BU School of Law

CALIFORNIA ZAPPERS:
A PROPOSAL FOR CALIFORNIA'S COMMISSION ON THE 21ST CENTURY ECONOMY

Boston University School of Law Working Paper No. 09-01
(January 8, 2009)

Richard T. Ainsworth

CALIFORNIA ZAPPERS: A PROPOSAL FOR CALIFORNIA'S COMMISSION ON THE 21ST CENTURY ECONOMY

Richard T. Ainsworth

On December 11, 2008 California Governor Arnold Schwarzenegger and legislative leaders announced appointments to the Commission on the 21st Century Economy. The mandate is to propose ways to modernize the California revenue system by April 15, 2009. The Governor is concerned with the "feast-or-famine" budget cycles, and Senate President pro Tempore Darrell Steinberg emphasized that the Commission is expected to provide a, "… much needed outside perspective on what exactly needs to be done to bring our tax system up to date."

Assembly Speaker Karen Bass wants the Commission to provide a "…thorough review of California's economic structure, to modernize and stabilize a system built for the 1930s,…" but Senate Republican Leader Dave Cogdill expects "… revenue-neutral recommendations to improve our broken budget system while ensuring our state remains competitive in a global economy." Assembly Republican Leader Mike Villines anticipates, "… positive and lasting changes … focusing on tax reforms that will encourage economic growth, job creation and opportunity … not … higher taxes…"[1]

This is a classic tax reform effort. The Commission has a nearly impossible goal of crafting a stabilizing, revenue neutral tax reform that will modernize the tax system, provide jobs and growth but not raise taxes. Not many suggestions will meet all of these requirements, but this proposal might.

This paper suggests that the Commission on the 21st Century Economy look carefully at one aspect of digital tax fraud – automated sales suppression, or digital skimming of cash sales with modern electronic cash registers (ECRs). This proposal considers the California tax system from the outside – it adopts a comparative international perspective. Recognizing that the 21st Century economy is digital at its core, foreign governments have observed that fraudsters have automated many traditional tax evasion methods including cash skimming operations. These new ways of performing old frauds have made frauds difficult to detect without the assistance of technology-sensitive legislation (and regulation) as well as technology-intensive audit tools. In short, from a foreign perspective it appears that California might find that a digital hole has been cut through the bottom of the modern ECR and significant sales tax receipts, taxable business profits, and personal income are falling through. Foreign revenue authorities are making efforts to plug this hole, as of yet California has not done so.

Specifically, this proposal asks the Commission to recommend that a randomized, statistically valid study be taken of automated sales suppression within the State. The study should consider add-on software (zappers), factory or distributor installed software (phantomware), and manually re-programmed ECRs (self-help phantomware). The Commission should further recommend that if the results of this study align with the results of similar

[1] Office of the Governor, Press Release, *Gov. Schwarzenegger and Legislative Leaders Announce Appointments to Bipartisan Commission on the 21st Century Economy* (Dec. 11, 2008) GAAS:826:08 *available at* http://gov.ca.gov/index.php?/press-release/11233/ (last visited Dec. 16, 2008).

(foreign) studies then appropriate legislative (or regulatory) changes should be enacted to meet this challenge. A technology-intensive audit response will most likely (but not necessarily) also be required.

It should be emphasized that as of this writing, California has not uncovered a single instance of technology-assisted skimming. After considering the foreign evidence the Commission should ask – is this absence because Californians are not skimming cash sales with technology, or is this absence because the California skimming technology works so well that the fraud is not being detected? If the later is the case, then time may be of the essence. Considered from a global perspective, it is reasonably clear that we are moving into a fourth generation of automated sales suppression, and with each generation the fraudsters are becoming more difficult to uncover.[2] One of the reasons this problem has not been better addressed may be because almost all of the work in this area is being done in foreign languages – French, German, Portuguese, Dutch and Swedish.

SCOPE OF THE PROBLEM - STUDIES

The leading government studies of automated sales suppression are from Quebec and Germany. The UK is in the process of completing a national study and results are expected in 2009. The German and Quebec studies both underpinned the need for significant legislative reforms. Neither government has made the full studies available to the public, but a government-to-government exchange could be arranged. Summaries have been released, and they arrive at similar conclusions.

Quebec. The government of Quebec conducted two studies focused on the restaurant sector. The first study gathered its subjects from the customer list of a known distributor/developer of automated sales suppression software. This investigation (the First Inspection Wave) examined 70 systems and uncovered 41 zappers.[3] A more statistically accurate investigation followed (the Second Inspection Wave). It was based on a random sample of businesses within the restaurant and hospitality industry. This survey, conducted by Finances Quebec, found that 16% of all sales went unreported.[4]

Both of these studies were relied upon by the Quebec Minister of Revenue, Jean-Marc Fournier, when he announced legislative changes, enhanced enforcement efforts, and a pilot project designed to counter the penetration of sales suppression technology in the restaurant sector on January 28, 2008. He indicated:

> Although the majority of restaurant owners 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 taxes and sales taxes. Tax losses in this sector

[2] For a discussion of the fourth generation of sales suppression software, a problem that Sweden seems to be dealing with currently see: Richard Thompson Ainsworth, *Zappers and Phantomware: Are State Tax Administrators Listening Now?*, 49 STN 103 (July 14, 2008).

[3] Dave Bergeron & Richard Ainsworth, *Zappers (Automated Sales Suppression)* 12, powerpoint presentation at the New York Prosecutors Training Institute (Syracuse, NY) July 31, 2008 (on file with author).

[4] *Id.* at 13 (but noting further that the 16% figure measures all skimming frauds, not just skimming with Zappers).

> are significant. Revenue Quebec estimates them at $425 million for the 2007-2008 fiscal year.[5]

Other things being equal,[6] because the California economy is roughly 61% larger than the Quebec economy, a similar study in the California restaurant sector might find tax losses to be in the $700 million range.[7] Although restaurants are a popular area for sales suppression (because they have a high concentration of cash sales) it is clear from Dutch and Brazilian investigations that grocery and convenience stores, hairdressers and butcher shops also have very high concentrations of automated sales suppression.

Germany. The Interim Report of the German Working Group on Cash Registers indicates that the Group was "… aware of [technology-assisted] fraud amounting to 50% of companies cash receipts."[8] The Working Group does not separately quantify the kinds of *technology-assisted* fraud involved.

The Working Group's 50% observation is supported by a report made by the German Federal Audit Office (BHR) to the German Parliament in 2003. In this report the BHR appears to focus only on factory installed software.[9] The BHR concludes that the potential loss in Germany is in the billions of euros:

> The Federal Audit Office (BHR) has complained that later models of electronic cash registers and cash management systems now fail to meet the principles of correct accounting practice when it comes to recording transactions … The risk of tax fraud running into *many billions* [of euro] should not be underestimated in cash transactions.[10]

Both the BHR's observations and the Working Group's study are further buttressed by summaries from studies conducted by three German federal states. These studies are limited,

[5] 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*; (English trans. *For more equity in the restaurant sector it is required that [business is conducted] above the table*) *available at* : http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp (last visited August 7, 2008). See also the accompanying powerpoint presentation, *Facturation obligatoire dans le secteur de la restauration*, *L'évasion fiscale au Québec, Sous-déclaration des revenus dans le secteur de la restauration*; (English Trans. *Tax Evasion in Quebec : Obligatory Billing in the Restaurant Sector – Under-declaration of revenues in the restaurant sector*) 3 (January 28, 2008) (in French) (on file with author, with translation).

[6] Of course things are not equal. Take for example the tax rates: California's combined state and local consumption tax rate is 7.25% whereas Quebec's is 7.5% (Quebec includes the federal GST in the rate base of the QST).

[7] Quebec's 2007 GDP was $992,850 million (expressed in 2002 dollars); California's 2005 GDP was $1,622,116 million (revised October 26, 2006). Thus, 992,850/1,622,116 = 61%; 61% x 425 = 259; 425 + 259 = 684. Board of Trade of Montreal, *Composition of Quebec's GDP*, (updated July 3, 2008) *available at* http://tableaudebordmontreal.com/indicateurs/activiteeconomique/compositionpib/compositionpibqc.en.html?mode=print (last visited Dec. 17, 2008); California Department of Finance, Economic Research, *California Statistical Abstract*, Table D-1: Gross State Product [source: US Department of Commerce, Bureau of Economic Analysis] *available at* http://www.dof.ca.gov/html/fs_data/stat-abs/toc.htm

[8] Working Group on Cash Registers: Interim Report 5 (Mar. 16, 2005) (Ger.) (translation on file with author).

[9] *Id.* at 5 (listing the following attributes: (1) erasing all data entries, (2) resetting the zero counter, (3) unwarranted counter-entries, (4) unwarranted use of the training mode, and (5) suppressing the grand total memory).

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

because they focus only on the restaurant sector. But, they too conclude that sales suppression is a significant problem:

> One federal state is currently implementing a special "restaurant" initiative. Checks already made have led to average upward revisions of 46% of original turnover. A comparable initiative in another federal state resulted in over half the cases (54%) having upward revisions of 60% of declared turnover. Fraud amounting to 25% was detected in a fifth of the cases, and was as high as 5% in the remaining 26% of cases. A third federal state has found that around 45% of till receipts involving cash are subject to upward revisions ranging from 20% to 118%.[11]

ZAPPERS AND PHANTOMWARE

Skimming cash receipts is an old fashioned tax fraud; a fraud traditionally associated with small or medium sized enterprises. Large businesses with formalized internal control mechanisms, external accountants, and professional management structures do not normally engage in skimming,[12] although personal conversations with auditors from Revenue Quebec indicate that this may not be a solid assumption any more. Businesses that skim frequently keep two sets of books (one for the tax man, the other for the owner). In its simplest (non-technological) form there are two tills, and the cashier simply diverts some cash from selected sales into a secret drawer. A record of the diversion may be maintained, but it will be kept outside the formal accounting system. Businesses that skim rarely do so with credit card transactions precisely because these sales can be documented externally through the banking system. Skimming frauds thrive when the owner (or a close family member) is the cashier.[13]

Technology is changing how businesses skim. The agents of change are software applications – phantom-ware and zappers. Phantom-ware is a "hidden," pre-installed programming option(s) embedded within the operating system of a modern electronic cash register (ECR). It can be used to create a virtual second till and may preserve a digital (off-line) record of the skimming (a second set of digital books). The physical diversion of funds into a second drawer is no longer required, and the need for manual recordkeeping of the skim is eliminated. Because phantom-ware programming is part of the operating system of an ECR its use can be detected with the assistance of a computer audit specialist.

Zappers are more advanced technology than phantom-ware. Zappers are special programming options added to ECRs or point of sale (POS) networks. They are carried on memory sticks, removable CDs or can be accessed through an internet link. Because zappers are not integrated into operating systems their use is more difficult to detect. Zappers liberate

[11] *Id.* at 5.
[12] EU Commission, Fiscalis Committee Project Group 12, Cash Register Project Group, *Cash Register Good Practice Guide*, ¶ 2.5 (Dec. 2006) (on file with author).
[13] See for example the use of double tills to manually skim cash receipts in the UK at Aleef Garage Ltd. This was a £5.3 million tax fraud, and according to Steve Armitt, Group Leader HMRC Criminal Investigations indicated, "… the investigation was made all the more difficult because of the closed ranks of the employees involved some of whom were close family members … [t]hose involved tried to make it as difficult as possible for the cheating to be discovered." HMRC News Release, Company Directors Jailed for £5million Fraud 1 (Nov. 13, 2007) *available at* https://www.gnn.gov.uk/content/detail.asp?NewsAreaID=2&ReleaseID=330199 (last visited Aug. 8, 2008)

owners from the need to personally operate the cash register. Remote skimming of cash transactions is now possible without the knowing participation of the cashier who physically rings up the sale. This attribute of zappers allows the incidence of skimming fraud to migrate beyond the traditional "mom and pop" stores. Zappers allow owners to place employees at the cash register, check their performance (monitor employee theft), but then remotely skim sales to cheat the taxman.

While California has uncovered no zappers or phantomware applications, the Province of Quebec (alone) has brought 230 cases to court.[14] In the early days Quebec was concerned that the software that facilitated this fraud was US made and was sold over the internet for $500.[15] Canadian subsidiaries of US companies were early providers.[16] Soon however, the design and installation of this software became a "cottage industry" for local IT professionals.[17]

[14] Roy Furchgott, *With Software, Till Tampering Is Hard To Find*, NYT C6 (August 20, 2008) indicating:

> [T]he Canadian province of Quebec may be the world leader in prosecuting zapper cases. Since 1997, zappers have figured in more than 230 investigations, according to the tax collecting body Revenue Québec, which has found an active market for the software. In making 713 searches of merchants, Revenue Québec found 31 zapper programs that worked on 13 cash register systems.

Available at: http://www.nytimes.com/2008/08/30/technology/30zapper.html?scp=1&sq=With%20Software,%20Till%20Tampering%20Is%20Hard%20to%20Find%20%20comments&st=cse

[15] Craig Silverman, *Zapped!*, HOUR (Feb. 19, 2004) *available at*: http://www.hour.ca/news/brief.aspx?iIDArticle=783 (last visited Feb. 15, 2008).

[16] Turcotte v Quebec (Ministry of Revenue) 1998 CarswellQue 1041, [1998] R.D.F.Q. 110 Superior Court of Quebec. This case involved the MRQ investigation of Gamma Terminal, Inc., a wholly owned Canadian subsidiary of an American company, Gamma Micro Systems. This investigation began in 1997 and focused on the distribution of the Gamma Restaurant Management System. It eventually lead to a number of conviction of restaurants that used this system to delete sales records, including the companies 136530 Canada, Inc. and San Antonio's Grill. Revenue Quebec, Press Release, *Deux sociétés coupables d'avoir utilisé un camoufleur de ventes dans des restaurants de Laval et de Repentigny* (English Trans. *Two companies guilty of having used a camoufleur sales in restaurants in Laval and Repentigny*) April 25, 2005 *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/25avril.asp (in French, translation on file with author) last visited August 6, 2008.

[17] Consider for example the cases of (1) Audio Lab LP; (2) Michael Roy; or that of (2) Luc Primeau.

Audio Lab LP: On April 8, 2004 Revenue Quebec announced that it executed four search warrants on the numbered company 9061-1184 Quebec Inc. which operated a restaurant under the name San Antonio Grill in Laval, Quebec. The allegation was that a "sales Zapper" (*camoufleur de ventes*) was used delete sales records. The Zapper was on a diskette used in connection with the restaurant's computer system. Revenue Quebec, News Release, *Le ministère du Revenu soupçonne le restaurant Grill San Antonio de Laval d'avoir utilisé un zapper* (Eng. Trans.*Tax Evasion: The Ministry of Revenue Suspects the Restaurant Grill San Antonio de Laval of having used a Zapper*) (Apr. 8, 2004) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2004/08avril.asp (in French only, last visited Dec. 18, 2008). Next year, on April 25, 2005, Revenue Quebec announced that the director of San Antonio Grill pleaded guilty to using a Zapper. (The director, Mr. Apostolos Mandaltsis, was personally fined.) A related company of similar name, Grill San Antonio in Repentigny, also pleaded guilty to similar offences. Revenue Quebec, News Release, *Deux sociétés coupables d'avoir utilisé un camoufleur de ventes dans des restaurants de Laval et de Repentigny* (Eng. Trans. *Two Companies Guilty of having used Zappers in Restaurants in Laval and Repentigny*), *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/25avril.asp (in French only, last visited Dec. 18, 2008). Later that year, on October 1, 2005, Revenue Quebec announced that it executed five more search warrants in Montreal and Laval with respect to Audio Lab LP, Inc. It was under suspicion of having developed and marketing a sales Zapper, software that was compatible with its own restaurant cash register software, Softdine. Revenue Quebec, News Release, *Revenu Québec enquête sur un concepteur de logiciel de point de vente soupçonné d'avoir conçu et distribué un camoufleur de ventes* (Eng. Trans.

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 Dec. 18, 2008). Softdine was the operating software in the cash registers at San Antonio's Grill in Laval, and at Grill San Antonio in Repentigny. On June 26, 2007 Audio Lab LP, Inc. pleaded guilty to charges of having, "… designed and marketed a computer program designed to alter, amend, delete, cancel or otherwise alter accounting data in sales records kept by means of a software that [Audio Lab LP] had designed and marketed." In other words, it pleaded guilty to developing a Zapper to "add-on" to its own commercial software (Softdine) that it provided to restaurants for use in their POS systems. Press reports directly link this conviction to the investigation begun at Grill San Antonio in Laval in 2004. Revenue Quebec, News Release, *La société Audio L.P. inc. condamnée pour fraude fiscale* (Eng. Trans. *The Company Audio LP, Inc. Convicted of Tax Evasion*) (Sept. 21, 2007) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2007/21sep.asp (in French only, last visited Dec. 18, 2008).

Michael Roy: Before the first warrants were issued in Audio Lab LP Revenue Quebec had successfully brought to conclusion an extensive investigation of twenty-eight restaurants doing business under the name Stratos. Each of the restaurants in the Stratos chain used Zappers. To dispose of the excess cash from skimmed sales (1) a double billing system was put in place with suppliers (to conceal purchases made in cash), and (2) wages were paid to employees in cash (without being reported as income). The guilty pleas from this investigation came in waves – nineteen companies pleading guilty on September 26, 2002; another six pleading guilty on October 11, 2002, and the four remaining pleading guilty on March 21, 2003. Press releases provide details of only the final ten companies. In aggregate the taxes and penalties for these companies came to $1,816,070.90, but the real thrust of the news releases were that "… the Department has conducted searches in order to establish proof that the designer of the IT function associated with the cash register software Terminal Resto had participated in the scheme set up by restaurants in the Stratos chain." The breakdown is: $429,179.07 (GST) + $492,023.11 (PST) + $214,589.55 (federal penalties) + $625,028.89 (provincial penalties) + $55,250.28 (judicial fees). Revenue Quebec, News Release, *Tous les restaurants Stratos coupables de fraude fiscale en lien avec l'utilisation du zapper* (Eng. Trans. *All Stratos Restaurants Convicted of Fraud in Connection with the use of a Zapper* (Mar. 18, 2003) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/18mars.asp (in French only, last visited Dec. 18, 2008). That proof was forthcoming on April 25, 2003, when Mr. Michel Roy and his two sons Danny and Miguel were convicted of tax evasion. The father (Michel) was the creator of the Zapper that worked with Resto Terminal. He promoted it and made the sales. His sons (Miguel and Danny) installed the software and designed the civil fraud. Aggregate fraud penalties assessed against the Roys were $1,064,459. Revenue Quebec, News Release, *Des amendes de plus de un million de dollars - Un père et ses deux fils condamnés pour fraude fiscale en lien avec le* zapper (Eng. Trans. 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 Dec. 18, 2008).

Luc Primeau: Revenue Quebec announced on March 17, 2003 that seven Patio Vidal restaurant franchises and a bar, La Tasca, from Gatineau, Quebec as well as another bar named O'Max in Masson-Angers, Quebec were convicted of adding Zappers to their Microflash cash register software (later upgraded to a new version called Caracara). Even though guilty pleas were entered on March 14, 2003, a search warrant had already been executed the previous December against the designer of Microflash and Caracara, because the software developer was suspected of also being the developer of the associated Zapper program. Revenue Quebec, News Release, *M. Marcel St-Louis de l'Outaouais coupable de fraude fiscale liée à l'utilisation d'un zapper* (Eng. Trans. *Mr. Marcel St. Louis de l'Outaouais Convicted of Tax Evasion related to the use of a Zapper*) (Mar. 17, 2003) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/17mars.asp (in French only, last visited Dec. 18, 2008). On October 17, 2005 Luc Primeau admitted using his software to assist these companies to evade $435,000 in GST and QST. They skimming $2.7 million is cash sales. Mr. Primeau was fined $20,000 for his involvement. However, Mr. Primeau was more than a Zapper salesman, he considered himself a provider of management services (admittedly focused on how to "manage Zappers") for which he also charged a fee. Revenue Quebec determined that not only did Mr. Primeau fail to report GST and QST of $33,725.45 on his own sales (of Zappers), but he also failed to report income of $155,084.99 in services income Zapper management advice). Revenue Quebec, News Release, *Le concepteur d'un camoufleur de ventes de Boucherville plaide coupable à diverses accusations portées par le fisc québécois* (Eng. Trans. *The Zapper Designer of Boucherville Pleads Guilty to Various Charges brought by Inland Revenue Quebec* (Oct. 26, 2005) *available at*:

FOUR GENERATIONS OF AUTOMATED SALES SUPPRESSTION TECHNOLOGY

In general we are considering software programs that are used in conjunction with ECRs or point of sale (POS) systems to alter business records, allowing owners to skim cash receipts. The term *automated sale suppression device*[18] is a general classification for all software programs used or designed to facilitate cash skimming. *Phantom-ware* is a sub-classification. It includes the first two generations of automated sales suppression devices – *self-help phantom-ware,* and *factory (or distributor) installed phantom-ware*. *Zappers* are a third generation of automated sales suppression devices. A fourth generation of this software appears to be under development now, a foreign (or extra-jurisdictional) zapper that is provided to users over the internet, which alters domestic records from a distance, and removes both the program and the developer from the immediate grasp of the local tax authorities.

Phantom-ware.[19] Phantom-ware is programming placed within a modern ECR or POS system that can be used to hide the skimming of cash sales. Phantom-ware is "hidden" (in the sense of not being disclosed in user manuals). Its use, operation, and even its existence may be very difficult to detect on audit.

Phantom-ware re-programs an ECR or POS system so that selected types of cash sales are not recorded (receipts can be renumbered to follow a new sequence, Z Reports and X Reports can be altered, and the Electronic Journal can be brought into conformity with all other changes). This programming exists on most systems for good (but not often needed) business purposes, and for which there are good reasons for having it "hidden" from employees. For example during a bankruptcy sell-off of business assets a buyer of the ECR would want to clear the

---

http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/26oct.asp (in French only, last visited Dec. 18, 2008). The real reason Mr. Primeau did not report this income probably [no one really knows] had to do with the fact that he was being paid out of the $2.7 million in skimmed cash sales from the nine companies where he sold, installed and managed his Zappers. These funds probably needed to be kept "hidden" (to facilitate the overall success of the fraud), and in a sense represented his "share" of the skimmed profits.

[18] "Automated sales suppression," "electronic sales suppression," or "sales suppression technologies" is the preferred expression of the Canadian Revenue Authority (CRA) these days. For example, at the 2007 International Tax Dialogue Conference the Director General SME Directorate, Compliance Program Branch indicated:

> One of the most popular means to suppress sales is to utilize electronic suppression of sales technologies, such as "Zapper." The CRA is actively working with provincial counterparts (through the FPTUEWG – Federal/Provincial Meeting of the Underground Economy Working Group) to address Zapper and other point-of-sales suppression technologies.

Jim Gauvreau, *SME Audit and Verification Strategies and Techniques Based on Risk Detection and Risk Selection,* ITD Global Conference on Taxation of Small and Medium Enterprises 14 (parallel session 4, stream B) (Buenos Aires, Argentina)(Oct. 17-19, 2007) *available at*: http://www.itdweb.org/SMEconference/documents/parallel/4B%20GAUVREAU%20CANADA.pdf

A similar expression, "fraudulent risk software" is used in many EU documents. For example, the *Cash Register Good Practice Guide* dedicates Appendix F to "Fraudulent Risk Software." This *Guide* identifies forty-two different "risks" in Appendix B, assimilating everything from self-help phantom-ware through zappers and more within this expression. *See*, Fiscalis Committee Project Group 12, Cash Register Project Group, *Cash Register Good Practice Guide*, Appendix B & F(Dec. 2006) (on file with author).

[19] The term "phantom-ware" originates with this author, who after struggling with imprecise and overlapping terminology employed elsewhere, decided that a new expression was needed.

electronic journal. Programming is needed to do this, but one might not want the night shift manager to know how to do this with instructions set out in the user's manual.[20]

Because it relies on a manual re-programming of systems this is called *self-help phantom-ware*. Installers, distributors and manufacturers frequently provide help-desk support and will guide owners in the use of these "hidden" functions. Help-desk personnel may suspect, but have no reason to definitively know that a user is asking for help to commit fraud. The critical problem with these functions is that the ECR is commonly programmed (in addition) to not preserve a record of the re-programming action. There is a real danger to the fraudster if records are preserved. Government auditors might suspect fraud in a business that repeatedly programmed and re-programmed its ECRs to start and stop Z or X Report, or entries in the Electronic Journal.

When manufacturers or software providers take the next step and automate the re-programming of self-help phantom-ware (to reduce the likelihood of user re-programming errors) the risk that the manufacturer/software provider will be pulled into a criminal tax fraud audit is elevated. This is *factory-installed (or distributor-installed) phantom-ware.* It is the next generation of this software, and it presents a different constellation of legal and audit issues.

In this new generation the technology has changed.[21] The new technology only has one purpose – fraud. It is still phantom-ware – programming hidden in the software – but it requires very little operator-intervention to use. It can be identified by tax auditors only if the operating system of the ECR or POS system is broken down.

Zappers.[22] Zappers are not embedded in operating programs of ECRs or POS systems; they are add-on programs that are removed as easily as they are added to a system. Zappers can

[20] *See,* IRS, *Ex-Burger King Manager Sentenced in IRS Fraud Case for Skimming $180,000 in Cash* (relating the manual skimming fraud orchestrated by the night manager of a chain of Burger King restaurants that involved simply not ringing sales through the register, or voiding sales made, a fraud which would have been more easily carried out with technology but the user manual did not contain instructions for the night manager to perform the fraud in this way) *available at*: http://www.irs.gov/compliance/enforcement/article/0,,id=163019,00.html

[21] The *Cash Register Good Practice Guide* notes at ¶ 4.1:

> In countries that have no legislative requirement to use Fiscal Tills, tax auditors are now encountering increasingly sophisticated electronic till systems that present potentially enormous risks.
>
> These till systems are extremely vulnerable to all three risk types identified. In particular, new tills systems are being manufactured with "fraudulent risk" software installed as standard.

[22]"Zapper" is the term originally used "on the street" (in Quebec) to describe an automated sales suppression device. In the early days, a "Sales Zapper" was a specific commercially available product purchased (frequently over the internet for about $500.00). This product was identified by name in several investigative reports in the Canadian press in 1997, and was adopted by MRQ to describe all devices in this field.

When researching in French sources the expression used for the English word "zapper" is *camoufleur de ventes*. For example, Revenue Quebec describes the recent investigation into the activities of Logicaisse Ltd. As follows (emphasis added):

> Revenu Québec a des motifs raisonnables de croire que cette société a conçu et distribué un **camoufleur de ventes (communément appelé *zapper*)**, utilisé avec le logiciel RMS-Touch, dont elle est le distributeur exclusif au Québec, et qu'elle a permis à différentes sociétés, principalement des restaurants, de se servir de ce camoufleur pour dissimuler des ventes afin d'éluder le paiement des taxes et des impôts.

Which translates as:

be physically hidden during an audit. Zappers, like factory-installed phantom-ware, have no purpose other than to facilitate skimming by reconstructing (deleting, replacing or supplementing) ECR or POS system records.

Zappers are contained on CDs or memory sticks. Without a disclosure by the fraudster (or the distributor, or the zapper-developer) the use of a zapper is nearly impossible to detect. Traces of zapper use however, can be found when fraudsters are not careful, or if the zapper is not well designed. Occasionally back-up records remain in a POS system or an ECR that reference the original transaction data. For this reason, technical support is frequently needed

> Revenue Quebec has reasonable grounds to believe that this company has designed and distributed a **camoufleur sales (commonly called *zapper*)**, the software used with RMS-Touch, which it is the exclusive distributor in Quebec, and has enabled different companies, mainly restaurants, use this **camoufleur** to conceal sales to evade payment of taxes.

Revenue Quebec, Press Release, *Les systèmes informatiques Logicaisse ltée dans la mire de Revenu Québec* (Eng. trans. Computer systems Ltd. Logicaisse in the grasp of Revenue Quebec) (Mar. 12, 2008) a*vailable at:* *http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2008/12mars.asp* (in French only, last visited Dec. 18, 2008).

As late as April 25, 2001 the CRA was following MRQ usage. This was the expression used by Kevin Pratt at the FTA meetings in Louisville, Kentucky in February 2001 and was the expression used by Mr. Pinternal in a memorandum from Regional Attorneys Serge Clairoux and Jean Marois to Jean-Francois Normand at the Head Quarters for the Underground Economy. Here the CRA refers to a "Zapper Initiative," and indicates that CRA wanted to "take the lead" on this issue. However, this memo and others also concede that in fact the CRA was instead following the well marked path of the MRQ :

> **History**
>
> In December 1997, Radio Canada current affairs program "Le Point" ran a story about the use of Zappers. The week after, a meeting was held involving UE [Underground Economy], Investigations from HQ, Montreal and Ontario and Quebec provincial officers. As conclusion, it has been decided that HQ-UE should take the lead of this issue. A series of recommendations were also provided to Mr. Lacombe, former ADM. [The recommendations have been redacted.]
>
> Until now, the MRQ [Ministry of Revenue Quebec] has proceeded to complete several audits, Investigations and searches related to Zapper users. On May 12th, we received a press release from MRQ about the Nickles group who plead guilty to 74 charges of tax evasion. [The enclosed copy of the guilty plea has been redacted.] …
>
> **Definition**
>
> Zapper software programs are electronic means of concealing revenues. Taxpayers can delete 5, 10, 15 percent or more of their sales by activating an accounting software program. In order to eliminate as many trails as possible, Zappers are used mainly in cash transactions.

Memo obtained through a Request for Information pursuant to the Access to Information Act, R.S.C. (1985)(Can.) (on file with author).

"Zapper" is also the expression used in early OECD documents to describe the whole field of automated sales suppression devices (admittedly in the very last paragraph on the very last page of an e-commerce report):

> However, an intimate knowledge of how to manipulate computer systems is not required where unscrupulous software programs, such as "zapper" are developed. These programs are specifically designed to falsify records and hide certain transactions. News of these techniques generally spreads rapidly through an industry, especially traditional cash based industries. Tax authorities will have to be attuned to new tools to defeat the integrity of systems much as they must keep abreast of new tax dodges and schemes for illegally sheltering income. Tax authorities must also make sure that they have audit experts that are experienced in online business methods and models. They must catalogue and understand the digital footprints that electronic records leave and develop compliance models for online business types that provide a basis for comparison across tax paying entities.

OECD, REPORT BY THE TECHNOLOGY TECHNICAL ADVISORY GROUP (TAG) (Dec. 2000) 93.

when zappers are used, just as they are with phantom-ware applications – something that leads to long-term business-fraud relationships.

Although things have already developed beyond this point, it is common to find government reports that set out these three phases in automated sales suppression fraud in contrast to the manual skimming techniques of the past. Consider this assessment in the Interim Report of the German Working Group on Cash Registers[23] where the terminology used in this paper has been added in bold brackets:

> The fraud is perpetrated in different ways. One way is for taxable persons to totally fail to record some of their cash receipts. **[Manual skimming]** Another is for them to exploit the numerous tampering possibilities available through their electronic or computerised tills. **[Self-help Phantom-ware]**
>
> This is done by using the extensive programming options described in the till manual. As a result, information which has initially been entered correctly is falsified when stored and released. Till manufacturers confirm that customers enquire about such functions, and that they influence customer purchasing decisions. **[Factory-installed Phantom-ware]** What is more, special types of programmes are known to offer additional functions which are specifically designed to facilitate the doctoring of information. The programmes are created by external software manufacturers, rather than by till manufacturers. **[Zappers]**

International zappers. As revenue authorities began to identify phantom-ware applications, domestic developers responded with zappers that could be removed and hidden when an audit commenced. If a zapper is uncovered the auditors today have become very adept in finding the developer, his customer list, and then following up with audits on each of the developer's clients.

It has not been lost on the developers of automated sales suppression devices that the Quebec Ministry of Revenue (MRQ) was able to find zappers in seven Patio Vidal restaurant franchises, and two bars (La Tasca in Gatineau, and O'Max in Masson-Angers) by following the customer list of Luc Primeau.[24] Because Mr. Primeau was a local developer he increased the risk of detection for all his clients.[25] Similarly, when the Belastingdiest (Dutch IRS) was able to identify a locally designed zapper (used on produce scales in grocery stores to alter the data feed from the scales to the ECR) it was able to trace this zapper through approximately 1,200 businesses by simply following the customer lists of the local developer.[26]

An on-going Swedish investigation[27] (scheduled for trial late in 2008, now delayed until 2009) involves an ECR manufactured from Paris, France (TT PI Electronique) which is popular in Italy, Belgium, Portugal, Spain, Germany, Denmark, Australia, the US and North Africa. The

[23] Working Group on Cash Registers: Interim Report 5 (Mar. 16, 2005) (Ger.) (translation on file with author).

[24] See *supra* note 17.

[25] See *supra* note 17.

[26] LJN: AT 5876, District Court of Arnhem (Jul. 27, 2005) (in Dutch) (translation on file with author); Joan van den Dungen, *Software Company Confesses Shop Scales Fraud – Managing Director of Software Company Confesses Shop Scales Fraud*, TELEGRAAF (Feb. 7, 2003) (in Dutch) (translation of file with author).

[27] Martin Jansson, *Fraud by Using a Cash Register and Back-Office System*, (undated, unpublished paper) (on file with author).

operating system used in the specific TT PI Electronique ECRs under investigation includes a back-office program called Restodata.

The Restodata program is licensed and comes with a grey program dongle[28] on a memory stick. Directly attached to this dongle is a second (silver) memory stick that contains a zapper. The zapper used in this system has the ability to either (a) selectively change line items on a sales ticket (replacing expensive items with less expensive items and reducing the related VAT charges) or (b) perform a fully automated "zapping" of all transactions so that total sales for a day would be reduced by a specified amount. As a result, this zapper allows a fraudster to custom tailor his zapping. However, one of the most distressing aspects of this case is the following comment by Martin Jansson, the Swedish auditor who found this zapper:

> In this case the restaurant under investigation used a backoffice program called Restodata. According to the exe-file the program was produced by a company called "Restodata Inc." However, we haven't been able to find that name anywhere.[29]

The Swedish case is an excellent example of where zapper technology is headed. Zappers are being internationalized. In fact, if one examines the TT PI Electronique system with the zapper installed it is easy to see the system move from a Swedish interface to an English interface as the zapper is inserted into the POS system. Although not conclusive by any means, it does seem to suggest that the Swedish Tax Administration is up against a zapper that is a bit more difficult to trace than those found by the MRQ. The Swedish Tax Administration is most likely not looking at an in-house zapper, nor is it looking at a locally designed and distributed zapper. It is looking at a foreign zapper designed to facilitate local fraud.[30]

[28] A dongle is a small hardware key that plugs into the serial port or parallel port of a computer – used to ensure that only authorized users can copy or use a specific software application.

[29] Martin Jansson, *supra* note 27.

[30] Revenue Quebec encountered a similar problem in October 2002 when it began a large scale operation in connection with a zapper investigation that involved twelve search warrants in Montreal and Brossard. These parties were suspected of distributing a fraud-facilitating software that was developed in British Columbia. The press release indicates:

> C'est dans ce contexte que le Ministère a exécuté dans un premier temps, hier, un mandat de perquisition à Vancouver concernant un groupe lié de quatre sociétés qui conçoivent un logiciel utilisé dans la restauration. Elles sont soupçonnées d'avoir conçu un logiciel muni de la fonction illicite en question et de l'avoir vendu à des distributeurs qui, à leur tour, l'ont vendu à des restaurateurs. Précisons que le Ministère a obtenu la collaboration de l'Agence des Douanes et du Revenu du Canada.
>
> (It is within this context that the Ministry has implemented as a first step yesterday, a search warrant in Vancouver on a related group of four companies that design software used in restaurants. They are suspected of having developed a software bearing the illicit function [the zapper] in question and have sold to distributors [in Quebec] who, in turn, have sold to restaurants [in Quebec]. It should be noted that the Ministry has obtained the cooperation of the Agency of Customs and Revenue Canada.)

Although it appears that the search in British Colombia did not uncover zapper software [the suspect software performed normal bookkeeping functions] it is important to realize how much more difficult enforcement becomes when the developer is in a different jurisdiction from the distributor and the operator. In this case Revenue Quebec simply needed to work with the federal revenue authority to execute warrants. If this were a case where the developer was in a foreign jurisdiction Revenue Quebec would need to ask for federal treaty assistance.

Revenue Quebec, Press Release, *Zapper : Le ministère du Revenu perquisitionne au Québec et en Colombie-Britannique* (*Zapper : The Ministry of Revenue conducts searches in Quebec and British Columbia*) (in French only)

Consider for example the following e-mail exchange between UK and Swedish auditors about zappers. Agents from HMRC establishing a new anti-fraud audit group are asking their counterparts in Sweden for names of ECRs where zappers have been found as well as whether or not the zapper can be identified in a computer audit. The premise underlying this conversation is that zappers travel easily across international borders. The Swedish auditor's response [necessarily edited for confidentiality purposes] is:

> We have experience [with] several [types of] software but they are local. [They are] produced [developed] in Sweden. [I] don´t think that you have heard of {Zapper name omitted} or {Zapper name omitted} for example.
>
> One [other] system is from Canada I think, {ECR operating system omitted}, but we don´t know so much about it. Other systems are {ECR operating system omitted} from {manufacture's name omitted} and {ECR operating system omitted} from {manufacture's name omitted} but in these system we haven´t revealed any fraud. In {Japanese manufacture's name omitted} there is a system with many names, one is {ECR operating system omitted} and [another] one is {ECR operating system omitted} but it is the same. It is a Spanish program as it seems and we have revealed a lot of fraud in this system and we also know how to reveal it. The {Japanese manufacture's name omitted} pc-system is installed in the cash register {model number of a specific ECR} and {model number of a different specific ECR} as I remember. I have heard that the Nederlands have a system that they have investigated with success but I don´t know the name of it. Perhaps that could be of interest for you. If you need I probably can provide a contact in the Nederlands. But I think the {Japanese manufacture's name omitted}-system should be common in the UK.[31]

It is interesting to note how the Swedish tax official (speaking to a UK auditor) easily goes from a discussion of:

- Swedish zappers (two specific kinds) to the
- Canadian ECR operating system that they work on, and then to
- Spanish zappers and the ECRs manufactured by a

available at : http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2002/24oct.asp (last visited Dec. 18, 2008).

Thus, consider the 2008 case of Logicaisse Computer Systems Ltd. This Quebec company is the exclusive distributor of RMS-Touch software. RMS Touch software in turn is designed and developed by Adler Microsystems Corp., dba RMS-TOUCH, a privately owned company, incorporated in 1986 in New Jersey. Adler is a US company with headquarters located in Fort Lee, about a mile north of the George Washington Bridge.

If Revenue Quebec suspected that the zapper used with RMS Touch was developed at Adler Microsystems and if it wanted to execute search warrants at Adler, it would be a far more complex undertaking than that involved in the British Columbia case. It would involve first a discussion with Canadian federal authorities, who would then enter into treaty discussions with US federal authorities, followed by further discussions with New Jersey authorities. It is important to note that there is no public indication that this kind of four-way enforcement effort has occurred in the Logicaisse case. It is the Canadian company (Logicaisse) not the American company (Adler) who is suspected of developing the zapper. For Revenue Quebec's description of the Logicaisse Ltd. investigation see *supra* note 22 [Revenue Quebec, Press Release, *Les systèmes informatiques Logicaisse ltée dans la mire de Revenu Québec* (Computer systems Ltd. Logicaisse in the grasp of Revenue Quebec) (Mar. 12, 2008) a*vailable at:* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2008/12mars.asp (last visited Dec. 18, 2008).]

[31] Personal e-mail communication, August 31, 2008 (on file with author).

- Japanese company which they work on.

The assumption throughout is that some of these ECR systems should be found in the UK, and if so, then so should the zappers that skim sales when they are installed on them.

SOLUTIONS – POLICY ORIENTATIONS

Globally, two policy orientations guide enforcement actions in this area – one approach is rules-based; the other is principles-based.[32] 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. 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. Jurisdictions taking this approach include the UK and the Netherlands. France has implemented a program of preventive audits that target technology providers.[33] A similar effort can be found in Quebec where the customer lists of audited technology providers have been used to roadmap later audits of businesses suspected of technology-assisted skimming.

Quebec is in transition between these policy orientations. Prior to January 28, 2008 Quebec was squarely with the group that preferred a principles-based approach. However, the Quebec Minister of Revenue, Jean-Marc Fournier, announced[34] that by late 2009 the MRQ will begin testing the *module d'enregistrement des ventes* (MEV).[35] The MEV will be used only 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).

Notably, the US does not have a coordinated zapper enforcement effort. It falls in neither camp. In fact, the US has only uncovered two zappers, one at Stew Leonard's Dairy in Norwalk Connecticut where $17 million in federal tax liabilities accrued from the skimming of a far large

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

[33] *Id.* at 6.

[34] 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 Dec. 18, 2008, translation on file with author).

[35] 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).

amount of profits,[36] 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.[37] The zappers in these cases were found almost by mistake. The *Stew Leonard's Dairy* case came about when a US Customs officer found more than $50,000 in cash in a suitcase carried by Mr. Leonard on one of his frequent trips to St Martin.[38] The *La Shish* case came about because the owners failed to file a tax return. Roy Furchgott of the New York Times reported that, "[a]uthorities declined to comment on how the reported crime was discovered, but according to court records, [the owner] failed to file a tax return in 2003."[39]

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 any state in the US became serious about this problem it might find that we might have a unique blend of rules and principles based solutions if we were to consider a simple extension of the Streamlined Sales and Use Tax Agreement (SSUTA).[40] Under the SSUTA certified third party software providers (CSPs)[41] 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 a state like California that the correct retail sales tax was being collected and remitted, while it could also assure federal authorities that 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.

SOLUTIONS – PRESENT APPLICATIONS

The final section of this paper will consider the range of current solutions to automated sales suppression software. Four approached will be described. The traditional fiscal till solution (employed by Greece) will be contrasted with the traditional principles-based solution (employed by the Netherlands). Because Germany will conclude the development of a smart card in 2009 that will extend, simplify and substantially reduce the costs of a fiscal till solution it will be considered next, along with a proposal to blend rules and principles based solutions in an extension of the SSUTA.

[36] 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).

[37] 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).

[38] *Leonard*, 37 F.3d at 35.

[39] Roy Furchgott, *With Software, Till Tampering Is Hard To Find*, NYT C6 (August 20, 2008).

[40] 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.

[41] *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.")

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.[42] When considered as a whole, these rules attempt to provide complete data security within an ECR.

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.

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).[43]

Data from the electronic journal memory is signed by a secure hash algorithm (SHA-1).[44] This hash value is permanently safeguarded and stored in the fiscal memory. Daily sums

[42] 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

[43] 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.

[44] 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).

(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.[45] 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.[46] A license to sell a specific ECR is issued by a special technical (inter-party)[47] body (committee) and will be issued only when the ECR conforms to all statutory technical specifications.[48] 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.

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

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

[46] 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 32, Appendix D, at ¶ 4.1.

[47] 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.

[48] 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.

document. The whole-day hash value is permanently saved in the FESD's fiscal memory.[49] This preserves all data on the document in detail.[50]

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.[51] 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.

Factory-installed phantom-ware must be removed before certification. If a self-help version of phantom-ware[52] 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[53] 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.

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

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

[51] 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%.

[52]For a discussion of self-help phantom-ware see: Richard T. Ainsworth, *Zappers and Phantomware: The Need for Fraud Prevention Technology*, *supra* note **Error! Bookmark not defined.**.

[53] 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).

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. 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 enforcement measures. 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.

THE NETHERLANDS:
COMPREHENSIVE TRADITIONAL AUDITS

The Netherlands is a principles-based jurisdiction, relying only on traditional audits to detect sales suppression technology. Fiscal till jurisdictions, like Greece, also must rely on audits, but not to the same extent and certainly not with the comprehensive scope as the Dutch. Technology does not replace auditing; it only makes 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, which functions like a Greek FESD, is designed with an auditor's eye. It harmonizes data feeds from widely diverse ECRs, and translates encrypted signatures on receipts into bar codes that can be scanned with hand-held optical readers.

The German assessment, also a fiscal till jurisdiction, 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….[54]

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 always 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 can find a way to get into the Black Box.[55] Similarly in 2007 *Operação Tesouro* (Operation Treasure-hunt) indicates that fraudsters have even been able to tamper 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.[56]

[54] 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).

[55] "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).

[56] *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 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 Dec. 17, 2008) (translation on file with author).

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.[57] 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 clearly at the other extreme. The Dutch are convinced that audits (alone) 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 a few 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.
>
> 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.[58]

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

[57] 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.

[58] 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).

can be seen in the Grand Café Dudok case.[59] 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).[60] 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[61] 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."[62] After this discussion "… an employee of [Straight Systems] visited [Dudok] and explained [and enabled] the application of the erase rule [or hidden delete function[63]], after which [Dudok] subsequently decided to start using [it] …"[64] 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

[59] 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).

[60] 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).

[61] 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).

[62] 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 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).

[63] 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."

[64] LJN: BC5500, at F3.

> 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![65]

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.[66]
- 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).[67]

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 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.[68]

The UK shares the Netherland's opinion,[69] 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.[70]

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

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

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

[68] 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 35 at slide 5.

[69] *See supra* note32, *Cash Register Good Practice Guide*, 1.4.4 & Appendix E.

[70] Jennifer Mitchell, HMRC: Local Comp SME Interventions, personal e-mail communication (Nov. 26, 2008) (on file with author).

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.[71] 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[72] 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[73] that they could form the basis of a solution to zappers.

The INSIKA project was charged with completing the technical specifications for a signature smart card by the summer of 2008.[74] Included with the technical specifications for the

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

[72] 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 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).

[73] 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).

[74] At the time of this draft the INSIKA project appears to be on schedule, although the time line for publication of the results have been pushed back from the summer of 2008 to the autumn, and now to the spring of 2009. Professor Zisky indicates:

signature smart card will be a determination of the data structures and formats, communication protocols and security analysis for the system.[75]

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….
>
> 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.[76]

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

> 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).

[75] 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).

[76] Norbert Zisky, *Manipulation Protection, supra* note 72, at ¶ 5.2 & 5.3.

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 there was no receipt (Greek and Quebec solutions are dependent on "legal receipts.") It would only matter that each item be registered in an ECR or POS system, and for that system to be 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. The Greek solutions cannot 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.[77]

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 concerns over 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. The cost to the government is expected to be $55 million.[78] 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.[79]

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

[77] 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).

[78] 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).

[79] Norbert Zisky, *Manipulation Protection, supra* note 72, at ¶ 5.1.

> 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.[80]

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."[81]

BLENDING RULES & PRINCIPLES: CERTIFICATION OF THIRD PARTY SERVICE PROVIDERS

Certification is the common thread among all zapper enforcement efforts. 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

[80] Personal e-mail communication, Professor Zisky (February 19, 2008) (on file with author).

[81] 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).

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.

Fortunately, there is another option – certification of intermediaries. This approach uses certified service providers (CSPs). CSPs are well known under the Streamlined Sales and Use Tax Agreement (SSUTA), and can be a useful tool for jurisdictions, like California, that seek to develop *less intrusive* and *less expensive* methods for combating automated sales suppression. Currently SSUTA 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 traditional CSP 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 would 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 automated system captures so that it can trust the CSPs attestation of the accuracy of the taxpayer's system; and (4) what is the most efficient and cost effective way for a CSP to satisfy this standard?

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

CSPs currently pull data directly from the ECR or POS system when they are used to determine taxability. This data is stored in an independent (tamper-proof) audit file, and is used by taxpayer to draft the invoice (receipt). The CSP maintains this file to protect itself from liability.

(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.[82] 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.

[82] 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.

This would be a form of comprehensive ECR monitoring,[83] but it is the private sector monitoring the private sector, not an intrusive government oversight program.

(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?*

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*,[84] 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.

[83] 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]."

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

Under the SSUTA model a service provider would 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.

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."[85] 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.[86]

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

[85] *Id.*, at 312-13 (emphasis added).

[86] 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).

researchers soon became aware that there was "…strong resistance against this online tracking of transactions [by the government]."[87] 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.
>
> 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*.[88]

Simply put, even when there is "nothing to hide" there are real privacy concerns when the government gets too intrusive.[89]

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.[90]

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 CSP option should remain open for all businesses. This would increase the pressure on those who do not use CSPs to maintain good records, and traditional audit resources could be more intensively focused on this subset.

CONCLUSION

Automated sales suppression is a global problem, and it will only grow in significance with the 21st century economy. The task in front of this Commission is not easy. It is difficult to

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

[88] 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).

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

[90] 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 77.

craft a stabilizing, revenue neutral tax reform that will modernize, provide jobs and growth but not raise taxes.

However, if there are significant drains on revenue from skimming cash sales, then not only are sales taxes that have been paid by the customer not being remitted to the government, but business income taxes are being under-reported, and most likely cash wages are being paid under the table (and also not reported). Solutions to this problem run from very expensive fiscal till regimes to intensive commitments of specialized audit resources. This is not an area where state and local tax enforcement can piggybacking on a federal audit. *Stew Leonard's Dairy* and the *La Shish Restaurants* are the only federal zapper audits, and neither of these were performed west of the Mississippi.

Fortunately there is a very cost-effective remedy in the CSP option. California has not joined SSUTA, but that does not prevent it from taking an arrow for the SSUTA quiver and directing it at this problem. But those steps will come later. At the moment California needs an empirically valid study of the automated sales suppression within the State, and the Commission on the 21st Century Economy should recommend that be undertaken. If the California study returns results like Quebec's and Germany's, then one would expect to see somewhere in the neighborhood of 50% of all ECRs infected with zappers or phantomware, and that revenue losses range somewhere in the neighborhood of 16% (sales tax, business income tax, payroll taxes and personal income taxes combined).

If results like this seem reasonably likely to the Commission, then it might also recommend that policy level decisions be made now on how to deal with this threat to State revenue – a rules-based fiscal till, principles-based comprehensive audits, or an extended SSUTA-like CSP approach.

In the meantime California might consider reading some foreign newspapers and begin to ask questions when a business with California operations is found to be using zappers to skim cash sales in a foreign jurisdiction. Zappers follow the commercial path cut by ECRs. They do not respect judicial boundaries. For example, when Celine Dion's Nickel restaurant chain was raided by Revenue Quebec, and each of the 32 Nickel restaurants in the Province were found using zappers, the zapper question should have arisen in the mind of the Florida Department of Revenue where there were 2 more Nickel restaurants. It certainly did in the mind of the Ontario authorities where the remaining 10 Nickel restaurants were located.[91]

[91] CBC.com, *Celine Dion-owned Restaurants Raided by Revenue Quebec*, (Nov. 10, 2000) *available at* http://www.cbc.ca/canada/story/1999/03/13/dion_restaurant990313.html. It should be noted that this article states:

> Executives of the Nickels chain went to great lengths Friday to distance Dion from the investigation into possible tax fraud. Gioia Pasqualini, the chain's marketing co-ordinator said: "We want to emphasize that Celine Dion is not part of the daily operations, the daily process at Nickels."

See also: Revenue Quebec, News Release, *Zappers : un administrateur de la société Gamma Terminal Inc. reconnu coupable* (Eng. Trans. *Zappers: Company Director Gamma Terminal Inc. Guilty*) (Nov. 15, 2000) (indicating that Rejean Turcott, the Director of Gamma Terminals Inc. pled guilty to selling zappers to the Nickel Restaurants) (French only) *available at http://www.revenu.gouv.qc.ca/fr/ministere/centre_information/communiques/ev-fisc/2000/15nov.asp*. It should be further noted that Mr. Turcott's company, Gamma Terminals Inc., is a Canadian company holding exclusive Canadian sales rights for a restaurant computer system manufactured by an American company, Gamma Micro Systems, with head offices in Montreal. *Turcotte v. Québec (Ministry of Revenue)*, 1998 CarswellQue 1041, [1998] R.D.F.Q. 110 (Superior Court of Québec).