2-28-2012

# Refund Fraud? Real-Time Solution!

Richard Thompson Ainsworth
*Boston University School of Law*

## Recommended Citation

Richard T. Ainsworth, *Refund Fraud? Real-Time Solution!*, 134 Tax Notes 1165 (2012).
Available at: https://scholarship.law.bu.edu/faculty_scholarship/1458

BU School of Law

# REFUND FRAUD?
# REAL-TIME SOLUTION!

Boston University School of Law Working Paper No. 12-01
(January 3, 2012)

Revised March 19, 2012

Richard T. Ainsworth

Electronic copy available at: https://ssrn.com/abstract=1978898

# REFUND FRAUD?
# REAL-TIME SOLUTION!

Richard T. Ainsworth

When seven million dependents vanished from the tax rolls in 1986 the IRS recovered three billion dollars in revenue.[1] A simple enforcement measure was applied. Taxpayers were required to list the social security number (SSN) for any dependent they claimed on their tax return. As the authors of *Freakonomics* explain, this measure worked because taxpayers who had found it easy to cheat previously now feared that they could be caught in real-time.[2] Costing next to nothing to implement, the benefits of this enforcement action continue to this day.

A similar enforcement measure could be employed against refund fraud. Even though the solution is not *as simple as* that adopted in 1986, it is similar. The effort is worth making. The revenue loss is much larger.[3] As before, the key to the enforcement effort is to convince the fraudsters that they can be caught[4] in real-time.[5]

[1] Margaret Milner, Commissioner of Internal Revenue, *Remarks at the Direct Selling Association Tax Seminar*, (July 19, 1990) 95 TAX NOTES TODAY 141-60; Doc 95-7092 (discussing the Tax Compliance Measurement Program and how these audits help the IRS determine areas where significant compliance improvements can be made).

[2] Steven D. Levitt & Stephen J. Dubner, *Freakonomics – a rogue economist explores the hidden side of everything*, 2006 (revised and expanded edition) at 238.

> So why do people really pay their taxes: because it is the right thing to do, or because they fear getting caught if they don't? It sure seems to be the latter. A combination of good technology (employer reporting and withholding) and poor logic (most people who don't cheat radically overestimate their chances of being audited) makes the system work.

[3] Estimating revenue yields from fraud prevention is difficult. Figures are more reliable in hindsight. This was the case with the 1986 enforcement effort. For example, consider the tax refund fraud in just the prison population. Prisoners accounted for 0.43% [455,097/106,420,200 = 0.43%] of all refund returns filed in 2005. IRS Criminal Investigation estimated that these returns accounted for 15.47% [$68,179,070/$440,773,403 = 15.47%] of all fraudulent refunds. For 2009 the IRS estimated that 44,944 false returns were filed by prisoners representing $295.1 million in false refund claims. Of these refunds the IRS prevented $256 million. Thus, $39.1 million in fraudulent refunds were issued to this group.

TIGTA believes these numbers are unreliable. "While the IRS can report on the number of false/fraudulent tax returns it identifies, it cannot measure the extent of prisoner tax fraud." Treasury Inspector General for tax Administration, *Significant Problems Still Exist With Internal Revenue Service Efforts to Identify Prisoner Tax Refund Fraud* 1 & 8 (Ref. No. 2011-40-009, December 29, 2010).

TIGTA places stolen/fraudulent SSNs at the heart of prisoner refund fraud. Looking at unaudited prisoner returns in 2005 TIGTA found 118,000 with duplicate and 298,000 with invalid SSNs. Treasury Inspector General for tax Administration, *The Internal Revenue Service Needs to Do More to Stop the Millions of Dollars in Fraudulent Refunds Paid to* Prisoners 2 & 3 (Ref. No. 2005-10-164, September 2005). Coming at this problem from another direction, TIGTA used a prisoner's true SSN to find many more suspect returns – instances where refunds were requested, but there was no valid W-2 for that individual (in other words, the W-2s with the returns were fraudulent).

> Our review identified that 253,929 (88%) of the 287,918 tax returns filed by a prisoner as of March 24, 2010, were not selected for screening [by the IRS]. Of those returns not screened, 48,889 individuals had no wage information reported to the IRS by employers. These 48,887 prisoners claimed refunds totaling more that $130 million including Earned Income Tax Credit (EITC) claims of $78.5 million.

Electronic copy available at: http://ssrn.com/abstract=1978898

This paper proposes a technology-based solution to refund fraud – W-2s (as well as 1099s)[6] should be "digitally signed." This solution is narrowly focused on *tax compliance*, and does not pursue broader concerns with identity theft that underpins some of the more serious instances of this fraud.[7] This solution is not "paper based." The digital signature is *both* an alpha-numeric string and a 2-D bar code and can be transmitted in an e-file as well as a paper document.

This proposal also recommends that W-4s and W-9s be "digitally signed" with a similar cryptographic hash function. A procedural change will require that digitally signed W-4s and W-9s be remitted to the IRS whenever an employee declares or adjusts withholdings, or whenever a 1099 recipient is presented with a request for tax identification data.

Employees will have the ability to independently check the accuracy of any digital signature associated with their employment by accessing an IRS web site that will

Treasury Inspector General for tax Administration, *Expanded Access to Wage and Withholding Information Can Improve Identification of Fraudulent Tax Returns*, Highlights (Ref. No. 2010-40-129, September 30, 2010).

[4] Representative Richard Nugent recently explained how brazenly refund frauds are undertaken in Tampa, Florida. The Tampa Police indicate to him that the criminals are convinced that the IRS will do nothing. They use names of deceased people to file false returns. One person filed over 1,000 returns and collected $2.4 million in refunds. SSNs are found on websites like ancestory.com. "Make It Rain [return filing] Parties" are held in hotel rooms with Internet access. The Tampa Police even know how the money is laundered.

> How does Tampa PD know all of this? The criminals are telling them.
>
> Even after they've been read their Miranda Rights, the crooks are laying out their entire process to the cops. They're freely admitting their crimes, because they don't think federal officials will do anything about it. Unfortunately, it seems the criminals are right.

*Testimony of Rep. Richard Nugent Before the Committee on Oversight and Government Reform Subcommittee on Government Organizations, Efficiency, and Financial Management*, at 1-3 (November 4, 2011).

[5] IRS, New Release, *IRS to Host Public Meeting December 8 on Real-Time Tax System*, IR-2-11-114, Nov. 30, 2011. Announcing the "kick off" of a series of public meetings where the IRS will solicit comments on changing the traditional "look-back" model of tax compliance with a "real-time" model. The proposal in this paper supports this effort and would allow real-time verification of W-2s and 1099s.

> Under the vision of a real time tax system, the IRS could match information submitted on a tax return with third-party information right up front during processing … today the IRS conducts a significant number of compliance activities months after the tax return has been filed and processed. … This after-the-fact compliance approach can create problems and frustrations for both taxpayers and the IRS.

[6] To keep the argument relatively simple, the application of this proposal to the various Form 1099s will not be developed in great detail in this paper. In addition, the use of Form 4852 (Substitute for Form W-2, Wage and Tax Statement), which was used extensively by prisoners in Florida to secure fraudulent refunds, will not be discussed. Sally Kestin, *Florida Inmates are No. 1 in Filing Fraudulent Tax Returns from Prison*, SUN SENTINEL (March 19, 2011) *available at*: http://articles.sun-sentinel.com/2011-03-19/news/fl-prison-tax-fraud-20110319_1_tax-refunds-jonathan-ellsworth-bogus-returns.

[7] Even though a major identity theft incentive (fraudulent tax refunds) is eliminated by this solution, this paper does not focus on identity theft *per se*. There is a mix of inter-agency policy questions around identity theft that this paper leaves undisturbed. Notable for their absence is any discussion of identity theft and Social Security fraud, or identity theft and the Department of Homeland Security's immigration policy.

identify mis-matches (if any). Employees will be able to demand that their employer correct any signatures found to be in error.

### *Refund Fraud & Identity Theft*

According to the IRS, taxpayers submit false income documentation (W-2's and 1099's) under their own SSNs almost as often as identity thieves submit false returns with stolen identities. Each of these types of fraudsters have the same goal – to get the IRS to issue a false refund.

> For Processing Year 2011 (through September 10, 2011), the IRS reported that it had identified over 1.6 million tax returns with more than $12 million claimed in fraudulent tax refunds … [and] of the 1.6 million tax returns identified as fraudulent for Processing Year 2011, a total of 851,602 of these tax returns, with $5.8 billion in associated fraudulent refunds, involved identity theft. … [But,] overall, the IRS does not know how many identity thieves are filing fraudulent returns and how much revenue is being lost.[8]

Clearly, a *tax solution* must reach two groups – legitimate taxpayers and outright thieves. A *tax solution* will not prevent identity theft, nor will it solve SSN theft. It does not need to do so to be successful. This is not to say that preventing refund fraud may go a long way to reducing these thefts. However, identity and SSN theft occur for many more reasons than simply to secure false refunds from the tax system.

Identity theft is the fastest growing fraud in the US. According to the Federal Trade Commission, in 2009 about 9.9 million Americans were victims of identity theft, an increase of 22% from the number of cases in 2007.[9] SSNs, along with name and date

[8] J. Russell George, *Identity Theft and Tax Fraud,* testimony at 7-8, Hearing Before the Committee on Oversight and Government Reform, Subcommittee on Government Organization, Efficiency and Financial Management, US House of Representatives (November 4, 2011). (The testimony also indicates (at 7) that the IRS claims to have prevented 94% of these refunds or $11.5 billion, leaving $500 million unaccounted for.)

[9] Kristin M. Finklea, *Identity Theft: Trends and* Issues, CONGRESSIONAL RESEARCH SERVICE (January 5, 2010) 7-5700 (R40599) at 1 (further indicating that the FTC estimates US consumers suffer losses of $50 billion to this fraud). Federal Trade Commission, *Consumer Sentinel Network Data Book for January – December, 2008 through February, 2009* (indicating that identity fraud has been the most common complaint for the past eleven years) *available at*: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf

of birth, are the three most critical elements of a person's identity.[10] Theft of just a SSN can have a wide-ranging impact.[11]

### *Proposal*
### *Self-certified Tax Documents*

W-2's should be secure, self-certifying documents. The IRS needs to be able to confirm in real-time that the W-2 attached to a return has been:

(a) issued by the stated employer (name & address);
(b) under the stated employer's identification number (EIN);
(c) to the named employee (name & address);
(d) under the employee's specified social security number;
(e) for the stated amount of wages, tips or other compensation; and
(f) with the specified federal income tax withheld.

If the IRS can immediately confirm the validity of the W-2s submitted with returns, then refund fraud will be substantially eliminated. A fraudster who knows that the IRS will quickly identify that the fabricated W-2 he intends to submit is a forgery then he will not go forward with the fraud. In fact, with a little bit of advertising, the IRS should be able to make sure most potential fraudsters are discouraged before they start.

Making W-2s into secure, self-certifying documents is not difficult. There are two models for doing this in a tax context: (a) the Brazilian model of self certified invoices and transportation documents used to monitor VAT compliance in cross-border business-to-business transactions;[12] and (b) the Belgian/Quebec model of self-certified cash register receipts used to monitor retail consumption taxes.[13]

In these jurisdictions technology encrypts and preserves the basic elements of each cross-border transaction (Brazil), or retail sale (Belgium/Quebec). It converts this data into a unique alpha-numeric string of characters, and reproduces the result as a bar code on the relevant tax document (receipt or invoice).[14] Tax auditors immediately confirm the validity of the documents with hand held scanners.

[10] Daniel Bertoni, *Social Security Numbers: Use is Widespread and Protection Could Be Improved*, USGAO Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives (June 21, 2007) at 1:

> Since its creation the SSN has evolved beyond its intended purpose to become the identifier of choice for public and private sector entities and is now used for myriad non-Social Security purposes. This is significant because a person's SSN, along with name and date of birth, are the key pieces of personal information used to perpetuate identity theft.

[11] SSNs are critical to the functioning of three major agencies – the Social Security Administration (SSA), the Department of Homeland Security (DHS), and the IRS. In addition, a large number of state and federal agencies collect SSNs and become the targets for SSN theft.

[12] Other countries do the same. Chile, Ecuador, Colombia and Mexico have similar systems in place.

[13] Other countries do the same. Sweden, Italy, Argentina, Poland, Mexico, Venezuela, Greece, Russia, Ethiopia, and Slovakia have similar systems in place.

[14] The basic elements of a sales transaction include (a) the name of each item purchased [or associated PLU code], (b) the price per item, (c) the taxability of each item [differences in rates are also recorded], (d) the totals [tax and gross], (e) the name of the business making the sale, (f) the businesses tax identification

To solve refund fraud in the US 1099s also need to be secure, self-certifying tax documents. The IRS should be able to confirm in real-time that valid 1099s support income, deduction or withholdings on related tax returns. Certifying 1099s is as important for limiting refund fraud as is the certification of W-2s. The data that needs to be secured on a 1099-MISC (for example) falls into the same six basic categories:

(a) the name and address of the payer;
(b) the issuer's tax identification number (EIN);
(c) the name and address of the recipient;
(d) the recipient's tax identification number (TIN);
(e) up to eighteen numerical values including the stated amount of:
- rents,
- royalties,
- other income,
- fishing boat proceeds,
- nonemployee compensation, excess golden parachute payments -
- any other income amounts; and

(f) the specified amount of:
- federal income tax withheld; and
- state tax withheld; or
- other amounts.

### *Mechanism*

Under this proposal each employer/payer issuing a W-2 or 1099 will be required to have these documents digitally signed. The signature will be reproduced on the W-2 or 1099 in two forms: (1) a fixed-size alpha-numeric bit string, and (2) a 2-D bar code. Making the digital signature physically obvious to any observer of the paper forms is key to the self-enforcing nature of this proposal.

Taxpayers, who are accustomed to scanning everything from groceries to airline tickets, will know intuitively that these new W-2s and 1099s are secure and fraud resistant. With a small amount of advertising the IRS should be able to explain widely that the digital signature means not only (a) that the IRS has already received the data from the employer/payer, but also (b) that common scanning technology will allow an immediate check of return information with the Service's data-base.

Along with the critical data elements of each tax document the employer/payer will be required to enter into the hash function certain identifying data: (a) a code identifying the individual who performed the encryption, (2) the date and time that the encryption was performed, and (3) the place within the numeric sequence of encrypted documents where a specific cryptographic procedure was carried out. The encrypting algorithm will be determined by the IRS and provided to the employer/payer.

number, (g) the date and time of the transaction, and (h) the sales agent involved. In jurisdictions where this kind of technology is used on invoices issued between businesses the encryption would additionally cover (i) the name of the purchasing business, (j) the address of the buyer, (k) the tax identification number of the buyer, and (l) the name of the agent involved in the transaction.

There are several ways to carry out this digital signing. Following the Brazilian (inter-state business-to-business) model each employer/payer would be required to transmit to a secure IRS web site all required data in an XML file. The IRS will take this data and produce the required a digital signatures, and return to the employer/payer a printable W-2/1099 filled out and digitally signed in accordance with the taxpayers input.

For a detailed discussion of the Brazilian model, please see Appendix A.

A second way to carry out this encryption process is to follow the Belgian/Quebec (secure cash register) model. Under this model the IRS would provide the employer/payer with an encryption module (activated by insertion of an IRS issued smart card) that will connect a business computer with the W-2/1099 form printer (or e-file program). The record of all W-2/1099 encryption operations will be transmitted remotely to the IRS daily or on demand. A record of all encryption transactions will also be preserved within the internal memory of the device for five to ten years.

For a detailed discussion of the Quebec/Belgian model, please see Appendix B.

Importantly, none of this is new. These solutions have been tried, proven to be effective, and widely adopted albeit in a VAT, not income tax context, but they work. They work because they use real-time data collection and real-time data-security to identify and prevent tax fraud. These technological responses are directly applicable to refund fraud.

### *Application of the Brazilian Model to US Refund Fraud*

The U.S. could imitate Brazil to get real-time control over the accuracy of W-2s and 1099s and put an end to refund fraud.

To implement a Brazilian-type solution the IRS will need a referential database of employers and employees (for W-2 compliance) and payers and recipients (for 1099 compliance). The database will associate employers/payers (by name, address and EIN) with their employees/recipients (by name, address and SSN). There are number of ways to secure this database: (1) the National Directory of New Hires (NDNH),[15] (2) the Social

[15] Sec. 453 (i) of the Social Security Act [42 U.S.C. 653]. The name, address, and SSN of all newly hired employees as well as the name, address and FEIN of the employer is in the database. [Sec. 453A(b)(1)].

The NDNH is operated by the Federal Office of Child enforcement of the Department of Health and Human Services. NDNH has three files: (1) The New Hire (W-4) file - containing information on all newly hired employees as reported by employers to each State Directory of New Hires (SDNH). Federal agencies report directly to the NDNH. (2) The Quarterly Wage (QW) File - contains quarterly wage information on individual employees from the records of State Workforce Agencies (SWA) and federal agencies. When an individual is working more than one job during the reporting period, separate QW records are established for each job. (3) The Unemployment Insurance (UI) File - The UI file contains unemployment insurance information on individuals who have received or applied for unemployment benefits, as reported by SWAs. The states only submit claimant information that is already contained in the records of the state agency administering the UI program. Under current law the Secretary of the Treasury has limited access to the NDNH database. Sec. 453(i)(3) allows access for three purposes: (1)

Security Administration (SSA),[16] and/or (3) the IRS could construct its own list based on previously filed information returns. Because both the NDNH[17] and the SSA database have accuracy problems,[18] an internal IRS procedure using W-4s and W-9s is recommended (although it could be cross matched with the NDNH and SSA databases).

STEP 1: Submission to the IRS of the essential personal identifiers from all: W-4s (Employee Withholding Allowance Certificate)[19] and W-9s (Request for Taxpayer Identification Number and Certification). Currently W-4s and W-9s are retained in the files of the employer or payer and not submitted to the IRS.

- Employers are currently required to solicit from their employees a signed W-4 (or substitute) at the commencement of employment, and employees are required to comply with this request.[20] Penalties apply.[21]

administering section 32 [EITC]; (2) administering section 3507 [advance payment of EITC]; (3) “verifying a claim with respect to employment *in a tax return*.” (emphasis added) The major drawback to the NDNH is that it omits independent contractors. It is focused on “new hires” and the UI file is potentially the largest.

The NDNH is a classic source of data for the IRS to verify suspected false W-2s. A fraudulent W-2 (using a valid name and SSN but issued on a new employer’s account) would on its face appear to the IRS that a taxpayer has a “new job.” If the name and SSN match, but a different employer appears on the W-2 then the NDNH should contain this name. If it does not, then the IRS might suspect fraud (although there could be simply a data error in the NDNH).

[16] The SSA issues SSN to all US citizens and most non-citizens who are lawfully admitted to the US and who have permission to work. Lawfully admitted non-citizens may also qualify for an SSN for on-work purposes when a federal, state or local law requires an SSN to be obtained in order to receive a particular welfare benefit or service.

[17] 88% and 96% of the SSN/name combinations submitted to the NDNH by states and federal agencies respectively can be verified. Unverified combinations are not added to the NDNH database. The accuracy of the QW reports are estimated to be 93% and 98% from state and federal agencies respectively. US Department of Health and Human Services, Administration for Children and Families, *Accuracy of Data Maintained by the National Directory of New Hires and the Effectiveness of Security Procedures* (Report to the House of Representatives Committee on Ways and Means and the Senate Committee on Finance (July 31, 2001) *available at*: http://www.acf.hhs.gov/programs/cse/pubs/2002/reports/ndnh_data_accuracy.html#

[18] The SSA estimates that the records of 3.6 million citizens and lawful immigrants are in error. Statement of Testimony of Tyler Moran, *Hearing on the Social Security Administration’s Role in Verifying Employment Eligibility*, before the Subcommittee on Social Security of the House Committee on Ways and Means, at 7, n. 41, citing from Transcript from Hearing on Employment Eligibility Verification Systems (Subcommittee on Social Security, Committee on Ways and Means, US House of Representatives, June 7, 2007).

[19] This requirement would revert to and extend earlier IRS policy to submit some (but not all) W-4s. On its web site under *Withholding Compliance Questions & Answers* the IRS indicates:

> **Q1: In the past, as an employer, I was required to submit all Forms W-4 that claimed complete exemption from withholding (when $200 or more in weekly wages were regularly expected) or claimed more than 10 allowances. What Forms W-4 do I now have to submit to the IRS?** A1: Employers are no longer required to routinely submit Forms W-4 to the IRS. However, in certain circumstances, the IRS may direct you to submit copies of Forms W-4 for certain employees in order to ensure that the employees have adequate withholding. You are now required to submit the Forms W-4 to IRS only if directed to do so in a written notice or pursuant to specified criteria set forth in future published guidance.

*Available at*: http://www.irs.gov/individuals/article/0,,id=139412,00.html

[20] IRC §3402(f)(2)(A)

[21] IRC §6721

- Payers are currently required to solicit a signed W-9 (or substitute) from independent contractors.[22] Penalties apply.[23]
- Employers and payers are entitled to rely upon W-4s and W-9s under current law without submitting them to the IRS for verification.[24] This will change.
- Employers and payers will be required to send the essential identifiers of a W-4 (name, address and SSN) or W-9 (name, address and SSN/EIN) to the IRS in an XML file.

STEP 2: Matching, digital signatures and taxpayer notification.

- *Matching.*[25] The IRS will match the employee's/recipient's data (name, address, SSN) as well as the employer's/payer's (name, address, SSN/EIN) data with
  - IRS files,
  - SSA files, and (if deemed appropriate)
  - NDNH database.
- *Digital signature*. If all data matches, the IRS will create a digital signature of this data (alpha-numeric hash function and 2-D bar code) and provide a downloadable W-4 or W-9 containing the alpha-numeric hash function and 2-D bar code (an e-file could be substituted). The *taxpayer* will be notified of the match, and be provided with a copy of the encrypted results of the matching. Employers/payers should retain W-4s and W-9s with the hash and bar codes. Having the taxpayer's report in paper (with the alpha-numeric hash function and 2-D bar code visible) will be an aid to deterrence.
- *Un-matched data*. If the data provided does not match, the IRS will notify the employer/payer and the *taxpayer*, and indicate a web site where the taxpayer can:
  - Confirm the mis-match
  - Indentify the specific mis-matched element
  - Take actions to correct errors in the IRS, SSA, or NDNH databases, and
  - Download from the website a corrected W-4 or W-9 with the appropriate alpha-numeric hash function and 2-D bar code.

STEP 3: Taxpayers who have *un-matched data* (who cannot produce a W-4 or W-9 with an appropriate alpha-numeric hash function and 2-D bar code) will be informed of *tax consequences* and encouraged to access the IRS, SSA or NDNH systems to make corrections.[26] The more significant *tax consequences*[27] are:

[22] IRC §31.3406(h)-3(a)

[23] IRC §§ 6721 & 6722

[24] IRC §§ 301.6724-1(d) & §31.3406(h)-3(c) (employers and payers acting in a responsible manner can avoid penalties associated with using wrong SSNs or names on W-2s or 1099s if they rely on taxpayer representations made on W-4s and W-9s, and if they have no reason to believe there are errors).

[25] Both the IRS and the SSA currently operate on-line matching programs. See: IRS, *On-line Taxpayer Identification (TIN) Matching Program*, Publication 2108A (July 2011) (discussing the Taxpayer Identification Matching Program which available only for payers – not recipients – and functions for Form 1099, not W-2s); GAO, *Social Security Numbers – Coordinated Approach to SSN Data Could Help Reduce Unauthorized Work* GAO-06-458T (February 16, 2006) (indicating that the SSA runs an Employee Verification Service [EVS] and a web-based SSN Verification Service [SSNVS] which can be used by employers to verify the names and addresses employees free of charge).

[26] Very often the errors will be nothing more that data entry or life changes.

- *W-2 Employees*.
    - Without verification of name, address and SSN, requests for withholding allowances will not be approved by the IRS (a lock-in letter will issue to the employer after a specified period of time);[28]
    - If corrections are not made, and if the employer uses the same *un-matched data* on the employee's W-2 the employee's return (and any related refund) will be processed more slowly by the IRS.
- *1099 Recipients*.
    - Without verification of name, address and SSN, the recipient will be subject to back-up withholding at 28%;[29]
    - If the payer uses the same *un-matched data* on the recipient's 1099 then claims for credits based on earned income [including EITC, CTC and ACTC] will not honored, because it is not clear if the income was actually earned by the person claiming the credit.

STEP 4: A similar matching, digital signature and notification process will be repeated when W-2s and 1099s are issued. W-2s and 1099s with digital signatures can be immediately verified and matched to the returns they accompany.[30]

- *Employers* will enter completed W-2s into an IRS web site.
    - The web site will push the data through a hash function,
    - The encrypted name, address and SSN on the W-2 will be matched with the encryption on the previously submitted W-4,
    - A "digital signature" (alpha-numeric string and 2-D bar code) based on the W-2 data will be produced, and then
    - Placed on a downloadable W-2.
- *Payers* will enter completed 1099s into an IRS web site.
    - The web site will push the data through a hash function,
    - The encrypted name, address and SSN on the 1099 will be matched with the encryption on the previously submitted W-9,
    - A "digital signature" (alpha-numeric string and 2-D bar code) based on the 1099 data will be produced, and then
    - Place on a downloadable 1099.

[27] This proposal focuses on *tax consequences.* There should be no employment or immigration impact. Employers are still allowed to hire workers (or engage independent contractors) who have mis-matched essential personal identifiers. Withholdings will be higher, and tax returns will be given more scrutiny, but this is only to be expected when the IRS has not been provided with sufficiently accurate identity information.

[28] A lock-in letter directs an employer to withhold taxes for a specific employee at a specified rate (Letter 2800C). A companion letter to the taxpayer (Letter 2801C) informs the employee of the IRS action. See: Treasury Inspector General for Tax Administration, *Withholding Compliance Program Results Are Trending Favorably, but Program Enhancements Are Needed*, Ref. No. 2010-40-030 (March 23, 2010) (indicating that lock-in letters are a very effective enforcement device of the IRS's Withholding Compliance Program).

[29] IRC § 31.3406(j)-1(b).

[30] A line could be added to the 1040 series of returns asking for the alpha-numeric signature from each W-2 attached to a return. In addition,

STEP 5: Tax returns will be scanned on receipt (name, address and SSN) and compared with the "digital signature" (alpha-numeric hash function and 2-D bar code) for each W-2 and 1099 associated with the return.[31] Returns with matching codes would receive expedited processing.

STEP 6: W-2s and 1099s without digital signatures will remain valid. The representations of income earned and withholding made on them will be respected. However, returns supported by these documents will be given special scrutiny, and taxpayers filing them will know in advance that the nature of their problem involves a mis-match of basic personal identifies (name, address, SSN) with the IRS, SSA or NDNH databases.[32]

### *Application of the Quebec/Belgian Model to US Refund Fraud*

The U.S. could imitate the Quebec/Belgian ECR/POS encryption system to get real-time control over the accuracy of W-2s and 1099s and put an end to refund fraud.

To implement a Quebec/Belgian-type solution the IRS would need to mandate that employers/payers or their third-party payroll providers acquire a device like either the MEV (government issued) or SDC (privately purchased, but manufactured to government specification). The device would encrypt the basic data on W-2s, W-4, W-9s and 1099s and place an alpha-numeric hash function and 2-D bar code on each form. Forms could be checked, or cross-referenced by scanning the bar codes.

A Quebec/Belgian solution would be the least disruptive to businesses that produced a large number of W-2s, W-4s, W-9s and 1099. The MEV/SDC device would simply be connected between a designated "payroll computer" and the form printer. Encryption would be automatically performed, and the alpha-numeric string and bar code would be placed on the documents in IRS-assigned places.

This solution can be set out in STEPS as follows:

STEP 1: Employers/payers are required to remit to the IRS *tentative* W-4s (Employee Withholding Allowance Certificate) and W-9s (Request for Taxpayer Identification Number and Certification). This transmission will constitute a "request to encrypt" the name, address and SSN of the employee/recipient on the appropriate W-4 or W-9.

[31] Taxpayers would have the option of either attaching a 1099 to their return or reproducing the alpha-numeric signature on their returns. Software programs will be able to reproduce 2-D bar codes on spaces provided on returns.

[32] Updating SSA records has been a problem for both the DHS and the IRS because of SSA policy constraints. For example, SSA records may contain errors relating to the work status of an individual:

> SSA officials maintain that it is their policy to make changes to the Social Security record only if the SSN holder initiates the changes and provides evidentiary documents from DHS.

Testimony of Barbara D. Bovbjerg before the Subcommittee on Social Security and on Oversight, Committee on Ways and Means, House of Representatives, *Social Security Numbers – Coordinated Approach to SSN Data Could Help Reduce Unauthorized Work*, GAO-06-458T (February 16, 2006) at 11.

STEP 2: The IRS will use SSA and IRS databases to match the basic identity data on the W-4/W-9. The IRS will then return to the employer/payer and to the employee/recipient a match/non-match notice.[33]

- A "match" notice will authorize the production of a final W-4/W-9. The "match" notice will become part of the encryption that includes the name, address and SSN on the W-4/W-9 that will be places on the forms in an alpha-numeric string and bar code as a "digital signature."
- A "non-match" letter will contain two sets of instructions, one for the employer/payer and the other for the employee/recipient. A period of time will be granted within which errors can be identified by the employee/recipient and corrections can be made by the employer/payer:
    - The *employee/recipient* will be told the location of a web site where the individual can:
        - Confirm the mis-match
        - Indentify the specific mis-matched element
        - Take actions to correct errors in the IRS or SSA databases, or the submission made to the employer/payer, and
    - *matched data* on the employee's W-2, the employee's return will be subjected to heightened scrutiny and any related refund will most likely be delayed.
- *For 1099 recipients*.
    - Without verification of name, address and SSN, the recipient will be subject to back-up withholding at 28%;
    - If the payer uses the same *un-matched data* on the recipient's 1099, then claims for credits based on earned income [including EITC, CTC and ACTC] will not honored until it becomes clear through an audit that the income was actually earned by the person claiming the credit.

STEP 4: A similar matching, digital signing, and notification process will be repeated when W-2s and 1099s are issued.

- *Digital signature*. The digital signatures on these documents will contain both:
    - the basic personal identity data previously encrypted on the W-4s/W-9s, and also,
    - all income and withholding numbers from these documents.
- *Matching*. W-2s and 1099s with digital signatures can be immediately verified and matched both to the prior W-4s/W-9s, but also to the returns they accompany.
- *Notifications*. The IRS will notify employers/payers and employees/recipients of:
    - *Mis-matching of basic personal data*. If personal data had changed since the W-4/W-9, or W-2/1099 had issued and the tax return contained different personal data, then corrections would be required.

[33] The SSA runs a verification program (SSNVS) that responds immediately to verify 10 workers or more, and larger requests of 250 names or more can be handled in a batch file with results available the next business day. *Supra* note 31, at 4, GAO Testimony of Barbara D. Bovbjerg.

- *Numerical.* If the tax return or the W-2/1099 had amounts that were inconsistent with the cryptographic hash string or bar code, then an audit may commence.

STEP 5: Tax returns will be scanned on receipt (name, address and SSN) and compared with the "digital signature" (alpha-numeric hash function and 2-D bar code) for each W-2 and 1099 associated with the return.[34] Returns with matching codes would receive expedited processing.

STEP 6: Returns accompanied by W2s and 1099s that either have no digital signature, or mis-matched data will remain valid. The representations of income earned and withholding made on the W-2s and 1099s will be respected. However, the returns will be given special scrutiny, and taxpayers filing them will know in advance that the nature of the delay in processing is something that could have been corrected.

## CONCLUSION

This proposal targets refund fraud. The intent is not only to block the fraud but to make it exceptionally obvious to potential fraudsters that simply fabricating W-2s or 1099s or using stolen identities will not work any more.

There are five classes of filing mis-match/refund frauds that this proposal addresses. It is highly effective with the first four, and less so with the fifth. The fraud targets are:

1. Identity mis-matches (when SSA/IRS databases do not match identity-data on the forms/returns filed);
2. When legitimate W-2s or 1099s are altered by taxpayers;
3. When fraudsters steal identities and then file false returns;
4. When taxpayers collude with professional tax-preparers (2-party collusions), and
5. When businesses, professional tax-preparers and taxpayers collude (3-party collusion).

Adding encryption, putting an alpha-numeric hash function and 2-D bar code on each W-2 and 1099 (or adding the same data sets to fully digital e-form equivalents) is something that fraudsters would find exceedingly difficult to replicate. This will stop the vast bulk of this fraud. Valuable IRS resources will be freed-up for enforcement efforts elsewhere.

The overall intent of this proposal is to replicate the 1986 enforcement effort when seven million dependents vanished from the tax rolls by simply requiring that SSNs be recorded for each dependent. The present day equivalent is an alpha-numeric string and a 2-D bar code – a digital signature – that needs to be required on several basic IRS

[34] Taxpayers would have the option of either attaching a 1099 to their return or reproducing the alpha-numeric signature on their returns. Software programs will be able to reproduce 2-D bar codes on spaces provided on returns.

forms. Doing this would be to reach for the real-time enforcement that Commissioner Shulman seeks.

# APPENDIX A
# EXAMPLES FROM 2011
# THE FIVE CLASSES OF REFUND FRAUD & HOW THEY CAN BE STOPPED

Each example of refund fraud listed below is drawn from an IRS case that closed in 2011. Similar criminal litigation examples, illustrating the same kinds of refund frauds, can be found stretching back ten or more. The years change, but the types of refund frauds do not. The audit, legal, and other enforcement efforts committed to this fraud are significant. Cost estimates are not available.

(1) *Identity mis-matches (when SSA/IRS databases do not match identity-data on the forms/returns filed)*. This is a continuing problem for the SSA,[35] and the IRS (as well as the DHS). The problem is *not* that there are no mechanisms to correct mis-matches (on line systems, phone centers, letter or fax communication vehicles are all available); the problem is that the correction-systems in place are voluntary, and employer-focused. There are no incentives (on the employer side) to make them work.

Under either of the encryption-based models discussed here (the Brazilian Internet-based approach or the Quebec/Belgian MEV/SDC modules) mis-matches would be identified early, and correction would be incentivized. An individual whose basic identifiers (name, address, SSN) are not aligned with SSA or IRS databases is told very early on. Real consequences to doing nothing are spelled out – withholdings will be increased. The incentives are real, but they are not new. These incentives have been part of the IRC for years. What is new is that an automated mechanism will now make them work.

(2) *Legitimate W-2s or 1099s altered by taxpayers*. It is relatively easy for a taxpayer to alter a legitimate W-2 or 1099 (to increase stated withholdings, or increase stated income to qualify for larger refundable credits), attach the altered forms to a tax return, and receive a larger refund.

[35] The cost to correct the estimated number of mismatches in the SSA database is $60 million per year ($300 x 20 million mismatches per year).

> Returns with mismatched TINs cannot be filed electronically and must be processed through a more expensive, time-consuming, and labor-intensive process. In addition, the SSA reports that 20 million, or five to ten percent, of the Forms W-2 filed each year contain a mismatch between the name and SSN. The cost of trying to resolve each mismatch averages over $300, whereas the cost of a normal posting is less than fifty cents.

Francine J. Lipman, *The Taxation of Undocumented Immigrants: Separate, Unequal, and Without Representation* 9 HARVARD LATINO L. REV. 1, 24 (2006) citing Paula N. Singer & Linda Dodd-Major, *Identification Numbers and U.S. Government Compliance Initiatives,* 104 TAX NOTES 1429, 1433 & 1435 (September 20, 2004).

For example, Dion Jones falsified her own W-2Gs over an eighteen-month period to secure $92,854 in fraudulent refunds.[36] This tax loss was small compared to the $839,866 that Dora Argote secured using the same simple scheme.[37]

Falsified withholdings fraud can be carried out with 1099-OIDs as well. Michael Thomas McQuillen altered 1099-OID forms on two returns to induce fraudulent refunds of $155,986.65.[38] The indictment in his case indicated that McQuillen was something of a master at this fraud. He had filed returns for four other years with fabricated 1099-OIDs and claimed fraudulent refunds for an additional $175,373.50.[39]

The real master (and promoter) of 1099-OID fraud may have been Nicole Bermudez. She was found guilty[40] of assisting forty other individuals with Original Issue Discount schemes that cost the treasury $20 million in illegal refunds.[41] Ms. Bermudez charged a fee equal to 20% of the fraudulent refund from her "clients" for assisting in the production of the 1099-OIDs.[42] She also filed the with the IRS the withholder's copy of the form.

This type of refund fraud is completely eliminated under either the Brazilian or Quebec/Belgian encryption procedures. Requiring all W-2s and 1099s to include a cryptographic hash function (an alpha-numeric string, and 2-D bar code) derived from the characteristics of the document itself is the key. A scan of the digital signature will immediately reveal if the income and withholding amounts on the forms are original.

By requiring a digital signature on the related W-4s and W-9s, and requiring them to be filed with the IRS at the commencement of the income relationship allows "digitally matching" of the encrypted signatures. This can no longer be a "one-off" fraud where false documents appear only with the returns.

A taxpayer that considered this kind of fraud would be deterred by the technology. If the fraudster had the capacity to produce some kind of alpha-numeric string, and 2-D bar code to place on the forms, it would be highly unlikely that the codes would reflect IRS encryption. A fraudster would fear being caught in real time.

[36] First Superseding Indictment (June 1, 2010) *United States of America v. Isaac Roitman Schultz & Dion Demetri Jones* (C.D. CA.) (Doc No. 6) 2:07-cr-01055-JHN.

[37] Plea Agreement for Dora Argote (July 8, 2010) *United States of America v. Dora Argote* (C.D. CA.) (Doc. No. 62) 2:09-cr-00349-AHM.

[38] Entry of Guilty Plea (March 3, 2011) *United States of America v Michael Thomas McQuillen* (D. AZ.) (Doc. No. 42) 4:10-cr-00240-CKJ-JJM.

[39] Indictment (February 3, 2010) *United States of America v Michael Thomas McQuillen*, (D. AZ.) (Doc. No. 1) 4:10-cr-00240-CKJ-JJM.

[40] United States Pretrial Memorandum (December 8, 2010) *United States of America v. Nicole Bermudez,* (N.D. CA.) (Doc. No. 57) 5:10-cr-00123-JW (finding for losses incurred in Ms Bermudez case were $5,083,609.25 with restitution ordered of $2,488,613.38).

[41] Indictment (February 24, 2010) *United States of America v. Nicole Bermudez,* (N.D. CA.) (Doc. No. 1) 5:10-cr-00123-JW.

[42] United States Pretrial Memorandum (August 9, 2010) *United States of America v. Nicole Bermudez,* (N.D. CA.) (Doc. No. 27) 5:10-cr-00123-JW, at page 3, n. 1.

(3) *Fraudsters that steal identities and then file false returns.* Stealing the basic elements of an identity, and using this identity to secure fraudulent refunds is relatively easy. A stolen name and social security number can be purchased over the Internet.[43] It can be taken from hospital-bound patients,[44] the homeless,[45] girl scouts,[46] or spirited away while clearing debris in buildings destroyed by Hurricane Katrina.[47] The dead and prison inmates are another source of valid SSNs as are foreign individuals who have been students in the US[48] or citizens of Puerto Rico[49] or the US Virgin Islands.[50]

For example, Haroon Amin and Ather Ali filed 250 false returns using the names and SSNs of deceased individuals.[51] The names and SSNs were obtained over the Internet. Amin and Ali prepared false W-2s indicating that these deceased individuals earned income from employers that had never employed them.[52] The W-2s indicated that excess taxes had been withheld, and refunds were due. "Home addresses" were locations (or commercial mail boxes) that Amin and Ali controlled. Amin and Ali entered guilty pleas.[53]

Although Amin and Ali claimed over $2 million in false refunds over a two-year period, only $258,594.00 was actually paid. Federal Express sent the refunds that were made to overseas banks in Armenia and Pakistan where they were deposited.

[43] Information (February 1, 2011) *United States of America v. Johnson Coker* (D. N.J.) (Doc. No. 44) 3:11-cr-00046-FLW (purchased the identities – name address, date of birth, and SSNs – for hundreds of individuals, and filed thousand of returns over a five year period sought refunds of $11.5 million, of which $3.2 million was received).

[44] Indictment (September 15 2010) *United States of America v. Levonne V. Stewart* (M.D. LA) (Doc. No. 1) 3:10-cr-00139-BAJ-CN (used the identities of nursing home patients secured by virtue of her work at the homes to file 30 false returns claiming refunds of $102,913).

[45] Government's Lodging of Plea Agreement (February 4, 2011) *United States of America v. Trang Dinh* (C.D. CA.) (Doc. No. 33) 2:10-cr-00357-JHN-1 (an employee of the LA County Department of Social Services used the names and SSN of DSS clients to file 197 false returns seeking $2,212,996 in false refunds).

[46] *United States of America v. Holly M. Barnes*, 2010 WL 2044913 (N.D. Fla.) (as the leader of a girls scout troop the SSNs of the girls was secured on a "medical emergency" form and used to file fraudulent returns with fake W-2s in the names of the girls for $87,976.70 in false refunds).

[47] Indictment, (April 15, 2011) *United States of America v. Tarshia McGary* (E.D. LA) (Doc. 1) 2:11-cr-00093-JCZ-DEK (using names and SSNs of individuals found in buildings destroyed by Hurricane Katrina fraudulent returns were filed using the Turbo Tax website).

[48] Indictment (July 8, 2010) *United States of America v. James McKibbin et al.* (N.D. ILL.) (Doc. No. 1) 1:10-cr-00583 (using the names and SSNs of foreign students from Romania who had been in the US but returned home returns were filed seeking over $100,000 in false refunds).

[49] Notice of Appeal (October 6, 2011) *United State of America v. Harold Gonzalez Roque* (W.D. N.C.) 3:09-cr-00177-MOC (in a case still under appeal Harold Gonzalez Roque and others were convicted of using names and SSNs of Puerto Rican residents to secure $12,342,117 in false refunds).

[50] See the discussion of PC Tax Services and GLM Tax Services below.

[51] Indictment (December 4, 2008) *United States of America v. Haroon Amin & Ather Ali* (C.D. CA) (Doc. No. 1) 5:08-cr-00242-RHW.

[52] The names and EINs of these companies were secured through a friend of the co-conspirators who was a certified public accountant.

[53] Judgment (October 3, 2011) *United States of America v. Haroon Amin & Ather Ali* (C.D. CA) (Doc. No. 170) 5:08-cr-00242-RHW.

Marvin Berkowitz (and nine co-conspirators[54]) replicated the Amin/Ali fraud on a much larger scale. The Berkowitz conspirators filed more than 4,000 false federal and state returns[55] seeking fraudulent refunds of $26 million federally and $17.8 million from states.[56] The Berkowitz fraud continued for six years and involved both fabricated W-2s and 1099s.

The identities that the Berkowitz conspirators stole belonged to prison inmates[57] and deceased individuals. In this case most of the money was transferred to Israel where it was deposited in local banks by a law firm in Jerusalem.[58]

Neither the Amin/Ali nor the Berkowitz frauds are possible under the Brazilian or the Quebec/Belgian encryption procedures. Fraudsters seeking to file false returns with stolen identities (names and SSNs) also need names, addresses, and FEINs of employers/payers. This data may be easy to find but the digital fingerprint on prior W-4s and W-9s as well as the digital fingerprint on the W-2s and 1099s associated with the returns are nearly impossible to replicate.

If this kind of fraud were attempted after the institution of either of the encryption systems proposed here, the tax returns would be suspect on arrival at the IRS (or state revenue authorities). Returns filed without a digital signature (the alpha-numeric string, and 2-D bar code) would immediately raise audit flags; those with false alpha-numeric strings, and fraudulent 2-D bar codes would fail a simple scanning test. Regardless of the outcome, refunds would not issue.

(4) *Taxpayer/professional tax-preparer collusion (2-party collusion)*. Collusions attacks are always more difficult to stop than attacks by lone fraudsters. The most common collusion is among professional tax return preparers and return filers. When this collusion occurs the common pattern involves a promise of significantly larger refunds in exchange for substantially higher return reparation fees. The preparer carries out the fraud.

Rosemary Robinson was involved in a very simple scheme. She produced false W-2s for twelve individuals over two years who had no income so that they could qualify for the Earned Income Tax Credit.[59] Ms. Robinson received $8,500 for her services.[60] If

[54] The co-conspirators were all family members living in the U.S. Marvin Berkowitz, who appears to have been the leader of the conspiracy, moved to Israel at the beginning of the conspiracy.

[55] Estimates are that 3,500 federal and 500 state returns were filed. The states impacted were: Arkansas, Arizona, California. Washington, D.C., Hawaii, Iowa, Kentucky, Louisiana and Massachusetts.

[56] The refunds actually issued in this case were $2.2 million from the US Treasury and $2.8 million from the various states.

[57] The names and SSNs of prison inmates were obtained from court records at various federal courthouses. In other instances the prison inmate identities were purchased from people with access to this information.

[58] Indictment (August 4, 2009) *United States of America v Marvin Berkowitz* (N.D. ILL.) (Doc. No. 16) 1:09-cr-00144.

[59] Indictment (March 24, 2011) *United States of America v. Rosemarie Robinson* (W.D. N.Y.) (Doc. No. 1) 6:11-cr-06058-DGL-JWF.

[60] Statement of the Government with Respect to Sentencing Factors (August 31, 2011) *United States of America v. Rosemarie Robinson* (W.D. N.Y.) (Doc. No. 14) 6:11-cr-06058-DGL-JWF.

the fraud had been fully effective losses would have been $86,979.00. Some payments were intercepted, and actual losses were $54,125.48.

The same collusion fraud was carried out by two related tax-prepares that marketed their "services" in the US Virgin Islands from their business locations in Georgia. PC Tax Services owned by Vernon Roberts filed clients returns electronically with an Electronic Filing Identification Number (EFIN). Gregory Shepherd owned GLM Tax Service and did the same. Both firms were established and did business primarily in Georgia, however they hired Guillermina Carmona (a resident of the US Virgin Islands) to recruit tax clients in the US Virgin Islands. The lure she used was the "special knowledge" these firms had on how to qualify for the EITC.

Resident of the US Virgin Islands have valid SSNs but are not required to file US returns (and do not qualify for the EITC) if they do not reside on the mainland for more than half the year. To secure EITC refunds for these "clients" false Georgia addresses were provided, fraudulent W-2, 1099s as well as false dependency exemptions were provided. The fraud continued for six years.[61] Carmona entered a guilty plea,[62] Vernon Roberts[63] and Gregory Shepherd were found guilty at trial. Restitution for aggregate tax losses was set at $1,119,095.

(5) *Collusion of businesses/professional tax-preparers/taxpayers (3-party collusion)*. This collusive attack on the tax system is very difficult to prevent. If the employer (who drafts the W-2s) is colluding with the employees (who receives the W-2s), as well as with the accountant (who does all the returns) are cooperating, then encrypting the data on the forms sent to the IRS will not be an effective barrier to fraud. Fortunately, this degree of collusion is not that common. There is only one case like this in 2011 – Mack Edwards.

Mack Edwards[64] owned MD Edwards, a construction company in the Saint Louis Missouri area. Edwards conspired with Hestine Mason,[65] his tax return preparer, to file false tax returns based on fraudulent W-2s Edwards issued to employees. The W-2s indicated wages that were not earned and withholding that were not withheld.

The twelve employees involved were required by Edwards to use Mason for return preparation. Edwards and the employees split the fraudulent refunds that were generated by this scheme. Mason was paid $300 to $500 per return. Edwards and the

[61] Indictment (March 24, 2010) *United States of America v. Vernon A. Roberts, Gregory Shepherd & Guillermina Carmona* (N.D. GA.) (Doc. No. 1) 1:10-cr-00138-ODE-GGB.
[62] Transcript of Guilty Plea (September 7, 2010) *United States of America v. Vernon A. Roberts, Gregory Shepherd & Guillermina Carmona* (N.D. GA.) (Doc. No. 68) 1:10-cr-00138-ODE-GGB.
[63] Jury Verict – Vernon A. Roberts, (September 24, 2010) *United States of America v. Vernon A. Roberts, Gregory Shepherd & Guillermina Carmona* (N.D. GA.) (Doc. No. 89) 1:10-cr-00138-ODE-GGB.
[64] Indictment (September 23, 2010) *United States of America v. Mack Edwards* (E.D. Mo.) (Doc. No. 2) 4:10-cr-00490-CDP.
[65] Information (April 7, 2010) *United States of America v. Hestine I Mason* (E.D. Mo.) (Doc. No. 1) 4:10-cr-00202-CDP.

employees split the fraudulent refunds.  Both Edwards and Mason entered guilty pleas, and restitution was ordered for the $51,229.00 in false refunds that were issued.[66]

How the IRS uncovered this fraud is unclear.  Many documents in the case remain under seal, and correspondence with IRS Criminal Investigation has not provided an insight.

[66] Judgment (March 2, 2011) *United States of America v. Mack Edwards* (E.D. Mo.) (Doc. No. 36) 4:10-cr-00490-CDP.