ZAPPERS & PHANTOM-WARE:
A GLOBAL DEMAND FOR TAX FRAUD TECHNOLOGY

Boston University School of Law Working Paper No. 08-20

Richard Thompson Ainsworth

This paper can be downloaded without charge at:


The Social Science Research Network Electronic Paper Collection:

http://ssrn.com/abstract_id=1139826
ZAPPERS & PHANTOM-WARE: A GLOBAL DEMAND FOR TAX FRAUD TECHNOLOGY

Richard Thompson Ainsworth

There is a demand-market for technology that facilitates tax fraud. By all accounts the providers in this market are working in a growth industry.

In the short term this is bad news for those concerned with tax policy and information privacy. In the long term however, the fight against technology-assisted fraud is stimulating the development of a more robust technology base within tax

---

1 Take for example recent EU efforts to increasing employment in labor-intensive sectors through tax incentives. Member States are allowed to experimentally reduce the VAT on supplies of certain services because it is believed that the VAT savings would be passed through to the consumer. Theoretically this will increase the demand for these services, leading to increased job creation and a reduction in related black market jobs. The EU Commission’s assessment of this policy is inconclusive [EU Commission, Report from the Commission to the Council and the European Parliament – Experimental application of a reduced rate of VAT to certain labor-intensive services, COM(2003)309 final at 25-26, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0309:FIN:EN:PDF]. How much more inconclusive would the Commission’s assessment have been if it had factored zappers into its analysis? The target of this tax policy is the very same cash-intensive SMEs that are increasingly relying on zappers and phantom-ware to obscure sales data.

The Netherlands provides a specific example. VAT on hairdressing services was reduced from 19% to 6% under the experimental procedure. After a trial period the Netherlands cannot demonstrate that this reduction had an impact on employment in the hairdressing sector [Martine Olde Wolbers & Arnold Ziegelaar, Effects of the Lowering of VAT rates on labor-intensive services – Final Report, B2315, at 54-55 (Sept. 24, 2002) TAXUD/5359/2002-EN available at: http://ec.europa.eu/taxation_customs/resources/documents/nl_en.pdf]. Simultaneous with the rate reduction the Netherlands found it necessary to step up audits on hairdressers because of widespread use of sales zappers [See B&F Optics BV]. Thus, are the ambiguous results of Wolbers & Ziegelaar the result of a flawed tax policy or are they the result of an inability to make any accurate measurements in this sector? Tax fraud has always complicated micro-measurements of tax policy impact, but when technology accelerates the scope of the fraud macro-measurements also become suspect. [Personal e-mail communication, Ben van der Zwet, Feb. 14, 2008, on file with author].

The temporary provision dealing with labor-intensive services can be found in the SIXTH COUNCIL DIRECTIVE of 17 May 1977 on the harmonization of the laws of the Member States relating to turnover tax – Common system of value added tax: uniform basis of assessment (77/388/EEC) 1977 O.J. (L 145) 1, at Art. 28(6). On November 28, 2006 the SIXTH COUNCIL DIRECTIVE was repealed and replaced with the RECAST VAT DIRECTIVE (RVD). Council Directive 2006/112/EC on the Common system of value added tax, O.J. (L 347) 1, at Arts. 106-08. Dual citations (to the old and recast versions of the Sixth Directive) will be used throughout this document.

2 Although some of the proposed solutions to zappers simply involve increased training for auditors, others involve securing the integrity of electronically stored data in all ECRs. Encryption is recommended to prevent manipulation and deletion. Mandates that manufacturers uniformly adopt simplified Standard Audit File – Tax (SAF-T) are also suggested. However, at the extreme, there are also proposals for centralizing the records for all transactions in a jurisdiction. [Panos Zafiropoulos, Safeguarding Electronic Tax Data – Data Locking: Fiscal Electronic Signing Devices in Athens, Greece (November 2007) at 12 (considering, but not recommending a centralized data-base) (powerpoint slides on file with author); Milan Prokim, Draft Prepared For – Fiscalis FPG 12, Cash Register Project Group, Technical and Functional Specification of Turnover Controllers, paper presented at Innsbruck, Austria (April 2007) at 7 & 57 (indicating that, “All misuses of fiscal cash registers, fiscal printers, non-fiscal cash registers and non-fiscal printers listed in the document titled Cash Register Misuse Guide are inherently solved by a new device called a turnover controller [jurisdiction-wide central data bank] ... ”) (on file with author)].
administrations, and this is good news for those who believe that a sophisticated technological infrastructure is needed to resolve difficult questions of tax design.3

Technology-assisted fraud puts pressure on the development of marketplace controls; controls that certify the accuracy of business information. Some controls are in place today – more are on their way. Current solutions are both voluntary,4 and mandatory.5 Eventually we should expect to see comprehensive certification regimes that make all business systems transparent.

The technology-assisted frauds that tax administrations are responding to today not only involve large movements of goods that can involve publicly traded companies – missing trader intra-community (MTIC, or carousel) fraud is an example in the EU6 –

---

3 Richard T. Ainsworth, Biometrics: Solving the Regressivity of VATs and RSTs with “Smart Card” Technology, 7 FLA TAX REV. 651 (2006) (arguing that advances in technology, digitized biometric identifiers in IDs, and certified tax compliance software at point of sale terminals would allow the design of surgically applicable exemptions in consumption taxes, replacing the universal exemption structure now in place almost everywhere).

4 The Streamlined Sales and Use Tax (SSUTA) is an example of a voluntary certification regime. Under the SSUTA tax calculation software is certified by Member States. Businesses that use certified software (or that contract with trusted third-party providers that uses certified software) are insulated from liability for any errors in determining the proper tax. See: SSUTA § 301 (voluntary registration); § 402A (amnesty rules); § 501 (certification provisions). The SSUTA is available at: http://www.streamlinedsalestax.org. See also: Richard T. Ainsworth, Zappers: Technology-assisted Tax Fraud, the SSUTA and Encryption Solutions, THE TAX LAWYER (forthcoming, 2008) (arguing that the SSUTA could be extended so that the data content of ECRs could also be certified).

5 Norbert Zisky, Manipulation Protection: Electronic Cash Registers an POS Systems, (unpublished paper in German presented to the Fiscalis FPG 12, Cash Register Project Group, Mar. 18, 2004) (English translation and original on file with author) (arguing for the adoption of a mandatory smart card solution whereby all ECRs would be sealed and embedded with a smart card that would encrypt essential cash register functioning); Panos Zafiropoulos, Electronic Signatures & PKI Cryptography – Electronic Transmission of Invoices and Special “Fiscal Electronic Signing Devices” Some Notes and Comments, (unpublished paper, on file with author, presented to the Fiscalis FPG 12, Cash Register Project Group, Nov. 2005) (presenting on behalf of the Greek Ministry of Economy and Finance and further suggesting that the EU should adopt the system of mandatory ECR certification that is employed in Greece, and the use of a fiscal electronic signing device (FESD) connected to each cash register). Mandatory regimes can be found in Bulgaria, Italy, Turkey, Lithuania, Latvia, Poland, Russia, Hungary, Brazil, Argentina, and Venezuela. Fiscalis Committee Project Group 12, Cash Register Project Group, Cash Register Good Practice Guide, Appendix D, at 1.

6 Ashley Seager & Ian Cobain, Carousel fraud: Bogus Deals keep Customs in a Spin: Smart Criminals Stay Ahead of Investigators – Russian Mafia and IRA Linked to Swindles, THE GUARDIAN (May 9, 2006) at 7 (interviewing fraudsters named Colin and Andy they find them “… hunched over a couple of PCs in an apartment in a new city center development in the north of England...initially trad[ing] in computer software… Andy developed software which created a ‘virtual carousel,’ generating all the paperwork needed to convince Customs that a sequence of genuine sales had taken place. “You can turn the carousel in just 10 minutes, and then you just have to wait 30 days for the money to come in,” says Colin. “You can run it around five companies but there are up to 300 that can be sued [in the software]. Each spin can give you up to 200,000 pounds. The longest it stays in any bank account is two hours. It’s no good being on a 90-day VAT repayment arrangement, you have to be on 30 days so you get your money back at the end of the month.”). Richard T. Ainsworth, Carousel Fraud in the EU: A Digital VAT Solution, 42 TAX NOTES INT’L 443 (May 1, 2006) (arguing that if the D-VAT were to be adopted in the EU than carousel fraud could be eliminated); Richard T. Ainsworth, MTIC (carousel) fraud: Twelve Ways Forward: Two Ways “Preferred” – Has the Technology-based Administrative Solution Been Rejected? TAX PLANNING INT’L –
they also involve technology-driven frauds in small and medium sized enterprises (SME). The most notable of the SME frauds is the use of technology to skim cash receipts at electronic cash registers (ECRs).

This paper focuses on two technology-accelerants of SME tax fraud – zappers and phantom-ware. Zappers and phantom-ware are in common use because they are difficult to detect, generate huge returns on minimal investment, and are widely available. They are widely available because very few jurisdictions restrict their manufacture, sale or distribution. In addition, zappers and instruction (technical assistance or help desk support) in the use of factory-installed phantom-ware translate into meaningful sales advantages for ECR manufacturers, distributors and installers. Is it any wonder that we are seeing a global push-back by tax administrations? Is there any wonder that comprehensive certification regimes encompassing a company’s entire tax-technology profile are being contemplated?

ZAPPERS & PHANTOM-WARE

Zappers and phantom-ware are programs that are added-on (zappers) or factory installed (phantom-ware) to modern ECRs or point-of-sale (POS) systems. Some programs (zappers) have no legitimate purpose other than to facilitate cash skimming at the point-of-sale. Others programs (phantom-ware) may have legitimate (non-fraud) purposes, although these purposes are somewhat obscure (remote from normal business uses). Phantom-ware programs are frequently hidden (in the sense of not being disclosed in user manuals), making their use and even their existence difficult to detect on audit.

INDIRECT TAXES (Mar. 2008) (arguing that selective certification of businesses engaged in intra-community trade in sectors deemed to be susceptible to MTIC fraud would resolve this fraud more effectively than the wholesale redesign of the VAT currently under consideration as a possible solution); Commissioners of Customs & Excise and Attorney General v. Federation of Technological Industries and Others, Case C-384/04 (May 11, 2006) [2006] ECR I-04191 (responding to joint and several liability provisions that were seriously impacting legitimate chip suppliers, and holding that a taxable person, to whom a supply of goods or services has been made and who knew, or had reasonable grounds to suspect, that some or all of the value added tax payable in respect of that supply, or of any previous or subsequent supply, would go unpaid, may be made jointly and severally liable, with the person who is liable, for payment of that tax).

Perhaps the best analogy to zappers and phantom-ware is a Ferrari. A Ferrari provides far more than basic transportation; it provides speed. How fast can a Ferrari go? The WikiAnswer is 202 mph. See, WikiAnswer at: http://wiki.answers.com/Q/How_fast_can_a_Ferrari_F50_can_go]. Thus, even though it is illegal almost everywhere to drive at 202 mph there is an active (and legal) market for Ferraris. No government (other than the Indian State of Karnataka) requires that speed governors be installed on Ferraris as a condition of vehicle registration (and in Karnataka this requirement only applies to commercial registration).

The makers of zappers and phantom-ware see the world the same way. Just because a computer program has the potential to be used for fraud (just as a Ferrari has the potential to travel at 202 mph) should not make its manufacture, sale or distribution illegal, nor should it allow the government to step in and regulate the ECRs that contain them.

But what if the only thing a zapper or phantom-ware does is facilitate tax fraud? Does this make a difference with respect to their manufacture and possession? Additionally, does the fact that these programs obscure and delete records that pertain to funds that belong to the government from the beginning make a difference? Because businesses have fiduciary obligations with respect to the transaction taxes they collect, does this give the government the right to regulate the ECRs that record taxes paid by the consumer? Perhaps, collecting transaction taxes is more like driving a school bus than driving a Ferrari, and the governor may have a regulatory interest in controlling the “speed” of these programs.
With training a fraudster can skim cash receipts with phantom-ware as effectively as with a zapper.

Zappers are commonly temporary installations. A CD or memory stick containing a zapper is inserted into a POS system to reconstruct (delete, replace or supplement) ECR records from a network. 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. 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.

A further distinction between zappers and phantom-ware is helpful. A zapper is more likely to be placed on the server in a POS system (multiple ECRs linked in a network with one or more computers, printers and other data terminals), whereas phantom-ware frequently inhabits stand-alone ECRs.

Regardless of the type of programming involved, both zappers and phantom-ware facilitate the systematic skimming of cash receipts by deleting records of cash sales, re-numbering receipts to disguise the deletion, and the production of conforming financial reports. In some cases these programs can be so thorough that they reach out beyond the ECR and the sale system itself to bring inventory and employee time records into line with the deletions.

The impact of a cash skimming fraud is felt throughout a revenue system. The most immediate losses are to consumption tax revenues (VAT or retail sales tax), but skimmed profits are also excluded from business taxes and not included in the personal income taxes of the owners (as distributions or dividends). The cash hoard from a successful skimming operation is almost always used to compensate employees under the table. Tax losses are further realized in the personal income tax of wage-earning employees as well as wage-indexed social security and medicare premiums. In some cases fraudsters structure above-the-table payments to allow employees to qualify for welfare assistance.8

The range of technology-regulation being considered by governments in response to these frauds stretches from the development of a centralized data-base to collect and

---

8 HM Revenue & Customs, News Release, Company Directors Jailed for £5million Fraud, (Nov. 13, 2007) (describing a cash skimming fraud which used two tills at a chain of newsagent’s shops in the Liverpool area where employees were paid low wages on the books, but “top up wages” from the cash hoard – HMRC indicated that, “[b]ecause of the fraudulent payroll operated by the company, numerous employees were able to make claims for working family/new tax credits, state benefits intended to help families in low-paid employment, to which they were not entitled. The employees were not low paid. They were receiving not only the declared wages but also the top up wages, funded by the cash which was being siphoned out of the business and hidden from HMRC.”).
retain all records of all retail sales in a jurisdiction;\(^9\) to mandatory government certification of each and every ECR in use in a jurisdiction;\(^10\) to direct encryption by the government of the raw transactional data passing through an ECR or POS system – without regard for the background system that generates it – a solution that has seen both market-segment\(^11\) and a whole-market\(^12\) permutations; to voluntary third-party encryption and third-party certification of ECRs.\(^13\) There are of course advocates for minimal regulation and traditional audit-enforcement, admittedly with significant enhanced technology training. The audit approach is most effective when there is authority to perform comprehensive audits – a simultaneous examination of all relevant taxes (income, consumption, and welfare levies).\(^14\)

\(^9\) Milan Prokin, *Technical and Functional Specification of Turnover Controllers – Draft Prepared for Fiscalis FPG 12 Cash Register Project Group*, (undated; on file with author) at 7. Professor Prokin, Faculty of Electrical Engineering, Belgrade proposes a system whereby “All misuses of fiscal cash registers, fiscal printers, non-fiscal cash registers and non-fiscal printers listed in the document titled Cash Register Misuse Guide are inherently solved by a new device called a turnover controller … [a central database where government serves store all transaction data]”

\(^10\) Greece has issued a series of decrees dealing with the technical specification that all sellers of cash registers in Greek territory must meet. The specifications are exceptionally detailed, running about 124 pages in total. See: CODIFICATION OF/ ADDENDA TO TECHNICAL SPECIFICATIONS FOR INLAND-REVENUE APPROVED REGISTERS AND SYSTEMS (OPERATING PROCEDURES) available at http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=pisa_notif_overview&iYear=2004 &inum=135&lang=EN&sNLang=EN

\(^11\) Quebec, focusing on the restaurant and catering sector of the economy, has determined to affix to cash registers a mini computer or module that will record each transaction passed through the ECR. The module is expected to cost $650.00 and will be tested on ECRs in 50 volunteer restaurants in November 2009, with mandatory adoption in all restaurants by 2011. See: Quebec Ministry of Revenue, Press Release *Pour plus d'équité dans la restauration : il faut que ça se passe au-dessus de la table* (Jan. 28, 2008) available at: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp; Québec Ministry of Finance, *Facturation obligatoire dans le secteur de la restauration: L’évasion fiscale au Québec* (Jan. 28, 2008) (power point presentation, translated and on file with author); Caroline Rodgers, *Québec va de l’avant pour stopper la fraude fiscale, HOTELS, RESTAURANTS & INSTITUTIONS* (Feb. 12, 2008) available at: http://www.hrimag.com/spip.php?article2771 (in French only, translations with author).

\(^12\) A comprehensive approach seems to be favored by Germany, and is currently under development. Rather than use mini computers, the German preference is to require that smart cards be embedded in all ECRs to encrypt an record all transactions passing through the terminal. Norbert Zisky, *Manipulationsschutz Elektronischer Registrierkassen und Kassensysteme* (Manipulation Protection for Electronic Cash Registers and POS Systems) (Mar. 15, 2004) (in German, translation on file with author).

\(^13\) This is the approach of the SSUTA supra note 4, and has been proposed in Richard T. Ainsworth, *Zappers: Technology-assisted Tax Fraud, the SSUTA and Encryption* (forthcoming *THE TAX LAWYER*, 2008).

\(^14\) Traditional audit methods are preferred in the UK, the Netherlands, France and other jurisdictions that have a more liberal approach to cash regulation and adopt generic legislation. See Fiscalis Committee Project Group 12, *Cash Register Good Practice Guide, supra* note 5, at ¶ 3.2.1. Ben B.G.A.M. van der Zwet, (personal e-mail correspondence Apr. 16, 2008) (on file with author)

Well our [NL] 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.
PHANTOM-WARE

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

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

During this conversation the Straight Systems managing director explained the existence of a “hidden delete” option in the Finishing Touch cash registers. The court indicated that this was, “… a hidden menu option that, after enabling said option, allowed operators of catering establishments to delete cash register receipts from the system.” After this discussion “… an employee of the defendant visited [Dudok] and

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 it was for the benefit of the entrepreneur.


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

18 Straight Systems BV is a Netherlands company that specializes in single-service ECR systems where all hardware and software are developed “in house.” The company web site offers a 24-hour help desk where there is “… one point of contact for all hardware and software for checkout’s front office and back office systems.” Available at: http://www.straight.nl (in Dutch, translation on file with author) (last visited May 24, 2008).

19 LJN: AX6802, at Consideration of the Evidence (Jun 2, 2006) (in Dutch) (translation on file with author). The case discusses three software programs: Twenty/Twenty; Finishing Touch; Tickview.exe. Twenty/Twenty was a US touch-screen program that did not have a phantom-ware application. Straight Systems BV added the phantom-ware application to Twenty/Twenty and renamed the program Finishing Touch. Using just this program you can view the sales ticket and change data. With a secret command the Tickview.exe program within Finishing Touch can be activated and the operator is asked if they would like
explained the [technical] application of the erase rule [or hidden delete function²⁰], after which [Dudok] subsequently decided to start using [it] …²¹

This case finds criminal tax fraud liability not only with the restaurant operators, but also with the suppliers of the Finishing Touch cash registers. As a consequence, the court is very clear about the operation of the “hidden delete” function. It indicates: The defendant’s cash register program includes various features to adjust the receipts later on. These possibilities are clearly described in the manual and are found easily in the menu structure of the program. If a receipt is adjusted using these functions, a “record” thereof is kept in the files so that any adjustments can be established afterwards. In addition [there is], a hidden option [that] exists to delete receipts. This function is not described in the manual and is also not included in the menu structure. Moreover the retrieval of this option is very complicated and only possible if the defendant explained this to the buyer. Contrary to the other features, use of this hidden option does not leave any traces in the files that are written to the disk. As a result, it is impossible at a later date to establish that the receipts have been deleted, hence this can, in principle, not be checked. It is self-evident that completely removing receipts from the books is a pre-eminent means for hiding turnover from the Internal Revenue Service.²²

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

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

In view of the special characteristics of the hidden option and the existence of the program’s other features for making adjustments, the court cannot imagine any other purpose for the hidden option than the illegal manipulation of turnover figures. The court is therefore firmly convinced that the defendant, as the seller, was aware of this. By selling to delete the whole ticket. If an affirmative response is given then the system records a “no sale” and the entire audit trail to the original data is eliminated. Ben B.G.A.M. van der Zwet, (personal e-mail correspondence May 28, 2008) (on file with author).

²⁰ The trial court in Rotterdam refers to the phantom-ware application as a “hidden delete function” whereas the appeals court in The Hague refers to the phantom-ware as “the erase rule.”
²¹ LJN: BC5500, at F3.
²² Id.
this software to a catering establishment, the defendant knowingly and willfully accepts the considerable chance that the buyer will use the program to delete turnover to conceal it from the Internal Revenue Service, with all associated tax consequences. ...In view of the context within with the delete option was discussed [between the managing director of Straight Systems BV and the owner-manager of Dudok], the court assumes that the managing director of the defendant, and hence the defendant, knew that [Dudok] wanted to dupe the Internal Revenue Service.23

It is particularly troubling to the appeals court that not only is, “[t]his erase rule actually made available to various customers, [but that the] defendant also offered support to customers – also in respect of this erase rule – by means of a helpdesk. Viewed against this background, making the erase rule available is part of the normal conduct of the business of the defendant.”24

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

The ECR/POS system market-place. How dynamic, how diverse, and how competitive is the market-place within which ECR/POS systems are bought and sold? If regulation is imposed, how responsive would the market be to this regulation?

Answers will differ from country, but a relatively accurate assessment can be made based on the data from jurisdictions that regulate already – jurisdictions that have adopted mandatory certification regimes for ECR/POS systems. The figures for Greece were relied upon in the Cash Register Good Practice Guide to paint this picture, but similar figures can be produced in with the records kept by any of the other “fiscal memory”25 (or “fiscal till”) jurisdiction.26 These jurisdictions require all entrepreneurs to use only certified tills, and further obligate each of them to secure the memory of their machines for tax audit purposes.

There are about 10 million people in Greece, and approximately 800,000 SMEs. These SMEs operate roughly 300,000 to 350,000 ECRs and POS systems. There is a

---

23 Id.
25 The Cash Register Good Practice Guide, supra note 5, Appendix D, at 1 indicates:
   Fiscal memory is where cash register transactions are permanently recorded. This memory is sealed and may only be accessed by authorized personnel or tax audit officials. Retail businesses cannot trade unless they have an approved cash register, which is subject to inspection and certification by tax authorities
26 Other “fiscal memory” jurisdictions include Argentina, Brazil, Bulgaria, Hungary Italy, Lithuania, Latvia, Poland, Russia, Turkey and Venezuela. Id., at 1.
sizeable turnover in ECR/POS systems each year – somewhere between 30,000 to 40,000 systems are replaced annually. Competing for this turnover business are approximately 50 importers or manufacturers, and together they offer in excess of 300 different fiscal machines. The major players in this market are from Germany and Italy, but there are also a significant numbers of non-EU sellers with American, Japanese and Chinese providers being the most significant.

No manufacturer dominates the market; no systems dominate the market. With a healthy range of providers and product, it seems reasonable to conclude that the ECR/POS system market-place in Greece remains robust even though fiscal regulation has been in place since 1988. If the “fiscal memory” regulation has not adversely impacted the market, it has adversely impacted phantom-ware applications in Greek ECRs. The Department Manager of Fiscal Electronic Cash Registers and Systems for the Greek Ministry of Economy and Finance (when comparing Dutch or Quebec litigation with Greek litigation in this area) indicates, “[b]ecause 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 [as there are in other non-fiscal memory jurisdictions].”

Certification appears to have both eliminated phantom-ware fraud and leveled the playing field in the ECR/POS system market-place. Things are very different in non-fiscal memory jurisdictions. Technological-assistance for cash skimming fraud is a selling-point in these markets. As the Greek official referenced above indicates:

Cash Register producers … don’t make their models with identical functions. They make their machines according to market “requirements.” They know for example that in UK there is no specific legislation or other tech specs or approval requirements for cash registers. Furthermore, it is widely known that there is no chance for a producer to sell his models in a “non-fiscal” country (like UK) if these models don’t have (less or more) built-in hidden capabilities and thus to facilitate the owner-user to manipulate stored data and cause confusion to auditors.

On the other hand, every model which is going to be sold in the territory of a “fiscal country” (like Greece, Italy, Poland, Hungary, etc.) must be approved and licensed. Thus, it has to be compliant with the specific national legislation regarding cash registers. This means that the producer must make its model compliant with the specific national legislation regarding cash registers. [ECR manufacturers] … will never apply for exactly the same model being sold in UK to be licensed in Greece or Hungary. [They know] … (or must have been informed) about the specific Greek … requirements and will make the appropriate changes and proper conformations (adjustments) to the firmware and/or to the hardware of the given model. (emphasis added)

28 Panagiots (Panos) Zafeiropoulos, personal e-mail communication (May 10, 2008) (on file with author).
29 Panagiots (Panos) Zafeiropoulos, personal e-mail communication (May 6, 2008) (on file with author).
Competition in the unregulated market-place (the “non-fiscal” countries) puts exceptional pressure on sales personnel looking for an advantage to make a deal. This clearly motivated Straight Systems BV in the Dutch cases considered above. The unlevel playing field has becomes a breeding ground for phantom-ware and zappers in the Netherlands.

This is not to say that honest sales people are not present in the market-place. Some individuals and companies simply refuse to violate ethical principles just to make a sale. This appears to be what was behind a reported call into the Connecticut Department of Revenue.

My only recent instance that involved a “zapper” like product was an anonymous call my office received from someone in the cash register business looking for information on filing a complaint against a competitor. Apparently the caller was attempting to make a sale at a restaurant and was informed that another company attempting to secure the same sale had offered to install such a program in the register if he/she was given the sale. The caller did not elaborate as to who the other salesperson was employed by or any specifics about the workings of the program.30

“SELF-HELP” PHANTOM-WARE

There is a kind of “poor man’s” phantom-ware that is widely available on almost all major ECR/POS systems, but it requires a bit of technical expertise and considerable care to carry out effectively. The selling point of the Finishing Touch system (particularly the “Tickview.exe” functionality) was that this kind of “self-help” was fully automated.

It is important to recognize that all phantom-ware applications need not be “hidden programming” embedded in the ECR/POS system as in the Dudok/Straight Systems cases – dedicated programming that is designed only to manipulate sales. Phantom-ware outcomes can be achieved by knowledgeable operators working with legitimate programming options commonly (although occasionally “obscurely”) available on modern ECRs. The problem for the fraudster using “self-help” phantom-ware options is that mistakes are common, and their use can be detected through careful till interrogation.

CASIO TE-2000 ECR – refunds omitted from the daily sales reports. The following example of “self-help” phantom-ware application is set out in the Cash Register Good Practice Guide. The Guide indicates:

Owing to the massive range of standard programming options incorporated into modern ECR’s and POS systems, no guarantee can therefore be given that sales information contained in Z reports is reliable and complete. Current techniques used to check the traders audit trail by reference to sequential numbered, dated and timed Daily Z Reports is no

30 Michael J. O’Sullivan, Jr., Manager, Appellate Division, Connecticut Department of Revenue (Feb. 11, 2008) (on file with author).
longer sufficient to give assurance that the sales data being audited is accurate. Further checks may be necessary to verify the integrity of till reports submitted by traders … [p]rogram interrogation may reveal that the till operating systems have been reconfigured to suppress sales information …

In the following discussion some familiarity is assumed with Z Reports (“daily” and “periodic,” normally called Z1 and Z2), X Reports (“daily” and “periodic,” normally called X1 and X2) and Electronic Journal Reports. The example (one of many possible) set out in the Guide concerns a “self-help” sales suppression technique that allows skimming through refunds and the suppression of these amounts from Z Reports (the so called “non-resettable grand sales totals).

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

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

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

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

31 See supra note 5, Cash Register Good Practice Guide, Appendix E, at 4.1.1.
32 One of the most important functions of a cash register is to record sales, taxes collected, media totals, discount, voids, and more. The report printed at the end of day or shift that reports this information and resets it for the next day or shift is known as the "Z" report. The "Z" report function prints the sales on the cash register tape while erasing the data from the memory. A "Z" is a once only report for a set period of time. Many Cash Register have "Z2" feature that allows "Z" reports to be added together. When an operator "Z2's them out" they will erase these reports for a longer period of time. An example of a "Z2" report is a monthly report that will be used to date and record monthly cash register sales. Every time the register is "Z'd out" (Report taken) that total is erased from the daily sales files and added to the "Z2" file.
33 "X" reports are the identical in information and time span to the “Z” reports. “X” reports only provide reports, they do not reset, or clear the memory. "X" reports can be taken as often as needed with no effect on sales data recorded.
34 See supra note 5, Cash Register Good Practice Guide, Appendix G, at 1.2.

The electronic journal usually contains ALL transactions keyed into the more complex types of till systems and is therefore the definitive record to obtain for audit purposes. There are exceptions, where Electronic Journals can be programmed “not-to-store” certain keying transactions e.g. “Training Mode.” The Electronic Journal should not be confused with the "Z" tape as it is not a recap of the day’s sales. The Electronic Journal tape is supposed to be a “blow-by-blow” record of every transaction made “step-by-step.” It is most useful for going back during a day to look for mistakes that were made. This journal has been a staple in the cash register industry since its conception. It can be used to check the Z report.
“D” = digit

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

(1) select PGM mode
(2) press 3
(3) press SUB TOTAL
(4) press the program that needs to be reconfigured (i.e. 0822) on the numeric keyboard.
(5) press SUB TOTAL
(6) press the new program code (we are changing code 001000 to 003100)
(7) press the CA/AMT TEND key
(8) press SUB TOTAL

Some explanation is needed on what the code at item (6) means initially and then how the new code is derived. The previous code 00100 is interpreted as follows:

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

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

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

Our goal is to suppress the printing of RF totals and RF count, and suppress the printing of the non-resettable grand total on the daily reports. The code to do this is “003100” – as shown in the following table:

<table>
<thead>
<tr>
<th>Code</th>
<th>0</th>
<th>0</th>
<th>3</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short hand identifier</td>
<td>D6</td>
<td>D5</td>
<td>D4</td>
<td>D3</td>
<td>D2</td>
<td>D1</td>
</tr>
</tbody>
</table>

“D” = digit number

Once re-programmed, “[t]he daily read/reset reports printed in X and Z modes will not print the non-resettable grand total and refund transactions made in the RF mode and RF key.” The Guide runs two examples based on this re-programming. The first (using the “001000” code) shows:

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

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

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

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

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

Reliance on the Electronic Journal in a CASIO TE-2000 is not a “fail-safe” check for tax auditors. There are significant problems with the completeness and correctness of the data in the Electronic Journal. The Dutch Tax Administration has examined more advanced CASIO systems, the CASIO QT-6000 and CASIO TE-4000, and is convinced that Electronic Journals in even these machines are not secure. The main risk (in all

---

35 See supra note 5, Cash Register Good Practice Guide, Appendix E, at 4.7.

36 See supra note 5, Cash Register Good Practice Guide, Appendix B, at 3.3 (Risk number 40) and 5.2.6.2 (discussing a “hidden function” on the CASIO QT-7300 machines that allows the Electronic Journal to be turned on and off).

37 Id.
CASIO machines) is that the RAM on which the data are preserved is too small and there is no mechanism to store data on an external medium. As a result, when the RAM is full, data is simply over-written. The only way to access (and preserve) the Electronic Journal data on a CASIO machine is to use the back office program CASIO Hospitality, but on this medium also there is no assurance of completeness and correctness of the data.\footnote{Personal e-mail communication, Ben van der Zwet (May 30, 2008) (on file with author).}

Effectively, CASIO machines cannot be relied upon to preserve business records. They can be programmed to delete records on the Z Reports and the X Reports, and can be relied upon to delete data in the Electronic Journal automatically (after certain volume limits are reached).

**ZAPPERS**

Zapper technology takes the fraud of skimming cash sales to new levels of sophistication. Zappers need to be seen from the perspective of the market-place that has produced them. Zappers respond to the inherent risk of detection in phantom-ware applications. Because phantom-ware is embedded in the same ECR/POS system that is the subject of the tax audit, there is always a risk that a careful till interrogation will uncover how the fraud is accomplished.

Zappers minimize this risk. Zappers are physically kept apart from the ECR/POS system they manipulate. Zappers are kept on cassettes,\footnote{U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), aff’d. 67 F.3d 460 (2nd Cir. 1995). Stew Leonard’s Dairy is one of the few litigated US zapper cases. The fraud involved the skimming of cash sales in excess of $17 million and was undetected for over ten years. The zapper in this case was developed by the Dairy’s IT professional and was kept on a cassette in a hollowed out book in the library of the owner. The zapper itself needed to be updated by the IT professional whenever the NCR, the ECR provider for the Dairy, updated the technology in their ECRs.} CDs, or memory sticks.\footnote{Ongoing Swedish investigations of the TT PI Electronique ECRs using a back-office program called Restodata. The Restodata program is licensed with a grey program dongle on a memory stick. [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.] Directly attached to this dongle is a second (silver) memory stick that contains the zapper. Litigation in Sweden is expected in late 2008. Martin Jansson, *Fraud by Using a Cash Register and Back-Office System*, (undated, unpublished paper) (on file with author).} They are inserted temporarily into the ECR/POS system to perform sales manipulations. When the procedure is completed, the zapper is removed. If a zapper is well developed – if it is designed by someone with detailed knowledge of the operating code it is being used on – then no trace of the original data trail will remain. Everything will be re-written, and the program that did it will be gone.

*The pressures that breed the zappers.* The wide use of zapper technology in a particular jurisdiction seems to be a function of (or, a response to) the convergence of three significant technological, legal and market pressures: (1) a street-level awareness that there is technological available to quickly, cheaply, and invisibly skim cash sales; (2) the awareness that criminal sanctions and aggressive enforcement actions are being directed at phantom-ware suppliers (the ECR/POS systems suppliers whose systems include phantom-ware); and (3) the pressure that ECR/POS system distributors and sales
In a highly competitive commercial market, personnel feel to perform (to make sales) where these three pressures are elevated zappers flourish.

Technical capacity: Skimming cash receipts from the till of a SME is a very old tax fraud. If conducted on a small scale it is very difficult to detect. However, on a large scale cash skimming inevitably leads to a double set of books, one for the auditor and the other for running the business. While it is possible to skim large sums with a simple double till system (as in the UK Aleef Garage Ltd. case), it soon becomes apparent to the fraudsters that technology will reduce the likelihood of detection by simply making the recordkeeping much easier (as in the Australian Ronen case). Technology’s attraction is that it makes the same fraud much less visible. If detection is a concern and if simplicity is an objective, then a zapper is much preferred over phantom-ware because a zapper can be physically hidden and it requires no re-programming of software (as long as the base technology of the ECR/POS system does not change).

The Ronen case illustrates the pressure of technological capacity very well. It is abundantly clear from this case that the Ronens were concerned that the manual skimming operation they had developed would be detected as the Australian GST came in. It is also clear (in retrospect) that their fears were misplaced. The court noted that the


42 Regina v. Ida Ronen; Regina v. Nitzan Ronen; Regina v. Izar Ronen, 2005 NSWSC 991.

43 Over a ten year period from 1991 through February 7, 2001 Ida Ronen and her two sons skimmed an estimated AUD$15 to $17 million in cash sales from their clothing business (Dolina). During most of the time the Ronen fraud was taking place Australia did not have a national consumption tax. In July 2000 the Wholesale Sales Tax was replaced by the Goods and Services Tax (GST) and this had a dramatic affect on the Ronen fraud. The court noted: A complication arose in the middle of the 2000 calendar year. As from 1 July 2000 the Goods and Services Tax regime was introduced. This posed a considerable problem for the offenders because proper compliance with the requirements of the GST laws would have revealed in a dramatic manner the amount of cash takings received in each of the retail shops. The intercepted telephone calls to which I have made reference show the substantial concerns of each of the offenders had about this situation. They show their attempts to devise a system to overcome the problem that they perceived might well bring about their undoing. Ronen, 2005 NSWSC, at ¶24 (emphasis added)

Mrs. Ronen took two steps, both of which involved technology. (1) A computer program was developed (by George Segal, Mrs. Ronen’s “de-facto husband”) to calculate the amount of cash that could be skimmed. (2) A technology consultant, Mark Talbot, was hired to set up a computer system that would allow Mrs. Ronen to run false till rolls for each retail outlet.
Ronen skimming would not have been uncovered through a standard audit, because this “… conspiracy came to light only by chance. It appears, as a result of telephone intercepts being placed on another person’s telephone service, that the Ronens’ involvement in the distribution of large amounts of money from Australia to overseas locations was detected [and it was only by following this lead was the skimming technology uncovered].”

However, for this analysis the important point to understand is the motivation – the reason for making the decision to move into technology to skim cash sales. In Ronen this decision was largely controlled by perceptions – the perception that there was an increased risk of detection in a GST audit, and the perception that technology (specifically a custom-made zapper) offered the best shelter from detection.

In other words, once it becomes widely known in the market-place that the technology to easily skim sales is readily available fraudsters are drawn to it.

Criminal sanctions. When jurisdictions aggressively pursue developers of fraud-facilitating technology with financial penalties and criminal sanctions the technology does not go away – it morphs into technology that (a) does not remain within the user’s hardware, and (b) is provided by intermediaries, not the ECR/POS system manufacturer.

Developer-focused criminal enforcement activity is on the rise in the Netherlands. LJN: AX6802 and the appeal LJN: BC5500 both focused on the Straight Systems BV (the developer of the phantom-ware option in the Finishing Touch system) more so than the Grande Café Dudok (the user of the system).

Similarly, in the B&F Optics case the District Court of Amsterdam determined that hairdressers underreported income tax and VAT returns because B&F Optics B.V. (formerly B&F Computer Systems B.V.), “… provided the means by supplying software allowing the skimming off of turnover …”

In B&F Optics the phantom-ware was not pre-installed (as with the Finishing Touch software), but was installed by the manufacturer, “on request of the taxpayer.” But after installation it remained on the customer’s ECR. The software, … was quite sophisticated. The hairdresser would enter a percentage that he wanted to be skimmed. The software searched for clients that would not leave traces in other file. So a male, who had not made an appointment [appointment were recorded in a separate file], did not need a hair-coloring [hair-colorings were also recorded in a separate file] and who paid in cash was the perfect record to be deleted.

\[44\] Ronen, 2005 NSWSC, at ¶28.
\[45\] B&F Optics B.V. (District Court of Amsterdam (Aug. 11, 2005) (in Dutch) (translation on file with author).
\[46\] Id., at ¶ 3.
\[47\] Personal e-mail communication, Ben van der Zwet, Feb. 14, 2008 ( on file with author).
The program searched for records of that type with a total turnover that corresponds to the desired percentage of skimming. [This was] an almost perfect solution. It took quite some effort to find the traces of this [software]. … Some hundreds of hairdressers have been visited by tax auditors to get the files and to perform a deep tax audit.48

Importantly, the thoroughness of the B&F Optics investigation, the visits to “hundreds of hairdressers” was prompted by the desire to build a criminal case not just against the users, but against the software company, and its “de facto” director, Hein van de Weijer.

A further variant can be found in LJN: AT5876, a case dealing with phantom-ware placed in the weighing scales of shopkeepers selling fresh produce. The software program (called Analysis), “… allowed the reduction of daily turnover to as little as 49%.”49 The local news accounts provide more details on the scope of the criminal investigation into the developer:

Managing director R. Velema of the software company Micro Craft confesses to the Fiscal Intelligence and Investigation Service (‘FIOD’) that he developed a module for weighing scales allowing shopkeepers selling fresh produce to manipulate their sales figures. According to his lawyer … the managing director acted on the instruction of two large suppliers of computer-controlled weighing scales. … Dozens of greengrocers, butchers, fish dealers, poulterers throughout the country were raided as well. In the next months, some 800 fellow shopkeepers can expect a visit from the FIOD-officers. The FIOD suspects that shopkeepers cook their books on a large scale using the special Langlauf-module allowing the amounts of the cash register weighing systems to be changed at a later time. The so-called creaming-off module makes it possible to enter completely different sales figures in the books, as a result of which the Internal Revenue Service misses out an a tremendous amount of tax revenues. … Micro Craft supplied over 400 Langlauf-modules to shopkeepers throughout the country. Moreover, a weighing scale [company] apparently also supplied hundreds of copies.50

Once again the installed phantom-ware (this time installed on weighing scales that are connected to ECRs, not on the ECR itself) is found in multiple businesses (over 1,200) but the focus of the criminal investigation is against the software developer.

However, LJN: AT5876 is a good example of how this fraud is morphing as tax administrations pursue it. In this case not only is the phantom-ware not placed in the ECR, but it is developed by a computer specialist who did not directly benefiting from its sale.

---

48 Id. (with minor editing to correct grammar and spelling).
49 LJN: AT 5876, District Court of Arnhem (Jul. 27, 2005) (in Dutch) (translation on file with author).
“My client spent three days in custody”, said the criminal lawyer. “He has put all his cards on the table. In his module, he had built in a functionality that could be used to commit fraud. He did not do this with criminal intent. He was bound to two large suppliers he could not refuse. When he found out three years ago that it was extensively abused, he stopped the supplies. He did not earn a penny with it, either. He was simply naive.”

It is only a short step from these phantom-ware cases to the real zappers that are designed and distributed by individuals not associated with the hardware they are used on, and that are physically removed after they manipulate sales figures. An example of the difficulties that a zapper can cause a tax administration can be seen in the Swedish case that is expected to go to court this summer.

The cash register (hardware) that was used to skim cash sales in a restaurant under audit is a TT PI Electronique. This cash register is a popular restaurant model in significant use in Italy, Belgium, Portugal, Spain, Germany, Denmark, Australia, the U.S.A. and North Africa. The software program operating the suspect cash register is 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.”

The Restodata program comes with a “… grey program dongle on a memory-stick, [and another] … silver memory-stick [the zapper].” The difficulty the Swedish tax administration is having with this investigation is precisely the difference between phantom-ware and zappers – once the zapper is found, its trail leads only back to the single restaurant where it was found. In other words, all TT PI Electronique cash registers are not necessarily suspect. This is a very different fact pattern from the restaurants that used Finishing Touch cash registers, or the hairdressers that used B&F Optics machines, or the over 400 greengrocers that used Micro Craft Langlauf-modules.

Highly competitive markets. Using the Greek data as a base-line – a country of 10 million people with 800,000 SME’s operating roughly 300,000 to 350,000 ECRs or POS systems from 50 different importers and manufacturers from within and without the EU – there is clearly competition in the ECR market-place. Competition is intense for the replacement/upgrade business as 30,000 to 40,000 systems turnover annually. Similar market profiles can be drawn globally.

If this market is dissected carefully at its core are another set of SMEs – the ECR/POS system distributors and installers. Both of these entrepreneurial groups work significantly on a commission basis that is contingent on the sale of new ECRs or POS systems. They stand between the user and the manufacturer.

51 Id.
52 This cash register has been manufactured in Paris, France since 1983. It can be seen at http://www.picashysteme.ch (in French) (last visited May 31, 2008).
53 Martin Jansson, supra note 40.
54 Id.
55 See infra text at note 27.
If there is a heightened street-level demand for skimming technology, and if an elevated threat of criminal sanctions creates unacceptable risk levels for major manufacturers to get involved,\(^{56}\) then there is a vacuum created that can be filled by middlemen. It seems clear in many jurisdictions that these agents are filling the void, providing (designing, distributing, and providing tech support for) the next generation skimming technology – the zapper.

**Logicaisse Ltd.** On March 12, 2008 Revenue Quebec executed eight search warrants in Laval, Montreal, Mascouche, and Chateauguay. The object of the warrants was Logicaisse Ltd., one of Quebec’s largest cash register specialists,\(^{57}\) a company that sells, rents, and provides maintenance for cash registers. The press release indicated:

Revenue Quebec has reasonable grounds to believe the company has developed and distributed a zapper … software used with RMS-Touch, \(^{56}\) Only one case has been found where a major manufacturer of an ECR/POS system has developed and distributed a zapper – AMG Corporation’s “Quanto” produced to defeat its own certified software (Robot) uncovered by the Operation Internet by the State Tax Administration of Minas Gerais, Brazil. Even cases like LJN: AX6802 and LNJ: BC5500 involving the factory installed phantom-ware in the Finishing Touch ECRs are not common, although the self-help kinds of phantom-ware continue to be available on major ECR systems. The careful re-programming requirements for self-help phantom-ware presents barriers to user adoption, but also shelters the manufacturer that provides these options, because there are commonly more than one good (non-fraud-facilitating) reason for having these options available.

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

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

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

...Preliminary evaluations indicate that these corporations illegally withheld between 40% and 50% of taxes owed…. \(^{57}\) 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 effected 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.


which it is the exclusive distributor in Quebec, [and] which has enabled different companies, mostly restaurants, to use zappers to conceal sales in order to avoid payment of taxes.\footnote{Revenue Quebec, Press Release, \textit{Les Systemes Informatiques Logicaisse Ltee dans la Mire de Revenue Quebec}, (Mar. 12, 2008) available at: \url{http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2008/12mars.asp} (in French) (translation on file with author).}

RMS-Touch is a privately owned American company, located in Fort Lee New Jersey about a mile north of the George Washington Bridge. An IBM Business Partner and an NCR Solution Provider it is known as the pioneer in restaurant Point Of Sale systems (POS), introducing in 1987 the first non proprietary, PC based restaurant touch screen Point Of Sale system. It is a leader in restaurant, bar and supermarket systems.\footnote{See: RMS-Touch, Company Profile, available at: \url{http://www.rmstouch.com/ID202.htm}}

It appears that Revenue Quebec believes that Logicaisse Ltd. has married its position as the exclusive distributor of: (1) CRS, Samsung and Sharp cash registers (hardware) with (2) its exclusive distribution rights in RMS-Touch (software), and (3) a zapper that it developed on its own, but that works in conjunction with the RMS-Touch system. Logicaisse Ltd. therefore would be classic middleman responding to a street-level demand for fraud-facilitating technology with a zapper added to third-party products for which it holds the exclusive distribution rights. This may be in part the reason it has been the number one distributor of Samsung products in the world since 1998.\footnote{See: Logicaisse, Ltd., Company History, available at: \url{http://www.logicaisse.com/html/english/logicaisse/historique.php}}

\textit{Audio Lab Inc.} A similar investigation by Revenue Quebec several years earlier gives some idea of the time commitment needed in a zapper investigation where the objective is to target the developer (as much, if not more than individual users). On April 8, 2004 Revenue Quebec announced that it executed four search warrants on the numbered company 9061-1184 Quebec Inc. which operated a restaurant under the name San Antonio Grill in Laval, Quebec. The allegation was that a “sales zapper” \textit{(camoufleur de ventes)} was used to delete sales records. The zapper was on a diskette.\footnote{Revenue Quebec, News Release, Tax Evasion: \textit{Le Ministre du Revenue Soupconne le Restaurant Grill San Antonio de Laval d’avoir Utilise un Zapper} (The Ministry of Revenue Suspects the Restaurant Grill San Antonio de Laval of having used a Zapper (Apr. 8, 2004) available at: \url{http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2004/08avril.asp} (in French only, last visited Jun. 1, 2008) (translation on file with author).}

The next year, on April 25, 2005, Revenue Quebec announced that the director of San Antonio Grill pleaded guilty to using a zapper,\footnote{The director, Mr. Apostolos Mandahtsis, was personally fined $65,681.00 and $10,300 respectively for PST (Provincial Sales Tax) and GST (federal Goods and Services Tax). Taxes and interest were due in addition.} and a related company of similar name, Grill San Antonio in Repentigny, also pleaded guilty to similar offences.\footnote{PST and GST fines of $23,416 and $8,603 were due in addition to taxes and interest.}
Later the same year, on October 1, 2005, Revenue Quebec announced that it executed five more search warrants in Montreal and Laval with respect to Audio Lab LP, Inc. This company was under suspicion of having developed and marketing a zapper that worked with Softdine, a restaurant cash register software that it also manufactured.\footnote{Revenue Quebec, News Release, Revenue Quebec Investigation of a Software Designer Outlet Suspected of having Developed and Distributed Zappers (Oct. 14, 2005) available at: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/14oct(2).asp (in French only, last visited Feb. 8, 2008).} Softdine was the operating software in the cash registers at San Antonio’s Grill in Laval, and at Grill San Antonio in Repentigny.

On June 26, 2007 (more than three years after execution of the initial search warrants in this case) Audio Lab LP, Inc. pleaded guilty to charges of having, “… designed and marketed a computer program designed to alter, amend, delete, cancel or otherwise alter accounting data in sales records kept by means of a software that [Audio Lab LP] had designed and marketed.” Press reports directly link this conviction to the investigation begun at Grill San Antonio in Laval in 2004.\footnote{Revenue Quebec, News Release, The Company Audio LP, Inc. Convicted of Tax Evasion (Sept. 21, 2007) (on the conviction fines were imposed of $12,475) available at: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2007/21sep.asp (in French only, last visited Feb. 8, 2008).}

Mr. Michel Roy. Another investigation by Revenue Quebec shows how zapper development and installation morphed into a cottage industry for close family members who were software developers and installers. This investigation involved twenty-eight restaurants doing business under the name Stratos. Each of the restaurants in the Stratos chain used a zapper.

To dispose of the excess cash from skimmed sales (1) a double billing system was put in place with suppliers (to conceal purchases made in cash), and (2) wages were paid to employees in cash (without being reported as income). The guilty pleas from this investigation came in waves – nineteen companies pleading guilty on September 26, 2002; another six pleading guilty on October 11, 2002, and the four remaining pleading guilty on March 21, 2003.

Press releases provide details of only the final ten companies. In aggregate the taxes and penalties for these companies came to $1,816,070.90, but the real thrust of the news releases was that “… the Department has conducted searches in order to establish proof that the designer of the IT function associated with the cash register software Terminal Resto had participated in the scheme set up by restaurants in the Stratos chain.”\footnote{The breakdown is: $429,179.07 (GST) + $492,023.11 (PST) + $214,589.55 (federal penalties) + $625,028.89 (provincial penalties) + $55,250.28 (judicial fees). Revenue Quebec, News Release, All Stratos Restaurants Convicted of Fraud in Connection with the use of a Zapper (Mar. 18, 2003) available at: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/25avril.asp (in French only, last visited Feb. 8, 2008).}
That proof was forthcoming on April 25, 2003, when Mr. Michel Roy and his two sons Danny and Miguel were convicted of tax evasion. The father (Michel) was the creator of the zapper that worked with Resto Terminal. He promoted it and made the sales. His sons (Miguel and Danny) installed the software and assisted the restaurant in committing the fraud. Aggregate fraud penalties assessed against the Roys were $1,064,459.67.

Mr. Luc Primeau. A final case shows how completely small providers/middlemen can become the critical component in the proliferation of zappers in a marketplace.

On March 17, 2003 Revenue Quebec announced that seven Patio Vidal restaurant franchises and two bars (La Tasca, from Gatineau, Quebec and O’Max in Masson-Angers, Quebec) were convicted of adding zappers to their Microflash cash register software (later upgraded to a new version called Caracara). Guilty pleas were entered on March 14, 2003.

However, this was not the end of the investigation, because a search warrant had been executed the previous December on developer of Microflash and Caracara. Suspicions were strong that this developer was also the developer of the associated zapper.

On October 17, 2005 Luc Primeau, the developer of Microflash and Caracara, admitted that he supplied other software that assisted these and other companies to evade GST and QST. Together these companies skimmed $2.7 million in cash sales.

However, Mr. Primeau was more than a zapper developer and salesman – he considered himself to be a provider of management services (admittedly management that focused on how to properly use a zapper) for which he charged a fee. Revenue Quebec determined that not only did Mr. Primeau fail to report GST and QST of $33,725.45 on his zapper sales, but he also failed to report income of $155,084.99 in income based on the “zapper management” services he was providing.

WHERE ARE THE AMERICAN ZAPPERS?

One of the anomalies of this research is that there are very few reported cases of phantom-ware and zappers used in America to skim cash sales. What accounts for this omission?

There are only two US zapper cases on record, Stew Leonard’s Dairy (a local supermarket chain) in Norwalk, Connecticut and the La Shish chain of thirteen restaurants in the Detroit, Michigan area.

Stew Leonard’s Dairy is “[t]he largest criminal tax case in the history of Connecticut.” A zapper was used to skim 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.

Recently, Talal Chahine and his wife, Elfat El Aouar, replaced Stew Leonard’s Dairy as the leading US zapper case. Elfat was sentenced, May 16, 2007, to 18 months for tax evasions. Talal remains a fugitive (believed to be in Lebanon) with a warrant issued for his arrest. Together they zapped more than $20 million in cash sales over a four year period from their restaurants (La Shish) and sent the funds in small denomination cashier’s checks to Hezbollah in Lebanon.

These cases appear to be the only litigated US zapper cases. With only two US cases, the perception is that zappers and phantom-ware are not a US problem. For example, when the following question asked of the Pennsylvania Department of Revenue:

“Have you seen a zapper in Pennsylvania?”

The answer was:

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

But there is a US connection to the zappers and phantom-ware found overseas. The first Canadian zappers were designed and distributed in Canada by a US company.
In the Netherlands, the base program that supported the phantom-ware functionality in the Final Touch software was of US origin. Additionally, the RMS-Touch program that was modified by Logicaisse Ltd. to skim cash sales was of US origin.

However, even though there are connections, and even though zappers and phantom-ware are exceptionally common in the global restaurant business, and even though New York is the only North American city with a larger restaurant business than Montreal, the New York City District Attorney’s Office has not seen zappers or phantom-ware in use there. An e-mail to that office asked:

“Did you ever find a zapper, or hear about a zapper in New York City?”

The answer received was:

“Not yet. [But that d]oes not mean they are not around.”

Assuming the New York City District Attorney’s Office is right. Just because we cannot see zappers and phantom-ware being used to skim cash sales, does not mean they are not around – what then accounts for the scarcity of American cases? There are two places to look for the answer: (1) relative tax rates – maybe the American tax rates are significantly different from those in the EU and Canada, and as a result there is no incentive to skim cash sales in America; or (2) enforcement efforts – maybe the American tax enforcement efforts are significantly different, and as a result we do not pick-up on all the technology-assisted fraud that is going on.

If skimming yielded far greater returns in Europe or Quebec than in the US, one might suppose that hat this would be a reason for high numbers of zapper and phantom-ware frauds overseas and low number of them reported in the US. However, when the tax rates (income and consumption tax) are considered, the financial incentive to skim cash sales appear to be almost identical inside and outside the US.

For example, skimming a 100 euro cash sale in the Netherlands will immediately put 119 euro in the owner’s pocket (the VAT rate is 19%), and reduce his corporate tax by 34 euro (the standard income tax rate is 34%). The net gain in the Netherlands would be of 153. The same result would be found in Sweden, where skimming a 100 kroner sales would put 125 kroner immediately in the owners pocket and reduce his corporate tax by 28 kroner. The net gain would again be 153.

In Quebec skimming a 100 dollar cash sale would immediately put 110 dollars in the owner’s pocket, and reduce his corporate tax by 32.02. The net gain would be 142.02 dollars, the lowest return-on-zapping of the four examples considered here. In Connecticut skimming a 100 dollar cash sale would put 106 dollars immediately into the

---

76 Personal e-mail communication with Gilda Mariani (Money Laundering and Tax Fraud Unit) (May 18, 2008) (on file with author).
owner’s pocket and reduce his corporate tax by 42.5 dollars. The net gain would be 148.5 dollars.

<table>
<thead>
<tr>
<th></th>
<th>Connecticut</th>
<th>Quebec</th>
<th>Netherlands</th>
<th>Sweden</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate</td>
<td>35</td>
<td>22.12</td>
<td>34</td>
<td>28</td>
</tr>
<tr>
<td>Sub-national</td>
<td>7.5</td>
<td>9.90</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>42.5</td>
<td>32.02</td>
<td>34</td>
<td>28</td>
</tr>
<tr>
<td>Consumption</td>
<td>0</td>
<td>5</td>
<td>19</td>
<td>25</td>
</tr>
<tr>
<td>Sub-national</td>
<td>6</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>6</td>
<td>10</td>
<td>19</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td>48.5%</td>
<td>42.02%</td>
<td>53%</td>
<td>53%</td>
</tr>
</tbody>
</table>

Thus, there does not appear to be a significant difference in the financial incentives to skim cash sales in the US and in the overseas jurisdictions where zappers and phantom-ware litigation is high.

However, there is another way to look at this chart. The two US zapper cases hint that the difference between the US and overseas jurisdictions may not be in the rate of taxation, but in the structure of the tax system. Both Stew Leonard’s Dairy and the La Shish restaurant cases were federal income tax investigations. State sales tax actions followed the federal income tax investigation. In all foreign jurisdictions zappers and phantom-ware investigations are initiated through the consumption tax.

However, the US has no federal consumption tax. These kinds of audits are state-level audits, and there are significantly lower levels of State-Federal coordination when the State auditor is working in the retail sales tax as opposed to the income tax.

Perhaps then it is the American pre-occupation with the income tax, and a further emphasis on large case income tax examination that has placed zappers and phantom-

---

77 In the Stew Leonard’s Dairy case U.S. Customs searched Stew Leonard Sr. in the Spring of 1991, leading to the execution of search warrants on August 9, 1991 by special agents of the IRS Criminal Investigation Division. Leonard, 37 F.3d at 35; 75 YEARS OF CRIMINAL INVESTIGATION HISTORY, supra note 70, at 145. The State of Connecticut commenced its audit “… as a result of IRS actions, in February, 1992 …” Leonard, 254 Conn. 286, 289 (2003). On July 22, 1993 Stew Leonard pleaded guilty in the federal audit. The State’s audit was no where near completion at this time. A final Connecticut determination was not rendered until February 27, 1996.

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

Michigan law (Michigan Compiled Laws Section 205.28(1)(f)) prohibits divulging any facts or information obtained in connection with the administration of a tax, or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the department for a tax administered by the department. According, we are unable to provide you with the information you seek.

Personal e-mail communication, Feb. 4, 2008 (on file with author).
ware into our enforcement “blind spot?” Perhaps we just do not see what is going on in the ECRs and POS systems because we are looking elsewhere? Perhaps we trust Z Reports, X Reports and the Electronic Journals far too much?

If there is street-level awareness in the US that technology is available to quickly, cheaply, and invisibly skim cash sales, and if the US market-place for ECRs and POS systems is as highly competitive as it is elsewhere, then it is reasonable to expect that what Canada, the Netherlands, Sweden and Brazil are witnessing is also going on in New York City. We are just not seeing it.

If we cannot find this fraud in the US, we will not be ready to consider the smart card and encryption solutions that seem so necessary in foreign jurisdictions. If we are not ready to consider the smart card and encryption options, we are also not ready to consider the short-term tax policy and information privacy issues that are implicated by these developments, nor are we ready to consider how a more sophisticated technological infrastructure will help resolve some of the nagging questions of tax design. There is a lot to do, but first we need to find the zappers and the phantom-ware that are just as surely being used here as they are elsewhere in the world.