2-16-2009

Quebec's Module D'Enregistrement Des Ventes (MEV): Fighting the Zapper, Phantomware and Tax Fraud with Technology

Richard Thompson Ainsworth

QUÉBEC'S *MODULE D'ENREGISTREMENT DES VENTES (MEV)*: FIGHTING THE ZAPPER, PHANTOMWARE AND TAX FRAUD WITH TECHNOLOGY

Boston University School of Law Working Paper No. 09-09
(February 16, 2009)

Richard Thompson Ainsworth

QUEBEC'S *MODULE D'ENREGISTREMENT DES VENTES* (MEV): FIGHTING THE ZAPPER, PHANTOMWARE AND TAX FRAUD WITH TECHNOLOGY

Richard Thompson Ainsworth

On January 28, 2008 the Quebec Minister of Revenue, Jean-Marc Fournier, announced[1] that by late 2009 the MRQ will begin testing a device, the *module d'enregistrement des ventes* (MEV)[2] that is projected to substantially reduce tax fraud in the restaurant sector. By 2010 or 2011 MEVs will be mandatory in all Quebec restaurants, where they will assure accuracy and retention of business records within electronic cash registers (ECRs).

It is clear to the Minister that not only are large volumes of cash being skimmed, removed from the sales and profits records of restaurants by their owners, but also that this fraud against the public fisc is increasingly facilitated by technology – through the digital manipulation of business records kept by modern ECRs. Add-on software (zappers), factory or distributor installed software, and old fashioned manual re-programming of ECRs (phantom-ware) are the mechanisms through which the manipulations arise. Known generally in Quebec as *camifleur de ventes* (or sales zappers), the MRQ has pursued these devices over the past decade, and is convinced that something more than a traditional audit is needed to counteract the manipulations.

Based on more than 230 cases since 1997, and surveys of skimming activity in the restaurant sector, the Minister summarizes the situation as follows:

> Although the majority of restaurateurs comply with their tax obligations, the restaurant sector remains an area of the Quebec economy where tax evasion is rampant, both in terms of income tax and sales taxes. Tax losses in this sector are important. Quebec Revenue estimates that they are $ 425 million for the 2007-2008 fiscal year.[3]

The zappers (and phantom-ware applications) that are the major facilitators of this fraud are not confined to Quebec. Zappers and phantom-ware have spread throughout Canada[4] and around the world. It is not surprising therefore that a number of jurisdictions have looked at automated sales suppression and have adopted technological countermeasures, some of which

---

[1] 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) (Jan. 28, 2008) *available at* : http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp (last visited August 7, 2008, translation on file with author).

[2] Jean-Marc Fornier, *L'évasion fiscale au Québec : Facturation obligatoire dans le secteur de la restauration – Sous-déclaration des revenus dans le secteur de la restauration* (Tax Evasion in Quebec : Obligatory Billing in the Restaurant Sector – Under-declaration of revenues in the restaurant sector) 3 (January 28, 2008) (in French) (powerpoint presentation and translation on file with author).

[3] *Id.*

[4] Canada Revenue Agency, Tax Alert, *Businesses Warned Against Using Tax Cheating Software,* (Dec 9, 2008)

> The Canada Revenue Agency (CRA) is aware that electronic sales suppression software is currently being marketed and sold to Canadian businesses. Business owners are reminded that hiding income to evade taxes is against the law. Using this software is not worth the risk. … Businesses that have used electronic sales suppression software are suspected of having hidden thousands of transactions and millions of dollars in sales.

Available at: http://www.cra-arc.gc.ca/nwsrm/lrts/2008/l081210-eng.html (last visited Dec. 25, 2008)

are strikingly similar to the MEV. Other jurisdictions look to technology for answers, but differ with respect to the sophistication of the technology they would deploy. In yet other jurisdictions, traditional audit rather than technology is preferred – but the most successful of these "audit only" jurisdictions are adopting comprehensive (multi-tax) audit strategies with teams of auditors supported by computer specialists – in effect, a "super-sized" traditional audit.

This paper moves beyond a discussion of the variety of sales suppression programs in use – zappers and phantom-ware. Those matters have been considered elsewhere.[5] The concern here is on enforcement efforts, particularly the MEV. The intent is to assess the workability and effectiveness of the MEV solution by contrasting it with solutions adopted elsewhere.

ENFORCEMENT EFFORTS – GENERALLY

Two policy orientations guide enforcement actions in this area – one approach is rules-based; the other is principles-based.[6] They are not mutually exclusive – degrees of blending are common. Rules-based jurisdictions adopt comprehensive and mandatory legislation regulating, and/ or certifying cash registers. Jurisdictions taking this approach include Greece and Germany. With the adoption of the MEV, Quebec will also fall within this group. These jurisdictions are classified generally as "fiscal till" or "fiscal memory" jurisdictions.

Principles-based jurisdictions rely on compliant taxpayers following the rules. Compliance is enforced with an enhanced audit regime. Comprehensive, multi-tax audits (the simultaneous examination of income, consumption and employment returns) are performed by teams that include computer audit specialists. Audits are frequently unannounced and preceded by undercover investigations that collect data to be verified.[7] Jurisdictions taking this approach include the UK, Canada, and the Netherlands. France has implemented a program of preventive audits that target technology providers.[8] A similar effort can be found in Quebec where the

---

[5] Richard T. Ainsworth, *Zappers and Phantomware: The Need for Fraud Prevention Technology*, 50 TAX NOTES INT'L 1017 (JUNE 23, 2008); Richard Thompson Ainsworth, *Zappers and Phantomware: Are State Tax Administrators Listening Now?* 49 STATE TAX NOTES 103 (Jul. 14, 2008); Richard T. Ainsworth, *Zappers: Technology-assisted Tax Fraud, SSUTA and the Encryption Solutions*, TAX LAWYER (forthcoming 2009); Richard T. Ainsworth & Hiroki Akioka, Electronic Tax Fraud – Are there Zappers in Japan? (KANSAI U. REV. OF ECONOMICS, *forthcoming* 2009).

[6] Fiscalis Committee Project Group 12, Cash Register Project Group, *Cash Register Good Practice Guide*, 5-6 (Dec. 2006) (unpublished report on file with author).

[7] For example, the recent Canadian investigation in British Columbia into alleged distribution of sales suppression software by InfoSpec Systems Inc. involved an eight month undercover investigation by the Royal Canadian Mounted Police (RCMP). During this phase of the operation undercover RCMP officers posed as potential buyers of sales suppression software. This evidence supported allegations that InfoSpec Systems Inc. knowingly provided restaurants with zappers. Canada Revenue Agency, News Release, *Charges Laid in Large-Scale Tax Fraud Investigation* (Dec. 10, 2008) *available at*: http://www.cra-arc.gc.ca/nwsrm/rlss/2008/m12/nr081210-eng.html (last visited Dec. 25, 2008).

[8] Fiscalis Committee, *supra* note 6, at 6. This is the approach that Revenue Canada took in the InfoSpec Systems investigation. Targeting the software program (Profitek) "… documents, CDs, computer files, sales notebooks,an electronic calendar, e-mail and other client lists …" the CRA was able to conduct a nation-wide investigation which (according to the Vancouver Sun) is "… continuing and [CRA officials] expect more charges to be laid." Darah Hansen, *Cooking the Books: Four local restaurants are alleged to have been part of a high-tech scheme to evade tax on millions of dollars. Five people face 25 charges after nationwide investigation – but it's a worldwide problem,*

customer lists of audited technology providers have been used to roadmap later audits of businesses suspected of technology-assisted skimming.[9] Prior to the adoption of the MEV, Quebec fell squarely within a principles-based classification. Moving forward, Quebec will merge both approaches, even though it appears that Revenue Canada will continue to pursue only principles-based enforcement techniques.[10]

Notably, the US does not have a coordinated zapper enforcement effort.[11] In fact, the US has only uncovered two zappers, one at Stew Leonard's Dairy in Norwalk Connecticut where $17 million in was skimmed,[12] and the other at the LaShish restaurant chain in Detroit Michigan where $20 million in cash sales were zapped and allegedly sent to Hezbollah in Lebanon.[13] The US is particularly hampered in its approach to zappers – federal income tax audits are not well coordinated with state and local retail sales tax audits. In addition, computer audit specialists are not normally assigned to audits of small and medium sized enterprises (SMEs), and this is where the zappers are.

Nevertheless, if the US became serious about this problem it might have a unique blend of rules and principles based solutions in an extension of the Streamlined Sales and Use Tax Agreement (SSUTA).[14] Under the SSUTA certified third party software providers (CSPs)[15] could be tasked with assuring ECR accuracy. Not only is the SSUTA legal framework operational, but at present levels of technology a CSP could readily assure States that the correct retail sales tax was being collected and remitted, while it could assure federal authorities that

---

VANCOUVER SUN (Dec. 11, 2008) *available at*: http://www.canada.com/vancouversun/story.html?id=6c945ca6-f84a-43f6-86ad-221814731593&p=2.

[9] For example see the investigation of Audio Lab LP, Revenue Quebec, News Release, Revenue Quebec Investigation of a Software Designer Outlet Suspected of having Developed and Distributed Zappers (Oct. 14, 2005) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/14oct(2).asp (in French only, last visited Feb. 8, 2008); the investigation of Michael Roy, Revenue Quebec, News Release, Fines of more than One million dollars – A Father and his Two Sons convicted for Tax Evasion in connection with the Zapper (May 2, 2003) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/02mai.asp (in French only, last visited Feb. 8, 2008).

[10] In its recent Tax Alert dealing with sales suppression software the CRA emphasized that has "… over 5,000 employees dedicated to finding unreported business income and ensuring that the proper amount of taxes is paid, even when sales records are missing." Canada Revenue Agency, Tax Alert *supra* note 4.

[11] The *Stew Leonard's Dairy* case came about when a US Customs officer inspected a suitcase carried by Mr. Leonard on one of his trips to St Martin. *Leonard*, 37 F.3d at 35; The *La Shish* case came about because the owners failed to file a tax return. Furchgott reported that, "[a]uthorities declined to comment on how the reported crime was discovered, but according to court records, Mr. Chahine failed to file a tax return in 2003." Roy Furchgott, *With Software, Till Tampering Is Hard To Find*, NYT C6 (August 20, 2008).

[12] U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), *aff'd.* 67 F.3d 460 (2nd Cir. 1995) (details of the tax fraud are preserved in these appeals of the sentence).

[13] Press Release, U.S. Dept of Justice, Eastern District of Michigan, LaShish Financial Manager Sentenced for 18 months for Tax Evasion (May 15, 2007) *available at*: http://www.cybersafe.gov/tax/U.S.aopress/2007/txdv072007_5_15_ElAouar.pdf (last visited Feb. 3, 2008).

[14] Streamlined Sales and Use Tax Agreement (adopted November 12, 2002, amended November 19, 2003 and further amended November 16, 2004) § 203 (defining a CSP as "[a]n agent certified under the Agreement to perform all the seller's sales and use tax functions, other than the seller's obligation to remit tax on its own purchases.") *available at* http://www.streamlinedsalestax.org.

[15] *Id.*, at § 203 (defining a CSP as "[a]n agent certified under the Agreement to perform all the seller's sales and use tax functions, other than the seller's obligation to remit tax on its own purchases.")

zappers were not being used to underreport income. Certification of the CSP would need to be undertaken jointly (by state and federal agencies) as would oversight of their operation. Quebec has not considered a SSUTA/ CSP solution, but it might look at this option if it were to consider extending the MEV outside the restaurant sector.

STRUCTURE OF THE ARGUMENT

This paper will first present a rough schematic of a how a zapper facilitates a skimming fraud. Then it will consider three rules-based enforcement approaches: the Greek "fiscal electronic devices" or FEDs, the Quebec MEVs and the German "smart cards." Then it will examine the Dutch principles-based approach which is favored by the UK. A final section will consider how CSPs in a SSUTA framework could be used to achieve similar outcomes under a blended rules-based/ principles-based approach. Comparisons will be made throughout.

SCHEMATIC OF SKIMMING WITH ZAPPERS

Seven basic steps occur when cash purchases are zapped. It is helpful to set these steps out clearly before considering the enforcement actions that are directed against sales manipulation. This will not only help explain what a zapper does to facilitate skimming, it will illuminate the enforcement points that tax authorities press on to prevent zapping.

.

(1) a consumer[16] identifies goods or services for purchase;

(2) a cashier, waiter, or other sales associate produces a pro-forma bill[17] and presents it to the consumer for approval;[18]

(3) the consumer approves, offers to pay in cash,[19] and the pro-forma bill is finalized (agreed upon);

(4) the cashier "rings up" the sale in the ECR, generates an itemized record of each good or service sold;

(5) the ECR then directs the printer to issue an itemized paper receipt (invoice) for the customer that will include:

(a) a list of the items purchased;

---

[16] Zapping is associated with cash skimming frauds. It occurs in B2C transactions. B2B transactions are not vulnerable (unless under the retail sales tax some business transactions are included in the tax base). Under a VAT tax is imposed at each commercial stage, but each input tax is offset with an output tax and if records at one stage are fraudulent the records at the next stage would reveal this. Zapping would be pointless.

[17] This may occur by scanning a bar code, directly entering a PLU number, or by entering the name of an item (perhaps by pressing a touch screen).

[18] In a restaurant context this "pro-forma billing event" may or may not be noteworthy, but it occurs nevertheless. If a customer orders directly (and only) from the menu presented by the waiter, the pro-forma bill may be first drafted in pencil and then transferred to a digital ordering system associated with the ECR. In other instances a customer may begin a meal with an initial entre and then progressively order increased amounts of food and drink throughout the evening. The waiter would keep a running tally of the bill. It would be common in this case to present one or more pro-forma bills at various times to keep the customer aware of the total amount due.

In a grocery store context an itemized pro-forma billing is frequently visible on a LCD screen that the cashier and the customer can see as items are run through a scanner. All modern ECRs have the capability to present this pro-forma bill in formal and informal manners. The important point is that the pro-forma bill can be changed before the sale is "rung up." Changes occur by the customer and the operator acting in concert.

[19] Zappers target cash sales, because credit, debit, check or bank transfer transactions leave an audit trail.

(b) a price for each item;

(c) a taxability determination for each item;

(d) a segregated tax amount for each of the taxed items (in instances where all items at an establishment are taxed and taxed at the same rate – as they would be at a restaurant, for example – this function would be performed in aggregate);

(e) the amount of cash tendered;

(f) the net amount returned to the customer in change;

(g) the date and time of purchase;

(h) the name, address and identification number of the vendor;

(i) the receipt (invoice) number of the transaction.

(6) a series of electronic reports are now generated, based on transactions sent through the ECR. These reports are relied on by compliance auditors. The reports are:

(a) the daily Z Report (with re-set functionality);[20]

(b) the X Report;[21] and

(c) the Electronic journal.[22]

If, after step (6), we assume that a zapper is inserted in the ECR (or POS system), then we have a step (7) where we are able to eliminate from the ECR and the enterprise's business records all traces of (some or all) cash sales without fear of leaving a digital record of the manipulation. Phantom-ware applications would do the same thing, except their programming is embedded in the ECR's operating system, not temporarily added and then removed from the ECR.

At this point the customer has in his hands an accurate receipt (from step (5)), but the zapper is re-writing the internal memory of this receipt in the ECR – including the records in the Z Report, the X Report and the Electronic Journal. This re-writing creates a new sales profile within the ECR. Selected cash sales are omitted. For example, the ticket files (the digital record of specific invoices issued in sequence) would be renumbered if an entire ticket were eliminated. If only some items are removed from some tickets, or if a price is changed for an item on a

---

[20] One of the most important functions of a cash register is to record sales, taxes collected, media totals, discount, voids, and more. The report printed at the end of day or shift that reports this information and resets it for the next day or shift is known as the "Z" report. The "Z" report function prints the sales on the cash register tape while erasing the data from the memory. A "Z" is a once only report for a set period of time. Many cash registers have "Z2" feature that allows "Z" reports to be added together. When an operator "Z2's them out" they will erase these reports for a longer period of time. An example of a "Z2" report is a monthly report that will be used to date and record monthly cash register sales. Every time the register is "Z'd out" (Report taken) that total is erased from the daily sales files and added to the "Z2" file.

[21] "X" reports are the identical in information and time span to the "Z" reports. "X" reports runs only provide reports; they do not reset, or clear the memory. "X" reports can be taken as often as needed with no effect on sales data recorded.

[22] *See supra* note6, *Cash Register Good Practice Guide*, Appendix G, at 1.2.

> The electronic journal usually contains ALL transactions keyed into the more complex types of till systems and is therefore the definitive record to obtain for audit purposes. There are exceptions, where Electronic Journals can be programmed "not-to-store" certain keying transactions e.g. "Training Mode."

The Electronic Journal should not be confused with the "Z" tape as it is not a recap of the day's sales. The Electronic Journal tape is supposed to be a "blow-by-blow" record of every transaction made "step-by-step." It is most useful for going back during a day to look for mistakes that were made. This journal has been a staple in the cash register industry since the beginning. It can be used to check the Z report.

specific ticket, then amounts due will be re-calculated (and a new tax due determined). The altered ticket files will now confirm the altered Z Report, X Report and Electronic Journal. The ECR's records will not match customer receipts, but the records of the ECR will be internally consistent.

Thus, one of the common (traditional audit) approaches to detecting a zapper is for an audit team to visit an establishment suspected of using a sales suppression device (in advance of the audit), make cash purchases, save the receipts, and then try to match the receipts with the digital files in the ECR. This is in fact how MRQ uncovered its first zapper in 1996.[23]

The next thing to notice is that it is easy to skim sales without zapping. This can be done at step (2), but it requires collusion between the vendor and the customer. A consumer tendering cash could be orally offered a lower price (perhaps a tax-free price) when the pro-forma invoice is drafted. If the customer agrees, the sale would simply not be "rung up." As a result, no record of the actual (finalized) transaction would appear in the daily Z Report, or the X Report.

It is possible that the Electronic Journal might preserve a "trace" of the original transaction (if the pro-forma was drafted with the assistance of the ECR). The transaction would appear as an aborted sale. It would look to the auditor as if the customer declined the purchase when they saw the pro-forma invoice. In a restaurant context too many aborted sales might raise suspicions, because normally the meal has already been consumed. However, in a grocery or convenience store, a hairdresser's, or a butcher's shop where the custom might be to discuss a transaction based on a pro-forma invoice nothing might seem amiss at all.

Some fiscal till jurisdictions try to block frauds at step (2) by preserving each key stroke in the Electronic Journal. These jurisdictions certify each ECR. Tamper-proof Electronic Journals are made a requirement of certification.

The third thing to notice is that there is a period of time (after the sale is completed at step (3), but before the zapper is inserted) where the records within the ECR are complete and accurate. This period lasts at least up to step (5) – the point where the ECR directs the printer to issue an invoice for the customer. These records need to be accurate because the customer is demanding an accurate invoice.

As a result, many fiscal till jurisdictions focus on preserving tamper-proof invoices, and the sequencing of those invoices at step (5). This is, in fact, what the MEV does. The MEV makes every receipt useful for checking the ECR. For example even a credit card transaction (which was not tampered with) can provide evidence of manipulation, if an auditor can tell that the receipt was re-numbered. The MEV will indicate that some other receipt further up the chain is missing, and an auditor would then begin the search for the missing cash transactions.

Principle-based jurisdictions focus on this same point, step (5), but they need to directly find an altered receipt. Without an MEV it is difficult to tell if a sequence of receipts has been manipulated. This makes pre-audit cash purchases and saved receipts a critical component of a

[23] Ainsworth, *Zappers and Phantomware: Are State Tax Administrators Listening Now? supra* note 5, at 104, n.5

principles-based auditor's work-plan. Traces of a zapper can also be found by computer specialists examining the Electronic Journal as well as the X and Z reports produced at step (6).

A final thing to notice is that all critical elements of the tax return (at least all elements that would be derived from a specific ECR) are available at step (5). The items purchased [step 5(a)], the price charged [step 5(b)], the taxability determination [step 5(c)], and the tax collected per item or per invoice [step 5(d)] are all available. In addition, the tax has been received.

Thus, it is entirely possible that fiscal till jurisdictions could require real time pro-forma returns based on these figures. They could also require real time remission of the tax. In a retail sales tax jurisdiction this might constitute the entire return and payment. In a VAT jurisdiction this would represent only the output portion of the return. The input VAT credits (deductions) would need to be gathered from other files.

FISCAL TILLS: GREECE, QUEBEC AND GERMANY

In addition to Greece, Quebec and Germany, fiscal till jurisdictions include Argentina, Brazil, Bulgaria, Italy, Latvia, Lithuania, Poland, Russia, Turkey, and Venezuela.[24] Setting the Greek and German regimes alongside Quebec's MEV provides sufficient illumination so that the MEVs attributes can be appreciated.

GREECE
FEDs; FECRs, AFED Printers; FESDs

Greece has had comprehensive, rules-based fiscal till legislation in place for over twenty years. Technical specifications for Fiscal Electronic Devices (FEDs) were published widely in 2004.[25] When considered as a whole, these rules attempt to provide data security both at stage (2) and stage (5). In other words, the Greek approach is to secure data when the pro-forma receipt is being generated, and when the printer is being directed to issue the final receipt.

Under Greek rules FEDs are divided into two categories: (a) fiscal electronic cash registers (FECR) which are accompanied by autonomous fiscal electronic device printers (AFED Printers), and (b) fiscal electronic signing devices (FESDs). The first are used *only* in B2C transactions; the second may be used in B2C or B2B transaction. Both digitally sign tax-related documents.

---

[24] *See supra* note6, *Cash Register Good Practice Guide*, Appendix D, at 1.

[25] A European directive (98/34/EC) requires that whenever a Member State adopts new technical rules, specifications, or legal requirements the Member State is obliged to announce this to the EU before the rules take effect. According to this directive there is a minimal standstill period of three months. During this period any Member State (or the European Commission) has the right to express a "detailed opinion." The issue of a detailed opinion extends the standstill period for another three months, and allows further consideration of the rules by all parties. Greece made the technical specifications for FEDs public in 2004. As a result, the Greek rules are well known not only within the EU but among the larger community of ECR manufacturers and distributors. They are available in Greek as well as in official translations in three other languages, and can be accessed on the internet.
English: http://europa.eu.int/comm/enterprise/tris/pisa/cfcontent.cfm?vFile=120040135EN.DOC
German: http://europa.eu.int/comm/enterprise/tris/pisa/cfcontent.cfm?vFile=120040135DE.DOC
French: http://europa.eu.int/comm/enterprise/tris/pisa/cfcontent.cfm?vFile=120040135FR.DOC

FECRs and AFED Printers. Fiscal electronic cash register (FECR) is a term that includes ordinary stand-alone cash registers, and cash registers equipped with advanced connection capabilities (network or PC operated machines). Autonomous fiscal electronic device printers (AFED Printers) are fiscal printers that operate only via a connected computer. They have no keyboard or display terminal. They do more than just print receipts however. AFED Printers store and secure in their fiscal memory the data that has passed through them (revenue from sales, and taxes collected).[26]

Data from the electronic journal memory is signed by a secure hash algorithm (SHA-1).[27] This hash value is permanently safeguarded and stored in the fiscal memory. Daily sums (receipts and VAT amounts) are saved into the fiscal memory, cumulatively and on a daily basis. This function essentially preserves the X and the Z Reports along with the Electronic Journal.

The cost of FECRs varies from € 200-250 to € 800-1,000 depending on the manufacturer.[28] Every manufacturer, developer, or importer of ECRs into Greece must seek approval for each specific model that they intend to sell in the Greek market.[29] A license to sell a specific ECR is issued by a special technical (inter-party)[30] body (committee) and will be issued only when the ECR conforms to all statutory technical specifications.[31] Applications are made to the Department of Fiscal Electronic Cash Registers and Systems of the Ministry of Finance and must be accompanied by a working model of the system for which a license is sought. The committee has authority to examine any additional data (including experience in the field, business solvency, creditworthiness, technical capacity of personnel), and has the authority to recall and cancel licenses in cases where material changes have been made in systems or in the conditions under which the license was granted.

---

[26] The FECR and AFED Printers must be equipped with either a 2-roll paper printing station, or a 1-roll paper slip printer station as well as a daily Electronic Journal (EJ) memory. [EJ memory is different from fiscal memory. EJ memory stores all information slips and tickets ("legal receipts") from the issuance of the previous Z Report until the issuance of the next Z Report. It is sometimes called the Temporary Daily Slip Storage Memory (TDSSM). "Fiscal memory" on the other hand, is the basic secure element in the Greek system. It is based on a ROM – Read Only Memory – chip that is securely placed within the fiscal cash register. Into this memory all important fiscal data is stored.] EJ memory is either pluggable/unpluggable or fixed. It resides in the fiscal device and is always a flash memory.

[27] The Secure Hash Algorithm (SHA-1) was developed by the US National Institute of Standards and Technology. SHA-1 is a widely accepted data encryption tool. It produces a 40-character string by hexadecimal symbols (20 bytes), and the string [or the "hash value"] uniquely defines the processed data [in the case of an ECR issuing receipts in B2C transactions this data is the values on the printed receipt]. SHA-1 is described in detail in the Federal Information Processing Standard 180-2 (August 1, 2002) *available* at: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf (last visited Aug. 8, 2008).

[28] Personal e-mail communication with Panos Zafiropolous (February 24, 2008) (on file with author).

[29] There are roughly 300,000 to 350,000 FECRs and POS systems with secure recording devices (FESDs) in Greece. The turnover of these devices is between 30,000 to 40,000 machines annually. There are over 300 different models of ECRs certified for use in the Greek market representing approximately 50 different manufacturers, importers and distributors. *Cash Register Good Practice Guide, supra* note 6, Appendix D, at ¶ 4.1.

[30] An "inter-party" body under Greek rules is a committee where each member is assigned by one of the political parties in the Greek parliament. Although the term of office is for two years, the composition of the committee will change as political power shifts in Greek elections.

[31] Technical specification change with advancing technology, and revisions to the law are made every two to four years. Guidance on these matters comes primarily from specialized laboratories of National Technical University of Athens (NTUA). The NTUA is also assigned by the committee to perform all the necessary evaluation tests to carried samples of FCRs.

Once a model has successfully passed all tests, the committee issues and gives to the interested company a unique license number for the specific model. The license number is recorded by the National Wide Information Center of the Ministry of Finance and is printed on each receipt ("legal receipt") issued in each retail transaction. In addition, this number is required to be placed on a label that is visibly fixed to each machine. As a result, the certification of a specific ECR can be checked both through a visual inspection of the machine and by matching the license number on a machine with a given receipt.

FESDs. Under Greek rules a business owner can choose to use either a FECR (an ordinary, inexpensive certified cash register), or a fiscal electronic signing device (FESD). If an FESD is selected it probably means that the owner has capabilities, technology skills or a budget allocation that would allow the use of a sophisticated computer system.

FESDs are designed for B2B applications. They are used primarily to e-sign invoices, but can be used for any tax document including a final retail receipt. FESDs are connected to an entrepreneur's computer system via a dedicated port (RS-232; Ethernet RJ-45; USB). A driver must be installed to allow the computer system to interface with the FESD. Essentially, the FESD functions as a virtual printer allowing the entrepreneur's back office software (ERP system or accounting software package) to function normally. However, every tax document required to be signed is diverted through the interface to the FESD where a signature is created (the SHA-1 algorithm is applied) and a hash value is transmitted to (and printed on) each document. The whole-day hash value is permanently saved in the FESD's fiscal memory.[32] This preserves all data on the document in detail.[33]

Presently the cost of an FESD is between € 450 and € 650. Thus, a FESD alone can cost more than a FECR, and for this reason smaller businesses do not normally use FESDs to issue legal receipts.[34] Economies of scale also come into the picture because a single FESD can support many cash registers linked on a network. It can be installed remotely (even in another city), and need not be directly connected to the point of sale terminal.

An FESD owner is obligated to preserve signed documents and to store them on a safe digital medium (optical or magnetic). Thus, auditors can check the integrity of these files by running the same algorithm (SHA-1) and comparing the new hash value against the existing ones secured within the FESD's fiscal memory.

How FECRs with AFED Printers and FESDs defeat Zappers and Phantom-ware. Because FECRs are certified for compliance with all technical specifications set out in Greek law – a law that is supported and updated regularly by the research laboratories of the NTUA – it is a very simple matter to determine if a specific ECR has been tampered with.

---

[32] From a hardware and a security perspective, there is very little difference between an AEFD Printer (with an electronic journal) and a FESD.

[33] Personal e-mail communication from Panos Zafiropoulos at item D (February 24, 2008) (on file with author).

[34] In an effort to mitigate the cost of FESDs the tax law allows owners to depreciate FESDs as fixed assets over three years. There is also a government loan program to assist in the purchase of all FEDs (FCRs; AEFD Printers; FESDs). The interest on these loans is subsidized at 3%.

Factory-installed phantom-ware must be removed before certification. If a self-help version of phantom-ware[35] is on the ECR it will either be blocked or, or there will be a record of the manipulation so that its impact on revenues will be neutralized. Only true data from real transactions will be preserved and SHA-1 encrypted in the fiscal memory. Use of an add-on zapper will be a violation of the licensing regulations. It will be detected in the same manner as self-help phantom-ware. Severe penalties apply, but detection does require an audit.

Through the certification process the Ministry of Finance preserves a copy of all approved firmware. It is a simple matter to calculate a checksum value (CRC-32[36] or SHA-1) for the object code of the firmware. Any auditor can then read the contents of the program memory of a certified ECR and determine if changes have been made in the firmware (through phantom-ware or zappers) by comparing his reading with that of the file kept in the Ministry of Finance.

FESDs accomplish the same result as FECRs. Neither phantom-ware applications nor zapper installations are effective when an FESD is installed. The FESD will sign each document and preserve an encrypted trace in the fiscal memory of the device. Deletion or manipulation of the records associated with cash receipts is no longer possible without detection.

Thus, if a Greek vendor produces a pro-forma receipt though an ECR the details of the pro-forma receipt will be recorded in the Electronic Journal. If the ECR is a FECR this data enters the Electronic Journal, and if the AFED Printer is set up to capture this data it will be preserved in the fiscal memory and signed with a secure hash algorithm (SHA-1). Thus, it will be possible to identify enterprises that routinely offered customers lower prices in exchange for voiding the pro-forma invoice at step (2). This would not be possible with FESDs. FESDs are virtual printers, and if data is not being sent to a printer an FESD would have no need to e-sign it.

Both of the Greek solutions are very effective at step (5) enforcement. If a receipt is printed both the FECR with an AFED Printer solution, as well as the FESD solution will assure tax authorities that the tax collected on cash transactions have been recorded. It is important to note however, that all of these efforts are directed only at accurate record retention. Returns must still be prepared and filed, payments remitted for the taxes due or collected, and the revenue authority still needs to audit to insure compliance. Admittedly, this audit should be easier, but it is still needed.

QUEBEC – MEVs

[35]For a discussion of self-help phantom-ware see: Richard T. Ainsworth, *Zappers and Phantomware: The Need for Fraud Prevention Technology*, *supra* note 5.

[36] CRC-32, or cycle redundancy check, takes as input a data stream of any length, and produces as output a value of a certain space, commonly a 32-bit integer. The term CRC is often used to denote either the function or the function's output. A CRC can be used as a checksum to detect alteration of data during transmission or storage. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channels. The CRC was invented by W. Wesley Peterson. W. Wesley Peterson & D. T. Brown, *Cyclic Codes for Error Detection*, 49 PROCEEDINGS INST. RADIO ENGINEERS 228 (Jan. 1961).

Quebec is responding to sales suppression fraud much like Greece has responded, but on a much more limited scale. The problem identified in Quebec is the widespread use of zappers and phantom-ware in the restaurant sector.[37]

Compared to the Greek situation, the Quebec solution (set to be fully rolled out between 2010 and 2011) is limited in two respects: (a) its scope is limited to the restaurant sector, and (b) its range is limited to an FESD-like solution. Quebec has specifically rejected the "FECR with an AFED Printer" type of solution.[38] Like Greece, Quebec approaches the sales suppression problem from an adequacy of business records perspective. But also like the principles-based jurisdictions (the UK and the Netherlands) Quebec supplements technology solutions with very aggressive traditional audits.

The first major legislative response to zappers in Quebec came in June 2000 when bookkeeping and record keeping requirements were enacted specifying that electronically stored data, together with the means to read that data formed part of a Quebec business' regular bookkeeping obligations.[39] Because zappers make digital records unreliable it was then easy to specifically prohibit the design, manufacture, installation, sale or lease of zappers in the Province.[40] The last step was a presumption of use rule. It states that whenever the MRQ finds a zapper it is allowed to presume that the zapper was used to suppress sales.[41]

The business records that Quebec was primarily concerned about were the Z and X Reports, the Electronic Journal, as well as all of the digital supporting files that were kept in an ECR or POS system. These are the records that reside within an ECR at step (5). They are presumed accurate because these records are the basis of the data sent to the printer to produce the customer's receipt.

This brings Quebec to the place that all fiscal till jurisdictions end up – the legislatively defined "legal receipt."[42] The legal receipt is the central enforcement document in all fiscal till jurisdictions. Quebec is no exception as it mandates that all *restaurant sales* be accompanied by a receipt, and then further specifies that this receipt must pass through the *module d'enregistrement des vent* (MEV) where it is e-signed.

---

[37] Quebec performed two empirical studies of the zapper problem. The first was conducted soon after the June 2000 legislative reforms came into effect. It was a "bookkeeping and records" audit conducted on 70 enterprises. It uncovered 41 zappers. Soon thereafter the second, more scientific, study (TAX EVASION IN QUEBEC: SOURCES AND EXTENT) was conducted referenced *supra* note 35. The use of statistical sampling techniques made this second study more accurate and authoritative. Personal e-mail communication from Dave Bergeron (June 6, 2008) (on file with author).

[38] The alternative of certifying ECRs and mandating the use of a device similar to an AFED Printer was considered and expressly rejected for cost reasons. Personal e-mail communication from Dave Bergeron (Nov. 18, 2008) (on file with author).

[39] Act Respecting the Ministry of Revenue, R.S.Q., c. M-31, § 34 & 35 (Quebec).

[40] Act Respecting the Ministry of Revenue, R.S.Q., c. M-31, § 34.2 (Quebec).

[41] Act Respecting the Ministry of Revenue, R.S.Q., c. M-31, § 34.1 (Quebec).

[42] Requirement for "legal receipts" can be fiscal till jurisdictions like found in Hungary, Greece Finland, Portugal, Denmark, and Latvia. *See supra* note 6, *Cash Register Good Practice Guide*, Appendix A at ¶¶ 1.3.1.1-1.3.1.5 & D at 3.2.1 & 4.2.6.

Penalties for not issuing a legal receipt are serious. The 2006-2007 Budget for Quebec summarized the penalties as follows:

> 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.[43]

The legal receipt can be a very effective tool against skimming by collusion with the customer – step (2) skimming. If an establishment conspires with its customers to charge a lesser amount in exchange for engaging in cash transactions unaccompanied by a formal receipt, then the restaurant operator is in violation of the legal receipt rule. If surveillance detects the fraud, penalties will apply.

Revenue Quebec unveiled its plans for the MEV pilot project (scheduled to begin in late 2009) in January 2008. Participating restaurants must install the MEV microcomputer between their ECR or POS system and receipt printer.[44] The MEV will receive data from specified transactions (the drafting of guest checks, register receipts, or credit notes). From the extracted data the MEV will produce an encrypted numerical signature, and transmit it to the printer where it will be printed on the receipt from which it was derived. Both the e-signature and the recorded data will be preserved within the fiscal memory of the MEV for seven years.[45] Restaurants will be required to submit sales summaries, generated by the MEV, when they submit their tax declarations.

Revenue Quebec believes that the MEV will:

- permit restaurant patron to verify that the taxes they pay are properly recorded and assure them that these funds will be remitted to the State;
- facilitate the intervention of Revenue Quebec in cases where a receipt is not issued or recorded [step (2) skimming] or where attempts are made with zappers or phantom-ware to manipulate the data on the receipt [step (7) skimming];
- allow Revenue Quebec to easily verify whether or not a specific receipt has been recorded;
- preserve sales data for the statutorily required period;
- make the data-content of ECRs more uniform and easier to audit;
- allow Revenue Quebec to quickly identify cases where sales have not been declared.[46]

A critical difference between the Greek and the Quebec approaches is that under the Greek system, it is not necessary to have multiple FESDs in an establishment that networks

[43] FINANCE QUEBEC, 2006-2007 BUDGET: ADDITIONAL INFORMATION ON THE BUDGETARY MEASURES 144-45 (Mar. 2006).
[44] After the pilot project has ended, implementation of the device in all restaurants will take place gradually during 2010 and 2011.
[45] Revenue Quebec, *Tax Evasion in Quebec* (powerpoint), *supra* note 2 at slides 6-8.
[46] *Id*. at slide 12.

multiple ECRs – a grocery store or a large restaurant, for example. Although a single MEV might have been used in a similar manner, to e-sign receipts for multiple ECRs, this was deemed to be a security risk by Quebec authorities. Thus, an MEV has a one-to-one relationship with an ECR and a receipt printer.[47] This difference has a significant financial impact when the estimated $650 cost of each MEV is factored into the equation.

Nevertheless, the Quebec government has promised to provide the necessary number of MEVs to restaurants at no cost. The cost to the Quebec Treasury for the whole program is estimated to be $55 million.[48] There is no discussion in Quebec about extending MEV applications outside the restaurant sector, even though automated sales suppression technology is not confined to restaurant fraud.[49] It also appears that very small restaurants may not be required to use MEVs.[50]

MEVs however are not the end of the story. Quebec's view is that MEVs will not eliminate the need for traditional audit enforcement rather the MEV will supplement or extend the traditional audit.[51] MEVs will integrate into traditional audit strategies in three ways: they will be the basis for pre-audit investigation; they will allow rapid, digitally-efficient confirmation of compliance with business record requirements; they will bring efficiencies to formal audits by standardizing record formats.

With respect to the first item, after the March 23, 2006 Budget Speech Revenue Quebec accelerated the use of (non-audit) inspection teams.[52] These inspectors are charged with making unannounced visits of restaurants to inspect books and records and to take back-up copies of ECR and POS programs searching for zappers and other frauds. These teams are comprised of an auditor and a computer specialist. With MEVs these inspectors will be able to more quickly identify the irregularities that would warrant transferring a case for formal audit or criminal investigation.[53]

---

[47] *Id*. at slide 7 (showing one MEV connected to either a single ECR or a POS system is ambiguous in this regard and does not does not reflect this one-to-one relationship). Personal conversation with Dave Bergeron, August 11, 2008 clarified this issue.

[48] Caroline Rodgers, *Québec va de l'avant pour stopper la fraude fiscale*, HOTELS, RESTAURANTS & INSTITUTIONS (Feb. 12, 2008) *available at :* http://www.hrimag.com/spip.php?article2771 (in French only, translations with author).

[49] For example, zappers have been found in grocery stores in the US and the Netherlands; clothing establishments in Australia; hairdressers in France.

[50] FINANCE QUEBEC, 2006-2007 BUDGET: ADDITIONAL INFORMATION ON THE BUDGETARY MEASURES 144-45 (Mar. 2006) (indicating that the obligation of a restaurant to use MEVs will be dependent whether or not it will be obligated to remit a receipt to a customs, and that requirement is not expected to be universal, but instead one which is defined and limited by regulation).

[51] Panos Zafiropoulos, who represents the Greek revenue authority on the Fiscalis Committee's Cash Register Project Group responded to questions about Greek litigation on zappers as follows:

> Because of the very strict and quite detailed technical specifications that exist in Greek legislation, there are no infamous fraud cases regarding cash registers being used so far.

Personal e-mail communication (May 10, 2008) on file with author.

[52] Quebec v. Pare 2004 PTC-QC-83 (October 24, 2004) (concerning the use of warrants by inspection teams of the MRQ searching for zappers within the Squirrel computerized cash register system that the defendant held exclusive distribution rights to even though the inspection did not rise to the level of a formal audit).

[53] Richard T. Ainsworth & Dave Bergeron, *Zappers: Automated Sales Suppression*, 11 New York Prosecutor's Training Institute, Syracuse, NY (July 31, 2008) (power point presentation, on file with author).

Secondly, the e-signature envisioned for the MEV is not the same as the alpha-numeric SHA-1 hash value that is printed on the legal receipt in Greece.[54] The MEV prints a bar code which can be read by a pocket computer through an integrated optical scanner. The bar code will immediately verify that a receipt is a "legal receipt," that has been issued by a government-issued MEV, and that both income and consumption tax amounts have been properly recorded in the firm's business records.[55]

Thirdly, the MEV will make traditional audits more efficient by standardizing the data flows from ECRs and POS systems in use throughout the Province. It will no longer be necessary to have sub-specialist in particular ECRs available to assist MRQ auditors, because the MEV will standardize the data that an auditor will need to download on to a laptop computer to perform an audit.[56]

GERMANY
EMBEDDING SMART CARDS IN ECRs

The German Working Group on Cash Registers, comprised of the highest-tier central and regional tax authorities, has been examining automated sales suppression (both phantom-ware and zapper applications) in use in the country. An Interim Report has been released.[57] The problem is deemed to be serious, and a technological solution is entering the final stages of testing.

The German solution involves encrypting critical data from the ECR on smart cards securely embedded in ECRs. The German National Metrology Institute (PTB: Physikalisch-Technische Bundesanstalt) is the home of the INSIKA project (Integrierte Sicherheitslösung für Kassensysteme – Integrated Security Solutions for Cash Registers). INSIKA began work on prototypes of the solution in 2008.

Papers on encryption[58] by Dr. Norbert Zisky of the PTB convinced the German Working Group that encryption techniques had been sufficiently tested in secure communication settings with measuring instruments[59] that they could form the basis of a solution to zappers.

---

[54] For example, in a presentation by Panos Zafiropoulos at the November 2007 EU Fiscalis Exchange Program, *Safeguarding Electronic Tax Data: Data Locking, 'Fiscal' Electronic Signing Devices*, 7 the following signature string, representative of the e-signing script that would be found on a receipt issued by a Greek FESD is the following string: D5A63F82962AB37886F975820883A76415DB614E 0459 00083592 0410030925 EZI03013095.

[55] Revenue Quebec, *Tax Evasion in Quebec* (powerpoint), *supra* note 2 at slide 12.

[56] *Id.*, at 5 & 12.

[57] Working Group on Cash Registers: Interim Report (Mar. 16, 2005) (Ger.) (on file with author).

[58] Norbert Zisky, *Manipulation Protection – Electronic Cash Registers and POS Systems*, German Federal Standards Laboratory, Brunswick & Berlin (May 2005) (unpublished draft on file with author); Norbert Zisky, *Manipulationsschutz elektronischer Registrierkassen und Kassensysteme* German Federal Standards Laboratory, Brunswick & Berlin (Mar. 15, 2004) (Ger.) (unpublished draft on file with author). Since this early paper there have been a few modification to Professor Zisky's proposal. The critical changes include:

1. The signature device (smart cards) distributed by the tax authorities will be personalized to the tax payer not to the cash register (cash box);
2. The signature device will have a set of dedicated sum storages which will be controlled by the signature device itself. It [will] generate the relevant data from the set of data to

The INSIKA project was charged with completing the technical specifications for a signature smart card by the summer of 2008.[60] Included with the technical specifications for the signature smart card will be a determination of the data structures and formats, communication protocols and security analysis for the system.[61]

Based on the recommendations of the Working Group, Vectron Systems AG developed (and is currently demonstrating) a privately developed prototype of the German solution. Under the Vectron prototype, every record holding of sales data (or any other activity performed on a cash register) is secured through an encrypted hash total of the main data elements in the ECR. A secure electronic signature is issued for this data based on Public Key Infrastructure (PKI).

The essence of the German solution revolves around cryptography and smart card access to cryptographic data preserved within the cash register or POS system. If the revenue authority audits it can access the records of the cash register with a "key" to read the data and determine if there has been tampering. Dr. Zisky indicates:

> The fiscally relevant data records can be examined both locally and after their transmission over various communication channels, [processes will be] fully automatic with respect to their integrity and authenticity. For the electronic signature of the revenue office's special smart cards are used, which are integrated into the POS systems….

> be signed. In the [case where there may be] a loss of signed data the tax authorities [will be] able to read the stored data from the smart card. The sum storages [are required] to read out periodically and [are required] to be stored after signing.
>
> 3. The receipts [must] contain all relevant data for the verification of the transaction (including the signature). These [receipts will be] exactly the same [as those] in the memory (from the point of view of data modeling). With the help of [the memory record] you are able to validate each receipt. Falsification of receipts [is] not possible. But there is a little problem [currently]: If you have the paper receipt you [will need] to type in every character into your computer by hand (or you may use a scanner). The manual test of receipts without technical support will be the exception, but it [will be] possible.

Norbert Zisky, personal e-mail communication (Feb. 15, 2008) (on file with author).

[59] Luigi Lo Iacono, Christoph Rulans & Norbert Zisky, *Secure Transfer of Measurement Data in Open Systems*, 28 COMP. STANDARDS & INTERFACES 311 (Jan. 2006); SELMA Project http://www.selma-projekt.de (in German) (last visited Feb. 12, 2008).

[60] At the time of this draft (August 9, 2008) the INSIKA project appears to be schedule, although the time line for publication of the results seems to have been pushed back from this summer to this autumn. Professor Zisky indicates:

> With our technical work we [have] made a lot of progress. Important parts of the technical description are nearly finished. Th[ese] documents will be made available for the public in [the] autumn. But the general technical concept will be published earlier.
>
> In autumn the first ECRs will be equipped with the smart card. Our cash register working group has finished the work on the internal, professional concept. This concept contains all needed steps and structures to set up the smart card solution.
>
> As I said one of the most important steps will be the set up of the public key infrastructure. But the earliest date for the inevitable use will be January 1st 2012 or 2013.

Personal e-mail communication with Professor Zisky (July 10, 2008) (on file with author).

[61] Ben B.G.A.M. van der Zwet, *Note: Draft 20080201 – Fiscal Obligations for Cash Registers in the Netherlands* 10 (Feb. 1, 2008) (unpublished draft on file with author).

> The revenue office will provide a smart card with a crypto processor for each cash register. On these revenue office smart cards a cryptographic pair of keys with a secret and public key is produced. The public key is kept for later fiscal examination of the respective data. The certificate for the public key is also stored on the smart card themselves….
>
> In the case of the marking procedure [the encryption procedure] over the data record – it is "signed" when a hash value is formed, which is in turn coded by the secret key of the smart card. The formation of the hash value is a mathematical one-way function, which comprises a single (unique) value from the data set. It is the hash value that seals the data record (an electronic seal). The formation of the signature is used to assign the data record to the cash (involved in the transaction) and/ or the pair of keys. …
>
> For the conclusion of the verification process the two hash values are compared with one another. If these agree the integrity of the registered data record is authenticated.[62]

The German solution is a fiscal till solution, but it is far more flexible and potentially more comprehensive that either the Greek or the Quebec solutions. The German mandate is for all ECRs and POS systems to be fitted with a smart card containing a crypto processor that e-signs designated "tax-relevant data." With this device the entire Electronic Journal could be signed on a regular basis, or each transaction open or closed (sale, refund, training session, voided sale, or temporary record) could be designated as a tax relevant and signed whenever entered into the ECR. It would not matter under the German system if no receipt was issued. It would only matter that each item be registered in an ECR or POS system that is fitted with a smart card.

The government could conduct audits remotely, because the German solution is fully digital. A data feed could be taken directly from ECRs, or data could be transmitted through an e-mail attachment. Neither of the Greek solutions can do this. The Quebec MEV does present ECR data in a digital format, and could be used to facilitate remote audits on restaurants, but this expansion of audit capability has been rejected by the MRQ on policy and privacy grounds.[63]

---

[62] Norbert Zisky, *Manipulation Protection*, *supra* note 58, at ¶ 5.2 & 5.3.

[63] Dave Bergeron, personal e-mail communication on the rejection of remote audits performed by linking to taxpayer's MEV (Nov. 20, 2008) (on file with author). It is questionable whether or not the MRQ is dealing with a real privacy concern here, or merely the appearance of an intrusion on a protected privacy interest. There should be little that should be considered confidential in the bulk transmission of itemized business records setting out daily sales of goods or services, provided those sales are *not* further associated with an individual – an unsuspecting customer. It is the retention of a *customer's* personally identifiable information (PII) in business records that is a privacy concern. If not handled properly this may lead to an unpermitted government intrusions into private lives. See: Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEORGE. L. J. 123 (2007) (discussing the origins and different development paths of privacy law in the US and UK – the US with and individualistic understanding and the UK with a relational understanding – and indicating that unpermitted disclosure of PII within business records is central to both). Nevertheless, it is common in the transaction tax context to put protections in place whenever third-party access to tax data is contemplated. For example, section 321 under the Streamlined Sales Tax restricts retention of PII by CSPs performing tax calculations. Streamlined Sales and Use Tax Agreement (adopted November 12, 2002, amended November 19, 2003 and further amended November 16, 2004) *available at* http://www.streamlinedsalestax.org (last visited Feb. 3, 2008).

The Greek, Quebec and German solutions can also be distinguished based on "per unit" cost of implementation. The German solution is far and away the least expensive. Both Greece and Quebec have responded to the high costs of their solutions. Under the Greek regime the entire cost is born by business, although the government does provide tax breaks (accelerated depreciation) and financial assistance (low interest loans) to assist with hardware purchases. Quebec on the other hand plans to provide the MEV to businesses for free. In this context, one of the key features of the German solution is its low cost. Dr. Zisky indicates:

> In … this [German] approach … for the protection of electronic cash registers and POS systems against the manipulation of stored data [t]he large advantage … consists of the reaching of a comparatively high level of protection with only small hardware and software expenditures in the POS system being necessary.[64]

Dr. Zisky estimates an overall cost of 50 euro for the German smart card solution, itemized it as follows:

> The additional costs per ECR are the result of cost for the smart card (signature device), approx. 7-8 Euros, and for integration of the smart card to ECR, approx. 20 Euros (including hardware and software). [An] additional 20 Euros I calculate [are needed] for additional common costs (smart card distribution, administrative costs). Government subsid[ies] are not planned. But on the hand of tax authorities some expenditure is needed. Certificate management, test tools, training of the staff of tax authorities [need to be included in a full cost estimate].
>
> The price of smart cards is calculated on the base of more than 100,000 cards because they will be ordered by a central authority.[65]

In fact, Vectron's prototype of the INSIKA smart card solution has an even lower cost estimate. Vectron estimates a "single-unit end-user price of less than 25 euros."[66]

COMPREHENSIVE AUDIT: THE NETHERLANDS

All fiscal till jurisdictions rely on audits. All the technology – FECRs, AFED Printers, FESDs, MEVs, or smart cards – does not replace auditing; it only makes the auditing easier. Thus, Quebec announced an increase in the use of inspection teams in tandem with the announcement that MEVs would soon be deployed. The MEV itself is designed with an auditor's eye. It harmonizes data feeds from widely diverse ECRs, and it translates the encrypted signatures on receipts into bar codes so that they can be scanned with hand-held optical readers.

---

[64] Norbert Zisky, *Manipulation Protection, supra* note 58, at ¶ 5.1.
[65] Personal e-mail communication, Professor Zisky (February 19, 2008) (on file with author).
[66] Vectron, A.G., Tamper-proof POS Data for Projectgroep Onderzoek Administratieve Software (Oct. 31 2007), *available at* http://www.gbned.nl/downloads/xmllogistiek/poas/20071031%20Vectron.pdf (last visited Feb. 3, 2008).; Norbert Zisky, *Manipulation Protection – Electronic Cash Registers and POS Systems*, German Federal Standards Laboratory, Brunswick & Berlin (May 2005) (unpublished draft on file with author) at ¶ 5.7 (estimating 50 euros); Norbert Zisky, *Manipulationsschutz elektronischer Registrierkassen und Kassensysteme* German Federal Standards Laboratory, Brunswick & Berlin (Mar. 15, 2004) (Ger.) (unpublished draft on file with author).

The German assessment of the situation is similar to that in Quebec. Germany believes that fraud technology has advanced so far that success with traditional audits is virtually impossible without a secure technological record. The German Federal Audit Office (Bundesrechnungshof or BRH) indicated on November 24, 2003 to the Federal Ministry of Finance that:

> *The latest generation of cash registers and cash register systems makes it impossible for tax authorities to detect fraudulent declarations of cash receipts. In these systems, data that have been entered, as well as system-generated register and control data can be secretly tampered with. This leads to a high risk of lost taxes that cannot be overestimated. This situation must change immediately. …*
>
> The analysis reveals that auditors and tax investigators have constantly discovered fraudulent manipulations of cash registers and the data they store. However, such manipulations could only be discovered in older generations of electronic cash registers and cash register systems.
>
> Verification of data has become extremely difficult since the introduction of new cash registers and cash register systems….[67]

Brazil's experience with ECR manipulation reinforces the German and Quebec assessment. Reliance on technology – alone – to block manipulation is not sufficient. No matter how much security is placed over digital records, an audit is necessary. Brazil requires that a "Black Box" be attached to each ECR. The device secures the electronic journal, and can only be accessed by the tax administration. But as the 2008 criminal audit of all the supermarkets in Belém, *Operação Caixa 2* (Operation Second Register), demonstrates fraudsters intent on skimming will find a way to get into the Black Box.[68] Similarly in 2007 *Operação Tesouro* (Operation Treasure-hunt) demonstrated that fraudsters have been successful in tampering with the Black Box remotely. This operation, conducted in the State of Bahia, uncovered over three-hundred food service establishments that used software to manipulate data *before* it was sent to the Black Box.[69]

---

[67] BRH comments 2003, No 54, Federal Parliament circular 15/2020 at 197-198 (Nov. 24, 2003) (in German, emphasis in original) (original and translation on file with author).

[68] "Operação Caixa 2" (Operation Second Register) conducted by the Brazilian Federal Revenue service began on October 1, 2007. In the early stages it involved 50 fiscal auditors, 20 tax analysts and 20 support personnel (police units) operating in 10 teams in the city of Belém. On the first day of the operation five companies (supermarkets) were raided, 175 recording machines were confiscated and 60 were found to have irregularities. In addition 17 suppliers were searched. By the second day 4 more supermarkets were raided in Capanema and 2 more in Bragança were searched. "The fiscal auditor and coordinator of this activity, José Renato Gomes, affirms that yesterday's work is essential for finding out whether this kind of fraud is all coming from Belém, from the corporations supplying the equipment, or if it is being set up and carried out outside the State." Receita Federal fiscaliza supermarcados em Belém (Federal Revenue Service investigates supermarkets in Belém); Receita Federal dá prosseguimento à Operação Caixa 2 (Federal Reserve Gives the Go-ahead to Operation Caixa 2); Operação Caixa 2 divulga balance hoje (Operation "Caixa 2" to release results today) PLANTAO ONLINE EDITION (Oct. 1, 3 &18, 2007) *available at:* http://www.orm.com.br/plantao/comentar.asp?id_noticia=290720 (in Portuguese – sequence of posting on the Federal government web page) (translations on file with author).

[69] *Operação Tesouro* (Operation Treasure-hunt) in the State of Bahia involved:

> … seven businessmen from the bar and restaurant sector, as well as the owners of two information sector businesses, namely Networks and Stella Systems, accused of being responsible for the development of a tax evasion software program…. 28 search warrants … 35 teams … comprised of 264 people, … the civil police, civilian and military police officers, tax auditors, revenue

However, the Greek experience appears to stand in contrast to the Brazilian as well as in contrast to the German and Quebec assessments. Even though regular audits of FECRs, AFED Printers and FECDs are conducted by Greek authorities, no significant enforcement actions involving ECRs have reached the courts, or can be referenced by tax officials.[70] One might have expected things to be different (in light of the twenty-year certification experience Greece has with ECRs). It is not clear if this is a case of false-confidence in technology, or a case of superior technology, but in light of the Brazilian investigations, the Greek approach needs to be considered carefully.

The Netherlands is at the other extreme. The Dutch are convinced that audits are sufficient. They reject fiscal till technology. The fundamental emphasis in the Netherlands is on detailed, comprehensive, and technologically penetrating audits. Direct government intrusion into the recordkeeping systems of all businesses (encrypting the memory of all ECRs and POS systems) just to catch the fraudsters is avoided at all costs. Following a pure principle-based approach to enforcement, the Netherlands feels it can rely on good business practices and compliant tax payers.

However, Netherlands officials speak about performing "deep audits" – that is, audits that are not focused just on the sales records in the ECR. A "deep audit" considers businesses comprehensively – it looks at income taxes, consumption taxes and employment taxes simultaneously and with heavy stress on the interrelationships among taxes. Ben B.G.A.M. van der Zwet, lead auditor for technology compliance indicates:

> The Dutch Tax Authority is convinced that the appropriate approach is to use principle based laws in this area. This method involves maintaining the law by stimulating the compliance of taxpayers. It is premised on a belief that we should be working from a starting point of trust to get compliance, or to provide explanations.

> agents, prosecuting attorneys and intelligence professionals … According to the technicians involved … between 2005 and 2007 the fraudulent accountancy performed by the "Colibri" [hummingbird] software program permitted the illegal withholding of almost R$2 million. The number of establishments involved in the scheme may be as high as 300 in the food service sector alone … these businessmen have been withholding nearly 40% of their companies' turnover. … the Colibri software, developed by Networks, is a database program for commercial automation, commonly used by bars, restaurants and luncheonettes. The fraud consists in the use of the program with a certain configuration permitting the deactivation of the Receipt Issuing Device (ECF), and thus keeping the machine from issuing a receipt during payment for sales of products or services.

?Thecnological fraud?..Bahia::Fraude:Sonegação Fiscal Leva sete Empresários para a Prisão Terça-feira, (*Technological Fraud? Bahia:: Fraud: Seven Businessmen Imprisoned for Illegal Withholding of Taxes*) JOURNAL DA MIDIA (Oct. 2, 2007) *available at*: http://www.jornaldamidia.com.br/noticias/2007/10/02/Bahia/Sonegacao_fiscal_leva_sete_empres.shtml (in Portuguese) (last visited Feb. 17, 2008) (translation on file with author).

[70] The author has been in e-mail correspondence with Panos Zafiropoulos from the Greek revenue authority. Panos responds to an inquiry about Greek legal cases on zapper enforcement actions by noting:

> Because of the very strict and quite detailed technical specifications that exist in Greek legislation, there are no infamous fraud cases regarding cash registers being used so far.

Personal e-mail communication (May 10, 2008) on file with author.

> With respect to the problem of auditability and the completeness of sales for enterprises with sizable over-the-counter payments, the Dutch Tax Authority has decided to work to improve voluntary compliance.
>
> The Dutch Tax Authority is cooperating with software developers, suppliers and manufacturers of cash registers, branch organizations, and larger companies.[71]

The Netherlands has been successful with this approach. One of the best examples of how a comprehensive multi-tax audit can uncover data manipulations, and how this fraud is derivative of the symbiotic relationship that develops between SMEs and their ECR providers can be seen in the Grand Café Dudok case.[72] A *grand café* is a style of café that occupies a single large space welcoming a large amount of foot traffic and a large cash-based clientele, so it is an ideal business for skimming.

Dudok skimmed cash receipts with a primitive zapper and used a portion of the cash to pay employees under the table. The Belastingdienst (Dutch IRS) was suspicious of the low wages reported, and thought that additional (unreported) compensation might be being distributed (under the table).[73] Testimony in the case indicated that on the second day of the payroll audit the managing director of Straight Systems BV visited Dudok where he was approached by the Dudok's owner-manager. Straight Systems BV[74] supplied the Finishing Touch point-of-sale cash registers that were used by Dudok. The owner-manager explained that he was having difficulty accounting to the Belastingdienst for the wages that were being reported, in part because the auditors were also questioning the turnover that was reported. The numbers did not "seem right" to the auditors, and they were requesting back-up data, something that would lead them to the primitive zapper he was using.

The managing director of Straight Systems explained the existence of a more sophisticated zapper, a "hidden delete" option already embedded in the Finishing Touch cash registers. This was, "… a hidden menu option that, after enabling …, allowed operators of catering establishments to delete cash register receipts from the system."[75] After this discussion

---

[71] Ben B.G.A.M. van der Zwet, *Fiscal Obligations to Cash Registers in the Netherlands* 8 (Draft 20080206) (unpublished manuscript, on file with author).

[72] District Court of Rotterdam, LJN: AX6802 (Jun 2, 2006) *available at*: http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AX6802 (in Dutch) (translation on file with author); appealed to the District Court of The Hague where the judgment is upheld LJN: BC5500 (Feb. 29, 2008) *available at*: http://zoeken.rechtspraak.nl (in Dutch) (translation on file with author).

[73] LJN: BC5500, at F3. Prior to using the phantom-ware installed on its system Dudok was skimming sales in a very amateur fashion. The entire sales records of the POS system were deleted and records were reconstructed on x-cell spreadsheets. The examining agents did not trust the spreadsheets and asked for the POS records as a back-up to confirm what they were being shown on the audit. This in turn lead to the conversation with Straight Systems BV where Dudok was informed that they already had phantom-ware that might solve this problem installed in their system. Ben B.G.A.M. van der Zwet, (personal e-mail correspondence May 28, 2008) (on file with author).

[74] Straight Systems BV is a Netherlands company that specializes in single-service ECR systems where all hardware and software are developed "in house." The company web site offers a 24-hour help desk where there is "… one point of contact for all hardware and software for checkout's front office and back office systems." *Available a t:* http://www.straight.nl (in Dutch, translation on file with author) (last visited May 24, 2008).

[75] LJN: AX6802, at Consideration of the Evidence (Jun 2, 2006) (in Dutch) (translation on file with author). The case discusses three software programs: Twenty/Twenty; Finishing Touch; Tickview.exe. Twenty/Twenty was a US touch-screen program that did not have a phantom-ware application. Straight Systems BV added the phantom-ware

"… an employee of [Straight Systems] visited [Dudok] and explained [and enabled] the application of the erase rule [or hidden delete function[76]], after which [Dudok] subsequently decided to start using [it] …"[77] Once more, Ben B.G.A.M. van der Zwet observes:

> The most interesting thing about [Dudok] is that the discovery of the fraud was completely the benefit of a good and thorough tax audit. Based on our principle based law, tax officers were not satisfied getting the total reports and MS excel work-pages with total sales etc. They wanted the detail information of the POS. The tax officers persisted in their efforts to get the detailed information. This forced the entrepreneur to ask the POS supplier to help him out. Because [the entrepreneur] was aware that once the POS records were audited the fraud would instantly be clear.
>
> Straight Systems was helpful by installing an additional hidden feature of the POS system. Records in the POS could [now] be deleted and the records renumbered so that no gaps would appear.
>
> A thorough investigation of the tampered databases revealed the deleting of the records anyway. So this was not simple bad luck [for the taxpayer] but a good audit job of the Tax administration![78]

The court upheld criminal tax fraud determinations in the Dudok case under income, value added, and payroll taxes. Both the restaurant operator and the ECR/ software provider were convicted. Other successful audit-intensive cases in the Netherlands include:

- Microcraft Software which developed Analyse (aka, CX Analyse and Retail) as a management information system for grocery stores, butchers and bakers. It worked off a combination of ECRs and grocery scales. The zapper could be started with a hidden combination of key strokes, and the user could then indicate a percentage of turnover that would be skimmed.[79]
- B&F Software and Computers B.V. developed *Beleids Informatie Systeem* (B.I.S.) for hairdressers and an add-on program for zapping cash sales through POS and client information systems. After entering a percent to skim the system selects customers to eliminate (for example male walk-ins without appointments paying cash without special services).[80]

Thus, it is clear that an intensive and comprehensive audit approach works against automated sales suppression devices. There are a number of sizeable cases in the Netherlands and a much larger number of cases in Quebec that demonstrate the effectiveness of this

---

application to Twenty/Twenty and renamed the program Finishing Touch. Using just this program you can view the sales ticket and change data. With a secret command the Tickview.exe program within Finishing Touch can be activated and the operator is asked if they would like to delete the whole ticket. If an affirmative response is given then the system records a "no sale" and the entire audit trail to the original data is eliminated. Ben B.G.A.M. van der Zwet, (personal e-mail correspondence May 28, 2008) (on file with author).

[76] The trial court in Rotterdam refers to the phantom-ware application as a "hidden delete function" whereas the appeals court in The Hague refers to the phantom-ware as "the erase rule."

[77] LJN: BC5500, at F3.

[78] Ben B.G.A.M. van der Zwet, (personal e-mail correspondence Apr. 16, 2008) (on file with author).

[79] LJN: AT 5876, District Court of Arnhem (Jul. 27, 2005) (in Dutch) (translation on file with author).

[80] B&F Optics B.V. (District Court of Amsterdam (Aug. 11, 2005) (in Dutch) (translation on file with author).

approach. Quebec however, unlike the Netherlands, feels that more than an audit is needed. The MEV is a rules-based supplement to the audit effort.[81]

The UK shares the Netherland's opinion,[82] and would prefer to avoid universal fiscal till solutions. However, this was prior to a recently completed National Pilot study of 941 enterprises where the first phantom-ware programs have been uncovered in the UK. Based on the scope of this fraud (something that has not been fully analyzed as of this writing), the UK may change its position.[83]

BLENDING RULES & PRINCIPLES: CERTIFICATION OF THIRD PARTY SERVICE PROVIDERS

Certification is the common thread among all the zapper enforcement efforts considered. This is apparent if we step back from the details. In each instance – the Greek, Quebec, German and Dutch – tax authorities responded to the threat of automated sales suppression in the same manner – they all looked for certification of digital records. Rules-based jurisdictions imposed *external* certification regimes to force businesses to keep trustworthy records; principles-based jurisdictions induced businesses to develop their own *internal* (self) certification regime. In all cases however, it is the reliability of digital records that is the main concern – and in all cases the question is whether the certification is trusted. Both approaches work. But neither approach (rules-based nor principles-based) comes without problems.

In the instance of rules-based jurisdictions the prospect of forcing all businesses to accept a government presence inside the recordkeeping function of private enterprises – the fiscal till solution – is considered (by some) to be far too intrusive. The observation is that this remedy is overly broad, and needs to be more focused. Why should *all* sales activity be certified through government oversight, just because *some* records are untrustworthy? In Quebec the government's MEV minicomputer must be placed between every ECR and printer in every restaurant. In Germany every ECR will be required to install a tamper-resistant, government-issued smart card that can be configured to record, encrypt and transmit everything that occurs within the ECR. In Greece no business can be conducted without processing transactions through a government certified ECR or FESD.

Principles-based jurisdictions are much more "hands-off" initially. Moral factors and good business practices are relied upon to make digital records trustworthy. Unfortunately, this solution requires oversight, and the oversight that works is an audit program that is both comprehensive and technologically-intensive. Even though it is more than unpleasant for a small business to respond to these kinds of audits, the real problem is not the complaints of the business owners it is the fiscal demands placed on the revenue authority that must conduct the audit. Funding is rarely sufficient to secure the necessary audit teams and computer audit specialists.

---

[81] The Quebec approach is to have the MEV together with specialized inspection teams, and a significant public awareness program. Revenue Quebec, *Tax Evasion in Quebec* (powerpoint), *supra* note 2 at slide 5.
[82] *See supra* note6, *Cash Register Good Practice Guide*, 1.4.4 & Appendix E.
[83] Jennifer Mitchell, HMRC: Local Comp SME Interventions, personal e-mail communication (Nov. 26, 2008) (on file with author).

Fortunately, there is another option – certification of intermediaries. This approach is used in the US with certified service providers (CSPs) under the Streamlined Sales and Use Tax Agreement (SSUTA). The SSUTA can be a useful template for jurisdictions seeking to develop *less intrusive* and *less expensive* methods for combating automated sales suppression. Currently CSPs perform all consumption tax compliance functions for their clients. They determine taxability and the correct rates. They prepare and file returns, make tax payments, and immunize the taxpayer from liability for errors (except taxpayer fraud).

Extending the CSP's obligations to include certification *by the CSP* to the government that *the taxpayer's ECRs and POS systems* are free from zappers and phantom-ware would create a new enforcement regime. Four questions need to be addressed: (1) how does a CSP get ECR and POS system data; (2) how would a CSP know the data it has is accurate; (3) what standards should the government use to certify a CSP's automated system – (in other words) what data does a tax authority want to be sure that a CSPs system captures so that it can trust the CSPs attestation of the accuracy of the taxpayer's system – i.e., that the taxpayer's ECR does not manipulate sales records; and (4) what is the most efficient and cost effective way for a CSP to satisfy this standard?

(1) *How does a CSP get ECR and POS system data?*

CSPs currently pull data directly from the ECR or POS system to determine taxability – at step (4). This data is stored in an independent (tamper-proof) audit file before it is used by the taxpayer to draft the invoice (receipt). The CSP maintains this file to protect itself from liability.

Unlike fiscal till solutions which preserve data that is sent to the printer from step (5)(a)(b)(c) and (d), or from step (6) when it is recorded in the X or Z Reports or the Electronic Journal, the CSP is actually involved in generating the critical data sets. In real time the CSP determines the taxability of transactions, calculates the tax, and passes this information back to the ECR. This event has a three-way data check: (a) the customer is demanding an accurate receipt – and the CSP and the taxpayer-business must produce it; (b) the taxpayer-business (that has a primary obligation to collect and correctly remit the tax) is demanding that the CSP perform this tax function accurately; and (c) the CSP (that is assuming all the tax compliance obligations of the taxpayer-business including remission of taxes from funds provided by the taxpayer) is motivated to be accurate (detect any fraud), because it has liability for all errors and must compensate the tax authority for errors out of its own funds.

A "legal receipt" is not required with a CSP-based system. It could be mandated to combat fraud occurring outside the ECR, or maybe as a further tool against the consumer-business collusions, but it is not necessary for the CSP.

SSUTA is a voluntary system. There are strong incentives to participate. Businesses participate to get relief from regular audit,[84] relief from penalties for tax calculation errors, and

[84] SSUTA *supra* note14, at §9(a).

relief from additional taxes (penalties and interest) that stem either from late changes in laws or errors in taxability determinations.[85]

CSPs participate for commercial reason – fees for service from the taxpayer, the State,[86] as well as money movement benefits. These benefits are offset by a shift in tax liability to the CSP if it makes errors. Only fraud by the taxpayer-client[87] removes this liability.[88] All CSPs insure against the risk of their own errors (so there is always a fund out of which missing taxes can be paid), and they retain confidential transactional data to defend themselves, if necessary.

(2) *How would a CSP know that the data it has is accurate (free from manipulation)?*

This is a key question. The most effective way to do this is to *adopt the German smart card* in the private sector. The German smart card can be configured to sign every event – completed sales, temporary records, refunds, test modes, open or partially completed transactions. Every key stroke can be recorded, collected and encrypted on the smart card, and then transmitted to the CSP.[89] Questions about any transaction, or the business records associated with any ECR could then be directed to the CSP. Only in cases of fraud would it be necessary for the tax administration to approach the taxpayer. If suspicions were raised it would be in the self-interest of the CSP to assist the government in determining the truth.

This would be a form of comprehensive ECR monitoring,[90] but it is the private sector monitoring the private sector, not an intrusive government oversight program.

---

[85] SSUTA *supra* note14, at §9(a).

[86] SSUTA *supra* note 14, at §§601-03 (providing that the government may enter into contracts with a CSP to compensate the service provider directly based on taxable transactions processed, or a percentage of instances where sellers without nexus volunteer to collect sales taxes that they are not otherwise obligated to collect)

[87] A CSP is also relieved from liability for charging and collecting the incorrect amount of tax if that error is caused by erroneous data provided by a member states on tax rates, boundaries, or taxing jurisdiction assignments, or if it is based on erroneous data provided by the member state in the taxability matrix. SSUTA *supra* note 14, at §§ 328 & 331.

[88] SSUTA *supra* note 14, at §9(a).

[89] Personal e-mail communication from Norbert Zisky (Nov. 17, 2008) (on file with author):

> You are right. If I get the data in Berlin from an ECR in Boston I am able to check the integrity (whether the data is unchanged against the original data) and the authenticity (whether the signature belongs either to the ECR or the tax payer). The kind of authentication depends on the operational concept of the tax body.
>
> In principle every transaction [final sales – step (5) and temporary transaction – step (2)] could be transferred to the auditor or a remote server.

[90] Not only could all transactions (final and temporary) be tracked and e-signed by the German smart card, all of this could occur in real-time. However, because the data is collected by government authorities the German planners indicate that they, " … will have a strong resistance against this online tracking of transactions." Personal e-mail communication from Norbert Zisky (Nov. 17, 2008) (on file with author). There is a Serbian proposal to do this, but it has not been well received. Milan Prokin, *Technical and Functional Specification of Turnover Controllers – Draft Prepared for Fiscalis FPG 12 Cash Register Project Group*, (undated; on file with author) at 7. Professor Prokin, Faculty of Electrical Engineering, Belgrade proposes a system whereby "All misuses of fiscal cash registers, fiscal printers, non-fiscal cash registers and non-fiscal printers listed in the document titled Cash Register Misuse Guide are inherently solved by a new device called a turnover controller … [a central database where government serves store all transaction data]."

(3) *What standards should the government use to certify a CSP's automated system – (in other words) what data does a tax authority want to be sure that a CSPs system captures so that it can trust the CSPs attestation of the accuracy of the taxpayer's system – i.e., that the taxpayer's ECR does not manipulate sales records?*

The data preservation standards that a CSP would need to meet if it were to certify the accuracy of business records in an ECR should be the same standards that a principles-based jurisdiction, like the Dutch, would set down for all ECRs. In *Your Cash Register and the Fiscal Accounting Obligations*,[91] the Dutch Tax Authority lists the requirements for a business wishing to bring their ECRs or POS system into compliance with Dutch law. They include:

- Detailed records available for the tax auditor if and when required.
- Electronic preservation of the details of transactions.
- Preservation of a complete audit trail.
- Taking adequate measures to guard against subsequent alterations in a manner that will assure that data-integrity is maintained.

The Dutch requirements may not be difficult for larger businesses, but for SMEs (which is where phantom-ware and zappers are found) the requirements are burdensome. Ben B.G.A.M. van der Zwet confirms:

> Hardly any of the cash registers or Point of Sale systems by themselves complies with the requirements set out by the Dutch Tax Authority. With larger companies this omission can be compensated for with adequate internal control measures. Without similar internal control efforts, SMEs that may be willing to comply with Dutch fiscal obligations will fail in their attempts.
>
> - Data needs to be stored electronically.
> - Facilities have to be implemented to export data to digital data carriers.
> - Settings of the software and the adequate database structures must support a proper audit trail.
> - Measures must be taken to assure the reliability of retained data.

Under the SSUTA model a service provider could not be certified unless it could assure tax authorities that its system accurately, completely, and automatically captured this data from the taxpayer's ECRs. With this data on hand the CSPs attestations would be highly credible.

(4) *What is the most efficient and cost effective way for a CSP to satisfy this standard?*

The smart card is the primer solution. It is far less expensive and captures far more data than any other option. The smart card is proven technology, and the CSP in a SSUTA context is a proven legal structure. Merging them in a CSP/ smart card solution makes a great deal of sense.

The only competing option is for the government to do it directly. However, even the German research teams working on the smart card project concede that direct government involvement compromises the effectiveness of the solution.

[91] Belastingdienst, *Your Cash Register and the Fiscal Accounting Obligations*, (2007) at ¶ 6, "Checklist for Cash Registers."

The German smart card solution comes from successful research in legal metrology, specifically the SELMA (Secure Electronic Measurement Data Exchange) project. The immediate goal SELMA was to "…ensure the secure transfer of measured *energy data* from decentralized meters to the authorized users via open networks."[92] SELMA succeeded. The project leaders summarized SELMA as follows:

> SELMA … developed a security architecture to establish trust in the electronic transfer of data from the meter to data acquisition systems and further to the customers. The introduced security mechanisms are based on asymmetric cryptography and more specifically on digital signatures that enable the signed measurement data to be verified and authenticated in conjunction with a suitable key management. Particular security units have been created that contain the necessary security mechanisms.
>
> The SELMA architecture represents a best practice solution of strong cryptographic mechanisms to secure a wide range of metrology applications and is compatible with appropriate European directives and guidelines.[93]

SELMA looked at natural gas meters. The SELMA solution assured multiple parties (traders, distributors, owners of distribution networks, and consumers) that remotely monitored meters were accurate. Based on an assumption that ECRs and POS systems were nothing more than a different kind of meter recording a different kind of data flow, the SELMA researchers suggested that the same solution could apply in this new context as well. As a result, a new project, INSIKA (Integrierte Sicherheitslösung für Kassensysteme – Integrated Security Solutions for Cash Registers) was opened in 2008 to consider this application.

There are two critical differences between SELMA and INSIKA: (1) the INSIKA data represents confidential tax information (not natural gas measures), and (2) the group of interested parties includes the government (whereas only private parties are involved in gas metering). The researchers soon became aware that there was "…strong resistance against this online tracking of transactions [by the government]."[94] As a result the SELMA solution was not able to be fully implemented in INSIKA. Dr. Zisky noted:

> The realtime, central collection of very large amounts of data is already being carried out today in different sectors of the economy. One example worth mentioning is the area of special contract customers for power supply. Of approximately 300,000 special contract customers, energy amounts recorded in intervals of 15 minutes are read out daily and stored centrally. These data, relevant to calibration law, provide the basis for the monthly billing. For the sake of completeness, the following should also be mentioned: work is currently being done towards securing measurement data cryptographically.

[92] *Id.*, at 312-13 (emphasis added).
[93] Luigi Lo Iacono, Christoph Rulans & Norbert Zisky, *Secure Transfer of Measurement Data in Open Systems*, 28 COMP. STANDARDS & INTERFACES 311 (Jan. 2006); The SELMA Project can be found at: http://www.selma-projekt.de (in German) (last visited Feb. 12, 2008).
[94] Personal e-mail communication from Norbert Zisky (Nov. 17, 2008) (on file with author).

> The *decisive difference between the example of energy data transfer and the realtime, central recording of tax-relevant data consists in the fact that the data must be collected by the authorities, rather than by a contracting partner*.[95]

Simply put, even when there is "nothing to hide" there are real privacy concerns when the government gets too intrusive.[96]

These are the same issues that confronted SSUTA. The real-time collection of tax data by the government was not acceptable to business, but it was acceptable when a third party did it. Thus, the issue changed. Now the question was whether or not the government could trust the third party as much as the taxpayer did, not whether or not the government should be trusted to collect the data directly. The SSUTA answer was "yes," the government could trust the third party, but only if the third party's systems were certified.[97]

SSUTA was born as an inexpensive, voluntary regime to streamlines sales tax compliance. It extends audit immunity to taxpayers who used CSPs, because the CSP is trusted by the government. A SSUTA-like system to prevent zappers and phantom-ware applications in ECRs could be made mandatory for all sectors of an economy or it could be applied only in high risk sectors or maybe it could be made mandatory only for those taxpayers who had previously been found to manipulate sales records. Even though mandatory for some the SSUTA should remain an option for all businesses. This would increase the pressure on those who do not use CSPs to maintain good records. Traditional audit resources could be more intensively focused on this subset.

CONCLUSION:
ASSESSING QUEBEC'S MEV

With the MEV set to be deployed in a select number of restaurants on a volunteer basis in November of 2009 it might be appropriate to offer an assessment of how effective the MEV might be, based on similar efforts elsewhere. There are five critical observations.

- The MEV will work. Coupled with a significant audit effort, the MEV will most likely be an effective zapper and phantom-ware deterrent in the Quebec restaurant sector. There are several reason for this: (a) the MEV is similar to the very effective FESD and FECR with AFED Printer that has been in use in Greece for over twenty years; (b) the MEV deployment is accompanied by a commitment to increase inspectors (pre-audit investigators) who will refer suspected fraudsters for full audits; and (c) the MEV will facilitate rapid pre-audit investigations by embedding bar-codes on each receipt that will verify that it is "legal." All of these factors bode well for the workability, effectiveness, and ultimately the success of the MEV.

[95] Norbert Zisky, *Manipulationsschutz elektronischer Registrierkassen und Kassensysteme* (Protecting Electronic Cash Registers and Point-of-Sale Systems against Manipulation)10-11 (Mar. 15, 2004) (unpublished paper in German) (translation on file with author) (emphasis added).

[96] Daniel Solove, *"I've Got Nothing to Hide"and Other Misunderstandings of Privacy*, 44 San Diego L.R. 745 (2007).

[97] There is a related issue of trust involving consumers. It was necessary to add provision to the SSUTA to protect personally identifiable information (PII) from disclosure when it was in the hands of the trusted third part. See *supra* note 63.

- The MEV is expensive. Quebec estimates that the MEV will cost approximately $650 per unit, an expense that will be born entirely by the Quebec government. $55 million is the estimated cost for full deployment of the MEV. These costs approximate the Greek costs, but are ten times the per unit cost of the German smart card, and they present Quebec with a scalability problem. In other words, if Quebec wants to eventually extend the MEV throughout the economy (and not just limit it to the restaurant sector) the magnitude of these expenses might force the government either to limit its financial support (as is the case in Greece) or move to the German smart card. Because zappers and phantom-ware are not confined to the restaurant sector, the scalability of the MEV solution needs to be considered in advance of full implementation.

- The MEV is an invoice-based solution. Quebec, like Greece and Germany, designed their solutions around the invoice (receipt), and passed laws mandating that a "legal receipt" must be given in each sale. This requirement raises the too-much-government-in-private-business concerns. Why should *every* sale need to be accompanied by an MEV-signed receipt when profits from only *some* sales are skimmed? However, this intervention into private business relationships is a necessary part of the enforcement regime because *the invoice is the trigger* that sets the whole data security process in motion. Resistance to the MEV could be reduced if a no-receipt-needed solution, like the CSP/ smart card, was considered.

- Extending a mandatory MEV solution outside the restaurant sector may be difficult. Finding volunteers for an MEV pilot project in some restaurants does not mean that the MEV will be widely accepted throughout the restaurant sector. Would a mandate work throughout the economy? Quebec's empirical work supports a restaurant initiative, but audit results in the Netherlands (as well as some early cases in Quebec) suggest that the problem is much more widespread – grocery stores, convenience stores and hairdressers are all suspect. In Germany there is considerable resistance to the smart card precisely because it is being considered for the whole economy. Quebec's sector-approach is unusual and may ultimately prove to be unstable – not solving the whole problem, and treating businesses unequally. Business incentives may be helpful in this effort, and by offering them Quebec would be taking a page from the principles-based jurisdictions. The SSUTA model highlights the incentives that have worked in the US.

- The MEV is not a real time solution. There is nothing in the MEV, in the German smart card proposal, nor in the Greek system that accelerate audit, return filing or tax remission into real time. Real time compliance is very possible with certified systems, but this would require adoption of a CSP/ smart card solution. It is an intriguing thought that the CSP/ smart card would not only stop the skimming frauds with zappers and phantom-ware, but it would bring tax compliance into real time.