

# BOSTON UNIVERSITY SCHOOL OF LAW

WORKING PAPER SERIES, LAW AND ECONOMICS  
WORKING PAPER NO. 08-07



**ZAPPERS: TAX FRAUD, TECHNOLOGY AND TERRORIST FUNDING**  
Forthcoming ABA Tax Lawyer: State and Local Edition, 2008

RICHARD THOMPSON AINSWORTH

This paper can be downloaded without charge at:

The Boston University School of Law Working Paper Series Index:  
<http://www.bu.edu/law/faculty/scholarship/workingpapers/2008.html>

The Social Science Research Network Electronic Paper Collection:  
<http://ssrn.com/abstract=1095266>

## Zappers: Tax Fraud, Technology and Terrorist Funding

Richard Thompson Ainsworth

“Zappers,<sup>1</sup>” or automated sales suppression devices, have brought unheard of efficiencies and economies of scale to a very simple tax fraud – skimming the cash sales that pass through point of sale (POS) systems, network connected electronic cash registers (ECRs). Until recently “the largest criminal tax case in the history of Connecticut,”<sup>2</sup> which also was the “largest computer driven tax-evasion case in the nation,”<sup>3</sup> was a Zapper case. Stew Leonard’s Dairy (a local grocery chain associated at one time with a dairy farm) in Norwalk Connecticut skimmed an estimated \$17 million in

---

<sup>1</sup> A “sales Zapper” is (was) a specific commercially available product identified through investigative reports in the Canadian press in 1997. Within weeks “Zappers” became the focus of intensive Provincial/Federal enforcement actions (activities are ongoing). The term “Zapper” became a short-hand expression referring to the whole class of automated sales suppression devices, and this is the manner on which it is used in this paper. Thus, in an April 25, 2001 internal memorandum from Regional Attorneys Serge Clairoux and Jean Marois to Jean-Francois Normand at the Head Quarters for the Underground Economy, Canadian Customs and Revenue Agency refers to the “Zapper Initiative,” and indicates:

### **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 12<sup>th</sup>, 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.).

<sup>2</sup> DEPT. OF THE TREAS., I. R. S. 75 YEARS OF CRIMINAL INVESTIGATION HISTORY (1919 – 1994) 146, available at [http://www.thememoryhole.org/irs/irs\\_75\\_years.rtf](http://www.thememoryhole.org/irs/irs_75_years.rtf) (last visited Feb. 3, 2008).

<sup>3</sup> Jacques Steinberg, *Connecticut Store Owner Sentenced in Tax Fraud*, NYT, Sec. B, page 1, col. 3 (Oct. 21, 1993)

receipts over a ten year period. The cash was taken in large denomination bills by suitcase to St. Martin in the Caribbean.<sup>4</sup>

More recently, Talal Chahine and his wife, Elfat El Aouar, owners of the thirteen store La Shish restaurant chain in Detroit, Michigan acquired the dubious distinction of replacing *Stew Leonard's Dairy* as the leading U.S. Zapper case. Although Elfat was sentenced, May 16, 2007, to 18 months for tax evasions, Talal remains a fugitive from U.S. authorities (believed to be in Lebanon) with a warrant issued for his arrest.<sup>5</sup> Together they zapped more than \$20 million in cash sales over a four year period and sent the funds in small denomination cashiers checks to Hezbollah in Lebanon.<sup>6</sup> Both *Stew Leonard's Dairy* and the *La Shish* restaurant cases were federal income tax investigations. Related State sales tax enforcement actions commenced after the federal investigation was well underway.<sup>7</sup>

---

<sup>4</sup> U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), *aff'd*, 67 F.3d 460 (2nd Cir. 1995) (although the tax case was settled, the details of the fraud are preserved in these federal sentencing appeals).

<sup>5</sup> 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](http://www.cybersafe.gov/tax/U.S.aopress/2007/txdv072007_5_15_ElAouar.pdf) (last visited Feb. 3, 2008).

<sup>6</sup> Press Release, U.S. Dept of Justice, Eastern District of Michigan, Superseding Indictment returned Against LaShish Owner (May 30, 2007) *available at*: [http://www.justice.gov/tax/usaopress/2007/txdv072007\\_5\\_30\\_chahine.pdf](http://www.justice.gov/tax/usaopress/2007/txdv072007_5_30_chahine.pdf) (last visited Feb. 3, 2008).

<sup>7</sup> In the *Stew Leonard's Dairy* case U.S. Customs searched Stew Leonard Sr. in the Spring of 1991, leading to the execution of search warrants on August 9, 1991 by special agents of the IRS Criminal Investigation Division. *Leonard*, 37 F.3d at 35; 75 YEARS OF CRIMINAL INVESTIGATION HISTORY, *supra* note 2, at 145. The State of Connecticut commenced its audit "... as a result of IRS actions, in February, 1992 ..." *Leonard*, 254 Conn. 286, 289 (2003). On July 22, 1993 Stew Leonard pleaded guilty in the federal audit. The State's audit was no where near completion at this time. A final Connecticut determination was not rendered until February 27, 1996.

The La Shish case seems to follow a similar pattern, although this cannot be stated with certainty. The only public information on the La Shish case is through court documents filed in the federal enforcement action. Nothing is public from the State of Michigan, although it would seem clear that along with the skimmed gross receipts would be skimmed sales tax. There is no record of a prior State of Michigan tax, or related search and seizure action. In a request for this information Mike Eschelbach, Administrative Law Specialist, Tax Policy Division replied:

Michigan law (Michigan Compiled Laws Section 205.28(1)(f)) prohibits divulging any facts or information obtained in connection with the administration of a tax, or information or parameters that would enable a person to ascertain the audit selection or

Zapper fraud is not confined to the U.S. Zappers are a significant problem in the European Union (EU) where it is under the intense scrutiny of a nine country research group, the Fiscalis Committee's Cash Register Project Group.<sup>8</sup> Zappers have been detected in Canada, Brazil, Australia, Sweden, Norway, Belgium, Portugal, Germany, the Netherlands and France. A German Working Group on Cash Registers, comprised of the highest-tier central and regional tax authorities, is examining Zappers. An Interim Report has been released.<sup>9</sup> Work on a technological solution to Zapper fraud is underway at the German National Metrology Institute (PTB: Physikalisch-Technische Bundesanstalt) where the INSIKA project (Integrierte Sicherheitslösung für Kassensysteme – Integrated Security Solutions for Cash Registers) was opened in 2008. A Canadian pilot project will test a similar solution in November 2009 in volunteer restaurants in Montreal and Quebec City.<sup>10</sup>

However, when the U.S. Zapper experience is placed alongside experiences in other countries, it is not the *similarity* in the fraud-mechanism (the Zapper) that is the most striking – it is the *difference* in the way Zappers are uncovered that catches one's attention. Outside the U.S. Zappers are identified primarily through consumption tax

---

processing criteria of the department for a tax administered by the department.

According, we are unable to provide you with the information you seek.

Personal e-mail communication, Feb. 4, 2008 (on file with author).

<sup>8</sup> The Cash Register Project Group is comprised of representatives of nine Member States (Belgium, Germany, Greece, France, Ireland, Hungary, the Netherlands, Turkey and the United Kingdom). The group is part of the Fiscalis Committee and reports to the Directorate-General Taxation and Customs Union on the "... identify[ication of] risks in cash registers and point of sale systems and develop[ment of] ideas on how to counter such risks." Fiscalis Committee – Action Plan 2005-2006, TAXUD/A2/NP (Feb. 15, 2005) *available at*

[http://www.finance.gov.sk/EN/Documents/1\\_Adresar\\_redaktorov/Valentovicova\\_Z/50929\\_29\\_Action%20Plan%202005-2006\\_EN\\_v2.2.rtf](http://www.finance.gov.sk/EN/Documents/1_Adresar_redaktorov/Valentovicova_Z/50929_29_Action%20Plan%202005-2006_EN_v2.2.rtf) (last visited Feb. 3, 2008). The details of the Group are *available at* <http://ec.europa.eu/transparency/regexpert/detail.cfm?ref=2092&l=F> (last visited Feb. 3, 2008).

<sup>9</sup> Working Group on Cash Registers: Interim Report (Mar. 16, 2005) (Ger.) (on file with author).

<sup>10</sup> Revenue Quebec, Press Release, For More Equity in the Restoration – It is Necessary that it Happens Above the Table (Jan. 28, 2008) *available at*: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiqués/autres/2008/28jan.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/autres/2008/28jan.asp) (in French only) (last accessed Feb. 12, 2008).

(VAT or GST) audits. Within the U.S. Zappers are uncovered primarily through federal income tax investigations.

Not surprisingly, the investigative results also differ. Consumption tax investigations tend to focus on the Zapper itself (a specific fraudster involved being of secondary importance). Income tax investigations tend to focus on a fraudster (with the specific Zapper involved being of secondary importance). The Zapper is seen simply as the means selected in this instance to commit the fraud. Consumption tax investigations frequently result in multiple enforcement actions against many unrelated (but competing) businesses, all of whom are using the same or similar Zappers.<sup>11</sup> In contrast, income tax

---

<sup>11</sup> For example, consider “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 supermercados 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](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).

A similar investigation (2007) also in Brazil, *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.

?Technological 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*)

investigations frequently result in isolated, single taxpayer enforcement actions. Thus, where consumption tax enforcement may uncover tens or even hundreds of Zappers within a market-place (many of whom may be engaged in relatively low levels of fraud), income tax enforcement actions focus on specific taxpayers (whose fraudulent activity either has a very significant revenue impact, or has other serious consequences – such as funding terrorist).

This paper (a) reviews U. S. and foreign experience with Zappers; (b) indicates how income tax enforcement (when undertaken alone) may miss the “full enforcement” mark; and (c) advocates technology-intensive, Federal/State cooperative enforcement efforts against Zappers. The primary recommendation is for creative use of certified tax software solutions under the Streamlined Sales and Use Tax Agreement (SSUTA).<sup>12</sup> A certified service provider<sup>13</sup> under the SSUTA, with current levels of technology can be employed in conjunction with the cryptographic cash register security process under development through the German “Tamper-proofing Electronic Cash Registers” project<sup>14</sup> to assure (a) that the correct retail sales tax is being collected and remitted, and (b) that cash receipts (the income tax issue) are not being skimmed by Zappers.

## SKIMMING CASH SALES

---

JOURNAL DA MIDIA (Oct. 2, 2007) *available at*: [http://www.jornaldamidia.com.br/noticias/2007/10/02/Bahia/Sonegacao\\_fiscal\\_leva\\_sete\\_empres.shtml](http://www.jornaldamidia.com.br/noticias/2007/10/02/Bahia/Sonegacao_fiscal_leva_sete_empres.shtml) (in Portuguese) (last visited Feb. 17, 2008) (translation on file with author).

<sup>12</sup> 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).

<sup>13</sup> *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.”).

<sup>14</sup> Working Group on Cash Registers, *supra* note 9, at 11. Vectron Systems AG has successfully worked out a technical solution to the cryptographic problem, and has presented their solution to German, Swedish and Dutch tax administrations. See Tamper-proof POS Data: 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).

Sales can be skimmed with or without Zappers. It is a simple matter of keeping two tills, one for the taxman and the other for the owner.<sup>15</sup> Businesses engaged in this kind of fraud target cash sales, because cash transactions have a narrower trail. Credit card transactions are more easily traceable. This “cash sales” attribute makes skimming frauds common in restaurants, supermarkets, hairdressers and phone shops.

A few examples of skimming frauds may be helpful. Skimming cash sales presents fraudsters with two basic problems: (a) how to keep the skimming a secret (from people who are involved in the business, but not benefiting from the skimmed proceeds – the other employees or the independent accountant<sup>16</sup>), and (b) what to do with the cash hoard once it has been segregated (depositing funds off shore,<sup>17</sup> paying special employees in cash “under the table,”<sup>18</sup> and keeping some of the true owners of the business hidden are some of the methods used<sup>19</sup>). These “risks” are a concern for fraudsters, and encourage them to find more “hidden” methods of skimming – methods that frequently involve technology.

---

<sup>15</sup> The Fiscalis Cash Register Project Group lists forty-two methods of skimming cash receipts (only some of which could be called Zappers) divided into three main groups or “risk types:” (1) Transactions not registered; (2) Manipulation of the records registered; and (3) Registration records that do not match accounting records. FISCALIS FPG 12, CASH REGISTER PROJECT GROUP, CASH REGISTER GOOD PRACTICE GUIDE, Appendix B, at ¶¶ 3.1 – 3.3 (unpublished report on file with author).

<sup>16</sup> *F-D Oil Company, Inc. v. Commissioner of Revenue*, 560 N.W.2d 701 (1997) (the informant on the skimming operation was the bookkeeper who reported the scheme to the Minnesota Department of Revenue and the U.S. Internal Revenue Service).

<sup>17</sup> *Stew Leonard's Dairy*, 37 F.3d at 35 (indicating that the skimming fraud was uncovered by U.S. Customs officers searching the luggage of Stew Leonard Sr. as he left for St. Martin).

<sup>18</sup> AUSTRAC, ANNUAL REPORT 2006-2007 at 22 (indicating that a skimming fraud was uncovered by the Australian Tax Office based on anonymous information that a restaurant was paying wages in cash and not remitting Pay As You Go tax. In this case the skimming fraud involved a Zapper that manipulated the sales reports. Funds were sent overseas in small dollar amounts and then loaned back to the restaurant. AUD\$8.4 million was collected in tax and penalties in this case that attracted the attention of the Australian money laundering agency as well as the ATO).

<sup>19</sup> *Nicholas Guercio & Victoria Constantine (formerly Guercio) v. Commissioner*, T.C. Memo 1983-554 (1983) (involving a bar owned by three individuals who tried to keep the skimming hidden by hiding ownership interests).

*Aleef Garage Ltd.* On November 12, 2007 seven people were jailed for over eleven years in Liverpool, U.K. for their part in a £5.3 million tax fraud that essentially involved skimming cash sales from newspaper sales and automobile repairs.<sup>20</sup> Aleef Garage Ltd., founded over twenty-five years ago, is among the largest family owned retailers in the North West U.K. with over fifty petrol stations and shops in the city centers of Greater Manchester, Lancashire and Cheshire. The business employed approximately 250 people with an annual turnover in excess of £92 million.<sup>21</sup> As reported in Director of Finance On Line:

The cash fund [that was skimmed] had been principally achieved by a number of newsagents operating two tills, but only declaring in the official records the money which was taken from one of them, and simply keeping quiet about the money that was taken in the second till.

The majority of [the Aleef] newsagent shops are in the center of Manchester and a city center newsagent is an ideal location for a fraud of this nature as there is rapid turnover of customers, most of whom are in a hurry, and all of whom are paying in cash. The conspirators deliberately suppressed the takings in one of the tills in their accounts and only declared the money in the other till to HMRC.<sup>22</sup>

The founder of Aleef Garage Ltd., Ahmed Patel, operated a charity – the Greater Lever Muslim Society. Cash from Aleef Garage Ltd. was laundered through this charity and then back to the Patel family.<sup>23</sup>

---

<sup>20</sup> HMRC News Release, Company Directors Jailed for £5million Fraud (Nov. 13, 2007) available at <https://www.gnn.gov.uk/content/detail.asp?NewsAreaID=2&ReleaseID=330199> (last visited Feb. 4, 2008) (indicating that along with the skimming fraud there were related tax frauds associated with suppression of stock purchases, and payment of tax free undeclared wages).

<sup>21</sup> Chris Osuh, *Aleef Bosses Jailed for Fraud*, Manchester Evening News, Nov. 11, 2007, available at: [http://www.manchestereveningnews.co.uk/news/s/1024144\\_aleef\\_bosses\\_jailed\\_for\\_fraud](http://www.manchestereveningnews.co.uk/news/s/1024144_aleef_bosses_jailed_for_fraud) (last visited Feb. 4, 2008).

<sup>22</sup> Adrie van der Luijt, *Directors Jailed for Accounting Fraud*, Directors of Finance On Line (Nov. 13, 2007) available at: <http://dofonline.co.uk/economy/directors-jailed-for-accounting-fraud9284.html> (last visited Feb. 4, 2008).

<sup>23</sup> The U.K. Charity Commission reported that the annual turnover of the Greater Lever Muslim Society never exceeded £10,000 in any year from the charity's formation in the 1990's up until 2002 (the year HMRC revenue audit began), although in excess of £2.5 million had been deposited through that time. Funds moved from the charity back to the Patel family through Channel Island accounts. HMRC News Release, *supra* note 20, at Notes for Editors 2; Chris Osuh, *supra* note 21.

The success of the *Aleef Garage* fraud depended on close family relationships.

Three sons of the founder, Mustaq Hussain Patel (53) – in charge of overall finances of Aleef, Iqbal Ahmed Patel (51) – in charge of staff and responsible for wages, and Mubarakali Ahmed Patel (55) – in charge of the newsagent side of the business, were the main conspirators.<sup>24</sup> As Steve Armit, 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.”<sup>25</sup>

It is not clear from published reports how the *Aleef Garage* fraud was initially uncovered, although the HMRC News Release does indicate that “... the cash was used to fund private life styles, [but it was also] transferred to other personal accounts including some in the Channel Islands.”<sup>26</sup>

*Stew Leonard’s Dairy*. Stew Leonard’s Dairy was also a “family owned and operated” business. Stew Leonard, Sr., the 80% owner, CEO, and Chairman of the Board of the Dairy masterminded the fraud. His main co-conspirators were (a) his brother-in-law, Frank H. Guthman, (b) Frank’s brother, Steven Guthman, and (c) Barry Belardinelli, the CFO, an unrelated employee who had worked for the store since it opened in 1969.<sup>27</sup>

The skimming fraud in Stew Leonard’s Dairy began to unravel when “... United States Customs officials searched [Stewart] Leonard [Sr.] as he was about to board a flight for St. Martin and found \$20,000 on his person and another \$50,000 in his luggage

---

<sup>24</sup> HMRC News Release, *supra* note 20, at Notes for Editors 3, 4 & 5 (others involved in the conspiracy were Nichole Marie Patel (34), Inayat Patel (34), Hanif Mahmed Patel (46), usman Abdullah Patel (45), Javeed Bashir (48), and Ibrahim Vali Patel (55)).

<sup>25</sup> *Id.* at 1.

<sup>26</sup> *Id.* at 1.

<sup>27</sup> Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d at 34.

...”<sup>28</sup> However, it was the owner’s son, Stewart Leonard, Jr., president of the Norwalk store who revealed the full scope of the fraud in a 36-page document filed with the court before sentencing. The younger Leonard received immunity from prosecution, in spite of being the person who at times, “... executed the computer program that doctored the store’s reported revenues.”<sup>29</sup>

*Nicholas Guercio & Victoria Constantine (formerly Guercio) v. Commissioner.*<sup>30</sup>

The *Guercio* case involved a bar that was open twenty hours per day (6 a.m. to 2 a.m.) serving customers on two shifts. Business was conducted only in cash, and the physical skimming of sales was very simply carried out. Tills for each shift were checked against cash register tapes (to prevent employee theft), but the owners presented the accountant only one of the tills and one of the cash register tapes for each day’s operation.<sup>31</sup> Bank deposits and tax returns were filed based on the funds and the tapes from the disclosed tills.

Each Monday the owners met, divided the cash from the withheld tills and destroyed the withheld register tapes. Because two of the owners, representing 80% of the equity interests were “hidden” behind Guercio (a nominee holder of their interests) most of the skimmed cash left the business each Monday without a trace.<sup>32</sup>

---

<sup>28</sup> *Id.* at 35.

<sup>29</sup> Jacques Steinberg, *supra* note 3.

<sup>30</sup> Guercio & Constantine, T.C. Memo 1983-554.

<sup>31</sup> Accountants and bookkeepers frequently become informants in skimming cases. For a case where a bookkeeper led the IRS and the Minnesota Department of Revenue to a cash skimming scheme in an auto repair shop see *F-D Oil Company, Inc. v. Minnesota Commissioner of Revenue*, 560 N.W.2d 701 (1997). Although the shop destroyed its records of invoices issued, the nature of the auto repair business is such that many customers kept accurate records of repairs (even those paid in cash) to substantiate later warranty claims. Thus, unlike the situation where cash payments are made in restaurants and bars, the auditors in *F-D Oil* could readily identify mismatches between the accounting records and actual repair services rendered.

<sup>32</sup> By keeping 80% of the ownership interests “hidden” the fraudsters in *Guercio* sought to forestall a bank deposits analysis whereby an individual’s reported income and nontaxable items are subtracted from total deposits to determine unreported income. For a restaurant skimming case where a bank deposits analysis is

## SKIMMING CASH SALES WITH TECHNOLOGY

It is a short step from the manually skimming of sales in *Aleef Garage Ltd.* and *Guerico* to the technology-assisted skimming in *Stew Leonard's Dairy* and *La Shish*. Why do some frauds move into technology, and others do not? The answer cannot be simply the size of the skimming. Certainly technology increases the capacity to skim cash sales. Large scale (multi-cash register) skimming is more possible with technology, although *Aleef Garage* indicates that with tight “family” controls million dollar skimming operations are very possible with a manual, two-till system. Technology also allows skimming operations to be conducted remotely (away from the tills) in a back room, or even off the business premises.<sup>33</sup> But this too is not necessary, if a close “family” is united behind the fraud.

It is apparent however, that the use of technology in skimming frauds is functionally related to two factors (a) business size, and (b) the fraudster’s perceived risk of detection. Business size defines the locus of this fraud – it establishes both the low and the high end. Because sophisticated POS systems are costly, very small businesses simply cannot afford to go digital. Thus, as the cost of technology falls, the lower end of the fraud locus will expand the field. Business size also determines the upper end of the locus. Because public companies (or large private companies) formalize their internal

---

successful see *William C. Beretta v. Commissioner*, T.C. Memo 1997-570. Mr. Beretta was an IRS employee, Collections Division, who also invested in restaurants.

<sup>33</sup> This was how the Zapper in the *La Shish* case operated. In response to an e-mail inquiry asking if the skimming fraud in this case was the result of (1) manual double-tills; (2) fraudulent use of factory installed software in ECRs; (3) a Zapper located on a server away from the ECRs, the U.S. Attorney in charge of the *La Shish* investigation [Ken Chadwell, USAMIE] indicated:

LaShish skimming was accomplished thru method number 3 at the off site server capable of producing two reports, one actual and one altered. The fake report was the result of a pre-programmed skim of cash receipts from each of 13 restaurants after the server received the true information electronically. The fictional report would also reflect fewer items being sold, for example, 25 falafels might become 10 for the day to match the false bottom line.

Personal e-mail communication Jan. 3, 2008 (on file with author).

controls, it is difficult to skim cash sales from these enterprises simply because skimming requires the removal of large amounts of cash from normal bank deposit procedures.

Third-party monitored internal controls will almost always prevent this.<sup>34</sup> Cash skimming is therefore a fraud dominated by small and medium sized enterprises (SMEs).

Assuming a business of appropriate size, the single factor that pushes (and pulls) a skimmer into technology is perception – the perceived “risk of detection” from government audits, and the perceived “shelter from detection” that technology offers. Therefore, to combat this fraud revenue authorities need a two-pronged approach – they need to: (1) increase the risk of detection, and (2) decrease the shelter of technology.

One of the most effective ways to increase the risk of detection is to coordinate income and consumption tax audits. There is a natural synergy between *annual* income tax audits of gross sales figures, and *transactional* consumption tax audits of a firm’s sales records. Where an income tax audit may be willing to sample sales data for errors, a consumption tax audit is inclined to become granular – make determinations on an invoice-by-invoice basis. This kind of coordination may be less likely in the U.S. than in most jurisdictions, because in the U.S. these taxes are not only audited by different agencies, they are audited by different levels of government altogether. In jurisdictions where there is both a national income tax and a national consumption tax (VAT or GST) coordination is much easier.

One of the most effective ways to decrease the perceived shelter of technology for cash sales skimming is to publicly demonstrate effective enforcement actions.<sup>35</sup> Another

---

<sup>34</sup> CASH REGISTER GOOD PRACTICE GUIDE, *supra* note 15, at ¶¶ 2.5 – 2.5.4.

<sup>35</sup> Revenue Quebec lists on their web site over 100 instances of successful enforcement actions against technology-assisted cash skimming frauds. *See*: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiques/ev-fisc/](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/) (in French only)

way of doing this is to underscore that technology is a double edged sword for business owners who are not computer specialist. When the computer specialist that sets up and maintains a skimming system is an outsider (an employee, or an independent contractor rather than a family member), this person frequently becomes the government's star witness (with immunity) when fraud is uncovered. There is, of course, a third way – one that is under active investigation and refinement in Canada and Germany – simply make ECRs and POS systems tamper-proof through technology (mandatory or voluntarily adopted).

The following cases from Australia, the U.S. and Canada demonstrate the earlier of these observations. The technology-based solutions of Canada and Germany are considered later.

*Regina v. Ida Ronen; Regina v. Nitzan Ronen; Regina v. Izar Ronen.*<sup>36</sup> Over a ten year period from 1991 through February 7, 2001 Ida Ronen and her two sons skimmed an estimated AUD\$15 to \$17 million in cash sales from their clothing business (Dolina).<sup>37</sup>

“...[T]he scope of the fraud represented by unpaid [income] tax was approximately [AUD] \$8.125.”<sup>38</sup> The court indicates that:

Mrs. Ronen managed the business for herself and, in effect for her sons. Customers of the retail outlets purchased by cheque, EFTPOS, credit or cash. The precise method varied over the period of the conspiracy. The method of implementation [of the conspiracy] agreement was simple in the extreme. In general terms Mrs. Ronen, on behalf of herself and her sons, skimmed from the takings most, if not all, of the cash and later distributed it to her sons and herself for their own purposes. ... For example, in the period of surveillance between April 2000 and 7 February

---

<sup>36</sup> 2005 NSWSC 991.

<sup>37</sup> A number of wholesale and retail businesses operated under this name: Dolina Enterprises Pty Ltd.; Dolina Fashion Group, and a joint venture between these groups. Clothing was sold through conventional (third-party) retail shops (Coles Myer, David Jones and Rockmans) as well as through shops run directly (Ronen Young Fashions, Dolina On Fovo, Fashion Bargains as well as a retail outlet opened on the factory premises. The retail outlets were heavily involved in discounting their clothing.

<sup>38</sup> *Ronen*, 2005 NSWSC, at ¶14.

2001, there was approximately 74% of the cash skimmed sent overseas or kept in the safe. ... [AUD]\$ 753,400.00 was sent overseas ... [AUD] \$209,525.00 was seized from the safe, ...<sup>39</sup>

During most of the time the *Ronen* fraud was taking place Australia did not have a national consumption tax. Like the U.S., Australia relied almost exclusively on the income tax, although beginning in 1930 there was a Wholesale Sales Tax on certain goods imported or produced in Australia.<sup>40</sup> In July 2000 the Wholesale Sales Tax was replaced by the Goods and Services Tax (GST) and this had a dramatic affect on the *Ronen* fraud. The court notes:

A complication arose in the middle of the 2000 calendar year. As from 1 July 2000 the Goods and Services Tax regime was introduced. This posed a considerable problem for the offenders because *proper compliance with the requirements of the GST laws would have revealed in a dramatic manner the amount of cash takings received in each of the retail shops*. The intercepted telephone calls to which I have made reference show the substantial concerns of each of the offenders had about this situation. They show their attempts to devise a system to overcome the problem that they perceived might well bring about their undoing.<sup>41</sup>

Mrs. Ronen took two steps, both of which involved technology. (1) A computer program was developed (by George Segal, Mrs. Ronen's "de-facto husband") to calculate the amount of cash that could be skimmed from each business, one that would take into account the GST and permit at least 10% of the cash receipts of each business to be regularly banked.<sup>42</sup> (2) A technology consultant, Mark Talbot, was hired to set up a computer system that would allow Mrs. Ronen to run false till rolls for each retail outlet. These false till rolls "... were intended to give the impression to the authorities, should

---

<sup>39</sup> *Ronen*, 2005 NSWSC, at ¶18.

<sup>40</sup> Australian Government, Australian Tax Office, Australian Tax History 1900 – Present, *available at*: [http://www.ato.gov.au/corporate/content.asp?doc=/content/tax\\_history.htm](http://www.ato.gov.au/corporate/content.asp?doc=/content/tax_history.htm). The Ronens were not subject to the Wholesale Sales Tax.

<sup>41</sup> *Ronen*, 2005 NSWSC, at ¶24 (emphasis added).

<sup>42</sup> *Ronen*, 2005 NSWSC, at ¶¶25 & 27.

they investigate, that the shops were regularly banking cash as well as other forms of takings related to the shops.”<sup>43</sup> The false till rolls were run at Mrs. Ronen’s apartment, not on the business premises. “Both Mr. Segal and Mr. Talbot [with immunity] gave evidence at the trial for the prosecution.”<sup>44</sup>

Although it is clear that the Ronens were very concerned about the impact of the GST, it is not at all clear that the *Ronen* fraud would have been uncovered through a standard GST audit. In fact, “[t]he conspiracy came to light only by chance. It appears, as a result of telephone intercepts being placed on another person’s telephone service, that the Ronens’ involvement in the distribution of large amounts of money from Australia to overseas locations was detected.”<sup>45</sup> Nevertheless, the dynamics of the *Ronen* case were largely controlled by perceptions – the perception that there was an increased risk of detection through a GST audit, and the perception that technology offered shelter from detection.

*Stew Leonard’s Dairy*. Skimming of cash receipts began in Stew Leonard’s Dairy in the 1970’s. The physical skimming was performed by the CFO, Barry Belardinelli who worked in the store’s vault room where he received bags of cash from the store’s cash registers.<sup>46</sup>

The skimming was manually coordinated by Belardinelli (with the amounts and days of the week when skimming would be performed designated by either Frank or Steven Guthman) until 1981 or 1982 when the skimming was automated. It is not specified in any of the cases what the exact motivation for the automation was, but it

---

<sup>43</sup> *Ronen*, 2005 NSWSC, at ¶26.

<sup>44</sup> *Ronen*, 2005 NSWSC, at ¶26.

<sup>45</sup> *Ronen*, 2005 NSWSC, at ¶28.

<sup>46</sup> *Leonard*, 37 F.3d at 33.

appears from the complexity of the program, that technology offered shelter from detection. The Second Circuit indicated:

To conceal the skim, defendants instituted a computer program that altered the stores sales data to account for the skimmed cash. Creation of the program was necessary to synchronize the data generated by the computerized cash registers with the information generated by Belardinelli's altered daily sales reports. In 1981 or 1982, Frank Guthman instructed Jeffrey Pirhalla, a store computer programmer, to write a complex program [called the "Equity Program"] that reduced the store's sales and financial data by the amount of the skimmed cash and permanently altered the data from which the books and records were created. The program left no audit trail that it had run. Frank Guthman operated it on the first day of each accounting week using the figures provided him by Belardinelli and kept the tape cassette containing the program hidden in his office. He instructed Pirhalla to keep the program secret and, from time to time, told Pirhalla to alter the program to keep up with the store's changing computers.<sup>47</sup>

Like *Ronen*, where fear of detection through a GST audit precipitated the automation, so too in *Stew Leonard's Dairy*, the fear of a Connecticut retail sales tax audit may have been a factor in automating this skimming fraud. Even though, "... only a minimal percent of the Dairy's sales are taxable [under the Connecticut sales and use tax],..."<sup>48</sup> the Equity Program was designed to "... never touch the 'sales tax collected' data generated by the scanning cash registers at the point of sale, nor other categories of data such as credit sales, gift certificates, bottle deposits, etc...."<sup>49</sup> If indeed this was a motivating fear in *Stew Leonard's Dairy*, the Equity Program proved to be a success. The State of Connecticut was never able to prove consumption tax fraud.

However, not only was the Equity Program designed to immunize the Dairy from retail sales tax irregularity, it was also designed to withstand the scrutiny of a standard

---

<sup>47</sup> *Id.* at 35.

<sup>48</sup> *Leonard*, 264 Conn., at 305 (estimates of taxable sales under the Connecticut sales and use tax ranged from less than 5% to as much as 15% of overall Dairy sales).

<sup>49</sup> Brief for Appellee at 17, *Stewart J. Leonard Sr. dba Stew Leonard's Dairy v. Commissioner of Revenue Services*, 264 Conn. 286 (2003) citing Pirhalla trans., 17-22 [AE 41-46].

income tax audit – specifically, an audit that would systematically endeavor to match purchases (inventory) against sales. As the Connecticut Supreme Court observed:

The Dairy's sales recording system was composed of a computerized cash register system that recorded the sales at the time of the transaction. At the point of sale, each product, which contained a universal product code (UPC) indicating its taxable or non-taxable status, was scanned and the resulting sales information was transferred to the main computer terminal. The Equity Program, among other things, altered some of the UPC-based computerized records of the Dairy's gross sales. Specifically, the program reduced *item and dollar sales* across a broad range of products to correspond with the amount of cash diverted each week.<sup>50</sup>

Both prices and units sold were adjusted in small amounts on designated days by the Equity Program. Minor price changes or small but evenly spread out increases in spoilage were designed to make the skimming nearly undetectable on normal audit. The Connecticut Superior Court makes this clear:

As an example, the program was designed to say that today's criteria for the sale of cucumbers would be 50 units. If more than 50 units of cucumbers were sold, the excess was diverted into the Equity Program. The Equity Program scanner went through *every single item* that was sold that day. The amount diverted was spread over a wide spectrum of products. *Some calculations amounted to pennies per item.*<sup>51</sup>

However, in spite of all this care and risk of detection reduction, just as in *Roenen*, the risk that could not be accounted for was the computer programmer himself. Once fraud was suspected, “[t]he IRS and U.S. Attorney [became] very interested in Mr. Pirhalla's first-hand knowledge, and immediately enlisted his cooperation in return for granting him immunity from prosecution. ... The IRS [also] retained the services of NCR [National Cash Register] personnel who were expert in the Dairy's computer

---

<sup>50</sup> Id., at 298 (emphasis added).

<sup>51</sup> Stewart J. Leonard Sr. dba Stew Leonard's Dairy v. Commissioner of Revenue Services, No. CV 980492503S, 2000 Conn. Super. LEXIS 991, at 4-5 (Conn. Sup. Ct. Jun. 10, 2003) (emphasis added).

system. They, along with Mr. Pirhalla, worked under the supervision of special agent Doreen Schultz, the IRS’s own computer book-keeping system expert.”<sup>52</sup>

*Audio Lab Inc.; Mr. Michel Roy; Mr. Luc Primeau.* It is not long before computer program specialist (like Mr. Talbot in *Ronen* and Mr. Pirhalla *Stew Leonard’s Dairy*) rather than working as employees begin to market their skills as independent “sales suppression consultants.” Such a consultant is someone who can not only provide the software, but he can install it, update it, and can assist owners as they scheme about ways to maximize the effectiveness of a Zapper within their particular businesses.

As Revenue Quebec began to aggressively audit this field it uncovered a significant underground economy, one that profited from the development, installation and management of Zappers – sales suppression software. Skimming was no longer something that an unscrupulous SME owner thought of on his own; it was something that was suggested to him (sold to him) by a technology consultant who could demonstrate how easy it was to carry out. It should be noted now, that rather than becoming the government’s “star witness” (with immunity), these consultants are the real target of investigations. It is the Zapper-consultants that are the carriers of this fraud throughout the underground economy.

*Audio Lab.* 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

---

<sup>52</sup> Brief for Appellee, *supra* note 49, at 17-18.

“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.<sup>53</sup>

Next year, on April 25, 2005, Revenue Quebec announced that the director of San Antonio Grill pleaded guilty to using a Zapper.<sup>54</sup> A related company of similar name, Grill San Antonio in Repentigny, also pleaded guilty to similar offences.<sup>55</sup>

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.<sup>56</sup> 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

---

<sup>53</sup> Revenue Quebec, News Release, 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/communiqués/ev-fisc/2004/08avril.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2004/08avril.asp) (in French only, last visited Feb. 8, 2008).

<sup>54</sup> The director, Mr. Apostolos Mandaltsis, was personally fined \$65,681.00 and \$10,300 respectively for PST (Provincial Sales Tax) and GST (federal Goods and Services Tax). Taxes and interest were due in addition.

<sup>55</sup> PST and GST fines of \$23,416 and \$8,603 were due in addition to taxes and interest. Revenue Quebec, News Release, 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/communiqués/ev-fisc/2005/25avril.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2005/25avril.asp) (in French only, last visited Feb. 8, 2008).

<sup>56</sup> Revenue Quebec, News Release, Revenue Quebec Investigation of a Software Designer Outlet Suspected of having Developed and Distributed Zappers (Oct. 14, 2005) *available at*: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiqués/ev-fisc/2005/14oct\(2\).asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2005/14oct(2).asp) (in French only, last visited Feb. 8, 2008).

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.<sup>57</sup>

*Mr. Michel 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.”<sup>58</sup>

---

<sup>57</sup> Revenue Quebec, News Release, The Company Audio LP, Inc. Convicted of Tax Evasion (Sept. 21, 2007) (on the conviction fines were imposed of \$12,475) *available at*: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiqués/ev-fisc/2007/21sep.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2007/21sep.asp) (in French only, last visited Feb. 8, 2008).

<sup>58</sup> 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, 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/communiqués/ev-fisc/2003/18mars.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2003/18mars.asp) (in French only, last visited Feb. 8, 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.<sup>59</sup>

*Mr. Luc Primeau.* In a pattern that should be becoming familiar, 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.<sup>60</sup>

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 in 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

---

<sup>59</sup> Revenue Quebec, News Release, Fines of more than One million dollars – A Father and his Two Sons convicted for Tax Evasion in connection with the Zapper (May 2, 2003) *available at*: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiqués/ev-fisc/2003/02mai.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2003/02mai.asp) (in French only, last visited Feb. 8, 2008).

<sup>60</sup> Revenue Quebec, News Release, 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/communiqués/ev-fisc/2003/17mars.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2003/17mars.asp) (in French only, last visited Feb. 8, 2008).

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).<sup>61</sup>

The real reason Mr. Primeau did not report this income probably 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. For these reasons, independent consultants (like Mr. Primeu, but not like Mr. Talbot in *Ronen* or Mr. Pirhalla in *Stew Leonard’s Dairy*) are treated more as part of the conspiracy rather than as “innocent” bystanders.<sup>62</sup> These computer specialists are rarely offered immunity, and are penalized directly (and in Quebec they are penalized severely) for the cash skimming frauds they knowingly facilitate.

#### MEASURING SIGNIFICANCE – SOLVING THE PROBLEM

How serious of a revenue problem is sales suppression (as a general matter)? Has it been/ can it be measured? Can a measurement of *technology-assisted* sales suppression be isolated? If so, can we sub-determine (within the incidence of *technology-assisted* sales suppression) the relative revenue loss from the use of factory installed “fraudulent risk software” as opposed to the revenue loss from “add-on” software programs – “Zappers?” In other words, where exactly is the problem?

---

<sup>61</sup> Revenue Quebec, News Release, The Zapper Designer of Boucherville Pleads Guilty to Various Charges brought by Inland Revenue Quebec (Oct. 26, 2005) (additional penalties of \$22,513.19 under the GST and QST, as well as income tax of \$17,297.08 and related penalties of \$26,621.35) *available at*: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiqués/ev-fisc/2005/26oct.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2005/26oct.asp) (in French only, last visited Feb. 8, 2008).

<sup>62</sup> It should be noted that both *Ronen* and *Stew Leonard’s Dairy* were primarily income tax audits, and the norm in these kinds of audits is to focus on the fraudster, not the Zapper. Whether or not Mr. Talbot or Mr. Pirhalla provided “Zapper consulting services” to other businesses is not discussed in either line of cases. If this had been a Quebec audit controlled by the MRQ one might have expected further developments in this direction.

These questions are important, because there are a range of different sales suppression fraud techniques, as well as a variety of different *technology-assisted* sales suppression methodologies. Counter measures differ among these fraud types.

This paper focuses on *technology-assisted* fraud of a particular type – Zappers. “Fraudulent risk” software is different, although it produces similar results. There are two types of “fraudulent risk” software; both are built in to the operating systems of modern the ECRs. Some of these programs are “hidden,” some are not. The “hidden” programs are “hidden” in the sense that their functions cannot be readily identified (even from a detailed examination of ECR owner manuals).<sup>63</sup> The other (“fraudulent risk”) programs are standard on most ECRs, but they present a “high degree of risk” in the sense that they may very easily be fraudulently used.<sup>64</sup> In both cases, the software itself is not inherently fraudulent. These programming options however, facilitate sales suppression in ECRs where an operator is otherwise inclined to skim cash sales.

Zapping software is a different type of *technology-assisted* sales suppression software. Zapping takes place on a network, not within an ECR.<sup>65</sup> Because network-

---

<sup>63</sup> “Hidden” functions are software operations that are not documented in the user manual, and may take an examination of source codes to detect. These functions vary from the abstract functional descriptions in the program flow chart. Detailed program documentation needs to be examined to identify them, and considerable expertise in software programming may be required when proving how (and when) they operate. Examples of “hidden” functions include (1) sales data reset – resetting all sales data on the terminal to zero; (2) turn off/ turn on the Electronic Journal; (3) master reset – clears out the entire memory of the till and brings it back to a default blank program after which the ECR determines which terminal it is by looking at others on the LAN and then prompts to import its program from one of the other terminals on the LAN. CASH REGISTER GOOD PRACTICE GUIDE, *supra* note 15, at Appendix B, ¶¶ 5.2.6 – 5.3.9.

<sup>64</sup> Other “high risk” (but not “hidden”) program options include: (1) fixed totalizers – non-resettable (Y/N) report a print (Y/N); (2) reset consecutive numbering; (3) report controls – do not print Z control; journal reports; time on reports; date on reports; consecutive numbers on reports; (4) check tracking; (5) print controls; (6) EFT control – cash back adds; cash back out drawer; gratuity adds; (7) Clerk features – manager; trainee; allow to correct features; (8) Clerk operations – allow use of no sale; item correct; void cancel etc.; (12) clerk mode control. CASH REGISTER GOOD PRACTICE GUIDE, *supra* note 15, at Appendix B, ¶¶ 5.3 – 5.3.9.

<sup>65</sup> Zapper programs are “add-on” programs that are loaded into the central computer integrating a multi-terminal POS system. A POS system is a combination of ECRs, other terminal equipment and a computer (or multiple computers) that are connected in a network configuration.

based systems are common, even in SMEs, *technology-assisted* sales suppression may occur in these businesses either through an ECR (“fraudulent risk” software) or within the central computer (Zapper software).

The focus of this article is on Zappers – other papers will consider the “fraudulent risk” software in both “hidden” and “high risk” configurations. Traditional remedies are available to counter “fraudulent risk” software. For example, the counter measure for factory installed “hidden” functionalities is to make them illegal. A cash register certification program can be established to detect “hidden” functions, and then it is a simple matter of not allowing non-certified cash registers to be sold or used in a jurisdiction. Both manufacturers and users can be penalized for selling or owning non-certified ECRs.<sup>66</sup>

Then again, if the problem is widespread *fraudulent* use of standard (but not necessarily “hidden”) programming, the remedy is somewhat different, but again it is a traditional one. Fraudulent use of “high risk” ECR functionality can be detected on audit. Admittedly, these audits require technological skills that are not widespread in tax administrations, but the government action in this case is to engage in intensive training programs for their audit staff so that they can detect these uses.<sup>67</sup>

Zappers however, are an entirely different story. Zappers are not factory installed on ECRs. They are frequently customized for specific businesses. They are downloaded into POS networks that connect the ECRs of a business. For example, the

---

<sup>66</sup> Argentina, Brazil, Bulgaria, Greece, Italy, Latvia, Lithuania, Poland, Russia, Turkey, and Venezuela are among the countries that certify cash registers currently. Penalties are applied for the sale or use of non-certified cash registers. CASH REGISTER GOOD PRACTICE GUIDE, *supra* note 15, at Appendix B, ¶1.

<sup>67</sup> An intensive training effort is the U.K. approach to fraudulent use of ECRs. CASH REGISTER GOOD PRACTICE GUIDE, *supra* note 15, at ¶¶1.4.4 & 3.2.1.

Connecticut Supreme Court describes the Zapper used in *Stew Leonard's Dairy* as follows:

The Dairy's sales recording system was composed of a computerized cash register system [with 25 ECRs] that recorded sales at the time of the transaction. At the point of sale, each product, which contained a universal product code (UPC) indicating its taxable or non taxable status, was scanned and the resulting sales information was transmitted to the main computer terminal. The Equity program, among other things, altered some of the UPC-based computerized records of the Dairy's gross sales. Specifically the program reduced item and dollar sales across a broad range of products to correspond with the amount of cash diverted each week. As we noted previously, the Equity program did this by writing over the original sales data, thereby rendering the original data irretrievable.

In our view, the result was akin to destroying the electronic equivalent of cash register tapes and replacing those tapes with ones containing false sales data.<sup>68</sup>

Neither certification of ECRs, nor technologically-sophisticated audits are effective against Zappers, because Zappers destroy the records they alter. If Zappers are the problem, then a solution will require securing not only the till, but the data within it. Doing this will involve taking some non-traditional steps. It will require that the government become directly involved in the certification of the production and retention process used to produce the primary business records at the point of sale. Thus, if governments are contemplating non-traditional approaches to *technology-assisted* sales suppression, it means that Zappers, rather than "hidden" or "high risk" functions are perceived to be the most serious part of this problem.

There are reports of two government-conducted studies measuring the *technology-assisted* sales suppression – one German, the other Canadian. Neither study is publicly available, although a brief summary of (some of) the German findings are available. The legislative/ administrative actions being taken (or considered) as a

---

<sup>68</sup> *Leonard*, 264 Conn., at 298.

consequence of these studies, suggest that Zappers have been determined to be the most serious of the *technology-assisted* sales suppression frauds.

*German Working Group on Cash Registers.* The Interim Report of the German Working Group on Cash Registers indicates that the Group was “... aware of fraud amounting to 50% of companies cash receipts.”<sup>69</sup> The Working Group does not separately quantify the kinds of *technology-assisted* fraud. The published assessment is an aggregate measure.

The Working Group’s 50% observation immediately follows supporting comments made by the German Federal Audit Office (BHR) to the German Parliament in 2003. Although it is not completely clear, the BHR seemed to focus on factory installed software,<sup>70</sup> not Zappers. The BHR determined that potential loss from inappropriate use of ECRs was in the billions of euros:

The Federal Audit Office (BRH) 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* should not be underestimated in cash transactions.<sup>71</sup>

The BHR’s statements and the Working Group’s observation are further buttressed with summaries from studies conducted by three federal *Land*. These studies are limited, because they focus only on the restaurant sector. But, they too conclude that sales suppression is a significant problem:

One federal *Land* 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 *Land*

---

<sup>69</sup> Interim Report, *supra* note 9, at 5.

<sup>70</sup> *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).

<sup>71</sup> BHR comments 2003, No 54, Federal Parliament circular 15/2020 *cited in Id.* at 5 (emphasis added).

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 *Land* has found that around 45% of till receipts involving cash are subject to upward revisions ranging from 20% to 118%.<sup>72</sup>

It is difficult to feel comfortable with this situation. Details are needed. The German public is being told that there is a problem, but it is not being told anything very specific about it. The same is true in Canada. The author is aware (from individuals who have had access to the Canadian study – conducted by the Quebec Ministry of Revenue) that the results in Canadian are consistent with those in German study, but in the Canadian case absolutely nothing (not even summaries) have been made available to the public. It would be very helpful to know the contours of these *technology-assisted* frauds.

*Legislative/ administrative actions.* Given that we are reasoning backward from government actions, not forward from empirical data, it is interesting to note that both Germany and Canada are moving in the same direction on this issue. There is no indication that Germany and Canada have coordinated their responses, but both appear to be very focused on Zappers. The Canadian approach appears to be a “classical” fiscal memory method; the German approach uses encryption and smart card technology. The “hidden” and “high risk” programming options on ECRs are a concern, but both countries are deeply committed to quickly rolling out non-traditional enforcement measures. It seems reasonable to conclude therefore, that the empirical data from these non-public studies has made a convincing case for Zappers.

---

<sup>72</sup> *Id.* at 5.

*Quebec, Canada.* The 2006-2007 Quebec Budget focused specifically on tax fraud in the restaurant sector and the inadequacy of traditional audit methods to uncover the fraud. The Budget's "additional information" document indicated:

Despite efforts to date by Revenue Quebec to counter such tax evasion, the *traditional methods* available to auditors seem to be inadequate for allowing them to trace all of the transactions hidden through various stratagems, such as using sales *Zappers*, failing to prepare invoices or to record certain invoices and reusing invoices.<sup>73</sup>

Several law changes were presented: (1) all restaurant operators would be required to issue invoices to customers, (2) a copy of the invoice would need to be retained by the restaurant, (3) by January 1, 2011 all restaurants that remit invoices will be required to use cash registers equipped with a Ministry of Revenue-certified microcomputer, (4) the microcomputer connected to the ECR would be required to be housed in a secure casing, and (5) the data in the microcomputer would then be the same data as that appears on the invoices.<sup>74</sup>

The Budget anticipated that some restaurants would be required to comply with these provisions by September 30, 2008. Those enterprises include: (1) any "new food establishment after September 30, 2008" and (2) restaurant owners who contravene certain tax obligations ... For example, restaurant operators who are caught by the tax authorities while using a sales Zapper to change, correct, erase, cancel or otherwise alter data without keeping the original data and the subsequent modifications, correction, deletions, cancellations or alterations made to them."<sup>75</sup> The September 30, 2008 date

---

<sup>73</sup> FINANCE QUEBEC, 2006-2007 BUDGET: ADDITIONAL INFORMATION ON THE BUDGETARY MEASURES 144 (Mar. 2006) (emphasis added).

<sup>74</sup> *Id.* at 145.

<sup>75</sup> *Id.* at 145 & n.111. On July 7, 2006 Revenue Quebec announced that 28 companies operating under the name of Casa Grecque pleaded guilty to Zapper fraud. The Budget Speech announcing the plan to require the adoption of cash registers equipped with microcomputers approved by Revenue Quebec had been given on March 23, 2006, and as a result Judge Lise Gaboury of the Court of Quebec decided to impose this

appears to have been too ambitious. The voluntary pilot program for this non-traditional enforcement effort is not slated to commence until November 2009.

Details of the enforcement effort and announcement of the delay were made public on January 28, 2008. A press release issued by Jean-Marc Fournier, the Minister of Revenue, indicated that a pilot project

... will begin in November 2009, [and] is aimed primarily at ensuring, with a group of volunteer restaurateurs from different regions, including Quebec and Montreal, the proper functioning of the technology and the registration of sales as well as the integration [of this program] with billing systems, before the gradual implementation of this model. ... [general] implementation of the model is expected to start in September 2010 and continue until November 2011. At the end of the gradual implementation, all restaurants will be required to use this technology.<sup>76</sup>

How the enforcement effort will work was revealed to the restaurant industry and this in turn was covered in trade journals. The contemplated solution involves "... a personal computer [that will be] connected to the cash register and to the [invoice] printer. [The PC] will record all transactions and produce an invoice with a bar code with a digital signature for each establishment. In addition the PC will be physically secured to prevent intrusion, for example with tamper-proof seals. The module will be the property of the restaurateur and they may use it to view the recorded data, but will not be able to modify it. ... At inspections the staff of Revenue Quebec can see the data and copy it."<sup>77</sup>

---

penalty in addition to monetary fines of CAN \$694,600 (QST) , \$232,574 (GST) and legal fees of \$72,826. Revenue Quebec, News Release, Tax Evasion: Restaurants in the Chain Casa Grecque Guilty of Tax Evasion (July 7, 2006) *available at*: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiqués/ev-fisc/2006/10juillet.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2006/10juillet.asp) (in French only, last visited Feb. 16, 2008).

<sup>76</sup> Revenue Quebec, Press Release, *supra* note 10.

<sup>77</sup> Caroline Rogers, *Quebec is Moving Forward to Stop Tax Evasion*, HOTELS, RESTAURANTS & INSTITUTIONS (Feb. 12, 2008) *available at*: <http://www.hrimag.com/spip.php?article2771> (in French) last accessed Feb. 12, 2008).

*Germany.* Germany is doing something very similar, but more technologically advanced. It is developing a system to protect cash register data through encryption. Germany has rejected the “classical” fiscal memory solution, an approach adopted by some EU and non-EU countries.<sup>78</sup> Although neither the German nor the Quebec approaches are in final form yet, there are distinct similarities – notably the intent to preserve data from each transaction and process performed on a cash register. This is a Zapper-focused effort – although it will also be effective against “fraudulent risk” software.

The German Working Group that recommended the encryption solution was chaired by Professor Norbert Zisky of the PTB (Physikalisch-Technische Bundesanstalt; the national Metrology Institute). It was Professor Zisky’s papers on encryption,<sup>79</sup> and the fact that these techniques had been tested in secure communication settings with measuring instruments<sup>80</sup> that seems to have persuaded the Working Group to move in this direction.

As a result, in early 2008 the PTB began the INSIA project (Integrierte Sicherheitslösung für Kassensysteme; Integrated Security Solution for Cash Registers). This project is also managed by Professor Zisky, and is charged with completing the technical specifications for a signature smart card (to be used in the encryption solution) by the summer of 2008. Included with the technical specifications for the signature smart

---

<sup>78</sup> A “classical” fiscal memory approach is to permanently secure the record of the till. It is an approach utilized with some success (but with notable difficulties) in Argentina, Brazil, Bulgaria, Ecuador, Italy, Turkey, Lithuania, Latvia, Poland, Russia and Venezuela.

<sup>79</sup> 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)

<sup>80</sup> 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).

card will be a determination of the data structures and formats, communication protocols and security analysis for the system.<sup>81</sup>

Based on the recommendations of the Working Group, Vectron Systems AG developed (and is currently demonstrating) a prototype of the 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. A secure electronic signature is issued that is based on Public Key Infrastructure (PKI). As Professor Zisky indicates:

In ... this 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.<sup>82</sup>

In fact, the Vectron prototype cost estimates are for a “single-unit end-user price of less than 25 euros.”<sup>83</sup> This contrasts with the Quebec estimates of CAN\$650.<sup>84</sup>

The essence of the “Zisky solution” revolves around cryptography and smart card access to cryptographic data preserved within the cash register or POS system. If the revenue authority audits, then it can access the records of the cash register with a smart card that has the “key” to read the data (and it will know that the data has not been tampered with). Zisky indicates:

The fiscally relevant data records can be examined both locally and after their transmission over various communication channels, fully automatic with respect to their integrity and authenticity. For the

---

<sup>81</sup> 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).

<sup>82</sup> Norbert Zisky, *Manipulation Protection*, *supra* note 79, at ¶ 5.1.

<sup>83</sup> Vectron, A.G., *Tamper-proof POS Data* *supra* note 14, at slide 30; Norbert Zisky, *Manipulation Protection*, *supra* note 79, at ¶ 5.7 (estimating 50 euros).

<sup>84</sup> Revenue Quebec, Press Release, *supra* note 76.

electronic signature of the revenue offices special smart cards are used, which are integrated into the POS systems....

The revenue office will provide a smart card with a Kryptoprozessor 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 Hashwert is formed, which is in turn coded by the secret key of the smart card. The formation of the Hashwert is a mathematical one-way function, which comprises a single (unique) value from the data set. It is the Hashwert 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 Hashwerts are compared with one another. If these agree the integrity of the registered data record is authenticated.<sup>85</sup>

Professor Zisky’s team is currently engaged in producing the technical specifications for the system. His group is working in close cooperation with the BMF (Ministry of Finance) Group on Cash Registers and the INSIKA project group funded by a grant from BMWi. The project is expected to be completed by June 2008. Three adjustments have been made from the papers presented in 2004:

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

---

<sup>85</sup> Norbert Zisky, *Manipulation Protection*, *supra* note 79, at ¶ 5.2 & 5.3.

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.<sup>86</sup>

## U.S. APPLICATIONS – U.S. CONTRIBUTIONS

If Zappers are a global problem, it is unlikely that their U.S. incidence is confined to *Stew Leonard's Dairy* in Norwalk, Connecticut and *La Shish* in Detroit, Michigan. In fact, the first news reports of Zappers in Canada indicated that Canadian Zappers were U.S.-made,<sup>87</sup> and that they could be purchased over the internet for roughly \$500.<sup>88</sup> One of the first Zapper cases in Canada involved a search warrant enforcement action against a Canadian subsidiary (Gamma Terminal) of a U.S. parent company (Gamma Micro Systems).<sup>89</sup> The search followed by two weeks the Radio Canada investigative report that broke the Zapper story, and a follow-up television program. Notable on the television program was the declaration by Rejean Turcotte, a technician for the company, that “we sell Zappers.”<sup>90</sup>

What is notable about the U.S. Zapper enforcement actions, as contrasted with those in other jurisdictions, is that in the U.S. it is the IRS on income tax audits that is uncovering Zappers. In almost all other jurisdictions Zappers are primarily a consumption tax (VAT or GST) issue. It is not that income tax consequences are ignored outside the U.S., it is just that they are secondary. This difference is reflected in the enforcement. Where the U.S. focuses on a particular fraudster, non-U.S. jurisdictions

---

<sup>86</sup> Norbert Zisky, personal e-mail communication (Feb. 15, 2008) (on file with author).

<sup>87</sup> Timothy Appleby, Rhe'al Se'guin & Geoffrey Rowan, *Restaurants' Tax Evasion Scam Pursued: System Found in Quebec may be Used elsewhere, Revenue Canada says*, THE GLOBE & MAIL (Dec. 5, 1997) at A:1.

<sup>88</sup> Craig Silverman, *Zapped!*, HOUR (Feb. 19, 2004) available at: <http://www.hour.ca/news/brief.aspx?iIDArticle=783> (last visited Feb. 15, 2008).

<sup>89</sup> *Turcott v Quebec (Ministry of Revenue)* 1998 CarswellQue 1041, [1998] R.D.F.Q. 110 (Superior Court of Quebec).

<sup>90</sup> *Id.* at ¶21.

focus on the Zapper – who sold it, who installed it, and how widely it had spread within the market-place before it was uncovered.

Part of the reason for the U.S.-enforcement/ foreign-enforcement difference may simply be the tax rates. Sweden has a considerable problem with Zappers – the standard Swedish rate is 25%. Comparatively, the highest retail sales tax rate in the U.S. is 9.35%.<sup>91</sup> The sales tax imposed on restaurant meals in Detroit, Michigan during the *La Shish* case was 6%, and the rate in Connecticut at the time of *Stew Leonard's Dairy* was 7.5 to 8%.<sup>92</sup> Another reason for the low level of State audits uncovering Zappers may be that coordination is difficult among the U.S. jurisdictions. There are over 11,000 retail sales tax jurisdictions in the U.S. when all the county, city and district taxes are considered. Sales tax compliance has become a burden for businesses in the U.S. just as sales tax coordination has become difficult. Thus, where the Zapper fraud in the 28 Stratos restaurants in Quebec was primarily concerned with a single set of QST and GST laws,<sup>93</sup> and the 300 food service establishments potentially involved with Zappers that was the focus of *Operação Tesouro* in the Brazilian State of Bahia were similarly focused on a single tax statute,<sup>94</sup> it is difficult to imagine the same situation in many U.S. locations.<sup>95</sup>

---

<sup>91</sup> Tennesseans for Fair Taxation, *Tennessee Has the Highest Sales Tax*, (these rankings use a weighted average (population) of sales tax rates from all municipal and county taxing jurisdictions within each state) available at: [http://www.fairtaxation.org/facts/sales\\_tax\\_rank.php](http://www.fairtaxation.org/facts/sales_tax_rank.php) (last visited Feb. 15, 2008).

<sup>92</sup> The sales tax rate at the time of the assessment was 6%, but because the audit period covered the period 7/83 – 3/92, the rate during the audit period started at 7.5%, went to 8% and then went to 6% (on 8/1/1991) were it stands today. It bears repeating that 85% to 95% of the sales in *Stew Leonard's Dairy* were non-taxable sales of dairy products, so the State's incentive to audit was low for this reason also. Appeals Officer Michael O'Sullivan, personal e-mail communication (February 16, 2006) (on file with author).

<sup>93</sup> See *supra* notes 58 to 59, and accompanying text.

<sup>94</sup> See *supra* note 11.

<sup>95</sup> Although some states, like Massachusetts, have a single state-wide retail sales tax, the same is not the case in states like Texas and Alabama.

*Streamlined Sales and Use Tax.* Technology has recently brought important efficiencies to the American retail sale tax through the adoption of the Streamlined Sales and Use Tax Agreement (SSUTA).<sup>96</sup> Currently 22 states are members.<sup>97</sup>

Perhaps the most innovative aspect of the SSUTA effort to remove the tax collection burden from vendors is the creation of a mechanism under which third-party tax collection agents, certified by the state under SSUTA literally assume all of the vendor's sales and use tax collection functions and do so at no cost to the vendor. A somewhat less radical but nonetheless innovative variation on this theme is SSUTA's provision for certifying tax collection software, whose proper use by the seller effectively insulates the seller from liability for any errors in determining the proper tax due to the appropriate jurisdiction.<sup>98</sup>

The SSUTA has no provision dealing with Zappers. Structurally, the SSUTA performs a delicate balancing of interests around the concepts of fraud and immunity. Take for example the third party certified service provider (CSP).<sup>99</sup> The CSP is an agent of the seller, and the CSP is liable for sales and use tax collection in each member state on all sales transactions it processes. However, the CSP is not liable for charging and collecting the incorrect amount of tax based on erroneous data provided by a member states on tax rates, boundaries, or taxing jurisdiction assignments, or on erroneous data provided by the member state in the taxability matrix.<sup>100</sup>

---

<sup>96</sup> 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>.

<sup>97</sup> Although the agreement itself was the product of the combined effort of 44 states and the District of Columbia, the 22 full-member states that are currently implementing the SST are: Arkansas, Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Nebraska, New Jersey, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Rhode Island, South Dakota, Tennessee, Utah, Vermont, Washington, West Virginia and Wyoming. Details, documentation and policy papers on the SST is available at <http://www.streamlinedsalestax.org/> (last visited Feb. 15, 2008).

<sup>98</sup> WALTER HELLERSTEIN & JOHN A. SWAIN, STREAMLINED SALES AND USE TAX (2007-2008) ¶ 7.11.

<sup>99</sup> SSUTA *supra* note 96, at §§601-03 (providing that the government may enter into contracts with a CSP to compensate the service provider directly based on taxable transactions processed, or a percentage of instances where sellers without nexus volunteer to collect sales taxes that they are not otherwise obligated to collect)

<sup>100</sup> *Id.* at §§ 328 & 331.

In addition, the seller is not liable for transactions processed by the CSP, unless “... the seller misrepresented the type of items it sells or commits fraud.”<sup>101</sup> And further more, “... in the absence of probable cause to believe that the seller has committed fraud or made a material misrepresentation, the seller is *not subject to audit* on the transactions processed by the CSP. [However, a] seller *is subject to audit* for transactions not processed by the CSP.”<sup>102</sup>

Thus, under the SSUTA, any seller using a CSP and operating a Zapper would be subject to audit on all “zapped” sales, just as any seller who utilized “hidden” or “high risk” functionality that is factory installed on ECRs would be open to audit on sales suppressed in this manner.

*The Fiscalis Committee’s Cash Register Project Group.* When the Fiscalis Cash Register Project Group analyzed sales suppression three risk areas were identified: (1) the risk of not recording – an integrity/ completeness issue where some transactions are not recorded in the primary sales registration system at all;<sup>103</sup> (2) the risk of data manipulation – an accuracy/ authenticity issue where the records of transactions are

---

<sup>101</sup> *Id.* at §9(a).

<sup>102</sup> *Id.* at §9(a) (emphasis added).

<sup>103</sup> This is not an insignificant issue. Take for example the case of Ecuador. ECRs are certified by the Ecuadorian IRS, and the program within the ECR must be “closed” or tamper-proof. If a consumer asks for a receipt it must be issued (and there is an incentive system in place that makes it advantageous to the consumer to do so). In addition, the IRS employs an “army” of fiscal *fedatarios* whose task it is to simulate purchases and request invoices. Those businesses that do not issue invoices are closed by the IRS. In 2007 one IRS regional office closed in excess of 13,000 businesses (often for a day or more, but frequently for longer periods). One of the companies closed in 2007 was Microsoft del Ecuador S.A.

The relevant Ecuadorian regulations and ruling dealing with cash registers are: Invoicing and Withholding Receipts Regulations, No. 3055 (Oct. 2002), as amended Decree No. 2586 (March 4, 2005) at Arts. 1, 12, 21, 41, 42 (Ecuador); Servicio de Rentas Internas Ruling, No. 9170104DGER-0580 (Nov. 2004) (Ecuador); Servicio de Rentas Internas Ruling, No. 327 (May. 2001) (Ecuador). A press notice dealing with the closures, including Microsoft del Ecuador S.A. closing states:

The Infractions Area of the North Regional Office of the SRI, has sanctioned 13,642 taxpayers with penalties (fines) and closures, for failure to comply with legal or regulatory duties.

Press notice, President’s Office (Oct. 5, 2007) *available at*:  
<http://www.presidencia.gov.ec/noticias.asp?noid=11253&hl=true>

changed or deleted without an audit trail; (3) the risk of audits – a conversion issue where the primary records are correct and complete, but the correct figures do not find their way into the tax return.<sup>104</sup> Where the SSUTA is concerned with the first and third risk factors, and not at all with the second; the German (Zisky/ Vectron) and Canadian solutions are concerned with the second risk factor, and not at all with the first and the third. There should therefore, be a natural synergy between these approaches.

### PROPOSALS AND CONCLUSION

A balanced pair of policy proposals and a suggestion that greater State-Federal coordination with respect to Zapper enforcement is needed forms the conclusion of this paper.

*Extending the scope of SSUTA certification.* The direct antecedents of the SSUTA are the National Tax Association's Communication and Electronic Commerce Project (early 1997)<sup>105</sup> and the Advisory Commission on Electronic Commerce<sup>106</sup> which was directed by Congress in 1998 to consider federal, state, and local tax issues with respect to Internet transactions. SSUTA was born out of State concerns over revenue losses from electronic commerce, concerns that were heightened by the adoption of the Internet Tax Freedom Act (1998).<sup>107</sup>

Interestingly, this is the same time period when American-made Zappers were being identified as a serious revenue problem in Montreal by the Canadian Broadcasting Corporation. It is the same time frame when *Stew Leonard's Dairy* was being litigated in

---

<sup>104</sup> CASH REGISTER GOOD PRACTICE GUIDE, *supra* note 15, at ¶2.3.1

<sup>105</sup> NTA, *Communications and Electronic Commerce Tax Project Final Report* (Sept. 7, 1999) available at: <http://ntanet.org>.

<sup>106</sup> Established by the Internet Tax Freedom Act § 1102(g)(2).

<sup>107</sup> Title XI of the Omnibus Consolidated and Emergency Appropriations Act of 1998, Pub. L. No. 105-277, §§ 1101-1104, 112 Stat. 2681-719 91998) (ITFA)

State and Federal courts in Connecticut. In a strange twist of tax-fate it seems that just as Americans were becoming concerned about revenue losses from the growth of the Internet, SMEs were zapping away tax revenues from “brick and mortar” establishments.

The SSUTA that developed out of the very serious tax policy debates of this period is largely premised on the good faith reliability of business records. Although this is a solid assumption within the large and mid-sized businesses (LMSB) group, it is not always valid within the SME realm, particularly when *technology-assisted* sales suppression is growing. In this context, it might be well worth the trouble of the SSUTA to consider extending its certification regime to ECRs and POS systems modeled on either the German or Canadian approach. Audit immunity could be extended along with the certification in the traditional SSUTA manner.

*Extending the Scope of the Fiscalis Cash Register Project Group.* The same issues can be considered from the perspective of the Fiscalis Committee’s Cash Register Group. The Cash Register Group concedes that very little is being done under the Project to deal with either non-recorded sales (risk one), or audit detection (risk three). Even with respect to sales record manipulation (risk two) there is disagreement among the Member States over whether a mandatory or a voluntary solution should be adopted. The difference is characterized as a rules-based (mandatory) versus a principles-based (voluntary) approach

Where Germany seems poised to require encryption and smart card on all ECRs, the Netherlands prefers a voluntary approach. The Netherlands applies a system of “... generic legislation ... [where] ...entrepreneurs are free to independently establish adequate business information and accounting systems ... and there are no fiscally related

legal requirements imposed on developers of software or on the manufacturers of cash registers.”<sup>108</sup>

One of the strongest attributes of the SSUTA is that it is a voluntary regime extending audit immunity to taxpayers that adopt certified systems, frequently through trusted third parties, CSPs, who assume liability for tax compliance. The key to the functioning of the SSUTA is the certification of software solutions. It would seem to be consistent with the Netherlands approach to tax administration to adopt a SSUTA-like structure that included as part of its certification regime the voluntary adoption of the Zisky/ Vectron encryption/ smart card solution. Perhaps, as in the Canadian legislation, it might be appropriate to require any business caught using a Zapper or other *technology-assisted* sales suppression technique to become a part of the certified system.

*Enhanced State-Federal cooperation over Zappers.* It is reasonably clear that Zappers (in the U.S.) are a threat to both State and Federal revenue systems. It is also reasonably clear that Zappers have become commonplace in the commercial marketplace.<sup>109</sup> When deployed widely, Zappers significantly reduce reported gross income,

---

<sup>108</sup> Ben B.G.A.M. van der Zwet, *supra* note 81, at 4.

<sup>109</sup> The German Working Group on Cash Registers is very concerned with the market-penetration of technology-assisted fraud:

The fraud is perpetrated in different ways. One way is for taxable persons to totally fail to record some of their cash receipts. Another is for them to exploit the numerous tampering possibilities available through their electronic or computerised tills.

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.* What is more, special types of programme 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.

Working Group on Cash Registers: Interim Report, *supra* note 9, at 5 (emphasis added). Similar reports can be found in the U.S.. Instances of cash register salesmen (under pressure to make a sale) being told that other competing companies will install Zappers can be found. Some times individuals report these competitors to the tax authorities. Personal e-mail communication Michael J. Sullivan (Feb. 11, 2008) (on file with author).

siphon off consumption taxes, and provide the funds out of which undeclared cash wages are paid to employees, or are sent to fund terrorist organizations. The same patterns play out in the EU, Latin America, and Asia. It is not just the Canadian experience that holds lessons for the U.S..

What makes Zappers so difficult to detect is that they are frequently designed, sold and maintained by the same people who develop industry-specific POS operating systems. In Canada: (1) the developer of the Softdine software system for restaurants also developed the Zapper that allowed its users to skim sales;<sup>110</sup> (2) Michel Roy, the designer of Terminal Resto software designed, serviced and installed the Zapper that allowed the 28 Stratos restaurants to skim sales when using his Terminal Resto program;<sup>111</sup> and (3) Luc Primeau designed the Zappers for his own Microflash software, and when Microflash was replaced with Caracara he designed the next generation Zapper to go along with it.<sup>112</sup> Software certification alone is not a barrier to Zappers. This was the shown in *Operação Internet* in Brazil.<sup>113</sup> This is the reason the German solution is to

---

<sup>110</sup> See *supra* text accompanying notes 53 to 57.

<sup>111</sup> See *supra* text accompanying notes 58 to 59.

<sup>112</sup> See *supra* text accompanying notes 60 to 61.

<sup>113</sup> Operation Internet was conducted by the State Tax Administration of Minas Gerais (a Brazilian State in the Southeast region - close to Rio and São Paulo). The AMG corporation produced not only government certified software (Robot) for cash registers operating in the state; it produced the Zapper (Quanto) that defeated it:

Three partners and a clerk at the AGM Consultancy and Systems Corporation, Ltd., based out of Juiz de Fora, were arrested yesterday, accused of developing a software program for dodging taxes. The company had been under investigation for three months prior to this, and in the State Revenue Secretary's estimation the program, which does not tally sales as required by law and produces no receipts, thus allowing for the monitoring of financial activity through unofficial accountancy, may be in use by at least 150 commercial establishments in the city.

All the financial activity recorded by this program was stored on a still unidentified, Internet based network server. The Revenue Department admits however that corporations based in other Zona da Mata-area cities, and even in Rio de Janeiro, may be using the same software.

...Preliminary evaluations indicate that these corporations illegally withheld between 40% and 50% of taxes owed.... *AGM was licensed by the State Revenue department to develop programs to perform accountancy functions for commercial*

encrypts all cash register processes. Simple certification of software is not sufficient, processes must be preserved – and it would be very helpful to have a trusted third party overseeing the use of the solution.

Securing the till would be a major undertaking in the U.S. It would be an expensive proposition if the “classical” fiscal memory approach is adopted, as in Canada. It would be less expensive, and very possibly more secure, if the Zisky/ Vectron encryption approach is adopted, based on the 25 euros “single-unit end-user” cost estimate of the Vectron prototype. However, Zisky/ Vectron does assume some government contribution in the design and provision of the smart cards to be installed. Encryption is the preferred approach, and is the method recommended in this paper.

More to the workability point of this solution however might be the resistance that might be encountered to federal or state mandatory regulation of ECRs or POS systems. Fortunately there is the SSUTA framework. If this voluntary system of certified compliance software were to be extended (particularly under the trusted third party, or certified service provider model) so that it included the certification of ECRs and POS systems, within a federal/state cooperative structure it could yield considerable compliance benefits. For example:

- (1) **certification of the gross sales figure** – a third-party installed encryption (or “classical” fiscal memory) system could stand in place of direct government

---

*establishments. They supplied customers with the official program, called “Robot,” along with the illegal program “Quanto,” which allowed sales to be effectuated without the issuing of receipts, with a mere press of a button on the cash register.*

“With this function the establishment’s owner would be able to simply choose when he wanted to have legal accountancy performed, and when he wanted to illegally withhold taxes,” said Luiz Pedri, regional superintendent of the Revenue department.

*Empresa de JF burlava o fisco via computador HOJE EM DIA (A JF-based Corporation defrauded the tax authorities via computer TODAY BRAZIL) (May 12, 2006) available at: <http://www.fazenda.mg.gov.br/empresas/ecf/noticias/hojeemdia12052006.pdf> (in Portuguese) (last visited Feb. 17, 2008) (translation on file with author) (emphasis added).*

- encryption of ECRs and POS systems under the condition that the encrypted data would be preserved for a sufficient period (10 years, for example), and under the further condition that the third-party would be responsible for determination, and remission of transaction taxes, as well as the proper reporting of the gross sales figure for income tax purposes;
- (2) **audit immunity for taxpayers** – businesses opting for the CSP solution with third-party encryption of ECRs and POS systems would be immune from audit, barring fraud – but if there was Zapper-type fraud, then primary liability for the fraud (taxes, penalties, interest, and return filing obligations) would rest with the third-party whose encryption of sales data was designed to prevent this fraud [for income tax purposes immunity would extend only to the sales (gross income) figures];
- (3) **certified encryption technology (smart cards and technical specifications)** – the federal government (in cooperation with the states) should undertake to develop the encryption technology [along the lines of the INSIKA project (Integrierte Sicherheitslösung für Kassensysteme – Integrated Security Solutions for Cash Registers) at the German National Metrology Institute (PTB: Physikalisch-Technische Bundesanstalt)] and provide this to certified third-party service providers;
- (4) **inspection of the ECRs and POS systems** – the states (in cooperation with the federal government) should undertake location-by-location verification of the proper function of encryption systems at ECRs and POS systems in their jurisdiction – this should be able to be accomplished with a smart card with PKI

(this would be a matter of “testing the encryption system” rather than directly auditing the encrypted numbers);

- (5) **business registration requirements** - in a manner similar to that adopted in Quebec, rules could be put in place such that any business caught skimming sales (by using Zappers or “hidden” ECR functionality or fraudulent use of “high risk” ECR functionality or not putting all sales through the cash registers) could be required to use a CSP extended to include ECR and POS encryption technology as a condition of retaining their business license.

This kind of approach to Zappers would require a degree and level of cooperation that is sorely needed across the federal/ state (income tax/ retail sales tax) divide. The benefits of cooperation will come from a sharing of expertise. It is only too clear that consumption tax auditors (VAT – GST – RST) have an entirely different vision of the Zapper problem. On one hand, consumption tax authorities in Canada, Brazil, and Australia as well as a large number of countries in the EU have shut down skimming operations that frequently involve hundreds of businesses. On the other hand, it is the federal pursuit of money-laundering activities through agencies like U.S. Customs (*Stew Leonard's Dairy*), and the U.S. Department of Homeland Security's terrorist prevention activities (*La Shish Restaurants*) that uncovers the largest international skimming frauds. AUSTRAC's involvement in the restaurant-based Zapper fraud in Australia is typical of these enforcement efforts.<sup>114</sup>

In the final analysis, what we need to guard against are state/ federal adversarial situations like that which developed in *Stew Leonard's Dairy*. Admittedly, (a) the skimming was first uncovered federally (by U.S. Customs); (b) the scope of the sales tax

---

<sup>114</sup> See *supra* note 18, and accompanying text.

fraud was limited to somewhere in the range of 5 to 15% of total sales; and (c) this fraud had been going on for over ten years and neither state nor federal auditors had uncovered it. Thus, there was an understandable federal concern with *Stew Leonard's Dairy*.

However, the income tax issue was not the end of the story. It is particularly difficult for any kind of audit (income tax audit or retail sales tax audit) to be performed when there are Zappers. Because a Zapper: (a) “permanently alter[s] the data;” (b) “le[aves] no audit trail and no trace that it ha[s] run,” and if (c) “store employees [are instructed] not to print the weekly sales reports until ... after the data-altering program was executed,” then auditing is nearly impossible.<sup>115</sup>

The State of Connecticut’s audit in *Stew Leonard's Dairy* was dependent on the federal audit. The parties stipulated that the only tangible evidence (aside from IRS and other testimony) was a single pair of “... Current Week Activity Reports for the week of June 26, 1991, one before the illegal application of the Equity Program and the other after the gross receipts figures were altered.”<sup>116</sup> The Equity Program itself (current and prior versions) were secured and retained by the IRS.<sup>117</sup>

The tax appeals officer’s (Michael O’Sullivan) analysis of these two reports, “... indicated a discrepancy between the sales tax that should have been collected for that week and the sales tax reflected in the financial reports.”<sup>118</sup> There was no more evidence of the fraud. “O’Sullivan attributed [the] discrepancy to the Equity program, although he

---

<sup>115</sup> *Stew Leonard*, 37 F.3d at 35.

<sup>116</sup> Brief for Appellee at 16, *Stewart J. Leonard Sr. dba Stew Leonard's Dairy v. Commissioner of Revenue Services*, 264 Conn. 286 (2003) citing Stip. ¶35b and exhibits 19 and 20 to the Stipulation, 2002 WL 43104803.

<sup>117</sup> *Stew Leonard*, 264 Conn. at 291 (indicating that the computer specialist, Pirhalla, testified that, “...the Equity program software and computer printouts reflecting the data manipulation had been taken and retained by the IRS.”)

<sup>118</sup> *Id.* at 292.

stated that he did not know how the program operated. He had tried to obtain a copy of the program from the IRS, but it denied his request.”<sup>119</sup>

Not only did the Supreme Court of Connecticut note that these events placed the Commissioner of Revenue Services in a very difficult position,<sup>120</sup> but the lower courts were similarly troubled. Writing in November 2001 the Connecticut Superior Court, looking back on the conclusion of the IRS audit, the federal guilty pleas, the sentencing, and two sets of appeals on the sentence (all of which were completed by October 4, 1995) Judge Arnold W. Aronson stated:

We found, in our prior decision in this case:

The revenue examiner used the settlement figures of the IRS because the IRS had possession of all the records of the Dairy that would be needed to conduct an actual audit, such as sales journals, daily reports, and cash receipts tapes. The IRS would not release these records to the DRS. (April 19, 2000 Memorandum of Decision, p. 5)

We note that a year and a half has passed since the issuance of our last memorandum and the commissioner apparently still has not obtained access to the plaintiff’s records. The commissioner continues to rely on the IRS settlement [as the primary basis for the Connecticut assessment]...<sup>121</sup>

Zappers are difficult enough to uncover without two revenue agencies compounding the problem by not sharing records, and more particularly not sharing knowledge of how a specific Zapper works with one another. If the consumption tax enforcement efforts in Canada, Brazil, and the EU are any indication, one might expect that the Connecticut DRS would use this knowledge to see if other (similar) Zappers were installed elsewhere in high-cash volume Connecticut businesses. The Canadian, or the

---

<sup>119</sup> *Id.* at 292.

<sup>120</sup> *Id.* at 292, n.4 (“It appears from the record that the unavailability of records was due in part to the plaintiff’s destruction of records, either by application of the Equity Program or the shredding of cash receipts, and in part to the IRS’ retention of certain records.”).

<sup>121</sup> IStew Leonard, 2001 Conn. Super. LEXIS 3239, at 7-8.

Brazilian, or the Netherlands approach would be to see if Mr. Pirhalla (the computer operator in *Stew Leonard's Dairy*) offered his services (as a consultant) to other firms that used the same NCR systems that were used at *Stew Leonard's Dairy*. Was there only one Zapper in Norwalk Connecticut during the ten years Mr. Pirhalla worked there? We will never know, because the agency most directly interested in *technology-assisted* skimming of cash sales in SMEs generally was not fully included in the investigation. Perhaps, one of the benefits from a joint effort to combat Zappers would be this kind of cooperation.