Electronic Tax Fraud : Are there "Sales Zappers" in Japan?

Kansai University Review of Economics
No. 11 (March 2009), pp. 1–34

Electronic Tax Fraud – Are there "Sales Zappers" in Japan?

Richard T. Ainsworth*
Hiroki Akioka**

Skimming cash receipts is an old fashioned tax fraud. Modern technology is changing how businesses skim. The agents of change are software applications – Phantom-ware ("hidden," pre-installed programming option(s) in ECRs) and Zappers (add-on programs for POS systems).

These programs are a serious problem in Canada, the Netherlands, Germany, Brazil, Australia and Sweden. Why are they not a concern in Japan?

Although it may be that they are not used in the Japan, it seems more likely that they are simply not being detected, because of insufficient (or technologically limited) audit resources. The authors hope to focus attention on this issue.

Keywords: Zappers; Phantom-ware; Tax fraud; Electronic Cash Register (ECR); Point of Sale (POS) system

Skimming cash receipts is an old fashioned tax fraud; a fraud traditionally associated with small or medium sized enterprises. Large businesses with formalized internal control mechanisms, external accountants, and professional management structures do not normally engaged in skimming.[1] Businesses that skim frequently keep two sets of books (one for the tax man, the other for the owner). In its simplest form there are two tills, and the cashier simply diverts some cash from selected sales into a secret drawer. A record of the diversion may be maintained, but it will be kept outside the formal accounting system.

* Adjunct Professor in Taxation at Boston University School of Law (Former Deputy Director of the International Tax Program at Harvard Law School) [mail to: vatprof@bu.edu]
** Professor of Macroeconomics at Kansai University [mail to: hiroki_akioka@post.harvard.edu]

[1] EU Commission, Fiscalis Committee Project Group 12, Cash Register Project Group, *Cash Register Good Practice Guide*, ¶ 2.5 (Dec. 2006) (on file with authors).

Businesses that skim rarely do so with credit card transactions precisely because these sales can be documented externally through the banking system. Skimming frauds thrive when the owner (or a close family member) is the cashier.[2]

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

Zappers are more advanced technology than Phantom-ware. Zappers are special programming options added to ECRs or point of sale (POS) networks. They are carried on memory sticks, removable CDs or can be accessed through an internet link. Because Zappers are not integrated into operating systems their use is more difficult to detect. Zappers liberate owners from the need to personally operate the cash register. Remote skimming of cash transactions is now possible without the knowing participation of the cashier who physically rings up the sale. This attribute of Zappers allows the incidence of skimming fraud to migrate beyond the traditional "mom and pop" stores. Zappers allow owners to place employees at the cash register, check their performance (monitor employee theft), but then remotely skim sales to cheat the taxman.

Although there is no public acknowledgement – in the press, in a court case, though any announcement by the Japanese National Tax Administration, or in any academic studies or papers – that Zappers and Phantom-ware are a fraud problem in Japan, a number of factors

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

suggest that Japan may be very fertile ground for this kind of technology-assisted fraud. Those factors include: (1) a high concentration of small to medium sized businesses;[3] (2) the fact that the retail economy is highly cash-based;[4] and (3) the high level of technology acceptance in the Japanese retail sector – electronic cash registers (ECRs) and point of sale (POS) networks are commonly employed in the retail trade.

It is something of an anomaly that Zappers and phantom-ware appear to be a very serious and well documented facilitators of skimming frauds in a wide range of developed countries (from Canada, to the Netherlands, as well as Germany, Brazil, Australia and Sweden) but they do not appear to be a concern in the two largest developed economies Japan and the United States. The US has encountered Zappers in just two cases, the $17million skimming fraud that involved Stew Leonard's Dairy (a grocery store) in Connecticut and the $20 million skimming operation that involved the LaShish restaurant chain in Michigan. Japan has reported no cases.

It has been assumed that Zappers and Phantom-ware escaped detection in the US for structural (jurisdictional) and audit support reasons.[5] The IRS, the agency with the most resources, is primarily concerned with income tax audits, and federal interest is only attracted when the fraud is very large. The American consumption tax, the retail sales tax, is the domain of state and local governments. Determining accurate sales figures for this tax is critical, but audit resources are very limited. As a result, significant skimming operations escape detection as they require more sophisticated audit techniques than the average state and local audit team possesses, but they are too small scale for federal auditors to focus on them.

[3] The Japanese Ministry of Finance defines a "small and medium size business" as an enterprise with capital of less than ¥100,000,000. Using this standard in FY-2006 there were 396,426 SME retail firms, representing 99.44% of all firms in this sector. The value added of these firms was ¥18,500,846,000,000 (or 62.36% of the whole value added of this sector). However, when considered in terms of the GDP these firms represent only 3.61% of the GDP (18,500,846,000,000/511,877,000,000,000). *Monthly Report of Financial Statistics #665*, Ministry of Finance, September 2007 (in Japanese).

[4] Reliable statistics on the cash economy in Japan are not as readily available as are statistics on the use of credit cards. Based on the best evidence available and compared with the US, the Japanese use of credit cards is less than half of that in the US leading one to believe that Japan would be twice as susceptible to Zappers as the US. In 2002, Japanese credit card use reached 12% of household consumption, whereas in the same period US credit card use was in excess of 25% (*Nilson Report, 777* (Dec. 2002).

[5] Richard T. Ainsworth, *Zappers: Technology-assisted Tax Fraud, the SSUTA, and the Encryption Solutions*, ABA Tax Lawyer (forthcoming, 2008).

The US experience contrasts dramatically with that of Quebec where over 275 Zapper cases have been prosecuted over the past ten years. This contrast has made it easy to assume that it is the comprehensiveness of the Quebec audit program that explains the difference. When the Ministry of Revenue in Quebec (MRQ) performs an audit it considers the full range of company taxes – income (federal and provincial); consumption (federal GST and provincial QST); and payroll (federal and provincial). The same is true in the Netherlands, Sweden, and Germany, all places where significant Zapper activity has been found. In the EU a common presumption is that comprehensive audits are the key to successful technology fraud detection.[6]

If this is the case, then what explains the Japanese result? Income, consumption and payroll taxes are all within the ambit of the National Tax Administration. Comprehensive audits are standard practice in Japan, and yet no Zappers or Phantom-ware manipulation of sales records have been found.

Although it may be that Zappers and Phantom-ware are not in use in the US and Japan, it seems more likely to the authors of this paper that they are being used (perhaps widely) but that insufficient (or technologically limited) audit resources are committed to detecting computer manipulations in the small and medium sized business sector. The authors hope that this paper will help to focus attention on this issue.

Technology-facilitated skimming is far more sophisticated and much more difficult to detect than traditional skimming. For example, some technology permits small amounts to be shaved from the sale of many products – essentially diverting a penny or two from every cash sale rather than eliminating an entire transaction; other technology reaches back into inventory to adjust purchase records so that lower purchases will match the lower (zapped) sales figures.[7] Because sophisticated

[6] Ben B.G.A.M. van der Zwet (Netherlands revenue administration) personal e-mail conversation August 11, 2008 (on file with authors).

[7] The Quebec experience has been that Zappers have not been widely used to adjust inventories, because the inventory management function within many POS systems is not widely used. Restaurants would manage inventories either though a different system, or manually. Personal e-mail communication from Dave Bergeron (Aug. 18, 2008) (on file with authors). This in turn has lead to the rise of the (Zapper) computer consultant who advises on tax evasion methods, for example saying: "If you erase $5,000 in sales, you must purchase under the table [make unrecorded purchases of inventory for cash] for $1,500. [And you must get] suppliers to participate [in the fraud]." Powerpoint presentation, Richard T. Ainsworth & Dave

zappers cover their own tracks (matching fraudulent inputs with fraudulent outputs) they defeat even the most careful auditors (if they are not technologically suspicious). Detection of Zapper and Phantom-ware fraud requires auditors to break down and analyze the programming of modern ECRs and POS systems.[8]

In the jurisdictions where documented skimming frauds have taken hold the marketplace has been observed to quickly become an unlevel playing field.[9] Honest businesses are pulled into fraud just to maintain competitive position. The gossip on the street (that skimming is easy, and that many are doing it) is amplified when the sales personnel from the major ECR and POS distributors demonstrate how phantom-ware and zappers work. "Hidden" programming options are promoted, help desk support is made available, and IT consultants provide troubleshooting services for operational glitches. All of this impacts the tax system. Business profits are underreported, consumption taxes are diverted, and a cash hoard develops out of which unreported wages are paid to favored employees without withholding for social security and other programs.

There are three major sections to this paper. The first section outlines the historical development of Zappers and Phantom-ware. The second measures the significance of this fraud. Two measures are used direct and indirect. The direct uses the few (empirical) studies that governments have made public on this problem. The indirect measure considers the case law which shows that large amounts of cash have been diverted by these programs, and that once established in a marketplace large numbers of businesses follow one another in adopting this technology.

Bergeron, *Zappers (automated sales suppression)*, New York Prosecutors Training Institute (July 31, 2008) at slide 6 (on file with authors).

[8] Ben B.G.A.M. van der Zwet from the Netherlands revenue administration indicates that in his experience this kind of audit benefits from, "thorough audits with correlation checks based on third-party investigations of purchases, and intensive surveying on location ..." Personal e-mail conversation August 11, 2008 (on file with authors).

[9] Jean-Marc Fournier, the Minister of Quebec Revenue indicated,

> Apart from the tax losses, tax evasion has negative repercussions in the restaurant sector, since it fosters unfair competition. Question of fairness for restaurateurs, those who respect their tax obligations, [expect] that the government should intervene to counter tax evasion and promote fair competition in the restaurant industry.

Revenue Quebec, Press Release, Jean-Marc Fornier, *Pour plus d'équité dans la restauration : il faut que ça se passe au-dessus de la table* (For more equity in the restaurant sector it is required that [business be conducted] above the table) *available at* : http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp (last visited August 7, 2008).

The final section considers government responses. Three technology-based responses are taken up: (a) the comprehensive response of the Greek government, which mandates certification of all ECRs used in the country as well adoption of fiscal electronic signing devices (FESDs) to generate an encrypted signature to be placed on all tax documents; (b) the plans underway in Quebec to mandate the use of a *module d'enregistrement des vents* (MEVs), or sales registration module in restaurants – a signing device similar to the Greek FESD – that will record, preserve, and print on each receipt an encrypted "signature" of the receipt (derived from critical elements of the receipt itself); and (c) the plans in Germany to develop (and then mandate usage of) a smart card in each cash register that will encrypt and record all transactions passing through an ECR (as well as the performance on non-transactional activities on an ECR) in a manner that permit highly efficient audits of standardized data with a hand-held reader[10] utilizing public key infrastructure (PKI) to access ECR records and operations.

SECTION 1:
FOUR GENERATIONS OF FRAUD-FACILITATING TECHNOLOGY FOR ECRs & POS SYSTEMS

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. The term *automated sale suppression device*[11] is a general

[10] Both German and Quebec solutions anticipate using "hand-held readers" during audits of ECRs. There is a difference in application. Under the German solution the "reader" will be able to access the records saved on the smart card embedded in the ECR. The reader in this instance will most likely be a lap-top computer. The data will be standardized to facilitate audit inquiries. Under the Quebec solution the "reader" is a scanner. This device will be able to scan the receipts of customers to quickly determine the validity of a particular receipt, and indicate the specific ECR that issued it. *See*: Quebec Ministry of Revenue, *Tax Evasion in Quebec: Under-declaration of revenues in the restaurant sector*, powerpoint presentation (Jan. 2008), slide 10 (in French,: *L'évasion fiscal au Québec: Sous-déclaration des revenus dands les secteur de la restauration*, translation on file with authors).

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

> One of the most popular means to suppress sales is to utilize electronic suppression of sales technologies, such as "Zapper." The CRA is actively working with provincial counterparts (through the FPTUEWG –

classification for all software programs used or designed to facilitate cash skimming. *Phantom-ware* is a sub-classification. It includes the first two generations of automated sales suppression devices – *self-help phantom-ware,* and *factory (or distributor) installed phantom-ware. Zappers* are a third generation of automated sales suppression devices. A fourth generation of this software appears to be under development now, a foreign (or extra-jurisdictional residing) zapper that is provided to users over the internet, which alters domestic records from a distance, and removes both the program and the developer from the immediate grasp of the local tax authorities.

Phantom-ware.[12] Phantom-ware is programming placed within a modern ECR or POS system that can be used to hide the skimming of cash sales. Phantom-ware is "hidden" (in the sense of not being disclosed in user manuals). Its use, operation, and even its existence may be very difficult to detect on audit.

Phantom-ware re-programs an ECR or POS system so that selected types of cash sales are not recorded (receipts can be renumbered to follow a new sequence, Z Reports and X Reports can be altered, and the Electronic Journal can be brought into conformity with all other changes). This programming exists on most systems for good (but not often needed) business purposes, and for which there are good reasons for having it "hidden" from employees. For example during a bankruptcy sell-off of business assets a buyer of the ECR would want to clear the 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.[13]

Federal/Provincial Meeting of the Underground Economy Working Group) to address Zapper and other point-of-sales suppression technologies.

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

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

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

[13] *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

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

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

In this new generation the technology has changed.[14] The new technology only has one purpose – fraud. It is still phantom-ware – programming hidden in the software – but it requires very little operator-intervention to use. It can be identified by tax auditors only if the operating system of the ECR or POS system is broken down.

Zappers.[15] Zappers are not embedded in operating programs of

involved simply not ringing sales through the register, or voiding sales made, a fraud which would have been more easily carried out with technology but the user manual did not contain instructions for the night manager to perform the fraud in this way) *available at*: http://www.irs.gov/compliance/enforcement/article/0,,id=163019,00.html

[14] 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.

[15] "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

ECRs or POS systems; they are add-on programs that are removed as easily as they are added to a system. Zappers can 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

> distributeur exclusif au Québec, et qu'elle a permis à différentes sociétés, principalement des restaurants, de se servir de ce camoufleur pour dissimuler des ventes afin d'éluder le paiement des taxes et des impôts.

Which translates as:

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

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

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

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

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

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

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

OECD, Report by the Technology Technical Advisory Group (TAG) (Dec. 2000) 93.

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.

Although things have already developed beyond this point, it is common to find government reports that set out these three phases in automated sales suppression fraud in contrast to the manual skimming techniques of the past. Consider this assessment in the Interim Report of the German Working Group on Cash Registers[16] where the terminology used in this paper has been added in bold brackets:

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

International zappers. As revenue authorities began to identify phantom-ware applications, domestic developers responded with zappers that could be removed and hidden when an audit commenced. If a zapper is uncovered the auditors today have become very adept in

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

finding the developer, his customer list, and then following up with audits on each of the developer's clients.

It has not been lost on the developers of automated sales suppression devices that the Quebec Ministry of Revenue (MRQ) was able to find zappers in seven Patio Vidal restaurant franchises, and two bars (La Tasca in Gatineau, and O'Max in Masson-Angers) by following the customer list of Luc Primeau. Mr Primeau was the developer and distributor of Microflash cash register software, and was also the developer of the zappers that each of these businesses used to defeat the Microflash operating system to skim cash sales.[17] Because Mr. Primeau was a local developer he increased the risk of detection for all his clients.[18] Similarly, when the Belastingdiest (Dutch IRS) was able to identify a locally designed zapper (used on produce scales in grocery stores to alter the data feed from the scales to the ECR suppression called Analysis) it was able to trace this zapper through approximately 1,200 businesses by simply following the customer lists of the local developer.[19]

An on-going Swedish investigation[20] (scheduled for trial 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[21] on a memory stick. Directly attached to this dongle is a second (silver) memory stick that contains a Zapper. The Zapper used in this

[17] 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/communiques/ev-fisc/2003/17mars.asp (in French only, last visited Feb. 8, 2008).

[18] 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/communiques/ev-fisc/2005/26oct.asp (in French only, last visited Feb. 8, 2008).

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

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

[21] 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.

system has the ability to either (a) selectively change line items on a sales ticket (replacing expensive items with less expensive items and reducing the related VAT charges) or (b) perform a fully automated "zapping" of all transactions so that total sales for a day would be reduced by a specified amount. As a result, this zapper allows a fraudster to custom tailor his zapping. However, one of the most distressing aspects of this case is the following comment by Martin Jansson, the Swedish auditor who found this zapper:

> In this case the restaurant under investigation used a backoffice program called Restodata. According to the exe-file the program was produced by a company called "Restodata Inc." However, we haven't been able to find that name anywhere.[22]

The Swedish case is an excellent example of where Zapper technology is headed. Zappers are being internationalized. In fact, if one examines the TT PI Electronique system with the zapper installed it is easy to see the system move from a Swedish interface to an English interface as the Zapper is inserted into the POS system. Although not conclusive by any means, it does seem to suggest that the Swedish Tax Administration is up against a zapper that is a bit more difficult to trace than those found by the MRQ. The Swedish Tax Administration is most likely not looking at an in-house Zapper, nor is it looking at a locally designed and distributed Zapper. It is looking at a foreign Zapper designed to facilitate local fraud.[23]

[22] Martin Jansson, *supra* note 20.

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

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

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

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

> We have experience [with] several [types of] software but they are local. [They are] produced [developed] in Sweden. [I] don't think that you have heard of {Zapper name omitted} or {Zapper name omitted} for example.
>
> One [other] system is from Canada I think, {ECR operating system omitted}, but we don't know so much about it. Other systems are {ECR operating system omitted} from {manufacture's name omitted} and {ECR operating system omitted} from {manufacture's name omitted} but in these system we haven't revealed any fraud. In {Japanese manufacture's name omitted} there is a system with many names, one is {ECR operating system omitted} and [another] one is {ECR operating system omitted} but it is the same. It is a Spanish program as it seems and we have revealed a lot of fraud in this system and we also know how to reveal it. The {Japanese manufacture's name omitted} pc-system is installed in the cash

federal treaty assistance. Revenue Quebec, Press Release, *Zapper : Le ministère du Revenu perquisitionne au Québec et en Colombie-Britannique (Zapper : The Ministry of Revenue conducts searches in Quebec and British Columbia)* (in French only) *available at* : http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2002/24oct.asp

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

If Revenue Quebec suspected that the zapper used with RMS Touch was developed at Adler Microsystems and if it wanted to execute search warrants at Adler, it would be a far more complex undertaking than that involved in the British Columbia case. It would involve first a discussion with Canadian federal authorities, who would then enter into treaty discussions with US federal authorities, followed by further discussions with New Jersey authorities. It is important to note that there is no public indication that this kind of four-way enforcement effort has occurred in the Logicaisse case. It is the Canadian company (Logicaisse) not the American company (Adler) who is suspected of developing the zapper. For Revenue Quebecés description of the Logicaisse Ltd. investigation see *supra* note 15 [Revenue Quebec, Press Release, *Les systèmes informatiques Logicaisse ltée dans la mire de Revenu Québec* (Computer systems Ltd. Logicaisse in the grasp of Revenue Quebec) (Mar. 12, 2008) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2008/12mars.asp]

> register {model number of a specific ECR} and {model number of a different specific ECR} as I remember. I have heard that the Nederlands have a system that they have investigated with success but I don't know the name of it. Perhaps that could be of interest for you. If you need I probably can provide a contact in the Nederlands. But I think the {Japanese manufacture's name omitted}-system should be common in the UK.[24]

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

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

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

SECTION 2: SIGNIFICANCE OF THE AUTOMATED SALES SUPRESSION PROBLEM

How significant is the automated sales suppression problem? There are several ways to answer this question: (a) a statistically accurate empirical study can measure the impact and the incidence of automated sales suppression in a jurisdiction; (b) a rough survey can be taken of published cases in multiple jurisdictions to gauge how large this financial fraud can become; and (c) cross-jurisdictional surveys of specific sales suppression devices can be taken to measure how deeply into the domestic economy these frauds become when they are accelerated by technology.

Empirical studies. The empirical studies in this area are limited. Two governments have reportedly conducted studies of automated sales suppression – Germany and Quebec. In both cases the studies supported proposals for legislative change; change that the revenue authorities felt was necessary to counter growing problems. Neither

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

government has made the full studies available, although summaries of their conclusions have been released. These studies reach similar conclusions.

Germany. There are three levels of German assessment: an inter-government task force analysis; a federal audit office assessment; and multiple state level assessments. They are discussed collectively in German materials, and appear to reinforce one another.

The Interim Report of the German Working Group on Cash Registers indicates that the Group was "... aware of [technology-assisted] fraud amounting to 50% of companies cash receipts."[25] The Working Group does not separately quantify the kinds of *technology-assisted* fraud involved; in other words it does not consider whether Germany has a phantom-ware or a zapper problem. Most likely, Germany is experiencing both (and more).

The Working Group's 50% observation is supported by a report made by the German Federal Audit Office (BHR) to the German Parliament in 2003. In this report the BHR appears to focus only on factory installed software (self-help phantom-ware).[26] The BHR concludes that the potential loss in Germany is in the billions of euros:

> The Federal Audit Office (BHR) has complained that later models of electronic cash registers and cash management systems now fail to meet the principles of correct accounting practice when it comes to recording transactions ... The risk of tax fraud running into *many billions* [of euro] should not be underestimated in cash transactions.[27]

Both the BHR's observations and the Working Group's study are further buttressed by summaries from studies conducted by three German federal states. These studies are limited, because they focus only on the restaurant sector. But, they too conclude that sales suppression is a significant problem:

> One federal state is currently implementing a special "restaurant" initiative. Checks already made have led to average upward revisions

[25] Interim Report, *supra* note 16, at 5.

[26] *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).

[27] BHR comments 2003, No 54, Federal Parliament circular 15/2020 *cited in Id.* at 5 (emphasis added).

> of 46% of original turnover. A comparable initiative in another federal state resulted in over half the cases (54%) having upward revisions of 60% of declared turnover. Fraud amounting to 25% was detected in a fifth of the cases, and was as high as 5% in the remaining 26% of cases. A third federal state has found that around 45% of till receipts involving cash are subject to upward revisions ranging from 20% to 118%.[28]

Quebec. The MRQ has conducted two studies of automated sales suppression. Similar to the studies by the German states, the Quebec studies also focus on the restaurant sector. The first study followed the customer list of an early zapper distributor/developer.[29] This investigation (the First Inspection Wave) examined 70 systems and uncovered 41 zappers.[30] This was followed by a more statistically accurate investigation (the Second Inspection Wave) that was based more broadly on a random sampling of businesses within the restaurant and hospitality industry. This survey found that 16% of all sales went unreported.[31]

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

> Although the majority of restaurateurs comply with their tax obligations, restoration remains an area of the Quebec economy where tax evasion is rampant, both in terms of income tax as sales taxes. Tax losses in this sector are important. Quebec Revenue estimates that the $ 425 million for the 2007-2008 fiscal year.[32]

[28] *Id.* at 5.

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

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

[31] *Id.* at 13.

[32] Revenue Quebec, Press Release, Jean-Marc Fornier, *Pour plus d'équité dans la restauration : il faut que*

High revenue loss cases. Revenue losses from automated sales suppression operations can be very significant and provide a good indirect measure of significance. The size of the losses do not appear to be correlated to the consumption tax rate – huge losses are just as common in low consumption tax jurisdictions as they are in high consumption tax jurisdictions. In addition, this fraud does not seem to be a function of the type of consumption tax employed – retail sales tax (RST) or value added tax (VAT). US and Australian automated sales suppression cases (low rate RST and VAT jurisdictions) tax illustrate how significant the revenue losses can be. The length of time these frauds went undetected (decades in some cases) also indicates how difficult it is for traditional audit techniques to uncover technology-based frauds.

US cases – Stew Leonard's Dairy ($17m over 10 years) & La Shish Restaurants ($20 over 4 years). There are two very large zapper cases in the US. Both represent long term automated skimming operations that involved millions of dollars in tax extending over many years.

Stew Leonard's Dairy (a Connecticut grocery chain associated at one time with a dairy farm) 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.[33]

Physical 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. In 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

_*a se passe au-dessus de la table* (For more equity in the restaurant sector it is required that [business is conducted] above the table) *available at* : http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp (last visited August 7, 2008). See also the accompanying powerpoint presentation, *Tax Evasion in Quebec : Obligatory Billing in the Restaurant Sector – Under-declaration of revenues in the restaurant sector*, 3 (January 28, 2008) (in French) (on file with authors, with translation).

[33] 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).

> generated by Belardinelli's altered daily sales reports. In 1981or 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.[34]

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.*[35]

A second US case, La Shish Restaurants, involved technology from the beginning. The La Shish fraud skimmed several millions more than Stew Leonard's Dairy and did so in less than half the time. La Shish Restaurants involved a zapper that skimmed more than $20 million in cash sales over a four year period. The funds were sent in small denomination cashier's checks to Hezbollah in Lebanon.[36] In this case a zapper was installed in the POS system that remotely coordinated the ECR's of all seventeen La Shish restaurants. The "zapping" was

[34] *Id.* at 35.

[35] 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).

[36] 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 (last visited Feb. 3, 2008).

done from home.

Australian case – Ronen ($17m over 10 years). 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).[37] "...[T]he scope of the fraud represented by unpaid [income] tax was approximately [AUD] $8.125m."[38]

During most of the time the *Ronen* fraud was taking place Australia did not have a national consumption tax. However, in July 2000 the Goods and Services Tax (GST) was introduced, and this had a dramatic affect on the *Ronen* fraud. Because of the GST the Ronen's decided that a zapper was needed if they were to continue skimming. A computer program was developed to calculate the amount of cash that could be skimmed from each business (taking into account the GST and allowing at least 10% of all cash receipts to be regularly banked).[39] In addition, a new computer system was installed that allowed Mrs. Ronen to run false till rolls for each retail outlet at her apartment.

High rate of penetration cases. A second indirect way to measure the impact of skimming frauds (carried out through automated sales suppression devices) have on an economic system is to assess the scope of software adoption. Are there just a few users, or are these devices employed more widely by many businesses in a community? The more wide spread the more likely it is that the competitive marketplace has been altered by the technology, making it almost a necessity to skim if one wants to make a reasonable profit. Because zappers and phantom-ware are software applications that work one-on-one with corresponding operating systems in ECRs or POS systems, this technological fraud spreads most rapidly when the underlying system is widely adopted.

Two Brazilian investigations illustrate these points: *Operação Internet* [Operation Internet] initiated by the State Tax Administration of Minas Gerais in 2006, and *Operação Tesouro* [Operation Treasure-

[37] 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.

[38] *Regina v. Ida Ronen; Regina v. Nitzan Ronen; Regina v. Izar Ronen,* 2005 NSWSC 991, at ¶14.

[39] *Ronen*, 2005 NSWSC, at ¶¶25 & 27.

hunt] conducted in the State of Bahia in 2007.

The target of *Operação Internet* was the AMG corporation. AMG not only produced the government certified software (called Robot) used in all Minas Gerais cash registers, it also produced and sold the Zapper (Quanto) that defeated it. Needless to say, Quanto was widely used. Press reports indicate that:

> 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 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.[40]

In the 2007 investigation, *Operação Tesouro* [Operation Treasure-

[40] *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 authors) (emphasis added).

hunt], that was conducted in the State of Bahia the target was two technology companies, Networks and Stella Systems. Software named Colibri [Hummingbird], developed and distributed by these companies, enabled businesses to deactivate the receipt printer,[41] and eliminate all record of selected cash sales. Colibri was used in hundreds of businesses and eliminated nearly half the receipts of some businesses. Press reports indicated:

> ... 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.[42]

[41] It should be noted that "deactivation of the receipt printer" essentially turns this into a traditional (manual skimming) fraud. However, it also needs to be noted that this kind of fraud facilitation strikes at the heart of the Greek (FESD) and the Quebec (MEV) responses to automated sales suppression. Both Greek and Quebec responses to such an action is severe financial penalties. In contrast, because the German "embedded smart card with PKI" solution records the basic "operations" of the ECR it would pick up these "deactivation" activities, and would place the German auditor in a position to identify this fraud more easily than the Greek or Quebec auditors.

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

SECTION 3:
ANSWERING THE TECHNOLOGY THREAT (WITH TECHNOLOGY) – GREEK, QUEBEC AND GERMAN SOLUTIONS

Some governments have taken very aggressive steps to block automated sales suppression technology from damaging revenue flows (rules-based jurisdictions). Others governments, taking a more liberal approach to cash registers, have relied on traditional methods to prevent technology-assisted skimming emphasizing increased auditor awareness and striving to make improvements in the auditor's knowledge and skill base (principles-based jurisdictions). The *Cash Register Good Practice Guide* characterizes this difference among jurisdictions as fundamental. The fiscal memory/ fiscal tills (or rule-based) approach is distinctive and different from the generic/ liberal legislation (or principle-based) approach. The *Guide* observed that, "... there is no country within the EU for which the situation does not correspond to [either a rules-based or principles-based] alternative[s]."[43]

The *Guide* lists Argentina, Brazil, Bulgaria, Greece, Italy, Latvia, Lithuania, Poland, Russia, Turkey, and Venezuela as examples of fiscal memory jurisdictions.[44] The U.K., the Netherlands, Belgium and France are among the countries that take a principle-based approach.[45] Although both approaches are successful,[46] this paper sets aside the

[43] *Cash Register Good Practice Guide, supra* note 1, at ¶ 3.3.

[44] *Id.* at ¶3.1.

[45] *Id.* at ¶3.2.1.

[46] For example, the authosr have been in e-mail correspondence with Ben B.G.A.M. van der Zwet from the Netherlands revenue administration (a principles-based jurisdiction) and Panos Zafiropoulos from the Greek revenue authority (a rules-based jurisdiction). Ben and Panos represent their respective countries on the Fiscalis Committee's Cash Register Project Group. Panos responds to an inquiry about Greek legal cases on zapper enforcement actions by noting:

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

Personal e-mail communication (May 10, 2008) on file with authors. The Netherlands on the other hand has a large number of zapper cases. In a conversation with Ben about the Dudok case he observes that:

> Well, our tax audit is (in principle) an overall audit that means that both the completeness of pay roll tax, VAT, and Income tax (private and/or corporate) have to be audited. These taxes have links:
>
> - If you want to pay under the table wages you need to have revenues not accounted for, if you have revenues not accounted for you pay to little VAT.
> - If you have more black money from revenues you did not account for, than you have to pay for under the table wages, you better use it for a nice holiday or a big car. If you do so you did not pay enough income tax.
> - This means that sometimes if we know of paying illegal employees we also correct VAT.
> - If we know of revenues not accounted for we want to know if the money was used to pay wages or if

principle-based approach and focuses entirely on a comparison of three of the rules-based or fiscal memory systems – the Greek, Quebec and German systems. These jurisdictions have decided to fight technology with technology.

The authors appreciate that Japan is well positioned to apply a principles-based or comprehensive audit approach to Zappers and Phantom-ware. A comprehensive audit scheme strongly supplemented with computer audit specialist would provide an effective remedy. The alternative approaches might not seem as intuitive. Because these approaches are not easily summarized, the remainder of this paper considers the three leading solutions using this approach.

GREECE
FEDs; FECRs, AFED Printers; FESDs

Greece is a fiscal memory jurisdiction, and has had comprehensive, rules-based fiscal till legislation in place for over twenty years. Technical specifications for Fiscal Electronic Devices (FEDs) were published widely in 2004.[47]

> it was for the benefit of the entrepreneur. If we get to know of businessmen buying big cars, kitchen, swimming pools in cash we want to know the source of the money.

Personal e-mail communication (April 16, 2008) on file with authors.

The matrix that does not seem to be successful in preventing technology-assisted skimming frauds is the principle-based jurisdiction that is not able to conduct comprehensive "Netherland-type" tax audits. The US is the classic example of this alignment. A thorough search of all US litigation has uncovered only two zapper cases, Stew Leonard's Dairy and the La Shish Restaurant case. Both cases are the result of federal income tax audits.

The US does not have a national consumption tax. The retail sales tax in all cases is a state or local levy, and there is very little cooperation between federal income tax auditors and state sales tax exam teams. As a result, a comprehensive income and consumption tax audit in the US is very rare. For further analysis of the US situation see: Richard T. Ainsworth, *Zappers and Phantomware: The Need for Fraud Prevention Technology*, 50 Tax Notes Int'l. 1017 (Jun. 23, 2008); *also at* Richard T. Ainsworth, *Zappers and Phantom-ware: A Global Demand for Tax Fraud Technology*, BU School of Law Working Paper No. 08-20, *available at*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1139826.

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

Under Greek rules FEDs are divided into two categories: (a) fiscal electronic cash registers (FECR) and autonomous fiscal printers – used only in all B2C transactions; and (b) fiscal electronic signing devices (FESDs) – used to digitally sign tax-related documents in B2B transactions, or which may be used to sign receipts issued in B2C transactions.

FECRs andAFED Printers. Fiscal electronic cash registers (FECRs) include ordinary stand-alone cash registers, and cash registers equipped with advanced connection capabilities (network or PC operated machines). Autonomous fiscal electronic device printers (AFED Printers) are fiscal printers that operate only via a connected computer. They have no keyboard or display terminal. These systems store and secure data (revenue from sales, taxes collected) in their fiscal memory.[48]

Data from the electronic journal memory (EJ Memory) is signed by a secure hash algorithm (SHA-1).[49] This hash value is permanently safeguarded and stored in the fiscal memory. Daily sums (receipts and VAT amounts) are saved into the fiscal memory, cumulatively and on a daily basis.

The cost of FECRs varies from € 200-250 to € 800-1,000 depending on the manufacturer.[50] Every manufacturer, developer, or importer of ECRs into Greece must seek approval for each specific model that they intend to sell in the Greek market.[51] A license to sell a specific ECR

French: http://europa.eu.int/comm/enterprise/tris/pisa/cfcontent.cfm?vFile=120040135FR.DOC

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

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

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

[51] There are roughly 300,000 to 350,000 FECRs and POS systems with secure recording devices (FESDs) in Greece. The turnover of these devices is between 30,000 to 40,000 machines annually. There are over 300 different models of ECRs certified for use in the Greek market representing approximately 50 different manufacturers, importers and distributors. *Cash Register Good Practice Guide, supra* note 1, Appendix D,

is issued by a special technical (inter-party)[52] body (committee) and will be issued only when the ECR conforms to all statutory technical specifications.[53] Applications are made to the Department of Fiscal Electronic Cash Registers and Systems of the Ministry of Finance and must be accompanied by a working model of the system for which a license is sought. The committee has authority to examine any additional data (including experience in the field, business solvency, creditworthiness, technical capacity of personnel), and has the authority to recall and cancel licenses in cases where material changes have been made in systems or the conditions under which the license was granted.

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

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

FESDs are designed for B2B applications. They are used to e-signing invoices, but can be used for any tax document including a retail receipt. FESDs are connected to an entrepreneur's computer system via a dedicated port (RS-232; Ethernet RJ-45; USB). A driver must be

at ¶ 4.1.

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

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

installed to allow the computer system to interface with the FESD. Essentially, the FESD functions as a virtual printer allowing the entrepreneur's back office software (ERP system or accounting software package) to function normally. However, every tax document required to be signed is diverted through the interface to the FESD where a signature is created (the SHA-1 algorithm is applied) and a hash value is transmitted to (and printed) on each document. The whole-day hash value is permanently saved in the FESD's fiscal memory.[54] This preserves all data on the document in detail.[55]

Presently the cost of an FESD is between € 450 and € 650. Thus, a FESD alone can cost more than a FCR, and for this reason smaller businesses do not normally use FESDs to issue legal receipts.[56] Economies of scale also come into the picture because a single FESD can support many cash registers linked on a network. It can be installed remotely (even in another city), and need not be directly connected to the point of sale terminal.

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

How FECRs with AFED Printers and FESDs defeat Zappers and Phantom-ware. Because fiscal electronic cash registers (FECRs) are certified for compliance with all technical specifications set out in Greek law – a law that is supported and updated regularly by the research laboratories of the NTUA – it is a very simple matter to determine if a specific ECR has been tampered with. Factory-installed phantom-ware must be removed before certification. If the self-help version of phantom-ware is on the ECR it will either be blocked, or there will be a record of its use so that its impact on revenues will be neutralized. Only true data from real transactions will be preserved and SHA-1 encrypted in the

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

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

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

fiscal memory. Use of an add-on zapper will be a violation of the licensing regulations. It will be easily detected and severe penalties will apply.

Through the certification process the Ministry of Finance is able to preserve a copy of all approved firmware. Thus, it is a simple matter of calculating a checksum value (CRC-32[57] or SHA-1) for the object code of the firmware. Any auditor can then read the contents of the program memory of a certified ECR and determine if changes have been made in the firmware (through phantom-ware or zappers) by comparing his reading with that of the file kept in the Ministry of Finance.

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

QUEBEC – MEVs

To counter the use of zappers and phantom-ware in the restaurant sector Revenue Quebec has unveiled plans for a pilot project (to begin in late 2009) where select restaurants will install microcomputers between their ECRs or POS systems and the receipt printer.[58] A new rule requiring all restaurants to issue paper receipts (with significant penalties[59] for failing to do so) has also been adopted. The

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

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

[59] The 2006-2007 Budget for Quebec indicated:

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

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

microcomputers, called *module d'enregistrement des ventes* (MEVs), or sales registration modules, are expected to function very much like Greek FESDs. However, unlike the Greek FESD that primarily targets B2B transactions, but may be used by businesses that employ sophisticated systems with B2C transaction, Quebec's MEV is exclusively used in a B2C context.

MEVs will receive data from specified transactions (the drafting of guest checks, register receipts, or credit notes). From the extracted data the MEV will produce an encrypted numerical signature of the document. This e-signature will be transmitted to the printer and then printed on the document from which the signature was derived. The signature and the recorded data will then be preserved within the fiscal memory of the MEV for seven years.[60] Restaurants will also be required to submit sales summaries, generated by the MEV, when they submit their tax declarations.

Revenue Quebec believes that these new rules and the MEV will:

- permit restaurant patron to verify that the taxes they pay are properly recorded will be remitted to the State;
- facilitate the intervention of Revenue Quebec in cases where a bill of sale is not issued or recorded or where attempts are made with zappers or phantom-ware to manipulate the data on the receipt;
- allow Revenue Quebec to easily verify that a specific receipt has been recorded or not;
- preserve sales data for the statutorily required period;
- make the data-content of ECRs more uniform and easier to audit;
- allow Revenue Quebec to quickly identify cases where sales have not been declared.[61]

The cost of an MEV is expected to be about $650. If they are operationally similar to Greek FESDs it will not be necessary to have multiple MEVs in restaurants that employ a network configuration. Although a single MEV might have been utilized to e-sign receipts for multiple ECRs when they are linked in a POS system, this was deemed

[60] Revenue Quebec, *Tax Evasion in Quebec* (powerpoint), *supra* note 32, at slides 6-8.

[61] *Id.* at slide 12.

to be insecure by Quebec authorities. The MEV will be used in a one-to-one relationship with receipt printers.[62] Nevertheless, the government has promised to provide the necessary number of MEVs to restaurants at no cost. The estimated cost to the Quebec Treasury is $55 million.[63] There is no discussion in Quebec about extending MEV applications outside the restaurant sector, even though automated sales suppression technology is not confined to restaurant fraud.[64] It also appears that very small restaurants may not be required to use MEVs.[65]

GERMANY
SMART CARDS EMBEDDED IN ECRs

A German Working Group on Cash Registers, comprised of the highest-tier central and regional tax authorities, is examining automated sales suppression (both phantom-ware and zapper applications). An Interim Report has been released.[66] Work on a technological solution involving the use of encrypted data recorded on smart cards that would be embedded in ECRs 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.

The German Working Group that recommended the encryption solution was chaired by Dr. Norbert Zisky of the PTB. It was Dr. Zisky's papers on encryption,[67] and the fact that these techniques had been

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

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

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

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

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

[67] Norbert Zisky, *Manipulation Protection – Electronic Cash Registers and POS Systems*, German Federal Standards Laboratory, Brunswick & Berlin (May 2005) (unpublished draft on file with authors); Norbert Zisky, *Manipulationsschutz elektronischer Registrierkassen und Kassensysteme* German Federal Standards

tested in secure communication settings with measuring instruments[68] that persuaded the Working Group to work on this solution.

The INSIKA project, also managed by Dr. Zisky, is charged with completing the technical specifications for a signature smart card by the summer of 2008.[69] Included with the technical specifications for the signature smart card will be a determination of the data structures and formats, communication protocols and security analysis for the system.[70]

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 in the ECR.

Laboratory, Brunswick & Berlin (Mar. 15, 2004) (Ger.) (unpublished draft on file with authors). Since this early paper there have been a few modification to Professor Zisky's proposal. The critical changes include:

1. The signature device (smart cards) distributed by the tax authorities will be personalized to the tax payer not to the cash register (cash box);
2. The signature device will have a set of dedicated sum storages which will be controlled by the signature device itself. It [will] generate the relevant data from the set of data to be signed. In the [case where there may be] a loss of signed data the tax authorities [will be] able to read the stored data from the smart card. The sum storages [are required] to read out periodically and [are required] to be stored after signing.
3. The receipts [must] contain all relevant data for the verification of the transaction (including the signature). These [receipts will be] exactly the same [as those] in the memory (from the point of view of data modeling). With the help of [the memory record] you are able to validate each receipt. Falsification of receipts [is] not possible.

   But there is a little problem [currently]: If you have the paper receipt you [will need] to type in every character into your computer by hand (or you may use a scanner). The manual test of receipts without technical support will be the exception, but it [will be] possible.

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

[68] 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).

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

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

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

[70] 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 authors).

A secure electronic signature is issued for this data based on Public Key Infrastructure (PKI).

The essence of the German solution revolves around cryptography and smart card access to cryptographic data preserved within the cash register or POS system. If the revenue authority audits, 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). Dr. 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 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 crypto processor for each cash register. On these revenue office smart cards a cryptographic pair of keys with a secret and public key is produced. The public key is kept for later fiscal examination of the respective data. The certificate for the public key is also stored on the smart card themselves....
>
> In the case of the marking procedure [the encryption procedure] over the data record – it is "signed" when a hash value is formed, which is in turn coded by the secret key of the smart card. The formation of the hash value is a mathematical one-way function, which comprises a single (unique) value from the data set. It is the hash value that seals the data record (an electronic seal). The formation of the signature is used to assign the data record to the cash (involved in the transaction) and/ or the pair of keys. ...
>
> For the conclusion of the verification process the two hash values are compared with one another. If these agree the integrity of the registered data record is authenticated.[71]

One of the critical differences among the Greek, Quebec and German solutions is the "per unit" cost of implementation. Both Greece and Quebec have responded to the high costs of their solutions. The Greek response involves accelerated depreciation of hardware and low interest loans to assist businesses to purchase the equipment. The

[71] Norbert Zisky, *Manipulation Protection, supra* note 67, at ¶ 5.2 & 5.3.

Quebec response is to fully subsidize required hardware purchases. In this context, one of the key features of the German solution is its low cost structure (and the refusal of the government to subsidize business acquisition of the solution). Dr. Zisky indicates:

> In ... this [German] approach ... for the protection of electronic cash registers and POS systems against the manipulation of stored data [t]he large advantage ... consists of the reaching of a comparatively high level of protection with only small hardware and software expenditures in the POS system being necessary.[72]

Dr. Zisky estimates a 50 euro cost for the German smart card solution, and he itemizes it as follows:

> The additional costs per ECR are the result of cost for the smart card (signature device), approx. 7-8 Euros, and for integration of the smart card to ECR, approx. 20 Euros (including hardware and software). [An] additional 20 Euros I calculate [are needed] for additional common costs (smart card distribution, administrative costs). Government subsid[ies] are not planned. But on the hand of tax authorities some expenditure is needed. Certificate management, test tools, training of the staff of tax authorities [need to be included in a full cost estimate].
>
> The price of smart cards is calculated on the base of more than 100,000 cards because they will be ordered by a central authority.[73]

In fact, the Vectron corporation's prototype of the INSIKA project's smart card solution has an even lower cost estimate. Vectron estimates a "single-unit end-user price of less than 25 euros."[74]

CONCLUSION

If the National Tax Administration perceives Phantom-ware and

[72] Norbert Zisky, *Manipulation Protection, supra* note 67, at ¶ 5.1.

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

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

Zappers to be a serious threat to revenue, and if Japan would like to consider a rules-based (fiscal memory) solution as opposed to a principles-based (comprehensive traditional audits supplemented with enhanced training in technology) solution, then the Greek, Quebec and German approaches to this problem need to be looked at carefully. This is an approach that fights technology with technology.

At this preliminary stage, it is possible to draw out (comparatively) the following features which distinguish the Greek, Quebec and German solutions:

- Greece certifies the operating system within all ECRs licensed to be sold in Greece. Neither Quebec nor Germany engages in this type of certification regime. The FECR solution has not been copied by these jurisdictions (although there are a number of jurisdictions that follow the Greek approach carefully).
- Greek oversight of electronic sales suppression and data manipulation extends throughout the supply chain. B2C as well as B2B transactions are handled. The German solution focuses only on ECRs in a B2C context. The Quebec solution is even more limited, focusing on ECRs in a B2C context, but only in the restaurant sector. Even within the limited restaurant sector it is very likely that not all Quebec restaurants will be covered.
- All three solutions (Greek, Quebec and German) involve data encryption. The German solution for example uses elliptical curve cryptography. However:
    - ○ both Greek and Quebec solutions focus exclusively on the encryption of data elements that are sent to a printer (for the issuance of a receipt in the case of B2C transactions; or for the issuance of an invoice, consignment notes or other tax documents needed in B2B transactions);
    - ○ the German encryption extends to other functions performed on the ECR – the operation of the ECR – even if those operations do not involve directing the printer to issue a receipt.
- Both Greek and Quebec solutions are in significant respects paper-based solutions – they both involve physically printing hash signs on paper receipts which can be checked by tax auditors against stored digital records of the same hash. The German solution does this also, but extends coverage to other ECR

operations and employs PKI functionality that allows auditors to immediately (and digitally) check the ECR for tampering.

  - The Greek ECR certification regime (but not when FESDs are being used with non-certified cash registers) reaches the same result (but not in the same way) as the German smart cards and PKI mechanisms. When Greek tax auditors check the object code of the installed firmware with SHA-1 and compare this hash with that retained when the ECR model was certified they will know (after the fact) whether or not the code has been tampered with.. The German system will "see" this tampering (manipulation of the object code) as it is going on.

- The German "PKI and smart card" solution is far and away the least expensive of the solutions considered here at a cost between €25-50. Cost estimates for the Canadian MEV appear to be approximately the same as the Greek FESD solution at $650 per unit for the MEV and approximately €450 to 650 for the FESD. The Greek solutions taken as a whole (encompassing FECRs, AFED Printers and FESDs) are probably the most expensive, particularly when the costs of FECR certification are added to cost of the hardware.[75]

[75] There is a real global perspective on enforcement in this area that is reflected in the opinion of Ben B.G.A.M. van der Zwet from the Netherlands revenue administration:

> The cost effectiveness [of the German solution] and the fact that this solution is applicable for multiple purposes might lead the PKI smartcard solution to be implemented for internal control [purposes] by small and larger companies to preserve transaction data against internal fraud. The German solution is a low cost [option] for SME's [an open market solution to securing data]. Securing of data [has not been possible/ cost effective] for SME's. [T]he traditional solutions to secure data were based on General Control measurements that are not applicable in small organizations.
>
> [As a result] this cost effective [German] solution might even be [considered] a break-through in principle based jurisdictions as well [as fiscal jurisdictions]. [Now] the cost of the solution is not a threshold [barrier] for entrepreneurs to [achieve] tax compliant registration of their business processes.
>
> A Global Standard ISO of Reliable Cash Registers would both be of help to manufacturers, tax compliant businesses, and could be implemented in rules based jurisdictions as well as in principle based jurisdictions.

Personal e-mail communication, Ben B.G.A.M. van der Zwet (August 11, 2008) (on file with authors).