3-20-2012

Refund Fraud? Real-Time Solution! Digital Security Borrowed from the VAT (Brazil, Quebec, & Belgium)

Richard Thompson Ainsworth
Boston University School of Law

REFUND FRAUD? – REAL-TIME SOLUTION! DIGITAL SECURITY BORROWED FROM THE VAT (BRAZIL, QUEBEC & BELGIUM)

Boston University School of Law Working Paper No. 12-15
(March 20, 2012)

Richard T. Ainsworth

REFUND FRAUD? – REAL-TIME SOLUTION!
DIGITAL SECURITY BORROWED FROM THE VAT
(BRAZIL, QUEBEC & BELGIUM)

Richard T. Ainsworth

This article provides support for a proposal to eliminate refund fraud in the U.S. by turning Forms W-2, and 1099 into self-certified/ self-authenticated tax documents. The proposal suggests that a "digital signature" of these documents should be taken *after* they are completed. The signature should then be made part of the final document.

This proposal was initially advanced in *Refund Fraud? Real-Time Solution!*[1] The underlying premise of that article was that the US could dramatically reduce, if not eliminate, refund fraud if it borrowing digital security techniques from the VAT. The article did not however, explain or expand upon these techniques from within the VATs where they were developed. This article takes up the VAT side of that analysis.

The problem. Each year the U.S. hands out millions of dollars in fraudulent refunds. Exact amounts are difficult to determine, but the known volumes and the ease with which the frauds are carried out make for alarming headlines. For example, when IRS Criminal Investigation indicated that in 2009 the U.S. *prison* population filed for $295.1 million in fraudulent refunds,[2] reporters in Florida were quick to claim that Florida was "number one" as the state with the most prisoners engaged in this fraud.[3]

A more complete statement of the problem, and not as sensational as the prisoner fraud statistic, was put forward by the US Treasury Inspector General for tax Administration (TIGTA) a few years later:

> 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 billion 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.[4]

---

[1] Richard T. Ainsworth, *Refund Fraud? Real-Time Solution!* 134 TAX NOTES 1165 (February 27, 2012), 2012 TNT 38-9, Doc 2012-1776

[2] 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).

[3] 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.

[4] 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.)

In other words, refund fraud in the U.S. is huge, but the true extent of it is unknown. Refund fraud either results from legitimate taxpayers submitting false income and withholding documents, or it results from an identity theft followed by the creation of fully fabricated returns. In all cases however, what the IRS is dealing with is a fraudulent document problem.

Why the proposal works. Real-time recognition that a fraudulent activity is immediately and obviously detectable by the IRS is how seven million false dependents were eliminated from the tax rolls in 1986. The IRS simply required social security numbers to be listed along with the dependents name on any the return claiming a dependent, and the problem was solved.[5] Fraudsters knew they would be caught.

A real-time tax system has real-time enforcement.[6]

The VAT. Unlike the annual income tax, the VAT is a transactional levy. It relies on huge number of detailed invoices, monthly and quarterly reports. Every B2B transaction, and every B2C retail sale produces a tax document that needs to be authenticated.

VAT frauds frequently manipulate these documents for gain, and VAT jurisdictions have spent a considerable amount of time and energy devising effective and efficient methods for determining if a document is legitimate (or original).

The strong suggestion is that the IRS should look to the VAT to solve refund fraud, because even though the tax is different, the administrative problem is the same. The refund fraud problem is essentially document verification problem. The VAT is very good at document verification. The IRS can learn from the VAT.

This paper looks at three VAT jurisdictions, Brazil, Quebec and Belgium, and explains how they use technology to solve document authentication problems. In each case a tax fraud is facilitated by false documentation, and the administrative response is to use technology to certify the documents and stop the fraud. In Brazil the fraud arises in the context of internal cross-border B2B transactions. In Quebec and Belgium the fraud is skimming profits from B2C cash and debit/credit card transactions.

Brazil
Solving "Invoice Sightseeing" with the NF-e and the CT-e
Applying the Solution to Refund Fraud

[5] 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).

[6] *See:* IRS, New Release, *IRS to Host Public Meeting December 8 on Real-Time Tax System*, IR-2011-114, November 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); IRS, New Release, *IRS to Host Second Real-Time Tax System Meeting*, IR-2012-10, January 18, 2012.

Brazilian tax administrations (federal and state) are undergoing a massive modernization process that is using modern information technology to put electronic controls on business transactions. A constitutional amendment was needed for sharing inter-government tax information.[7]

Electronic invoices & Electronic waybills for tax purposes. The overall tax modernization program in Brazil is called the Public Digital Bookkeeping System (SPED).[8] The Electronic Invoice (NF-e)[9] and the Electronic Waybill (CT-e)[10] are the two parts of this program that are important for comparative purposes. Both the NF-e and the CT-e programs began with pilots and are now firmly part of Brazilian commercial practice.

On September 15, 2006 Brazil began the NF-e pilot project. Six states with 19 of the largest Brazilian companies, some of them subsidiaries of US firms, covering a wide range of industries were involved.[11] 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 NF-e invoices.[12]

---

[7] Constitutional Amendment No. 42 of December 19, 2003 (See: *Constitution of the Federal Republic of Brazil* of October 5, 1988, Art. 37).

[8] 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.

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

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

[11] The six Brazilian states and the companies that participated in each and their industrial concentration are listed below. In all, there are 37 invoice-issuing commercial centers involved. In *Bahia* state the participants were: (1) Petrobras Distribuidora S/A. (state owned oil distribution company); (2) Companhia Ultragaz S.A. (gas company); (3) Ford Motor Company Brasil Ltda. (automobiles); (4) Gerdau Aços Longos S.A. (steel); (5) Sadia S.A. (food); (6) Souza Cruz S.A. (cigarette). In *Goiás* state: (7) Souza Cruz S.A. (cigarette). In *Maranhão* state: (8) Souza Cruz S.A. (cigarette) participated through another branch. In *Rio Grande do Sul* state: (9) Petrobras Distribuidora S/A. (state owned oil distribution company); (10) Companhia Ultragaz S.A. (gas company); (11) Dimed Distribuidora de Medicamentos S.A. (drug med. distributor); (12) General Motors do Brasil Ltda.; (13) Gerdau Aços Longos S.A. (steel); (14) Sadia S.A. (food); (15) Siemens VDO Automotive Ltda.; (16) Souza Cruz S.A. (cigarette); (17) Toyota do Brasil. In *Santa Catarina* state: (18) Petrobras Distribuidora S/A.; (19) Wickbold & Nosso Pão Indústrias Alimentícias Ltda.. In *São Paulo* state: (20) Petrobras Distribuidora S/A. (state owned oil distribution company); (21) Cervejarias Kaiser S.A. (beer); (22) Companhia Ultragaz S.A. (gas); (23) Eletropaulo Metropolitana Eletricidade de São Paulo S.A. (energy); (24) Eurofarma Laboratórios Ltda. (drug); (25) Ford Motor Company Brasil Ltda.; (26) General Motors do Brasil Ltda.; (27) Gerdau Aços Longos S.A. (steel); (28) Office Net do Brasil S.A; (29) Petrobras - Petróleo Brasileiro S.A. (oil); (30) Robert Bosch Limitada; (31) Sadia S.A.; (32) Siemens VDO Automotive Ltda.; (33) Souza Cruz S.A.; (34) Telefônica - Telesp Telecomunicações de São Paulo S.A.; (35) Toyota do Brasil; (36) Volkswagen do Brasil Indústria de Veículos Automotores Ltda.; (37) Wickbold & Nosso Pão Indústrias

[12] 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.

Following the success of the NF-e Brazil began the CT-e pilot project (October 25, 2007). This pilot involved two states (São Paulo and Rio Grande do Sul) and 43 companies and transportation firms. By March 1, and April 1, 2009 respectively the firms in Rio Grande do Sul and São Paulo began issuing legally binding CT-e documents.[13] Large-scale adoption of the CT-e began in 2010.[14]

How NF-e and CT-e operate. The NF-e and CT-e function in a very similar manner. The major difference between the systems is that the object of the NF-e is the goods that are sold across internal borders, whereas the object of the CT-e is the service of transporting these goods. An example following the NF-e helps explain how the system works.

Assume firm "A" (in state 1) sells goods to firm "B" (in state 2), and the goods will be transported by common carrier hired by firm "A."

STEP 1: Firm "A" will generate two electronic files in XML format[15] (one for the NF-e; the other for the CT-e) that will contain all necessary tax information for the sale of goods and the sale of transport services.

- The issuer digitally signs the files (to assure integrity of the data and its authorship);
- The files are transmitted (through the Internet) to the **State tax administration in State 1**; and
- The transmission constitutes a "request for authorization" to use a NF-e, or CT-e.

STEP 2: The State Tax Administration in State 1 (the origin state) acts on the authorization of use request, without which there can be no binding contract for the provision of goods, or no supply of services (these are commercial law rules). However, authorization is not difficult.

- The authorization system is fully automated (without human intervention);
- Authorization is available 24/7;
- The authorization process is a basic check of the XML file for accuracy and completeness;
- Although a period of up to 3 minutes had been allowed for the authorization process, the reality is that authorization takes a few seconds, and commonly takes only a millisecond.

---

[13] An important part of SPED is that once a firm begins to issue NF-e invoices, or CT-e electronic waybills paper replicas of these documents are not legally valid.

[14] Newton Oller de Mello, Eduardo Mario Dias, Caio Fernando Fontana & Marcelo Alves Fernandez, *The Implementation of the Electronic Tax Documents in Brazil as a Tool to Fight Tax Evasion*, PROCEEDINGS OF THE 13TH WORLD SCIENTIFIC AND ENGINEERING ACADEMY AND SOCIETY (WSEAS) INTERNATIONAL CONFERENCE ON SYSTEMS (2009) 449, 453, *available at*: http://dl.acm.org/citation.cfm?id=1627575&picked=prox.

[15] XML is an acronym for eXtensible Markup Language. It is a set of rules for encoding documents in machine-readable form. It is defined in the XML 1.0 Specification produced by the World-Wide Web Consortium (W3C), and several other related specifications. These are gratis open standards.

STEP 3: If the XML file is accurate, the State Tax Administration in State 1 responds in two ways, it:

- Returns to the Seller an Authorization of Use;
- Transmits the NF-e to the **Treasury Department of the Federal Revenue Service** (this is a national depository of all NF-e's issued in the country).

STEP 4: Firm "A" produces a simplified picture of the NF-e on plane paper to accompany the transit of the goods:

- The document is called DANFE (*Documento Auxiliar da Nota Fiscal Eletrônica*, or Electronic Invoice Auxiliary Document);[16]
- DANFE contains an access key with which the official NF-e can be accessed over the Internet for verification of data on the DANFE;
    - The access key is primarily a fixed-size alpha-numeric bit string;
    - The access key is also reproduced on the DANFE as a bar code in Code 128-C format;[17]
- The bar code is intended to facilitate verification of the NF-e at inspection stations on the internal Brazilian borders.

STEP 5: With the printed DANFE and authorization of the NF-e the shipment of the goods can begin.

STEP 6: The Seller will deliver (make available to) the buyer in **State 2** the following:

- NF-e (as a digital file) [and/or CT-e];
- Authorization of Use (as a digital file) [for both NF-e and/or CT-e] either
- DANFE (plane paper copy of the NF-e with internet access key) [or DACTE]

STEP 7: When goods are delivered to the Buyer, the Buyer will:

- Go to the web site of the **Treasury Department of the Federal Revenue Service** and use the access keys[18] to:
    - Check the validity of the DANFE;
    - Check the validity of the DACTE.

Brazilian cross-border tax fraud. SPED, NF-e and CT-e are not primarily directed at tax fraud, they are part of a larger move to e-documentation in commercial affairs. However, these particular documents are coordinated by the tax administrations and they do verify the tax on cross-border B2B transactions. The tax must be calculated and stated on the invoice in order for it to be considered complete.

---

[16] The same process is duplicated for transportation services. The only significant differences are: (1) instead of a NF-e the primary document is a CT-e; and (2) instead of a DANFE the paper reproduction is called a DACTE (*Documento Auxiliar do Conhecimento de Transporte*, OR Auxiliary Document of Electronic Waybill).

[17] Code 128 is a very high-density barcode symbol. It is used for alphanumeric or numeric-only barcodes. It can encode all 128 characters of ASCII. There are three types of Code 128, the A, B, and C versions. Brazil uses the "C" subtype.

[18] The access keys are available in alpha-numeric and bar code format on the DANFE and DACTE, but are also contained in the NF-e and CT-e electronic files.

As a result, these documents have almost eliminated one of the most difficult Brazilian cross-border tax frauds to deal with; a fraud called "invoice sightseeing." Oldman and Schenk explain:

> For example, assume that the rate in state A on domestic sales is 17 percent and on interstate sales to state B is 7 percent. A seller in state A sells goods to a "buyer" (a wholesaler) in state B. The wholesaler in state B then resells the goods to a small business back in state A and applies the interstate rate of 7 percent. [However,] only invoices are exchanged, the goods in fact are shipped from the seller in state A to the small business in state A, and the small business in state A saves 10 percent tax. This is tax advantageous if the small business is exempt … and cannot recover tax on purchases.[19]

In this example if the seller in state A has a valid NF-e and CT-e, and an authorization for use from the tax administration in state A, but if there is no record of the goods (or the transport) crossing the border to the buyer in state B, then the tax authorities would be alerted to a problem. There would be no record of the buyer accessing the national data-base at the Federal Revenue Service with the access keys on the DANFE and DACTE. The buyer/reseller would also not have a NF-e and CT-e for the resale and re-shipment of the goods back to state A (which according to the attempted fraud was *supposed to be happening)*. In addition, there would be a transport transaction from the seller in state A to the true buyer in state A for which there would be no CT-e on file at the Federal Revenue Service.

When de Mello, Dias, Fontana and Fernandez assess the effectiveness of Brazil's electronic tax documents against intra-state tax fraud they underscore that it is the *real-time control* that this system gives over commercial information flows that is the key to its success.

> On the side of the Tax Authorities, NF-e [and CT-e] represents an important tool to fight against tax evasion, as *it permits control, in real time, of the information on the commercial transactions* performed by the companies and as it permits the integrated work between the Federal and State Tax Authorities, upon the interchange of information.
>
> These electronic documents have common information and CT-e has fields that may refer to NF- e, … [listing a large number of common data fields].[20]

Application to refund fraud. Under the *Refund Fraud? Real-Time Soulution!* proposal each employer/payer issuing a W-2 or 1099 will be required to have these documents digitally signed when they are completed. 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.

---

[19] Alan Schenk & Oliver Oldman, VALUE ADDED TAX – A COMPARATIVE APPROACH 383 at n. 75.
[20] Newton Oller de Mello, et. al., *supra* note 14, at 454 (emphasis added).

There are six "critical data elements" in each of these documents.[21] Along with these data elements the employer/payer will be required to enter into the encrypting hash function three additional items of identifying data:

(a) a code identifying the individual who performed the encryption,

(b) the date and time that the encryption was performed, and

(c) the place within the numeric sequence of encrypted documents where a specific cryptographic procedure was carried out.

These last elements are normal bookkeeping controls in most corporate accounting departments. It is important for the company to know for example, that Mary Smith, an authorized payroll employee, was processing a specific W-2 for a specific employee on January 5 at 10:00 am and that this was the 500th W-2 processed this year. The IRS also needs to know that an authorized employee, and not an intruder drafted a specific W-2 or 1099.

The encrypting algorithm will be determined by the IRS and will be provided to the employer/payer. Under the Brazilian model this would be done through a secure transmission to an IRS web site. All required data would be in an XML file. The IRS will take this data, 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 taxpayer's input.

When a return is filed with an attached W-2, or an e-filed return is submitted, or when an independent contractor is declaring income from Form 1099-MISC it will be a

---

[21] The critical elements on an W-2 are:

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

The critical elements on a Form 1099 MISC are:

(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) numerical values (there could be up to eighteen) including the stated amount of:
- rents,
- royalties,
- other income,
- fishing boat proceeds,
- nonemployee compensation, excess golden parachute payments, etc.

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

simple automated matching process for the IRS to confirm the data represented on the return, and the data previously submitted and digitally signed through the Service's web site. Fabricating income (to qualify for Earned Income Tax Credits, the Child Tax Credit or the Additional Child Tax Credit), or fabricating income withholding amounts, or creating entirely fictitious returns will be impossible.

If the IRS follows the Brazilian model precisely, then the true W-2 or Form 1099-MISC will not be the form downloaded by the employer/payer, or provided to the employee, or attached to a return. The true document will be the digital document in the IRS database. What the employer/payer and employee/payee receive is only a copy. Like the Brazilian NF-e and CT-e, the only valid income and withholding amounts are the amounts recorded in the IRS database.

QUEBEC/BELGIUM

The Province of Quebec and the Belgian tax administration have both developed high-tech solutions that authenticate and preserve transactional data generated by electronic cash registers (ECRs)/point of sale (POS) systems to combat cash and credit/debit card[22] skimming frauds in retail sales.[23] Data manipulation by fraud-facilitating programs added to the ECR/POS system is the key to pulling these frauds off. Both the Quebec and Belgian solutions to this fraud involve encrypting transaction data and digitally signing sales receipts. The encryption modules secure the data on the business premises.

Although similar to the Brazilian solution, neither the Quebec nor the Belgian solution is Internet-based. Neither uses a remotely accessed, centralized (government operated) encryption facility. By performing the encryption locally the Quebec and Belgian models offer flexibility, freedom from Internet bottlenecks, and limitations caused by server capacity.

The Quebec approach differs from the Belgian in the manner in which the encryption is controlled and coordinated. In the Quebec model the security module (hardware and software) is under strict government control, whereas under the Belgian system the hardware can be manufactured by many third parties (to government specification), but the software and system activation mechanism are provided through a government issued smart card.

---

[22] At one time it was thought that this fraud only involved cash skimming. Recently it has become clear that this fraud has morphed into debit/credit cards sales when the card terminal is kept independent of the ECR/POS system. *New Regulations for Cash Register Systems* (*Nytt regelverk for kassasystemer*) at 57-58 (in Norwegian, translation of file with author) and proposed Checkout System Regulations (*Kassasystemforskriften*) § 2-5, second paragraph; § 2-8-3 and § 2-8-2(g), and proposed Bookkeeping Regulations (*Bokforingsforskriften*) § 5a-2, second paragraph; § 5a-14, third paragraph.

[23] For a discussion of the fraud technology, called Zappers, and the technology solution in Quebec see: Richard T. Ainsworth & Urs Hengartner, *Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud with Technology*, 57 CANADIAN TAX JOURNAL 719 (2009). For a companion study of the Zapper problem in the EU see: Richard T. Ainsworth, *Zappers - Retail VAT Fraud*, INTERNATIONAL VAT MONITOR (May/June 2010) 175.

Quebec. On January 28, 2008 the Quebec Minister of Revenue, Jean-Marc Fournier, responded to reports of significant fraud in the restaurant sector by announcing a data encryption pilot program.[24] The pilot began the next year followed by a mandatory rollout of the system in all provincial restaurants by November 1, 2011.[25] An estimated $425 million was being lost to fraud.[26]

Current estimates are that 70% of the lost tax is being recovered after the adoption of encryption modules, and without significant extra audit involvement. The reason for this success is apparently that the restaurant business owners are aware that all sales are being permanently recorded.[27] There are penalties for restaurateurs who make sales without entering them in the cash register system, so the recording is nearly assured.

Today, in every restaurant in the province Revenue Quebec has placed its microcomputers (*module d'enregistrement des vents* [MEVs], or sales recording modules).[28] They sit between the ECR/POS system and the restaurant's receipt printer.[29] All restaurants are required to issue paper receipts.[30] The MEV receives data[31] from all transactions (guest checks, register receipts, or credit notes), and produces a digital fingerprint (and a digital signature of the fingerprint). The signature is transmitted to the printer for inclusion on the receipt.[32] An auditor uses a scanner to verify that a receipt is

---

[24] Revenue Quebec, Press Release, Jean-Marc Fornier, *Pour plus d'équité dans la restauration : il faut que ça se passe au-dessus de la table* (For more equity in the restaurant sector it is required that [business is conducted] above the table) *available at* : http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp. See also the accompanying powerpoint presentation, *Tax Evasion in Quebec: Obligatory Billing in the Restaurant Sector – Under-declaration of revenues in the restaurant sector*, 3 (January 28, 2008) (in French) (on file with author, with translation).

[25] Alison MacGregor, *Restaurant Owners Want Anti-fraud Rules to Include All Retailers*, THE MONTREAL GAZETTE (November 1, 2011) *available at*: http://www.montrealgazette.com/business/Restaurant+owners+want+anti+fraud+rules+include+retailers/5634583/story.html

[26] *Supra* note 24 and accompanying powerpoint presentation.

[27] Personal e-mail communication, Gilles Bernard Assistant Director General Ministry of Revenue, Quebec (December 13, 2010) (indicating that estimates of losses were $420 million, and recovery is at $300 million or approximately 70%).

[28] Physically, the MEV looked like a relatively small 2 x 1 x 6 inch metal box that was connected to the printer and the ECR by standard cables.

[29] After the pilot project has ended, implementation of the device in all restaurants will take place gradually during 2010 and 2011.

[30] There are significant penalties for failing to issue receipts. The 2006-2007 Budget for Quebec indicated:

> Restaurant operators who fail to remit an invoice to a customer will incur a penalty of $100 as a result of this omission and will commit an offence for which they will be liable to a fine of no less than $300 and no more than $5,000. For a second offence committed within five years, the fine will be no less than $1,000 and no more than $10,000, and for any subsequent offence within that period, no less than $5,000 and no more than $50,000.

FINANCE QUEBEC, 2006-2007 BUDGET: ADDITIONAL INFORMATION ON THE BUDGETARY MEASURES 144-45 (Mar. 2006).

[31] Revenue Quebec will not disclose the data elements that are selected for encryption. It is "confidential for security reasons." Marc Simard, personal e-mail communication August 10, 2009 (on file with author).

[32] Marc Simard, Direction de la recherche en technologies liées au contrôle fiscal (DRTCF), Revenu Québec, explained in a personal e-mail (August 7, 2009) (on file with author) that,

accurate, that it was produced by the specific MEV registered to this business, and that the MEV has not been tampered with. The device internally preserves an encrypted record of all transactions for seven years.[33] Restaurants are required to submit sales summaries, generated by the MEV, when they submit their tax declarations. Auditors can also check systems on site.

Belgium. Belgium is concerned about the same fraud in its restaurant sector and is advancing a similar solution – a module permanently placed between ECR/POS systems and the receipt printer. Unlike Quebec, which controls (and pays for) the manufacture and installation of MEV hardware and software, Belgium instead sets hardware specifications for commercial manufacture, and provides encryption software in a smart card. Belgium had considered adding a feature that would remotely transmit results to the tax administration directly from the modules. This adaptation has been abandoned, but is available commercially.[34]

The Belgian device is tentatively set for first installations in October 2012, with full implementation completed by January 1, 2013. When a Belgian device come from the manufacturer it will be activated by insertion of a tax administration issued smart card and a PIN.[35] The smart card contains the encryption algorithm along with name address

---

> In addition to ensure the integrity of the information presented on the receipt, the solution designed by Revenue Québec ensures that the bar-code scanned by the hand-hold reader is produced by the certificate delivered by RQ to the specific MEV which generates this signature. The signature is produced by a combination of SHA-256 and ECC-224.
>
> This method uses a certificate which includes a public and a private key issued for each MEV with information that identifies the MEV and the restaurant.
>
> We choose the elliptic curve algorithm (ECC) to reduce the length of the result (to be converted to a barcode) and to maintain a good strength. The efficiency of ECC is well-known, since it provides similar cryptographic strength as RSA but uses shorter keys. For our case, ECC with a 224-bit key size provides similar strength to RSA with a 2048-bit size (see NIST-800-57 http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf).

[33] Revenue Quebec, *Tax Evasion in Quebec* (powerpoint), *supra* note 24 at slides 6-8.

[34] As of March 15, 2012 final Belgian regulations have not been released. There are strong indications from the Belgian Ministry of Finance that the remote access aspect of the early regulations has been dropped due to political and privacy concerns. Final regulations were expected in December 2011. Drafts however, have for some time been the topic of inter-governmental studies, and academic commentary. *See*: the Norwegian study *New Regulations for Cash Register Systems* (*Nytt regelverk for kassasystemer*) at 37-39 (in Norwegian, translation of file with author), and a Dutch Master's thesis by M. Leurink, *Beheersmaatregelen ter Voorkoming en Bestrijding van Datamaipulatie in Afrekensystemen* (Management Measures to Prevent and Combat Data Manipulation in Cash) (March 2011) at 36-44 (in Dutch, translation on file with author) *available at*: http://www.keurmerkafrekensystemen.nl/wp-content/uploads/2011/05/Beheersmaatregelen_tav_datamanipulatie_afrekensystemen_Leurink_mrt2011.pdf

[35] The PIN could be user-specific. A specific employee could be PIN-authorized to use the SDC and the authorization could be further limited to a certain number of uses per PIN (measured by the number of W-2s or 1099s the individual was responsible for processing. Alternatively, multiple smart cards could be approved to work with a single SDC, and then a PIN/smart card combination could be required to perform encryption. These are security issues that are easily resolved in the industry.

and TIN of the business. Once activated, the smart card will be permanently "locked" to the device.

As with the MEV, the Belgian device will print on each receipt an encrypted alpha-numeric string and bar code that includes the taxpayer's identity, the serial number of the device along with the date and time, each item purchased, the price, tax amount and method of payment. In addition to digitally signing the receipt the Belgian device will store encrypted data for five to ten years.[36]

Application to refund fraud. Under the *Refund Fraud? Real-Time Soulution!* proposal each employer/payer issuing a W-2 or 1099 will be required to have these documents digitally signed. The same signature considered under the Brazilian-type of solution would be required under a Quebec/Belgian-type of solution. It would include the same three administrative elements and the six critical data elements of these tax forms.[37]

To implement this solution the IRS will mandate that employers/payers or their third-party payroll providers acquire a device like either the MEV (which is government issued) or the Belgian device (which is privately purchased, manufactured to government specification, and activated with a government issued smart card). The device would encrypt the data elements 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.

The encrypting algorithm will be determined by the IRS and provided to the employer/payer on the smart card that activates the module. Because smart cards are permanently locked in a Belgian-type device or permanently embedded in a Quebec-type device the IRS will need to adopt procedures to randomly switch-out devices if a security breach is suspected.

As with the Quebec and Belgian modules the IRS could determine if a device had been tampered with by reading an error notification embedded in any digital signature, as well as by directly accessing a data-feed from the module either on site or transmitted to a remote location. Each day, or on a regular schedule determined by the IRS, the module should be required to transmit a full report of encrypted activity over a secure Internet link. The digital signatures of the transactions reported by the module will be retained in IRS data-bases as well saved within the module itself. When a tax return if filed with a W-2 attached, or where an independent contractor submits a Schedule C, the W-2 will be

---

[36] Marlies Leurink, *Beheersmaatregelen ter Voorkoming en Bestrijding van Datamanipulatie in Afrekensystemen* (Management Measure to Prevent and Combat Data Manipulation in Cash Register Systems (March 2011) (in Dutch, partial translation with author) *available at*: http://www.keurmerkafrekensystemen.nl/wp-content/uploads/2011/05/Beheersmaatregelen_tav_datamanipulatie_afrekensystemen_Leurink_mrt2011.pdf.

[37] *Supra* note 21.

self-certifiable through the encryption, and the Schedule C income will be confirmed through a simple data-input from the face of the return.[38]

CONCLUSION

The VAT has developed a wealth of advanced technology solutions to tax administration problems. It may be that the absence of a VAT in the U.S. makes these applications a little bit difficult to see from the IRS offices in Washington, D.C., but we should look nevertheless.

Document authentication is critical to the functioning of the VAT, and the burden of millions of invoices, monthly returns, statements and reconciliations has pushed VAT jurisdiction into technological solutions that are very different from what is being considered in the U.S. These solutions work. They are tested and have been found to be effective against serious VAT fraud.

The U.S. does not have a problem similar to Brazilian "invoice sightseeing." However, the Brazilian solution to it is very applicable to refund fraud in the U.S. The reason is that the core problem in both of these frauds is document authenticity.

The U.S. also lags behind most other countries in the pursuit of zapper software. The IRS only gets concerned about zappers in instances where the fraud seriously impacts a taxpayer's *annual* income.[39] However, the same problem in Quebec and Belgium is being attacked aggressively with technology. These solutions are also very applicable to refund fraud in the U.S. Once again, the basic problem is verification of tax documents.

Thus, it is easy to see how certain tax problems and their technological solutions are not on the IRS radar screen, and how others fly just below it. The IRS has an understandable blind spot when it comes to thinking about the VAT, but it needs to look

---

[38] It may be necessary to move some data fields to the face of form 1040 to facilitate data input, but the thrust of the forms revision should closely track the data needs of the security system.

[39] For example, there are only three reported cases of zappers in the U.S. In the Province of Quebec there are 250 litigated cases. The reason is simple. It is not that there are no zappers in the U.S., quite the contrary. The literature indicates that they are a computer application pioneered here and then exported globally. The reason is that zappers are considered to be a state and local problem centered around the retail sales tax.

The three U.S. zapper cases are: (1) Stew Leonard's Dairy in Danbury Connecticut. *See*: U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), *aff'd.* 67 F.3d 460 (2nd Cir. 1995) (although the tax case was settled, the details of the fraud are preserved in these federal sentencing appeals - $17 million sales skimmed over a 10 year period, with sales tax losses of $500,000 and a final determination of $1.4 million); (2) the LaShish restaurant chain in the Detroit, Michigan. *See:* Press Release, U.S. Dept of Justice, Eastern District of Michigan, *Superseding Indictment returned Against LaShish Owner* (May 30, 2007) (indicating that $20 million is cash sales were skimmed over a 5 year period); and (3) Theodore R. Kramer who installed zappers in Detroit, Michigan area strip clubs – although in this instance the tax amounts lost are not specified. *See*: U.S. Dept. of Justice, Eastern District of Michigan, *Michigan Software Salesman Pleads Guilty to Conspiracy to Defraud the Government* (November 17, 2010).

carefully at VAT solutions nevertheless. Some times what has been developed in the VAT can be very usefully in an income tax context.

Thus, from a comparative tax administration perspective, the VAT has a lot to offer the U.S.