobates who, inter alia, expropriate the identities of deceased children in order to defraud the public treasury.

<sup>6</sup> The DMF is available and utilized in another incarnation known as the Social Security Death Index (SSDI), and is often referred to as such.

<sup>7</sup> See, e.g. Doe 1 v. AOL, LLC, 719 F. Supp. 2d 1102 (N.D. Cal. 2010).

<sup>8</sup> E.g. Mike Salinero and Peter Bernard, *Personal Data Found in Trash Bins*, TAMPA TRIBUNE, 18 October 2009, p. 9; Lukas I. Alpert and Matthew Nestel, *WTC Identity Crisis - Ground Zero Workers' Personal Info Exposed*, N.Y. POST, 22 April 2008, p. 8; Cathy Zollo, *An Identity Trove Intact in the Trash*, SARASOTA HERALD-TRIBUNE, 23 October 2007, p. A1.

and finance institutions,<sup>12</sup> and casinos.<sup>13</sup> SSNs can be found amongst the images stored on the archival hard drives of copy machines,<sup>14</sup> and can, inadvertently or otherwise, be posted on bulletin boards in union halls.<sup>15</sup>

Paper records in transit can, in the event of a crash or other misadventure, be spilled, strewn and dispersed along the highway;<sup>16</sup> indeed, even the IRS's own couriers are susceptible to such traffic mishaps.<sup>17</sup>

Nor have the local law enforcement authorities always fully appreciated the significance of personal data in the wrong hands.<sup>18</sup>

---

<sup>9</sup> *E.g. Patients' Records Tossed into Dump*, RECORD [Stockton, CA], 16 June 2011.

<sup>10</sup> *E.g. Mary Mitchell, Lax Document Disposal Leaves Privacy in Shreds*, Chicago Sun-Times, 29 July 2010, p. 12.

<sup>11</sup> *See, e.g. Elizabeth Lazarowitz, PS Workers' Info Dumped for All to See*, N.Y. DAILY NEWS, 25 September 2009, p. 62..

<sup>12</sup> *E.g. ILLINOIS ATTORNEY GENERAL, PRESS RELEASE, ATTORNEY GENERAL MADIGAN SUES PAYDAY LOAN STORE AFTER CUSTOMERS' PERSONAL INFORMATION ENDS UP IN THE TRASH (15 October 2010), available on the Internet at <[http://www.illinoisattorneygeneral.gov/pressroom/2010\\_10/20101015.html](http://www.illinoisattorneygeneral.gov/pressroom/2010_10/20101015.html)>*.

<sup>13</sup> *See, e.g. United States v. Greer*, 640 F.3d 1011 (9th Cir. 2011, *cert. denied* \_\_\_ U.S. \_\_\_, 132 S. Ct. 834, 181 L. Ed. 2d 540 (2011)).

<sup>14</sup> *E.g. Jennifer Saranow Schultz, Identity Theft and Copiers*, N.Y. TIMES, 22 May 2010, p. 5.

<sup>15</sup> *See, e.g. Fisher v. Communication Workers of America*, 716 S.E.2d 396 (N.C. Ct. App. 2011), *appeal dismissed* 721 S.E.2d 231 (N.C. 2012).

<sup>16</sup> *E.g. Will Jayson Marin, Privacy Concerns Raised about Paperwork Spilled in Marin Highway 101 Mishap*, CONTRA COSTA TIMES, 5 May 2011.

<sup>17</sup> IRS, PROBLEM ALERT: IRS REPORTS SOME TAX PAYMENTS FROM 13 STATES LOST (September 23, 2005), available at 2005 TNT 185-56 (26 September 2005), formerly posted on Internet at <<http://www.irs.gov/newsroom/article/0,,id=98129,00.html>> (accessed December 12, 2005), (reporting that, in aftermath of traffic accident, approximately 30,000 tax payments sent to the IRS "were ejected into the San Francisco Bay and are not recoverable").

The apparent disappearance of the document from the IRS's website is not inconsistent with the IRS's cultural norm which places low priority on the proper preservation of its own historical records and documents. *See* SHELLEY L. DAVIS, UNBRIDLED POWER 38 - 47 (HarperBusiness, N.Y., 1997).

<sup>18</sup> *See, e.g. Paul Walsh, Stolen Data On 3.3 Million Loans is Found; Despite Publicity About the Theft, the Stolen Data Sat in a Minneapolis Police Evidence Room for Three Weeks*, MINNEAPOLIS STAR TRIBUNE, 17 April 2010, p. 1B.

And if the inadvertent release of SSNs poses a threat to individuals' identity security, then the intentional misappropriation of SSNs by fraud-minded individuals who abuse their trusts is all the more nefarious. This has already occurred in numerous incidents and settings, including but not limited to misdeeds by employees of hospitals and health care facilities,<sup>19</sup> real estate brokers,<sup>20</sup> Banks and mortgage lenders,<sup>21</sup> debt collection agencies and skip tracers,<sup>22</sup> tax return preparers,<sup>23</sup> military installations,<sup>24</sup> and government agencies<sup>25</sup> (including the IRS and state taxation authorities<sup>26</sup>). Enterprising identity thieves have been known to recruit individuals

---

<sup>19</sup> See, e.g. *United States v. Brown*, 399 Fed. Appx. 949 (5th Cir. 2010); *United States v. Cage*, 458 F.3d 537 (6th Cir. 2006); *Managed Care Solutions, Inc. v. Community Health Systems, Inc.*, 2011 U.S. Dist. LEXIS 138968 (S.D. Fla. 2011), *reconsideration denied* 2012 U.S. Dist. LEXIS 54901 (S.D. Fla. 2012); see also FBI, New Orleans Division, Press Release, *Pair Pleads Guilty to Stealing Patient Information to be Used for Personal Gain* (5 January 2012), available on the Internet at <http://www.fbi.gov/neworleans/press-releases/2012/pair-pleads-guilty-to-stealing-patient-information-to-be-used-for-personal-gain>.

<sup>20</sup> See, e.g. *United States v. Akinkoye*, 185 F.3d 192 (4th Cir. 1999), *cert. denied* 528 U.S. 1177 (2000).

<sup>21</sup> See, e.g. FBI, Los Angeles Division, Press Release, *Former Employee of Countrywide Home Loans Ordered to Pay \$1.2 Million in Restitution for Data Breach Involving Information for Millions of Individuals* (28 September 2011), available on the Internet at <http://www.fbi.gov/losangeles/press-releases/2011/former-employee-of-countrywide-home-loans-ordered-to-pay-1.2-million-in-restitution-for-data-breach-involving-information-for-millions-of-individuals>.

<sup>22</sup> See, e.g. *United States v. Cummings*, 395 F.3d 392 (7th Cir. 2005).

<sup>23</sup> See, e.g. *United States v. Peck*, 62 Fed. Appx. 561 (6th Cir. 2003).

<sup>24</sup> See, e.g. *United States v. Perkins*, 287 Fed. Appx. 342 (5th Cir. La. 2008).

<sup>25</sup> See, e.g. *United States v. Concepcion*, 795 F. Supp. 1262 (E.D.N.Y. 1992); N.Y. City Dept. of Investigation, Release #26-2007, *A Former City Employee Arrested by DOI in Tax Scam is Sentenced to Three Years of Probation in Federal Court* (23 April 2007), available on the Internet at [http://www.nyc.gov/html/doi/downloads/pdf/pr26vaught\\_04232007.pdf](http://www.nyc.gov/html/doi/downloads/pdf/pr26vaught_04232007.pdf).

<sup>26</sup> See, e.g. Testimony of J. Russell George, instant Hearing, pp. 13 - 14 (8 May 2012), available at 2012 TNT 90-56; see also New York State Office of the Attorney General, Press Release, *Former State Tax Department Employee Sentenced for Using Position to Steal Taxpayer Identities* (25 January 2010), available on the Internet at <http://www.ag.ny.gov/press-release/new-york-state-attorney-general-andrew-m-cuomo-former-state-tax-department-employee>.

employed in one or more of the aforementioned industries (and/or other lines of work which give them access to SSNs of employees, customers or clients) to commit fraud on a wholesale basis.<sup>27</sup>

In his Statement submitted for the Record of the 20 March 2012 Hearing of the Senate Finance Subcommittee on Fiscal Responsibility & Economic Growth,<sup>28</sup> the Commentator discusses the distinction between data security and the more inclusive concept of data stewardship.

Deficient data stewardship practices by the New York City Human Resources Administration (HRA) left that agency wide open for fraud. As noted by the court in sentencing some of the perpetrators of that fraud:

At the most basic level, HRA did not run simple computer checks with the federal Social Security Administration to determine if the social security numbers being used by the defendants had been issued. HRA also failed to forward prompt warnings to the local centers where a problem was brought to its attention. Many HRA workers were so poorly supervised that they did not understand the nature of the warnings they did receive. Information on computers indicating that many families shared the same apartment prompted no action. HRA also neglected to use the Department of Health's database of birth certificates to vet applicants.

While not criminally liable, those responsible for such lackadaisical administration must be considered key participants in this series of frauds.<sup>29</sup>

New York City's HRA interacts with approximately 3 million individuals (out of New York City's population of 8.2 million).<sup>30</sup> The deleterious effects caused by HRA's poor data stewardship practices can only be dwarfed exponentially by analogous data stewardship deficiencies on the part of the IRS, an agency which interacts with almost every business and household in America. The IRS itself must be considered a key participant in the identity thefts it has allowed to be perpetuated upon the public by, inter alia, its failure to correctly match and verify the SSNs of the purported dependents claimed by identity thieves.

The "mousehole" must be plugged by improving the IRS's data stewardship procedures and processes. The IRS's unvigilant practices in failing to verify the SSNs and other personal

---

<sup>27</sup> See, e.g. United States Attorney's Office, Southern District of Florida, Press Release, Last Three of Twelve Defendants Sentenced in Massive Bank Fraud and Identity Theft Ring (30 September 2011), available on the Internet at <<http://www.justice.gov/usao/fls/PressReleases/110930-04.html>>.

<sup>28</sup> Posted on the internet at <<http://www.fgs.org/rpac/wp-content/uploads/2012/04/senfincomm-taxfraud-20120320-corrected2.pdf>>, also available at 2012 TNT 56-30.

<sup>29</sup> United States v. Concepcion, 795 F. Supp. 1262, 1270 (E.D.N.Y. 1992).

<sup>30</sup> See N.Y.C. Human Resources Administration / Dept. of Social Services, *About HRA/DSS*, available on the Internet at <[http://www.nyc.gov/html/hra/html/about/about\\_hra\\_dss.shtml](http://www.nyc.gov/html/hra/html/about/about_hra_dss.shtml)>.

data need to be targeted; deep-freezing the DMF will not stop identity theft tax fraud practices such as those recounted by the witnesses at the various Hearings.

Of particular concern is IRS Deputy Commissioner Miller's testimony at this instant Hearing, wherein he states that the IRS is:

[L]everaging mechanisms to stop the growing trend of fraudulent tax returns being filed under deceased taxpayers' identities. First, we have coded accounts of decedent taxpayers whose SSNs were previously misused by identity thieves to prevent future abuse. Second, we are identifying returns of recently deceased taxpayers to determine if it is the taxpayer's final return, and then marking accounts of deceased taxpayers who have no future filing requirement. Of this season's filings, 91,000 returns have been stopped for this review. Third, we are working with the Social Security Administration in order to more timely utilize the information SSA makes available to us. And we are working with SSA on a potential legislative change to the practice of routine release of the Death Master File.<sup>31</sup>

Conspicuous by its absence is any reference to flagging the SSNs of deceased *dependents of taxpayers*.<sup>32</sup> Flagging the SSNs of *taxpayers* without also flagging the SSNs of decedents who might be the taxpayers' spouses or dependents would certainly not have prevented identity theft fraud such as that described by Mr. Agin at the 2 February 2012 Hearing<sup>33</sup> and by Mr. McClung at the 25 May 2011 Hearing<sup>34</sup> (and also referenced by Ms. Olson at this instant Hearing,<sup>35</sup> and indeed, by Chairman Johnson in his Opening Remarks to this Hearing<sup>36</sup>). Surely the IRS has been aware of the practice since at least 2004!<sup>37</sup>

---

<sup>31</sup> Testimony of Steven T. Miller, instant Hearing, p. 4 (8 May 2012), *available at* 2012 TNT 90-57.

<sup>32</sup> This includes deceased children under the age of one year who would not have been claimed as dependents on their parents' prior tax returns.

<sup>33</sup> Statement of Jonathan Eric Agin, Esq., Hearing on the Accuracy and Uses of the Social Security Administration's Death Master File, House Committee on Ways and Means Subcommittee on Social Security (2 February 2012), [http://waysandmeans.house.gov/UploadedFiles/Agin\\_Testimony202ss.pdf](http://waysandmeans.house.gov/UploadedFiles/Agin_Testimony202ss.pdf).

<sup>34</sup> Statement of Terry D. McClung, Jr., Hearing on the Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, A Drain on the Public Treasury, United States Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth (25 May 2011), <http://finance.senate.gov/imo/media/doc/Testimony%20of%20Terry%20McClung.pdf>.

<sup>35</sup> Testimony of Nina E. Olson, instant Hearing, p. 7 (8 May 2012), *available at* 2012 TNT 90-58.

<sup>36</sup> Chairman Sam Johnson, Opening Remarks, instant Hearing (8 May 2012).

<sup>37</sup> *See, e.g.* United States Attorney's Office, Press Release, 31 March 2004, *available on the Internet at* <http://www.justice.gov/tax/usaopress/2004/txdv04PSedore.html>.

In light of the IRS's prior known dysfunctions in tracking and processing the SSNs of individuals associated with taxpayers (as distinct from the taxpayer herself/himself),<sup>38</sup> Mr. Miller's statements can provide but sparse comfort to Messrs. McClung and Agin and their families, and to those apparently numerous families similarly situated. The IRS needs to establish the connection between the deceased dependent individual and the taxpayer who can rightfully claim the deceased individual as a dependent. And if indeed the IRS is in fact pursuing such measures but Mr. Miller's testimony did not clearly convey that fact, then Mr. Miller needs to clarify this to the Subcommittees and to the American public.

"Credible studies indicate that dates of birth are not the *sin qua non* of identity theft. The most common form of identity theft arises from credit card theft or check fraud, and ***the least common form arises from stolen social security numbers or other personal information.***" [emphasis supplied].<sup>39</sup> If misappropriated SSNs are the *least* common form of identity theft, then why is it that such identity thefts are so disproportionately common in connection with tax fraud upon the IRS?

Do not blame the DMF, but look to the IRS's deficient data stewardship practices. Do not blame the mouse, but blame the hole!

### C. The Supply and Demand of SSNs for Tax Fraud Purposes:

The proposals to block public access to the DMF are not at all encouraging when viewed through the prism of the economic supply and demand principles. SSNs are valuable commodities for which there is a demand.<sup>40</sup> Prison inmates have sold their own SSNs,<sup>41</sup> and indeed, deceased infants' parents have been known to sell their own departed children's SSNs for

---

<sup>38</sup> See, e.g. *United States v. Nielsen*, 1 F.3d 855, 857 (9th Cir. 1993), *cert. denied*, 525 U.S. 827 (1998); *Wallin v. Commissioner*, 744 F.2d 674, 677 (9th Cir. 1984); *United States v. Shafer*, 1996 U.S. Dist. LEXIS 56165 (E.D. Pa. 1996); *Grimland v. Commissioner*, T.C. Memo 1993-367; *In re Washington*, 172 B.R. 415, 418 - 419 (Bankr. S.D. Ga. 1994).

<sup>39</sup> *Texas Comptroller of Public Accounts v. Attorney General*, 354 S.W.3d 336, 355 - 356 (Tex. 2010) (citing Herb Weisbaum, *Identity Theft Problem: The Facts Behind the Fear*, MSNBC (Oct. 21, 2010, 7:42 AM) <[http://www.msnbc.msn.com/id/39763386/ns/business-consumer\\_news/](http://www.msnbc.msn.com/id/39763386/ns/business-consumer_news/)>).

<sup>40</sup> In addition to commanding a monetary price, SSNs can be stolen and/or bartered. See, e.g. *Fayton v. Goord*, 17 A.D.3d 753, 792 N.Y.S.2d 259 (N.Y. App.Div., 3d Dep't 2005).

<sup>41</sup> See, e.g. N.Y. State Dept. of Taxation & Finance, News Release, *Seven Charged For Preparing False Tax Returns* (22 March 2011), available on the Internet at <<http://www.tax.ny.gov/press/rel/2011/sweeppreparers032211.htm>>.

cash<sup>42</sup> (though, given the dependency exemption to the personal Income Tax,<sup>43</sup> parents most likely to consummate such a sale have a significant likelihood of being illegal aliens or other nonparticipants in the voluntary compliance with the income tax laws).

If the DMF were no longer accessible, the many of the fraudsters who depend upon it as a supply source for SSNs would look to other sources, including those previously mentioned in this Commentary, and would be quite willing to pay a higher price for them as a component of the cost of doing business. This would mean, for example, that the errant employees who misappropriate their employers' databases would be operating in a market in which their nefarious services might command a higher price than in an environment such as the one which recently prevailed, where the DMF is freely accessible.

While some embargoes and restrictions on the DMF may well be appropriate, the potentially corruptive effects of the resulting supply and demand curves upon the business and commercial environment ought not be ignored. One must also take into account recent healthcare legislation which serves to increase the demand for healthcare, add additional bureaucracy to facilitate healthcare and its financing, and thereby create more data and databases which would be subject to expropriation by unscrupulous employees.

#### D. Moving towards Solutions:

America has gotten itself into a situation in which an individual's SSN is so key to his or her daily activities and existence in society that the misuse of a SSN wreaks havoc in a broad spectrum of life. That the data security standards legislated for health care information<sup>44</sup> were never applied to many if not most realms outside the healthcare field only complicates the situation. Therefore, protections and safeguards need to be in place in order to prevent identity theft, and to limit the damages caused when identity theft does occur. The IRS must do its part in its own house in such regard, and, as reflected in Ranking Member Lewis's remarks,<sup>45</sup> will need the cooperation and assistance of other branches and departments of the government in order to do so.

---

<sup>42</sup> See, e.g. FBI, Jacksonville Division, Press Release, "Duval County Man Pleads Guilty to Federal Charges of Aggravated Identity Theft and False Representation of a Social Security Number" (22 February 2011), available on the Internet at <<http://www.fbi.gov/jacksonville/press-releases/2011/ja022211.htm>>.

<sup>43</sup> I.R.C. §§ 151 - 153.

<sup>44</sup> Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, Title II.

<sup>45</sup> Ranking Member John Lewis, Opening Statement, instant Hearing (8 May 2012), available at 2012 TNT 90-40.

Notwithstanding the differing (and often diametrically opposite) viewpoints of various constituencies, two matters are now indisputable:

- (1) There are no simple or ideal solutions; and
- (2) Doing nothing is not an option for the Congress.

There is no perfect solution, and any solutions concocted will inevitably displease one or more constituencies and cause complications in other areas.

The Commentator has no reason to question the integrity or goodwill of any of the witnesses at the instant Hearing or at any of the abovementioned related previous hearings; if anything, such attributes have been well proven and established. Nor does the Commentator have any quarrel with the qualifications or propriety of the line-up of witnesses; the constricting limitations inherent in the scope and diversity of the invited witness line-ups are easily remedied by the Subcommittees and their staffs inviting public submission of comments and according such comments serious regard.

Nevertheless, there is reason to fear that the Hearings might collectively function as a lynch mob against the public's (including the genealogical community's) interest in accessing the data in the DMF. There is concern that the targeting of the DMF is, perhaps, a convenient exercise in blame assignment so as to avoid the vexing issues inherent in crafting real solutions. As detailed above, the IRS's lax data stewardship practices facilitate the use of the information in the DMF to defraud the public fisc, and closing down the DMF to the public will not stop such depredations.

Ranking Member Becerra's Opening Statement states that "the question of the Death Master File -- the DMF -- also requires striking the right balance."<sup>46</sup> Mr. Black's testimony similarly speaks of "striking a balance between transparency that helps prevent fraud and protecting individuals from identity theft."<sup>47</sup> Striking a fair and appropriate balance needs to be the guiding principle in addressing the systemic problem.

Ms. Olson's dual-sided approach in (1) embargoing the release of info in the DMF for a period; and (2) delaying the sending of refund checks to taxpayers has much merit. Though, as acknowledged by Ms. Olson, her approach is not without downside, it can significantly stanch the raid on the public treasury, increase the likelihood of detection and prosecution, reduce the instances of legal and emotional distress inflicted upon the families of deceased identity theft victims, and boost the public confidence so critical to America's system of voluntary tax compliance.

---

<sup>46</sup> Ranking Member Xavier Becerra, Opening Statement, instant Hearing (8 May 2012), *available at* 2012 TNT 90-37.

<sup>47</sup> Testimony of David F. Black, instant Hearing, p. 4 (8 May 2012), *available at* 2012 TNT 90-59.

That the IRS has not done enough to help identity theft victims is well recognized and beyond cavil; indeed, the week prior to the instant Hearing saw the release of a report by Mr. George's own agency detailing the failings of the IRS in that regard.<sup>48</sup> The rights of identity theft victims must be recognized. This includes the right to know the identity of the identity thief, and the right of civil redress against him or her.

Included in the balance that must be struck is the right of the public to know some if not all of the information in the DMF. Genealogical research is one of many such legitimate uses of such information, of which other representatives of the genealogical community will no doubt provide further details to the Subcommittees in the commentaries they surely will submit.<sup>49</sup>

This Commentary concededly contains some assertions and predictions which may be viewed by some as harsh, extreme, or even cynical. If this Commentary is published as part of the record and made readily transparent and accessible to the public without restriction, then, in future years, public officials and private individuals alike will be able to seek out the Commentator and tell him how erroneous -- or how correct -- subsequent events will have proven those assertions and predictions to be.

10 May 2012

Respectfully submitted,



Kenneth H. Ryesky, Esq.

---

<sup>48</sup> Treasury Inspector General for Tax Administration, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service*, Report No. 2012-40-050 (3 May 2012), available on the Internet at <http://www.treasury.gov/tigta/auditreports/2012reports/201240050fr.pdf>.

<sup>49</sup> The Commentator, while certainly in favor of transparency of the DMF, shall defer to those other commentators from the genealogy community and shall not now take up the cudgels for the genealogists' perspectives, other than to remind the Subcommittees that the perceived want of transparency in certain genealogical records has led to a highly visible political distraction in the news media in connection with the President of the United States and doubts, in the minds of some, of his Constitutional eligibility to serve as such.