4-9-2013

E-Verify Can Stop Refund Fraud

Richard Thompson Ainsworth

Andrew Shact

BOSTON UNIVERSITY

E-VERIFY CAN STOP
REFUND FRAUD

Boston University School of Law Working Paper No. 13-6
(March 27, 2013)
(Revised April 9, 2013)

Richard T. Ainsworth
Boston University School of Law

Andrew Shact
VP and Tax Counsel, Hologic, Inc.

This paper can be downloaded without charge at:

E-VERIFY CAN STOP
REFUND FRAUD

Richard T. Ainsworth

Andrew Shact

Two issues in the current Washington debates need to be linked. E-Verify, the Internet-based database that allows employers to verify an employee's work eligibility that is at the center of the immigration debate,[1] is the ideal tool for stopping tax refund fraud. All that is needed is a digital signature of the E-Verify result, and the mandatory inscription of this signature on tax documents to make them self-authenticating.

The central features of this proposal have been made before.[2] The technology it requires is tried and proven. The processes and procedure it advocates are in place and effectively deployed in foreign jurisdictions, notably in VAT jurisdictions enforcing against VAT fraud.[3]

The heart of this linkage (the E-Verify/refund fraud linkage) is numerical. At least $5.2 billion in annual revenues are being lost through refund fraud – the cost for businesses to implement a fully mandated E-Verify system is $2.7 billion. If E-Verify solves refund fraud, there are funds available for a business credit with a considerable amount of money left over.

The $5.2 billion figure comes from the Treasury Inspector General for Tax Administration (TIGTA) who found that in Processing Year 2011, identity theft cost the US taxpayer in excess of $5.2 billion in undetected fraudulent tax refunds. TIGTA estimates that the five-year loss is $21 billion.[4] The $2.7 billion figure comes from a Bloomberg Report for the same time period indicating that a fully mandated E-Verify system for all employers would cost $2.7 billion (almost all of it in training expenses related to system implementation and worker appeals).[5]

E-Verify

The Department of Homeland Security (DHS) operates the E-Verify Internet database in partnership with the Social Security Administration (SSA). It is a voluntary

---

[1] Melissa Barnhart, *Controversial E-Verify System Integral Part of Immigration Reform Proposal*, CHRISTIAN POST (March 23, 2013) (indicating that a bipartisan group of eight congressmen have been secretly meeting for four years to craft an immigration proposal that includes e-verify).

[2] Richard T. Ainsworth, *Refund Fraud? Real-Time Solution!* (April 27, 2012) TAX NOTES 1165, *available at*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1978898

[3] Richard T. Ainsworth, *Real-Time Solution to Refund Fraud: VAT Lessons from Belgium, Brazil and Quebec*, 66 TAX NOTES INT'L 533 (May 7, 2012) *available at*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2026424

[4] TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting from Identity Theft*, 3 (July 19, 2012) Ref. No. 2012-42-080 (indicating that this amount is over-and-above the $6.2 billion that the IRS identified and prevented.)

[5] Jason Arvelo, *"Free" E-verify May cost Small Business $2.6 Billion: Insight*, BLOOMBERG GOVERNMENT (JANUARY 21, 2011).

system on the federal level, although twenty-one states require some or all employers to use it. Those states are: Alabama,[6] Arizona,[7] Colorado,[8] Florida,[9] Georgia,[10] Idaho,[11] Indiana,[12] Louisiana,[13] Minnesota,[14] Mississippi,[15] Missouri,[16] Nebraska,[17] North Carolina,[18] Oklahoma,[19] Pennsylvania,[20] South Carolina,[21] Tennessee,[22] Utah,[23] and

---

[6] Alabama requires all employers to use E-Verify. Jon Feere, An Overview of E-Verify Policies at the State Level (July 2012) *available at*: http://cis.org/e-verify-at-the-state-level.

[7] Arizona requires all employers to participate in E-Verify with all newly hired employees. *Id.*

[8] Colorado does not mandate E-Verify. However, public contractors must participate in either E-Verify or a Colorado program (the Department Program) run by the Colorado Department of Labor and Employment. *Id.*

[9] Florida requires (by executive order) all agencies under the direction of the governor to verify the employment eligibility of all new employees through E-Verify. Agencies not under the direction of the governor are "encouraged" to follow the same guidelines. *Id.*

[10] Georgia requires both public and private employers to use E-Verify during the hiring process. *Id.*

[11] Idaho requires state agencies to verify that new employees are eligible for employment under federal and state law. It does not specifically reference E-Verify. *Id.*

[12] Indiana requires state agencies and political subdivisions to use E-Verify to determine work authorization status of all employees hired. The requirement to use E-Verify also applies to public contractors. *Id.*

[13] Louisiana requires all state and local contractors who seek to do business with Louisiana to use E-Verify. *Id.*

[14] Minnesota requires use of E-Verify only for some public contracts. It requires state contracts for services in excess of $50,000 to require certification from vendors and subcontractors that they have implemented or are in the process of implementing the E-Verify program for all newly hired employees who will perform work under the contract. *Id.*

[15] Mississippi requires all employers to use E-Verify with new hires. *Id.*

[16] Missouri prohibits businesses from knowingly employing, hiring, or continuing to employ an illegal alien to perform work within the state of Missouri. E-Verify does not apply to all businesses, but those businesses that do use E-Verify are provided an affirmative defense that the business has not violated the prohibition of employing illegal aliens. All public employers are required to "actively participate" in E-Verify. *Id.*

[17] Nebraska requires use of E-Verify by state agencies (and political subdivisions) and by public contractors. Every contract between a public employer and public contractor must contain a provision requiring the public contractor to use E-Verify for new employees physically performing services within Nebraska. *Id.*

[18] North Carolina requires all counties and municipalities to use E-Verify. The State also requires private businesses to use E-Verify for new employees, but exempts any "seasonal temporary employee who is employed for 90 or fewer days during a 12-consecutive-month period." *Id.*

[19] Oklahoma requires public contractors and subcontractors to use E-Verify. Public employers are prohibited from entering into contracts for the physical performance of services within Oklahoma unless the contractor (and any subcontractor) uses E-Verify to verify the work authorization of all new employees. *Id.*

[20] Pennsylvania requires some public works contractors and subcontractors to use E-Verify. In order to ensure compliance, employers are subject to complaint-based and random audits. The law covers "construction, reconstruction, demolition, alteration, and/or repair work other than maintenance work, done under contract and paid for in whole or in part out of the funds of a public body" where the estimated cost of the total project is in excess of $25,000. *Id.*

[21] South Carolina requires all employers to use E-Verify. South Carolina is said to have one of the nation's most effective E-Verify laws. The state uses an audit process to ensure businesses are in compliance. *Id.*

[22] Tennessee requires that all state and local agencies and private employers enroll and participate in E-Verify or provide specified employment authorization or identity documents. The rules apply on January 1, 2012 (500 or more employees); July 1, 2012 (200-499 employees); and July 1, 2013 (6-199 employees). Private employers with 5 or fewer employees are exempt. *Id.*

[23] In Utah all private employers who employ more than 15 or more employees are required to use a "status verification system" to verify the employment eligibility of new employees. Utah does not mandate E-

Virginia.[24] In *Chamber of Commerce v. Whitting*, 563 US __ (2011) the Supreme Court ruled that states may constitutionally mandate the use of E-Verify.[25]

Short history of E-Verify. The Immigration Reform and Control Act (IRCA) of 1986 imposed employment-related restrictions on immigrants. It requires employers to inspect and verify the authenticity of documents provided by prospective employees. After reviewing these documents, employers must attest to an employee's eligibility by completing a Form I-9.[26]

There can be as many as twenty-six documents used to demonstrate eligibility. Many are prone to fraud and forgery. Thus, adhering to the IRCA was difficult for many employers. Differentiation between properly documented and undocumented immigrant was problematical, and as a result the IRCA did not fulfill its mandate (increasing job security for U.S. citizens and curbing unauthorized employment).

In response to a growing population of undocumented migrants, Congress passed the Illegal Immigration Reform and Immigration Responsibility Act (IIRIRA) in 1996. Under the IIRIRA, the federal government rolled out the Basic Pilot/Employment Eligibility Verification Program, allowing employers to confirm eligibility via an electronic verification system. It was initially available in the five states with the largest undocumented populations: California, Florida, Illinois, New York, and Texas. By 2003, all fifty states were participating.

Re-branding & Data entry. In 2007, the Bush administration enhanced the internal enforcement of immigration laws. The electronic verification system was re-branded as the E-Verify Program. The employee data input into E-Verify is:
- **employee's name (first, last, middle initial, and other names used)**;
- employee's date of birth;
- **employee's social security number**;

Verify. Businesses can use any other federal program the state deems equivalent to E-Verify, including "the Social Security Number Verification Service or similar online verification process implemented by the United States Social Security Administration." *Id.*

[24] In Virginia, E-Verify is required for state agencies and businesses contracting with Virginia. Employers with more than an average of 50 employees for the previous 12 months entering into a work or service contract in excess of $50,000 with any Virginia agency must register and participate in E-Verify. Failure to comply with the law results in the employer being debarred from contracting with any state agency for a period up to one year. Such debarment ends upon the employer's registration and participation in E-Verify. *Id.*

[25] *Witting* held that the provision of the Legal Arizona Workers Act that provides for the suspension and/or revocation of the business licenses of Arizona employers who knowingly or intentionally employ unauthorized aliens is not expressly preempted by the federal Immigration Reform and Control Act, which prohibits the knowing hiring of unauthorized immigrants and preempts state laws imposing sanctions on those who hire unauthorized immigrants. The Arizona law falls within the IRCA's exception that preserves state authority to impose sanctions through licensing and similar laws. Arizona's requirement that employers use the federal E-Verify system to confirm eligibility for employment is not impliedly preempted, as it does not conflict with the federal scheme. The federal statute establishing E-Verify does not constrain state action.

[26] The I-9 form is the *Employment Eligibility Verification* form of the DHS and SSA.

- the employee's citizenship status he/she attested to on the I-9;
- an A number (alien registration number) or I- 94 number (an 11-digit number that is found on the Arrival-Departure Record – Form I-94 or Form I-94A) if applicable; .
- the type of documentation provided on the I-9 to establish work authorization;
- the proof of identity provided on the I-9, and its expiration date, if applicable

Employee data can be correlated with employer data in the E-Verify system. Only registered employers can input employee data. To register a company must provide:
- contact information for the company "signatory" per the company's E-Verify memorandum of understanding;
- **company name (d/b/a is optional);**
- Data Universal Numbering System (DUNS) number (optional);
- physical address of the location from which the company will access E-Verify;
- company mailing address;
- **Federal Tax ID number of the company;**
- total number of employees from all company sites that will be participating (select from a range);
- parent entity (optional);
- administrator's name;
- the first three digits of the company's primary North American Industry Classification System (NAICS) code;
- the number of hiring sites that will participate in E-Verify in each state.

Four of the data-points entered into the E-Verify system are important for preventing refund fraud. They are highlighted in bold above (the employee's full name, the employee's social security number, the employer's name, and the employer's Federal Tax ID. In this proposal the E-Verify system will be required to take these four elements encrypt them, and reduce the result to a digital signature represented as an alphanumeric algorithm and as a 2D bar code.

Refund Fraud

The IRS encounters a wide range refund frauds each year. The magnitude of the actual and potential losses are staggering. While the IRS stops $6.2 billion, TIGTA estimates that another $5.2 billion escapes detection, and that over five years this un-stopped fraud will exceed $21 billion.

The IRS publishes a representative sample of the refund fraud cases it investigates on its web site.[27] Currently there are a total of two-hundred and twenty-three (223) cases spanning Fiscal Years 2010 (35); 2011 (76); 2012 (74), and 2013 (38) on the web. The cases are not classified, and appear without citation. It is possible however to use the IRS summaries to identify the underlying court proceedings, read them and construct an

---

[27] IRS, QUESTIONABLE REFUND PROGRAM (QRP) – CRIMINAL INVESTIGATION (CI), *available at*:
http://www.irs.gov/uac/Questionable-Refund-Program-(QRP)-Criminal-Investigation-(CI)

4

overview of the types of refund fraud that the IRS is dealing with. This analysis has been provided elsewhere.[28] These frauds break down into five major classes:

(1) *Purely fabricated identities* – this is a common fraud carried out by prison inmates where a fully fictitious individual and employment relationship is created (sometimes using the substitute W-2 earnings statement Form 4852), and requests are made to send multiple refunds to associates outside the prison.

(2) *Identity theft* – instances where an individual secures the name and SSN of another person (as well as the TIN of an unsuspecting business), and uses this information to fabricate false W-2s and returns, seeking fraudulent refunds for withholding never made (as well as refundable credits);

(3) *Taxpayer altered documents* - W-2's or 1099s from legitimate employment relationships can be altered – withholding can be increased or income amounts changed.

(4) *Taxpayer/professional tax-preparer collusion (2-party collusion).* Collusion frauds are always difficult to stop. The most common collusion is among professional tax return preparers and return filers. Commonly involving promises of significantly larger refunds in exchange for substantially higher return reparation fees. The preparer carries out the fraud.

(5) *Collusion of businesses/professional tax-preparers/taxpayers (3-party collusion).* This collusive attack is very difficult to prevent. Here the employer (who drafts the W-2s) is colluding with the employees (who receive the W-2s), as well as with the accountant (who does the returns) are cooperating in the fraud. In this instance, the solution proposed here is not an effective barrier to fraud. A traditional audit is needed.

In each of these refund fraud categories; categories that span the whole list of examples set out in the Questionable Refund Program for the past four years, there is one common denominator. Each of these frauds revolve around false documentation; documentation that cannot be immediately validated as legitimate by the IRS. This is a problem that can be solved, and has been solved in a number of tax jurisdictions with technology.

Self-validating Tax Documentation

W-2's and 1099s can be secure and self-validating. 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 (TIN);
(c) to the named employee;
(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

---

[28] *Supra* note 2 at *Appendix*.

5

the IRS will immediately identify his fraud will not go forward with his attempted theft. In fact, with a little bit of advertising, the IRS should be able to convince most potential fraudsters to stop 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;[29] and (b) the Belgian/Quebec model of self-certified cash register receipts used to monitor retail consumption taxes.[30]

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 alphanumeric string of characters, and reproduces the result as a bar code on the relevant tax document (receipt or invoice).[31] Tax auditors immediately confirm the validity of the documents with hand held scanners.

Mechanism

There are two steps to the solution. If we consider the five classes of refund fraud set out above, the first two (identity theft and identity fabrication) are solved directly by E-Verify, the second two (valid document alteration and two party collusion) are solved with an extension of the E-Verify at the time W-2s and 1099s are drafted.

A full solution would extend E-Verify procedure to all employees.

Identity theft and identity fabrication. Adding one step to E-Verify would eliminate both of these frauds. When the employer submits an employee's I-9 data to E-Verify the online system will be required to return to the employer an encrypted signature of the submission. The signature would be in two forms: an alphanumeric string of characters, and a 2D bar code that could be scanned easily.

This digital signature would be comprised of at least four elements: (a) employee's name, (b) employee's SSN, (c) employer's name, and (d) employer's TIN. Other data fields could be added. The key to fraud prevention is in the required usage of the signature. First, it would be required to be kept in the employment files so that a simple audit with a hand-held scanner could verify compliance with E-Verify. Secondly,

---

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

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

[31] 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 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. Part or all of this data can be encrypted for use in the digital sigature.

the digital signature would be a required field on any W-2 or 1099 issued by the firm to this employee.

W-2s or 1099s without the required digital signature would be invalid. The IRS could determine validity with a scanner and the entry of the name and SSN appearing on the associated tax return. The process could be fully automated.

Enforcement would be aided if employers provided "digital signature" labels with the W-2s or 1099s they issue so that the labels could be placed on the tax return in much the same manner as the SSNs of dependents are listed next to their names currently.

Valid document alteration and two-party collusion. To solve the next two types of refund fraud E-Verify would need to be extended. In this case, at the time an employer is drafting W-2s or 1099s to send to its workers, the E-Verify system would need to be accessed again.

This time the financial fields would be entered into E-Verify. For example, for a basic W-2 this would be the wage amount and tax-withholding amounts, along with the name and SSN of the employee and the name and TIN of the employer. Other data fields could be added. Once again E-Verify would return a digital signature of this information in an alphanumeric string of characters, and a 2D bar code that could be scanned easily.

Importantly, this second digital signature would also be a required field on any W-2 or 1099 issued to this worker. The audit process could be fully automated, and all W-2s or 1099's without this digital signature would be invalid.

Enforcement

In the first place, the IRS will be able to validate the authenticity of W-2s submitted on any return. In addition, because employers would be required to comply with the digital signature requirements, a penalty for non-compliance could be as simple as denial of the deduction for workers who were issued W-2s or 1099s without the required digital signatures.

This proposal therefore would replicate the IRS's most famous administrative enforcement action. In 1986 the IRS recovered three billion dollars in revenue when seven million fraudulent dependents vanished from the tax rolls.[32] 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.

If the SSN was not listed, the dependency deduction was not allowed. As the authors of *Freakonomics* explain, this measure worked because taxpayers who had found

---

[32] 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).

7

it easy to cheat previously now feared that they could be caught in real-time.[33] Costing next to nothing to implement, the benefits of this enforcement action continue to this day.

Workability

This proposal is not only workable; it works. A very similar system is in place in Brazil to monitor cross border trade in goods. The Brazilian system works 24/7 and applies to any cross-border sale of goods. The technology infrastructure in Brazil is considerably larger than is required for E-Verify.

Brazil is undergoing a dramatic tax modernization program called the Public Digital Bookkeeping System (SPED).[34] The Electronic Invoice (NF-e)[35] and the Electronic Waybill (CT-e)[36] are the centerpieces of this program. They are the important elements of SPED for E-Verify comparison purposes. Both function in a similar manner, NF-e for goods and CT-e for transport services.

On September 15, 2006 Brazil began a NF-e pilot project. Progress was rapid. By April 2009 there were 25,000 issuers of NF-e. By the end of 2010 there were over 500,000 firms involved in issuing digitally signed, cross-border NF-e invoices.[37]   The system is fully in place today.

The essence of the Brazilian system is that whenever goods cross an internal border an electronic file representing the invoice is sent (through the internet) to the tax administration of the state of departure, where it is checked and sent on to the Federal Treasury (again through the internet). The Treasury "digitally signs" the document with a fixed-size alphanumeric bit string (and a bar code in 128-C format). The bar code facilitates scanning-based verification. The invoice is returned to the carrier crossing the border (in less than 3 seconds) and is presented to the buyer and tax administration in the destination state.

The cross-border fraud in goods has been dramatically reduced in Brazil. The technology not only tracks the flow of goods, but its use in all cross-border transactions

---

[33] 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.

[34] SPED contemplates replacing paper tax and accounting books and documents with electronic versions where legal validity is confirmed with a digital signature. These digital documents will have legal precedence over paper replicas.

[35] NF-e is the acronym for *Nota Fiscal Eletrônica.*

[36] CT-e is the acronym for *Conhecimento de Transporte Eletrônico de Cargas*.

[37] Newton Oller de Mello, Eduardo Mario Dias, Caio Fernando Fontana & Marcelo Alves Fernandez, *The Evolution of Electronic Tax Documents in Latin America,* PROCEEDINGS OF THE 13TH WORLD SCIENTIFIC AND ENGINEERING ACADEMY AND SOCIETY (WSEAS) INTERNATIONAL CONFERENCE ON SYSTEMS (2009) 449, 297, *available at*: http://dl.acm.org/citation.cfm?id=1627575&picked=prox.

has convinced the fraudsters that they would be immediately identified if they tried to present goods in the destination state without a digitally signed invoice.

A different way to carry out the E-Verify encryption process would be 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). Digital signatures would be reproduced on the W-2/1099s.

The record of all W-2/1099 encryption operations under the Quebec/Belgian model would 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. Once again, every time the IRS is presented with a W-2/1099 the IRS would be immediately able to verify authenticity.

CONCLUSION

E-Verify, properly adapted and extended, is not only a mechanism that advances immigration reform; it is potentially a classic example of the best in modern tax reform. E-Verify can be use to achieve significant revenue results by preempting fraudsters before they act, rather than chasing them down after the fact. All that is needed is a digital signature inscribed on tax documents to make them self-authenticating.

The numbers tell the whole story. If we are loosing $5.2 billion annually in frauds that can be prevented with a fully mandated E-Verify system, then the $2.7 billion business cost for E-Verify implementation is something that can be easily accommodated with tax credits and deductions.

This is an immigration/tax reform link that needs to be made.