ZAPPERS AND PHANTOM-WARE AT THE FTA: ARE THEY LISTENING NOW?

Boston University School of Law Working Paper No. 08-21

Richard Thompson Ainsworth

This paper can be downloaded without charge at:


The Social Science Research Network Electronic Paper Collection:

http://ssrn.com/abstract_id=1147023
ZAPPERS AND PHANTOM-WARE AT THE FTA:
ARE THEY LISTENING NOW?

Richard Thompson Ainsworth

When the Federation of Tax Administrators (FTA) held a national Compliance and Education Workshop in Louisville, Kentucky (February 25-27, 2001) one of the invited speakers was Kevin Pratt, Manager, Underground Economy, Canadian Customs and Revenue Authority (CCRA). He spoke on Zappers.1

To the best of anyone’s present recollection,2 this was the first time zappers had been discussed with a large group of state-level US tax compliance professionals. However, most of the information that the CCRA presented to the FTA in 2001 was not its own – it was derivative. Zapper investigations were not an in-house specialty of the CCRA (although they were a matter of considerable concern).

Zapper investigations had been the specialty of the Quebec Ministry of Revenue (MRQ),3 and it was from the MRQ that the CCRA learned about zappers.4 Mr. Pratt’s presentation clearly

---

1 Kevin Pratt, Tax Evasion in a Electronic Environment – “Zapping, (power point slide 6, presented at the FTA Compliance Education Workshop, Louisville, Kentucky (Feb. 25-27, 2001) (on file with author). This invitation was timely. Just the week before (February 19-21, 2001) Mr. Pratt was speaking on this same topic at the Federal/Provincial Meeting of the Underground Economy Working Group at the Conference Center in Ottawa. His topic there was also the “Zapper.” This meeting ended with the following “Enforcement Strategy Proposal”

Zapper Software
- Share information pertaining to potential users and suppliers.
- Share MRQ [Quebec Ministry of Revenue] legislation to address compliance issues
- Identify key stakeholders for the development of an education/awareness plan.


2 It is apparent that the “present recollection” is not accurate. Mr. Pratt’s slides from 2001 note that the “MRQ previously presented the issue of “Zappers” to the FTA.” However, this author cannot find any record of this “presentation” within either the MRQ or the FTA. It may have been an informal presentation. See, supra note 1, at slide 6.

3 Revenue Quebec was first made aware of zappers in 1996. The early investigations by Revenue Quebec included tax years as far back as 1994. David Bergeron, Pacific Region ECAS Conference (date) (location of conference) slide 3.

4 After explaining the Canadian enforcement structure and how (under the Canadian system) the MRQ administers both Provincial and Federal level taxes (slides 1-6), and then providing a general definition of Zappers (slide 7), Mr. Pratt moves into a discussion of zapper enforcement actions taken by the MRQ. He indicated: (1) that the first searches for zappers were conducted in 1997, and that by 1998 a departmental committee was formed within the MRQ to review and propose solutions, and finally that over 100 searches had been conducted with many audits ongoing and that the MRQ had identified multiple zapper software programs; (slide 8) (2) that MRQ had set in motion a four phase action plan to deal with zappers (slide 9); and (3) provided an extended example set in grocery store fact pattern – a very simple “zapper-like” fraud that involved placing some ECRs in a network configuration “off line” so that their sales could be skimmed (slides 10 & 11). [Although not expressly revealed by Mr. Pratt, it is likely that this example is based on the Metro Supermarket investigation that was widely reported on in the Canadian press. See CP, Ottawa Still Struggling to Catch ‘Zapper’ Tax Cheats Five Years Later, THE BROCKVILLE RECORDER & TIMES (Ontario, Canada) at 47 (Jan. 2, 2003)]. Mr. Pratt’s presentation concluded with a re-statement of the “Enforcement Strategy Proposal” that were agreed upon the previous week at the Federal/Provincial Meeting of the Underground Economy Working Group, supra note 1.
indicates that he (and the CCRA) considered themselves to be conduits through which MRQ experiences were being shared. This was only right. Ever since the first real zapper case was assembled in 1997 by a persistent and very dedicated MRQ auditor,\(^5\) the MRQ had been working to defeat this technology-facilitated fraud.

Some things have changed in Canada since 2001, but not the MRQ’s leadership with respect to “all-things-having-to-do-with-zappers.”\(^6\) There are very good reasons for this, some of which will be considered here.\(^7\)

Over this same period of time some things changed in US state-level tax enforcement also, but not much has changed with respect to zappers. It has been as if the FTA did not take to heart what the CCRA had told it. Perhaps the CCRA’s talk (or an earlier presentation possibly made by the MRQ) was not persuasive, or perhaps by highlighting that it was Quebec’s experience with zappers (rather than direct CCRA experiences, or the experiences of other

---

\(^5\) The story is told that before anyone in any Canadian tax administration had heard of a zapper an MRQ auditor scheduled to audit a restaurant decided that she should patronize the restaurant she was to audit a few weeks later. She paid for her meal in cash, and saved her receipt. On audit she looked for the record of her purchase. What she found struck her as exceedingly strange. Instead of seeing (for example):

\begin{verbatim}
French onion soup ............$10.00
T-bone Steak ..................$25.00
Medium Rare
Total: ................................$35.00
\end{verbatim}

She saw that the electronic record of her meal had been changed to:

\begin{verbatim}
French onion soup ............$10.00
Medium Rare
Total: ................................$10.00
\end{verbatim}

The tax concern was that not only had the consumption tax (QST and GST) been re-calculated on a $10.00 base instead of the $35.00 base on which it had been paid, but the gross receipts of the business for income tax purposes was lower by $25.00. Some-how the entire line “T-bone steak …. $25.00” had vanished from the records, and the total bill had been recalculated.

However, there was a “trace” of the original purchase in the modified records. The “Medium Rare” designation (perhaps because it was on a separate line) remained. Now it appeared that a nonsensical “Medium Rare French onion soup” was ordered. By pulling on this thread the first Canadian zapper case unraveled. Personal communication from David Bergeron, (June 9, 2008) (notes of conversation on file with author).

\(^6\) Revenue Quebec posts news releases of significant tax evasion enforcement actions on its web site (in French only). Among these listings there are a large number of cases involving sales zappers (camoufleur de ventes).

From 2003 to 2008 there are eighty-eight cases. There are an even larger number of cases where zappers may have been involved, but the notice only indicates that a business “failed to report sales,” or “kept a double set of books,” or “failed to keep an accurate set of books.” Compared with other jurisdictions, like the Netherlands where there are less than ten litigated cases, or the US where there are two, or Sweden where there is one, or the UK and Ireland where there are none, this is a very robust enforcement record. The Revenue Quebec press releases on Tax Evasion are available at: [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/) (last visited June 13, 2008).

It should be noted however, that this may be an unequal comparison. If a zapper is found in a revenue enforcement action litigation may not necessarily be the norm. In fact, the Revenue Quebec site lists investigations and in most cases the taxpayers involved are simply pleading guilty, not contesting the determination. If the same pattern arises elsewhere, then barring postings like those of Revenue Quebec, one might not expect to be able to find a similar list. Then again, this author has not been able to locate any jurisdiction where there seems to be a similar concentration of zapper cases. Nothing even comes close to the Quebec statistics.

\(^7\) A further consideration of zappers, phantom-ware and the solutions that governments are using to cope with them is the topic of different (as yet unpublished) paper by this author. Leading approaches are those offered by Quebec, Germany and Greece.
Canadian provinces) Mr. Pratt unintentionally sent a message to the FTA that zappers were a Quebec-only problem.⁸

The US attitude is just now beginning to change. Zappers were discussed at the October 2007 FTA/MTC Audit and Technology Workshop, and then again at the March 2008 FTA Compliance Workshop.⁹ This paper tracks a third zapper discussion at the FTA, the presentation that this author was invited to give at the 2008 Annual Meeting on June 9, 2008.¹⁰ In spite of this renewed interest, the fact remains that to this day the US has uncovered only two zappers – the one at Stew Leonard’s Dairy in Norwalk, Connecticut¹¹ and another at the LaShish restaurant chain in Detroit, Michigan¹² Maybe this statistic is about to change?

This paper presents the case that zappers, or more generally automated sales suppression devices are a global problem. Zappers are everywhere because they have entered the bloodstream of the commercial marketplace. They are frequently the element that makes or breaks a deal for a new ECR or POS system. Businesses large and small are regularly offered opportunities to invisibly skim cash receipts with this technology, and many are taking advantage of it. Tax administrations are responding, and the US needs to join in this effort.

TERMINOLOGY

Terminology complicates research in this area, so it is best to define some terms and distinguish some usages in the beginning. In general we are examining software programs that are used in conjunction with electronic cash registers (ECRs) or point of sale (POS) systems to alter business records, allowing owners to skim cash receipts. This is a relatively new technology field (although it is an old fraud), and as with all technology areas there are “generations” of technology that follow (sometimes very rapidly) one upon another as the field develops. Thus, it is important that we adopt terminology that will not only allow us to discuss the whole field, but permit us to classify generational developments.

---

⁸ The assessment that zappers are a “Quebec-only” [or a “Canada-only”] problem seems to remain common currency. For example, when the following question was recently presented to the Pennsylvania Department of Revenue:

“Have you seen a zapper in Pennsylvania?”

The answer was:

“We do not have Zappers [in Pennsylvania. However, t]hey are being deployed in Canada … mostly in the restaurant businesses …”

Personal e-mail communication to Janis Holloway, responded to by Robert Coyne (May 16, 2008) (on file with author).

⁹ Personal e-mail communication from John Feldman (Jun. 11, 2008) (indicating that these meetings were for government personnel only) (on file with author).

¹⁰ Richard T. Ainsworth, Zappers: Technology-assisted Tax Fraud (power-point presentation on file with author).

¹¹ 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).

The term *automated sale suppression device*\(^{13}\) is the general classification for all software programs used or designed to facilitate cash skimming. *Phantom-ware* is a sub-classification. It includes the first two generations of automated sales suppression devices – *self-help phantom-ware*, and *factory installed phantom-ware*. *Zappers* are a third generation of automated sales suppression devices.

*Phantom-ware*.\(^{14}\) Phantom-ware is programming placed within a modern ECR or POS system that can be used to hide the skimming of cash sales. Phantom-ware is “hidden” (in the sense of not being disclosed in user manuals). Its use, operation, and even its existence may be very difficult to detect on audit.

Phantom-ware re-programs an ECR or POS system so that selected types of cash sales are not recorded (receipts can be renumbered to follow a new sequence, Z Reports and X Reports can be altered, and the Electronic Journal can be brought into conformity with all other changes). This programming exists on most systems for good (but occasionally remote) business purposes, and there are good reasons for having it “hidden” from employees. For example during a bankruptcy sell-off of business assets a buyer of the ECR would want to clear the electronic journal. Programming is needed to do this, but one might not want the night shift manager to know how to do this with instructions set out in the user’s manual.\(^{15}\)

Because it relies on a manual re-programming of systems this is called *self-help phantom-ware*. Installers, distributors and manufacturers frequently provide help-desk support and will guide owners in the use of these “hidden” functions. Help-desk personnel may suspect, but have no reason to definitively know that a user is asking for help to commit fraud. There is of course something akin to Admiral Nelson’s “turning a blind eye” here,\(^{16}\) as these systems do

---

13 “Automated sales suppression,” “electronic sales suppression,” or “sales suppression technologies” is the preferred expression of the CRA these days. For example, at the 2007 International Tax Dialogue Conference the Director General SME Directorate, Compliance Program Branch indicated:

One of the most popular means to suppress sales is to utilize electronic suppression of sales technologies, such as “Zapper.” The CRA is actively working with provincial counterparts (through the FPTUEWG) to address Zapper and other point-of-sales suppression technologies.


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

14 The term “phantom-ware” originates with this author, who after struggling with imprecise and overlapping terminology employed elsewhere, decided that a new expression was needed.

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

16 Admiral Horatio Nelson in the naval battle of Copenhagen (1801) when leading the attack against the Danish/Norwegian fleet (reportedly) willfully disobeyed an order from his commander Admiral Hyde Parker to disengage. He did this by placing his telescope to his eye that was blind and declared that he could not see the flags signaling disengagement. Nelson won the battle.
not preserve a record of the re-programming action. There is of course a real danger to the fraudster if they did, because a government auditor might suspect fraud in a business that repeatedly programmed and re-programmed its ECRs to start and stop Z or X Report, or entries in the Electronic Journal.

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

In this new generation the technology has changed, but the technology only has one purpose – a fraud purpose. It is still phantom-ware – programming hidden in the software – but it requires much less manual intervention to operate. It can still be found by auditors if the operating system of the ECR or POS system is broken down.

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

---

17 The Cash Register Good Practice Guide notes at ¶ 4.1:
In countries that have no legislative requirement to use Fiscal Tills, tax auditors are now encountering increasingly sophisticated electronic till systems that present potentially enormous risks.

These till systems are extremely vulnerable to all three risk types identified. In particular, new tills systems are being manufactured with “fraudulent risk” software installed as standard.

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

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

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

Which translates as:

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


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

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

Zappers are contained on CDs or memory sticks. They can be removed and hidden on the first signs of an audit. Without a disclosure by the fraudster (or the distributor, or the zapper-developer) the use of a zapper is nearly impossible to detect. Traces of zapper use however, can be found when fraudsters are not careful, or if the zapper is not well designed. Occasionally back-up records remain in a POS system or an ECR that reference the original transaction data. For this reason, technical support is frequently needed when zappers are used, just as they are with phantom-ware applications – something that leads to long-term business-fraud relationships.

THE DEVELOPMENT TIME LINE

Skimming cash sales is a traditional tax fraud. It has been practiced with two physical tills for a long time – one for the taxman and the other off the record. The traditional way of uncovering a cash skimming operation is to look for the other set of books, or to find a cash hoard, or to find that inventory purchases far exceed reported sales.

Needless to say, technology can make a lot of these detection points easier to hide. A digital second set of books is easier to hide than paper ledgers, and a good zapper program (particularly if it is placed on the server that integrates a network of ECRs and other accounting

In December 1997, Radio Canada current affairs program “Le Point” ran a story about the use of Zappers. The week after, a meeting was held involving UE [Underground Economy], Investigations from HQ, Montreal and Ontario and Quebec provincial officers. As conclusion, it has been decided that HQ-UE should take the lead of this issue. A series of recommendations were also provided to Mr. Lacombe, former ADM. [The recommendations have been redacted.]

Until now, the MRQ [Ministry of Revenue Quebec] has proceeded to complete several audits, Investigations and searches related to Zapper users. On May 12th, we received a press release from MRQ about the Nickles group who plead guilty to 74 charges of tax evasion. [The enclosed copy of the guilty plea has been redacted.]

Definition

Zapper software programs are electronic means of concealing revenues. Taxpayers can delete 5, 10, 15 percent or more of their sales by activating an accounting software program. In order to eliminate as many trails as possible, Zappers are used mainly in cash transactions.

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

“Zapper” is also the expression used in early OECD documents to describe the whole field of automated sales suppression devices (admittedly in the very last paragraph on the very last page of an e-commerce report): However, an intimate knowledge of how to manipulate computer systems is not required where unscrupulous software programs, such as “zapper” are developed. These programs are specifically designed to falsify records and hide certain transactions. News of these techniques generally spreads rapidly through an industry, especially traditional cash based industries. Tax authorities will have to be attuned to new tools to defeat the integrity of systems much as they must keep abreast of new tax dodges and schemes for illegally sheltering income. Tax authorities must also make sure that they have audit experts that are experienced in online business methods and models. They must catalogue and understand the digital footprints that electronic records leave and develop compliance models for online business types that provide a basis for comparison across tax paying entities.

systems) can also eliminate (“zap”) inventory records so that purchases closely match “zapped” sales. To accomplish this (inventory zapping) it is necessary to purchase a certain percent of inventory in cash.

Technology mitigates certain risks of detection, but technology can also bring with it new risks – particularly if the business owner (fraudster) is not comfortable with automation. Thus, the development line for sales suppression devices has been to try to devise “idiot-proof” systems. The following sections will present cases from along this development line: (a) traditional double tills, leading to (b) self-help phantom-ware, and then (c) factory-installed phantom-ware, and finally (d) zappers.

TRADITIONAL DOUBLE TILL CASES

Traditional double till cases are relatively easy to find. Traditional cash skimming fraud is not unique to any jurisdiction, nor is it unique to a particular tax system. It is just as common where the consumption tax is a VAT, as it is where the consumption tax is a retail sales tax. It is more common in family-owned businesses where knowledge of the skimming can be kept “hidden” among close relations.

Comparing the two examples that follow, Aleef Garage Ltd. and Guerico, one might have expected that the size of the Aleef Garage skimming operation would have warranted the use of technology (if only to keep the records straight). But technology was not employed. Thus, Aleef Garage gives some idea of how large a traditional skimming fraud can be. Guerico, on the other hand, shows how simply a double till skim can be set up.

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.19 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.20 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

---

19 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).
takings in one of the tills in their accounts and only declared the money in the other till to HMRC.\textsuperscript{21}

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.\textsuperscript{22}

The success of the \textit{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.\textsuperscript{23} As Steve Armitt, Group Leader HMRC Criminal Investigations indicated, “… the investigation was made all the more difficult because of the closed ranks of the employees involved some of whom were close family members … [t]hose involved tried to make it as difficult as possible for the cheating to be discovered.”\textsuperscript{24}

It is not clear from published reports how the \textit{Aleef Garage} fraud was initially uncovered, although the HMRC News Release does indicate that “… the cash was used to fund private lifestyles, [but it was also] transferred to other personal accounts including some in the Channel Islands.”\textsuperscript{25}

\textit{Nicholas Guercio & Victoria Constantine (formerly Guercio) v. Commissioner.}\textsuperscript{26} \textit{Guerico} is more typical of the size of a double till, manual skimming fraud. \textit{Guerico} involved a very small business. It 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.

The physical skimming of sales was very simply carried out. Each shift had its own till, and the tills for each shift were checked against cash register tapes (to prevent employee theft). The owners however, presented the accountant with only one of the tills and one of the cash register tapes for each day’s operation.\textsuperscript{27} Bank deposits and tax returns were filed based on the funds and the tapes from the disclosed tills.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{22} 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, \textit{supra} note19, at Notes for Editors 2; Chris Oshu, \textit{supra} note20.
\item \textsuperscript{23} HMRC News Release, \textit{supra} note19, 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)).
\item \textsuperscript{24} \textit{Id.} at 1.
\item \textsuperscript{25} \textit{Id.} at 1.
\item \textsuperscript{26} Guercio & Constantine, T.C. Memo 1983-554.
\item \textsuperscript{27} 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 \textit{F-D Oil Company, Inc. v. Minnesota Commissioner of Revenue}, 560 N.W.2d 701 (1997). Although the shop destroyed
\end{itemize}
\end{footnotesize}
Each Monday the owners met, divided the cash from the withheld till and destroyed the withheld register tapes. Because two of the owners, representing 80% of the equity interests were “hidden” behind Guerico (a nominee holder of their interests) most of the skimmed cash left the business each Monday without a trace.28

SELF-HELP PHANTOM-WARE

Double till skimming requires that some sales not pass through, or at least are not recorded in the official cash register records. The risk in doing this is that customers (if the cash registers are shut down) or employees – normally the accountant – (if cash register records are destroyed) will become suspicious, and turn in the fraudster. The alternative is to pass all sales through the cash register and selectively eliminate certain transactions from the records of all cash sales. In other words, the alternative is to do what Guericco did, but do it transactionally (line-by-line) instead of eliminating a full ten-hour shift each day.

The difficulty in doing this is that modern cash registers leave audit trails. Transactions are recorded in Z Reports ("daily" and "periodic," normally called Z1 and Z2),29 X Reports ("daily" and "periodic," normally called X1 and X2)30 and in the Electronic Journal.31 Thus, a fraudster who fears the risk that his customers (or his accountant) would reveal his fraud may look to the cash register to hide it.

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.

28 By keeping 80% of the ownership interests “hidden” the fraudsters in Guericco 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 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.

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

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

31 See supra note Error! Bookmark not defined., Cash Register Good Practice Guide, Appendix G, at 1.2.

The electronic journal usually contains ALL transactions keyed into the more complex types of till systems and is therefore the definitive record to obtain for audit purposes. There are exceptions, where Electronic Journals can be programmed “not-to-store” certain keying transactions e.g. “Training Mode.” The Electronic Journal should not be confused with the "Z" tape as it is not a recap of the day’s sales. The Electronic Journal tape is supposed to be a “blow-by-blow” record of every transaction made “step-by-step.” It is most useful for going back during a day to look for mistakes that were made. This journal has been a staple in the cash register industry since its conception. It can be used to check the Z report.
A very dedicated fraudster will discover this on his own – a less dedicated fraudster will learn from another businessman, an ECR or POS system sales person, or a “computer consultant” – but there is functionality inside most modern systems to selectively suppress entries. The rub is that some re-programming is required. This is the self-help phantom-ware option.

The following example (one of many possible) is set out in the *Cash Register Good Practice Guide*. It explains the re-programming that is necessary to support a specific “self-help” sales suppression. This re-programming allows cash to be skimmed by passing refund transactions through a CASIO TE-2000 cash register. This re-programming will suppress records of a refund in the Z Reports, the X Reports and the Electronic Journal. Once again, the problem for fraudsters using “self-help” phantom-ware is that mistakes can be made when re-programming, and if they are not careful the skimming can be detected through skillful till interrogation.

**CASIO TE-2000 ECR – refunds omitted from the daily sales reports.** The *Cash Register Good Practice Guide* indicates:

Owing to the massive range of standard programming options incorporated into modern ECR’s and POS systems, no guarantee can therefore be given that sales information contained in Z reports is reliable and complete. Current techniques used to check the traders audit trail by reference to sequential numbered, dated and timed Daily Z Reports is no longer sufficient to give assurance that the sales data being audited is accurate. Further checks may be necessary to verify the integrity of till reports submitted by traders … [p]rogram interrogation may reveal that the till operating systems have been reconfigured to suppress sales information …

In the CASIO TE-2000 the program that controls printing on Z Reports is READ/RESET REPORT PRINTING CONTROL, PROGRAM 0822. The procedure for reading (printing) the program is:

1. select PGM mode (the program mode switch);
2. press 3
3. press SUB TOTAL
4. press SUB TOTAL

When the program prints the setting information will be listed on the top of the report. It should indicate: “Program 0822, command code 00001000.” [Note: the program setting is 001000, however the program reading is an eight digit number, thus there is a prefix of “00” added. The prefix is not material to this discussion.] The following table breaks down the program code:

<table>
<thead>
<tr>
<th>Code</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short hand identifier “D” = digit</td>
<td>D6</td>
<td>D5</td>
<td>D4</td>
<td>D3</td>
<td>D2</td>
<td>D1</td>
</tr>
</tbody>
</table>

To reconfigure the 0822 program in the CASIO TE-2000 the following steps are taken:

1. select PGM mode

---

32 *See supra* note Error! Bookmark not defined., *Cash Register Good Practice Guide*, Appendix E, at 4.1.1.
(2) press 3
(3) press SUB TOTAL
(4) press the program that needs to be reconfigured (i.e. 0822) on the numeric keyboard.
(5) press SUB TOTAL
(6) press the new program code (we are changing code 001000 to 003100)
(7) press the CA/AMT TEND key
(8) press SUB TOTAL

Some explanation is needed on what the code at item (6) means initially and then how the new code is derived. The previous code 001000 is interpreted as follows:

(a) D6 set to “0” indicates “print first and last consecutive numbers of the day.”
(b) D5 set to “0” indicates three things:
   a. “skip zero total lines on department and transaction read/reset report”
   b. “skip zero total lines on PLU read/reset report”
   c. “skip zero total lines on hourly sales report.”
(c) D4 set to “1” indicates two things:
   a. “print the sales ratio on read/reset report”
   b. “do not suppress printing of the non-resettable grand total on the daily reports.”
(d) D3 set to “0” indicates two things:
   a. “suppress the printing of RF [refund] totals and RF count [both RF mode and RF key]”
   b. “print tax rate with tax totalizer.”
(e) D2 and D1 signify actions that are not relevant in this discussion

The new code “003100” changes the values at items D4 and D3. D4 is changed from “1” to “3.” D4 makes two statements. The first statement, “print the sales ratio read/reset report,” has a value of “0” for “no” and “1” for “yes,” and we want this statement to read “yes.” The second statement, “do not suppress printing of the non-resettable grand total on the daily reports,” has a value of “0” for “no” and “2” for “yes,” and we want this statement to also read “yes.” Thus, D4 needs to be “3” (or, 1 + 2 = 3). We are trying to suppress printing of the non-resettable grand total on the daily reports, so to do this we need to change D4 from “1” to “3.”

D3 deals specifically with the refund (RF) function, and we need to change this value from “0” to “1.” D3 makes two statements. The first statement, “suppress the printing of RF [refund] totals and RF count [both RF mode and RF key]” has a value of “0” for “no” and a value of “1” for “yes,” and we want to suppress the printing of the refunds, so this value needs to be “1.” The second statement, “print tax rate with tax totalizer,” has a value of “0” for “no” and “2” for “yes.” We do not need the tax rates to be printed, so the default setting of “0” is fine. Thus, D3 needs to be “1” (or 1 + 0 = 1) instead of “0.”

Our goal is to suppress the printing of RF totals and RF count, and suppress the printing of the non-resettable grand total on the daily reports. The code to do this is “003100” – as shown in the following table:
Once re-programmed, “[t]he daily read/reset reports printed in X and Z modes will not print the non-resettable grand total and refund transactions made in the RF mode and RF key.”[33] The Guide runs two examples based on this re-programming. The first (using the “001000” code) shows:

- sales of 1,000 (500 + 250 + 250),
- a refund of 250, and
- a cash-in-the-drawer total of 750.

The second (using the “003100” code) shows:

- sales of 750 (250 + 250 + 250),
- no refund, and
- a cash-in-the-drawer total of 750.

If in fact sales of 1,000 were made, and the business owner skimmed 250 from the ECR and rung this “skim” through the cash register as a refund, neither the Z Report (Z1 or Z2), nor the X Report (X1 or X2) would show it. Both the consumption tax on the sale (VAT or RST) and the income on the sale could easily go unreported. An audit that checked tax returns against the Z Report, even if cross-checked with the X Report would not detect the fraud.

The flaw in this particular fraud is that the refunds could show up in the Electronic Journal (that is of course if additional programming options are not selected to eliminate the printing of refunds in the Electronic Journal.)[34] Much the same fraud can be accomplished by recording live sales in the training mode. Training mode sales can be eliminated from Z and X Reports as well as the Electronic Journal.[35]

Reliance on the Electronic Journal in a CASIO TE-2000 is not a “fail-safe” check for tax auditors. There are significant problems with the completeness and correctness of the data in the Electronic Journal. The Dutch Tax Administration has examined more advanced CASIO systems, the CASIO QT-6000 and CASIO TE-4000, and is convinced that Electronic Journals in even these machines are not secure. The main risk (in all CASIO machines) is that the RAM on which the data are preserved is too small and there is no mechanism to store data on an external medium. As a result, when the RAM is full, data is simply over-written. The only way to access (and preserve) the Electronic Journal data on a CASIO machine is to use the back office program CASIO Hospitality, but on this medium also there is no assurance of completeness and correctness of the data.[36]

---

33 See supra note Error! Bookmark not defined., Cash Register Good Practice Guide, Appendix E, at 4.7.
34 See supra note Error! Bookmark not defined., Cash Register Good Practice Guide, Appendix B, at 3.3 (Risk number 40) and 5.2.6.2 (discussing a “hidden function” on the CASIO QT-7300 machines that allows the Electronic Journal to be turned on and off).
35 Id.
36 Personal e-mail communication, Ben van der Zwet (May 30, 2008) (on file with author).
Effectively, CASIO machines cannot be relied upon to preserve business records. They can be programmed to delete records on the Z Reports and the X Reports, and can be relied upon to delete data in the Electronic Journal automatically (after certain volume limits are reached).

FACTORY-INSTALLED PHANTOM-WARE

One of the best examples of a litigated factory-installed phantom-ware case is a Dutch case involving the Grand Café chain Dudok. A grand café is a style of café that occupies a single large space welcoming a large amount of foot traffic. The Dudok in Rotterdam, for example, is located in a converted warehouse. Its central location, comfortable leather furniture and liberal scattering of newspaper make it a high volume, cash-intensive cafe-bar-restaurant from breakfast through midnight.

Phantom-ware was first used by Dudok to skim cash receipts in the midst of a Dutch IRS examination. The IRS was initially concerned with staff salary. Payments were being made under the table, and the IRS was suspicious. Testimony in the case indicated that on the second day of the IRS audit the managing director of Straight Systems BV visited Dudok where he was approached by the owner-manager. Straight Systems BV was the supplier of the Finishing Touch point-of-sale cash registers that were used by Dudok. The owner-manager of Dudok explained that he was having difficulty accounting to the IRS for the turnover.

During this conversation the Straight Systems managing director explained the existence of a “hidden delete” option in the Finishing Touch cash registers. The court indicated that this was, “… a hidden menu option that, after enabling said option, allowed operators of catering establishments to delete cash register receipts from the system.” After this discussion “… an employee of the defendant visited [Dudok] and explained the [technical] application of the erase...
rule [or hidden delete function\(^{42}\)], after which [Dudok] subsequently decided to start using [it]...

This case finds criminal tax fraud liability not only with the restaurant operators, but also with the suppliers of the Finishing Touch cash registers. As a consequence, the court is very clear about the operation of the “hidden delete” function. It indicates:

The defendant’s cash register program includes various features to adjust the receipts later on. These possibilities are clearly described in the manual and are found easily in the menu structure of the program. If a receipt is adjusted using these functions, a “record” thereof is kept in the files so that any adjustments can be established afterwards. In addition [there is], a hidden option [that] exists to delete receipts. This function is not described in the manual and is also not included in the menu structure. Moreover the retrieval of this option is very complicated and only possible if the defendant explained this to the buyer. Contrary to the other features, use of this hidden option does not leave any traces in the files that are written to the disk. As a result, it is impossible at a later date to establish that the receipts have been deleted, hence this can, in principle, not be checked. It is self-evident that completely removing receipts from the books is a pre-eminent means for hiding turnover from the Internal Revenue Service.\(^{44}\)

This is a description of the essential characteristics of a phantom-ware system. It is an operating system designed for an ECR that for all practical purposes is fully transparent. All traditional programming options are explained in detail in the user’s manual, all traditional options are visible in the menu structure and the use of any of these options leaves a clear audit trail for both the owner and external auditors. However, transparency is apparent, not real. Embedded in the operating system is functionality that selectively eliminates sales records without leaving an audit trail. Knowledge of this functionality is passed secretly (almost always orally) from the ECR provider to the ECR user.

The appeals court in LJN: AX6802 reacts strongly to the following facts – the “hidden design” of the programming – the transmission of “secret knowledge” about its existence – the “secret instruction” that is provided in its operation:

In view of the special characteristics of the hidden option and the existence of the program’s other features for making adjustments, the court cannot imagine any other purpose for the hidden option than the illegal manipulation of turnover figures. The court is therefore firmly convinced that the defendant, as the seller, was aware of this. By selling this software to a catering establishment, the defendant knowingly and willfully accepts the considerable chance that the buyer will use the program to delete turnover to conceal it from the Internal Revenue Service, with all associated tax consequences. ...In view of the context within with the delete option was discussed [between the managing director of Straight Systems BV and the owner-manager of Dudok], the court assumes that the

\(^{42}\) The trial court in Rotterdam refers to the phantom-ware application as a “hidden delete function” whereas the appeals court in The Hague refers to the phantom-ware as “the erase rule.”

\(^{43}\) LJN: BC5500, at F3.

\(^{44}\) Id.
managing director of the defendant, and hence the defendant, knew that [Dudok] wanted to dupe the Internal Revenue Service.45

It is particularly troubling to the appeals court that not only is, “[t]his erase rule actually made available to various customers, [but that the] defendant also offered support to customers – also in respect of this erase rule – by means of a helpdesk. Viewed against this background, making the erase rule available is part of the normal conduct of the business of the defendant.”46

Saying that these practices are “part of the normal conduct of the business” of Straight Systems BV is tantamount to saying that this fraud is a cancerous mutation that goes well beyond the traditional fraud where cash receipts are skimmed through a two-till system. This is a fraud that has entered the bloodstream of the market-place. As a result, the government needs to consider market-level as opposed to single-business-enterprise-level responses.

ZAPPERS

Zappers represent the third generation of automated sales suppression technology. They were developed in response to (a) the inherent risk of detection in self-help phantom-ware applications (the re-programming errors that fraudsters would make were leaving traces of the fraud) and (b) the expanded risk to developers and manufacturers in factory-installed phantom-ware (with only one purpose – to facilitate skimming – knowledge of and participation in the fraud was becoming difficult to deny when the factory installed the program). The advantage of a zapper was that it could be removed from the system, and placed in your shirt pocket as soon as the auditors knocked on the door.

Zappers minimize risk of detection. They are physically kept apart from the ECR/POS system they manipulate. Zappers have been found on cassettes, floppy disks, zip disks, CDs, and memory sticks. They are inserted temporarily into the ECR/POS system to perform sales manipulations. When the procedure is completed, the zapper is removed. If a zapper is well developed – if it is designed by someone with detailed knowledge of the operating code it is being used on – then no trace of the original data trail will remain. Everything will be re-written, and the program that did it will be gone.

The cases below have been selected to draw out two points: (a) Zappers have been used to assist in the skimming of cash receipts since the dawn of the computer age – 1981 in the case of Stew Leonard’s Dairy, and (b) Zappers have spread around the globe – they have (for example) been found in the US, Australia, Brazil, Canada and Sweden. It is reasonable to assume that they are available everywhere.

The US and Australian cases exhibit custom-made Zappers – Zappers designed by in-house computer specialists to work only on the specific ECR or POS systems in place in their companies. The Brazilian and Canadian cases exhibit commercial Zappers – Zappers designed by (and sold separately by) the company or the individual who designed the specific ECR or POS systems program on which they operate, and are intended to be used widely in the market-

45 Id.
place. The Swedish case exhibits a Zapper of mysterious design. Although the Swedish Zapper works with a specific (foreign) operating system in a specific (foreign) ECR the developer is unknown, leaving the Swedish Tax Administration in the dark about whether this is an isolated in-house Zapper or a Zapper that it should expect to find in other similar operating systems.

In the US – Stew Leonard’s Dairy. Until recently “the largest criminal tax case in the history of Connecticut,”47 which also was the “largest computer driven tax-evasion case in the nation,”48 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 receipts over a ten year period. The cash was taken in large denomination bills by suitcase to St. Martin in the Caribbean.49

The 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 [the in-house name for the Zapper], 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.50

Stew Leonard’s Dairy is a microcosm of how the manual skimming of cash receipts has moved into technology. There are two pressures on an enterprise like Stew Leonard’s Dairy (a) the increased risk of detection from increasingly sophisticated auditors, and (b) the sheer complexity of small amounts of cash from an extremely diverse retail operation.

Skimming of cash receipts began in Stew Leonard’s Dairy in the 1970’s. This was a physical skimming. It was performed by the CFO, Barry Belardinelli who worked in the store’s vault room where large bags of cash were received daily from the store’s cash registers.51

48 Jacques Steinberg, Connecticut Store Owner Sentenced in Tax Fraud, NYT, Sec. B, page 1, col. 3 (Oct. 21, 1993)
49 U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), aff’ed. 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).
50 Leonard, 264 Conn., at 298.
51 Leonard, 37 F.3d at 33.
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). In about 1981 or 1982 the skimming was automated. 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.52

Mr. Pirhalla was a computer specialist with detailed knowledge of the operating system of the ECRs used in Stew Leonard’s Dairy. He was hired by Stew Leonard from the National Cash Register (NCR) company. It was important to employ someone like Mr. Pirhalla because Zappers need to be re-designed whenever the base operating system is updated. Running an old Zapper against records in an updated ECR may leave traces that auditors could use to detect the fraud.

However, Mr. Pirhalla himself was a risk that could not be minimized. 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 system. They, along with Mr. Pirhalla, worked under the supervision of special agent Doreen Schultz, the IRS’s own computer book-keeping system expert.”53

One of the special features of the Zapper in Stew Leonard’s Dairy was that it was designed to do more than “zap” cash sales. It was designed to withstand the scrutiny of a rigorous income tax audit – an audit that undertook to systematically match purchases (inventory) against sales. Both prices and units bought and 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

52 Id. at 35.
53 Brief for Appellee, supra note Error! Bookmark not defined., at 17-18.
diverted was spread over a wide spectrum of products. Some calculations amounted to pennies per item.\textsuperscript{54}

The Zapper in \textit{Stew Leonard’s Dairy} pre-dated memory sticks, CDs and zip files. This Zapper was kept on a cassette in a hollowed out book in Stew Leonard’s library. Obsolete versions of the program were kept by Frank Guthman at home in his basement.\textsuperscript{55}

\textit{In Australia – Regina v. Ida Ronen; Regina v. Nitzan Ronen; Regina v. Izar Ronen}.\textsuperscript{56} 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).\textsuperscript{57} “[T]he scope of the fraud represented by unpaid [income] tax was approximately [AUD] $8.125.”\textsuperscript{58} 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 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, … \textsuperscript{59}

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.\textsuperscript{60} 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

\textsuperscript{56} 2005 NSWSC 991.
\textsuperscript{57} 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.
\textsuperscript{58} Ronen, 2005 NSWSC, at ¶14.
\textsuperscript{59} Ronen, 2005 NSWSC, at ¶18.
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.\(^{\text{61}}\)

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.\(^{\text{62}}\) (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 they investigate, that the shops were regularly banking cash as well as other forms of takings related to the shops.”\(^{\text{63}}\) 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.”\(^{\text{64}}\)

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.”\(^{\text{65}}\) 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.

**In Brazil - Operação Internet.** *Operação Internet* or 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 was the eventual target. AMG produced not only government certified software (called Robot) for use in cash registers operating within the state; it also produced and sold the Zapper (Quanto) that defeated it.

Litigation in Brazil can take many years to work its way through the court system, and there is no reported cases based on *Operação Internet* available, however press reports describe the investigation this way:

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

\(^{\text{61}}\) Ronen, 2005 NSWSC, at ¶24 (emphasis added).
\(^{\text{62}}\) Ronen, 2005 NSWSC, at ¶¶25 & 27.
\(^{\text{63}}\) Ronen, 2005 NSWSC, at ¶26.
\(^{\text{64}}\) Ronen, 2005 NSWSC, at ¶26.
\(^{\text{65}}\) Ronen, 2005 NSWSC, at ¶28.
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 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.66

In Canada - Audio Lab Ltd. On April 8, 2004 Revenue Quebec announced that it executed four search warrants on the numbered company 9061-1184 Quebec Inc. which operated a restaurant under the name San Antonio Grill in Laval, Quebec. The allegation was that a “sales Zapper” (camoufleur de ventes) was used to delete sales records. The Zapper was on a diskette used in connection with the restaurant’s computer system.67

Next year, on April 25, 2005, Revenue Quebec announced that the director of San Antonio Grill pleaded guilty to using a Zapper.68 A related company of similar name, Grill San Antonio in Repentigny, also pleaded guilty to similar offences.69

Later that same 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

---


68 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.

69 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/communiques/ev-fisc/2005/25avril.asp (in French only, last visited Feb. 8, 2008).
with its own restaurant cash register software, Softdine. Softdine was the operating software in the cash registers at San Antonio’s Grill in Laval, and at Grill San Antonio in Repentigny.

On June 26, 2007 Audio Lab LP, Inc. pleaded guilty to charges of having, “… designed and marketed a computer program designed to alter, amend, delete, cancel or otherwise alter accounting data in sales records kept by means of a software that [Audio Lab LP] had designed and marketed.” In other words, it pleaded guilty to developing a Zapper to “add-on” to its own commercial software (Softdine) that it provided to restaurants for use in their POS systems. Press reports directly link this conviction to the investigation begun at Grill San Antonio in Laval in 2004. 

In Sweden - TT PI Electronique & Restodata. In an on-going Swedish investigation scheduled for court late in 2008 involves an ECR manufactured from Paris, France (TT PI Electronique) which is popular in Italy, Belgium, Portugal, Spain, Germany, Denmark, Australia, the US and North Africa. The operating system used in the specific TT PI Electronique ECRs under investigation includes a back-office program called Restodata.

The Restodata program is licensed and comes with a grey program dongle on a memory stick. Directly attached to this dongle is a second (silver) memory stick that contains a Zapper. Slides demonstrating the operation of the Restodata Zapper were presented by the author (with permission of the Swedish Tax Administration) at the 2008 Annual Meeting of the FTA on June 9, 2008. 

The Zapper used in this system has the ability to either (a) selectively change line items on a sales ticket (replacing expensive items with less expensive items and reducing the related VAT charges) as well as (b) perform a fully automated “zapping” of all transactions so that total sales for a day would be reduced by a specified amount. Although either approach could be used to reduce sales, this particular zapper allows a fraudster to custom tailor the zapping operation. However, one of the most distressing aspects of the early Swedish reports in this case is the following comment by Martin Jansson:

In this case the restaurant under investigation used a backoffice program called Restodata. According to the exe-file the program was produced by a company called “Restodata Inc.” However, we haven’t been able to find that name anywhere.


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

74 See supra note 10.

75 Id.
The Swedish case is an excellent example of where Zapper technology is headed. It is a direct result of the internationalization of cash skimming with Zappers. In the slides presented at the FTA is was possible to see the TT PI Electronique system move from a Swedish interface to an English interface as the Zapper was inserted into the POS system. Although this is not conclusive by any means, it does seem to suggest that what the Swedish Tax Administration is up against is a bit more difficult that what Revenue Quebec was up against in the Audio Labs, Inc. investigation, or what the State Tax Administration of Minas Gerais was up against in Operação Internet. The Swedish Tax Administration is most likely not looking at an in-house Zapper, nor is it looking at a locally designed and distributed Zapper. It is looking at a foreign Zapper designed to facilitate local fraud.

CONCLUSION

It is a very good sign that the FTA has begun to turn its attention to automated sales suppression devises – phantom-ware and zappers. Tax enforcement in the US needs to be directed at this problem. The states have some catching-up to do, and one of the best places to do it is just north of the border in Quebec.

Time is running on this problem. It is becoming more and more apparent that a fourth generation of automated sales suppression devices is coming on line. The next generation is likely to present considerable enforcement difficulties, because it will be international. Tomorrow’s problems will be more like those in the Swedish case. The developer will be unknown and foreign.

Zappers may once again be customized (like those Stew Leonard’s Dairy and Ronen), but instead of being developed in-house (where the IT specialist/ developer could be brought into the case on the side of the government in exchange for immunity) it is likely that the developer will be located outside the enforcing jurisdiction.

Internationalization of this area has some considerable advantages for the fraudsters. It has not been lost on the developers of automated sales suppression devices that the MRQ was able to find zappers in seven Patio Vidal restaurant franchises, and two bars (La Tasca in Gatineau, and O’Max in Masson-Angers) by following the customer list of Luc Primeau the developer and distributor of Microflash cash register software they all used. Luc Primeau it turned out, developed and sold the zappers for his own operating systems. However, in doing so, he increased the risk of detection for all his clients. Similarly, the Belastingdienst (Dutch IRS) was able to trace a locally designed zapper (used on produce scales in grocery stores –


called Analysis) through approximately 1,200 businesses by simply following the customer lists of the local developer. In this risk adverse industry, internationalization offers a buffer against detection. Zappers may well be going there.

In this regard, it was a welcome e-mail that this author received from the Deputy Commission for Tax Enforcement of the State of New York after the 2008 Annual FTA Conference indicating that he (for one) would be “reaching out” to the MRQ to learn how to build cases in this area. More states should follow this lead.

---


79 Personal e-mail from William Comiskey (June 11, 2008) (on file with author).