Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud with Technology

Richard Thompson Ainsworth and Urs Hengartner*

PRÉCIS

Le 28 janvier 2008, Jean-Marc Fournier, le ministre du revenu du Québec, a annoncé que d'ici la fin de 2009, Revenu Québec allait tester un nouvel appareil anti-fraude — le « module d'enregistrement des ventes » (MEV) — dans le secteur de la restauration. Le MEV est conçu pour détecter les enregistrements numériques des ventes qui ont été effacés ou supprimés dans les caisses enregistreuses électroniques et les systèmes au point de vente — un type de fraude qui contribue à plus de 425 millions $ par année de recettes fiscales non perçues uniquement dans le secteur de la restauration. Les études menées par le Québec indiquent que les restaurateurs recourent de plus en plus à la technologie pour modifier les enregistrements numériques dans le but de soustraire des revenus du fisc et d'éviter de déclarer et de verser les taxes qu'ils ont perçues. Le MEV aidera les vérificateurs de la province à mettre au jour ces activités frauduleuses.

Les autorités fiscales du monde entier ont adopté deux approches pour s'assurer de l'intégrité des enregistrements des ventes dans les secteurs à forte utilisation de l'argent en espèces : une approche axée sur les caisses enregistreuses, et une autre approche qui mise plutôt sur les principes de conformité et de coercition dans la promotion de bonnes pratiques commerciales. Avec la mise en place du MEV, le Québec prend les moyens pour devenir une administration fiscale axée sur les caisses enregistreuses.

L'article présente le MEV dans le cadre d'une analyse comparative. Les approches technologiques de l'Allemagne et de la Grèce (deux administrations axées sur les caisses enregistreuses) sont comparées avec celle des Pays-Bas (une administration fiscale qui mise sur les principes) qui prend appui sur d'intenses vérifications axées sur les technologies pour vérifier l'exactitude des enregistrements numériques.

Dans sa conclusion, l'auteur suggère qu'il y aurait lieu de s'inspirer du projet de rationalisation de la taxe de vente des États-Unis qui recourt à la certification par l'administration des technologies fiscales en vue d'assurer l'exactitude des déterminations des taxes sur les opérations.

[*] Richard Thompson Ainsworth is of the School of Law, Graduate Tax Program, Boston University (e-mail: vatprof@bu.edu). Urs Hengartner is of the David R. Cheriton School of Computer Science, University of Waterloo (e-mail: uhengart@cs.uwaterloo.ca).

ABSTRACT

On January 28, 2008, Quebec's minister of revenue, Jean-Marc Fournier, announced that by late 2009 Revenu Québec would begin testing an anti-fraud device—the "sales recording module" (SRM)—in the restaurant sector. The SRM is designed to detect the erasure of digital sales records in electronic cash registers and point-of-sale systems—a type of fraud that contributes to more than $425 million annually in lost tax revenues in the restaurant sector alone. Quebec studies indicate that restaurateurs are increasingly employing technology to alter digital records in order to conceal income from the business and avoid reporting and remitting taxes due. The SRM will assist provincial auditors in detecting such fraudulent activities.

Revenue authorities around the globe have taken two approaches to assuring the integrity of business records in cash-intensive industries: one approach secures the till; the other relies on principles of compliance and enforcement to encourage good business practices. With the introduction of the SRM, Quebec is taking steps to become a "fiscal till" jurisdiction.

This article considers the SRM in a comparative context. The technological approaches of Germany and Greece (both of which are fiscal till jurisdictions) are contrasted with the approach adopted in the Netherlands (a principles-based jurisdiction), which relies on intensive technology-based audits to assure digital record accuracy.

The article concludes with a suggestion that there may be something to learn from the US streamlined sales tax initiative, which employs government certification of tax technology to ensure the accuracy of transaction tax determinations.

KEYWORDS: FRAUD ■ TAX EVASION ■ RESTAURANTS ■ ANTI-AVOIDANCE ■ TECHNOLOGY ■ SRM

CONTENTS

INTRODUCTION

On January 28, 2008, the Quebec minister of revenue, Jean-Marc Fournier, announced[1] that by late 2009 Revenu Québec would begin testing a device, the "sales recording module" (SRM), which is projected to substantially reduce tax fraud in the restaurant sector.[2] On November 30, 2009, the pilot program was under way with 46 restaurants in seven cities involved. By 2010 or 2011, SRMs will be mandatory in all Quebec restaurants, where they will assure accuracy and retention of business records within electronic cash registers (ECRs). The Quebec government has promised to provide the necessary number of SRMs to restaurants at no cost. The cost to the Quebec treasury for the whole program is estimated to be $55 million.[3]

The problem that the SRM addresses is the erasure of sales records from the ECR through a back-office or ECR-embedded program. The ECR's records are the central (in some cases, the only) repository of business data. As a result, the ECR's data are relied upon by tax authorities to verify sales and income. The target is always cash. Credit, debit, cheque, or bank transfer transactions leave other audit trails, but cash transactions are found only in the ECR.

In Quebec, as in the rest of the world, restaurants are the most vulnerable to this fraud. The SRM targets this sector, although similar frauds could occur in grocery stores or any other business making cash sales directly to consumers. Business-to-business transactions are not covered by the SRM.

It is clear to Quebec's revenue minister that not only are large volumes of cash being skimmed (removed from the sales and profits records of restaurants by their owners), but this fraud against the public fisc is increasing. It is facilitated and accelerated by technology. The digital manipulation of business records kept by modern ECRs is all too prevalent. Add-on software (zappers), factory- or distributor-installed software, and old-fashioned manual reprogramming of ECRs (phantomware) are the mechanisms through which the manipulations arise. Two examples of zappers are shown in figures 1 and 2. Revenu Québec has pursued these devices (known generally as "camoufleur de ventes," or sales zappers) over the past decade, and is convinced that something more than a traditional audit is needed to counteract the manipulations.

[1] Revenu Québec, "Pour plus d'équité dans la restauration : il faut que ça se passe au-dessus de la table" ["For More Equity in the Restaurant Sector It Is Required That [Business Is Conducted] Above the Table"], *Communiqué de presse*, January 28, 2008 (online: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp) (translation on file with Richard T. Ainsworth, referred to in subsequent notes as R.T.A.).

[2] Revenu Québec, "L'évasion fiscale au Québec : Facturation obligatoire dans le secteur de la restauration—Sous-déclaration des revenus dans le secteur de la restauration" ["Tax Evasion in Quebec: Obligatory Billing in the Restaurant Sector—Under-Declaration of Revenues in the Restaurant Sector"], January 28, 2008 (PowerPoint presentation and translation on file with R.T.A.). The French term for the device is "module d'enregistrement des ventes" (MEV).

[3] Caroline Rodgers, "Québec va de l'avant pour stopper la fraude fiscale," January 28, 2008, at *Hôtels, Restaurants & Institutions* (online: http://www.hrimag.com/spip.php?article2771) (translation on file with R.T.A.).

Relying on more than 230 cases since 1997, and surveys of skimming activity in the restaurant sector, the minister of revenue summarized the situation as follows:

> Although the majority of restaurateurs comply with their tax obligations, the restaurant sector remains an area of the Quebec economy where tax evasion is rampant, both in terms of income tax and sales taxes. Tax losses in this sector are important. Quebec Revenue estimates that they are $425 million for the 2007-2008 fiscal year.[4]

The zappers (and phantomware applications) that are the major facilitators of this fraud are not confined to Quebec. Zappers and phantomware have spread throughout Canada[5] and around the world. It is not surprising, therefore, that a number of jurisdictions have looked at automated sales suppression and have adopted technological countermeasures, some of which are strikingly similar to the SRM. Other jurisdictions look to technology for answers, but differ with respect to the sophistication of the technology that they would deploy. In yet other jurisdictions, traditional audit rather than technology is preferred; however, the most successful of these "audit-only" jurisdictions are adopting comprehensive (multitax) audit strategies, with teams of auditors supported by computer specialists—in effect, a "supersized" traditional audit.

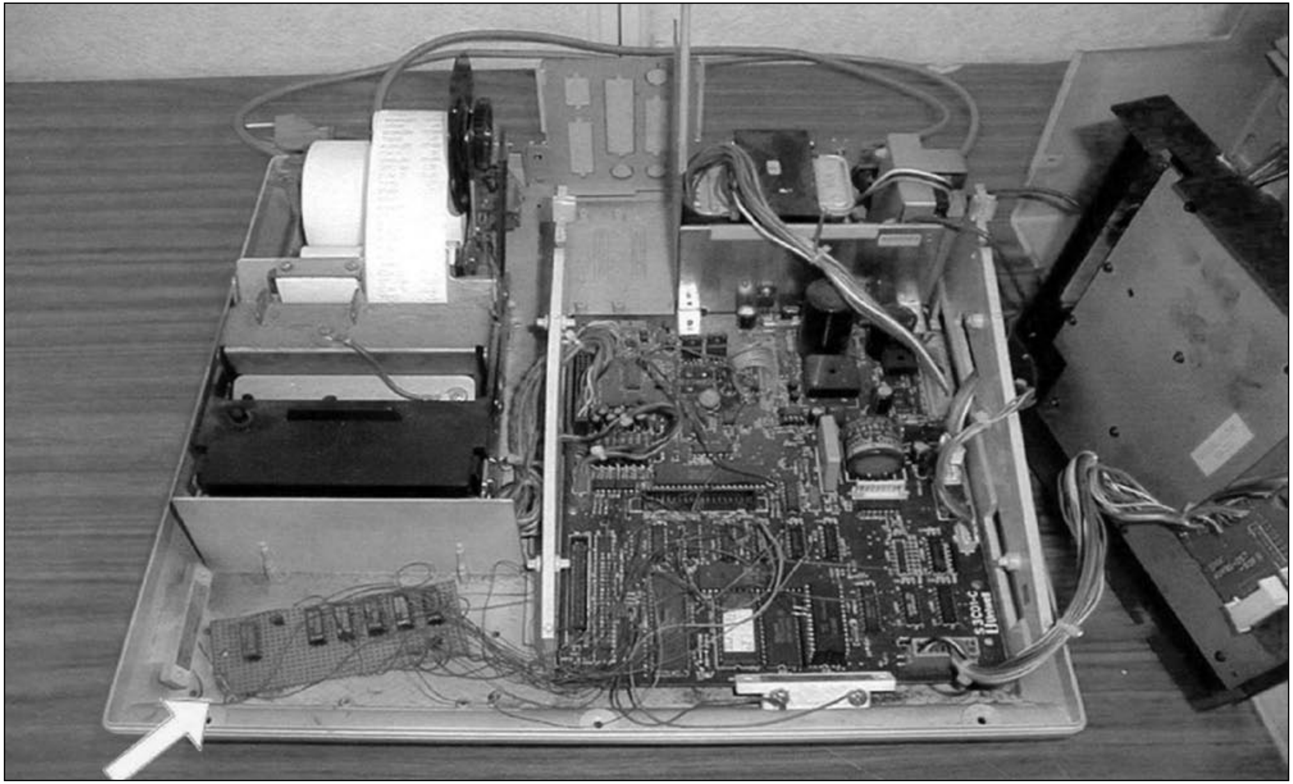
A review of approaches indicates that two policy orientations guide enforcement actions in this area: one approach is rules-based; the other is principles-based.[6] They are not mutually exclusive—degrees of blending are common. Rules-based

[4] Supra note 2. The basis for the minister's estimates is a rigorous empirical study performed by Quebec's Ministère des Finances, "Tax Evasion in Quebec: Its Sources and Extent" (2005) vol. 1, no. 1 *Economic Fiscal and Budget Studies* 1-6 (online: http://www.finances.gouv.qc.ca/documents/EEFB/en/eefb_vol1_no1a.pdf). In a personal e-mail communication, June 23, 2009 (on file with R.T.A.), Gilles Bernard, directeur général adjoint de la recherche fiscale, Revenu Québec, responded to a question on the $425 million figure used by the minister. Indicating ancillary losses of $8 million in other (unspecified) taxes, Bernard stated, "The tax losses are 417 M$ (QST + Income Tax). The QST [Quebec sales tax] represents 133M$ and the Income tax losses are 284M$. This last amount can be doubled to take into account the federal income tax."

[5] Canada Revenue Agency, "Businesses Warned Against Using Tax Cheating Software," *Tax Alert*, December 9, 2008: "The Canada Revenue Agency (CRA) is aware that electronic sales suppression software is currently being marketed and sold to Canadian businesses. Business owners are reminded that hiding income to evade taxes is against the law. Using this software is not worth the risk. . . . Businesses that have used electronic sales suppression software are suspected of having hidden thousands of transactions and millions of dollars in sales" (online: http://www.cra-arc.gc.ca/nwsrm/lrts/2008/l081210-eng.html). See also Darah Hansen, "Cooking the Books," *Vancouver Sun*, December 11, 2008: following allegations by the CRA that four Chinese restaurants in British Columbia had participated in a high-tech scheme that used zappers to evade tax on millions of dollars of receipts, five people were facing 25 charges as part of a nationwide investigation (online: http://www.canada.com/vancouversun/story.html?id=6c945ca6-f84a-43f6-86ad-221814731593&p=2). Also see infra note 8.

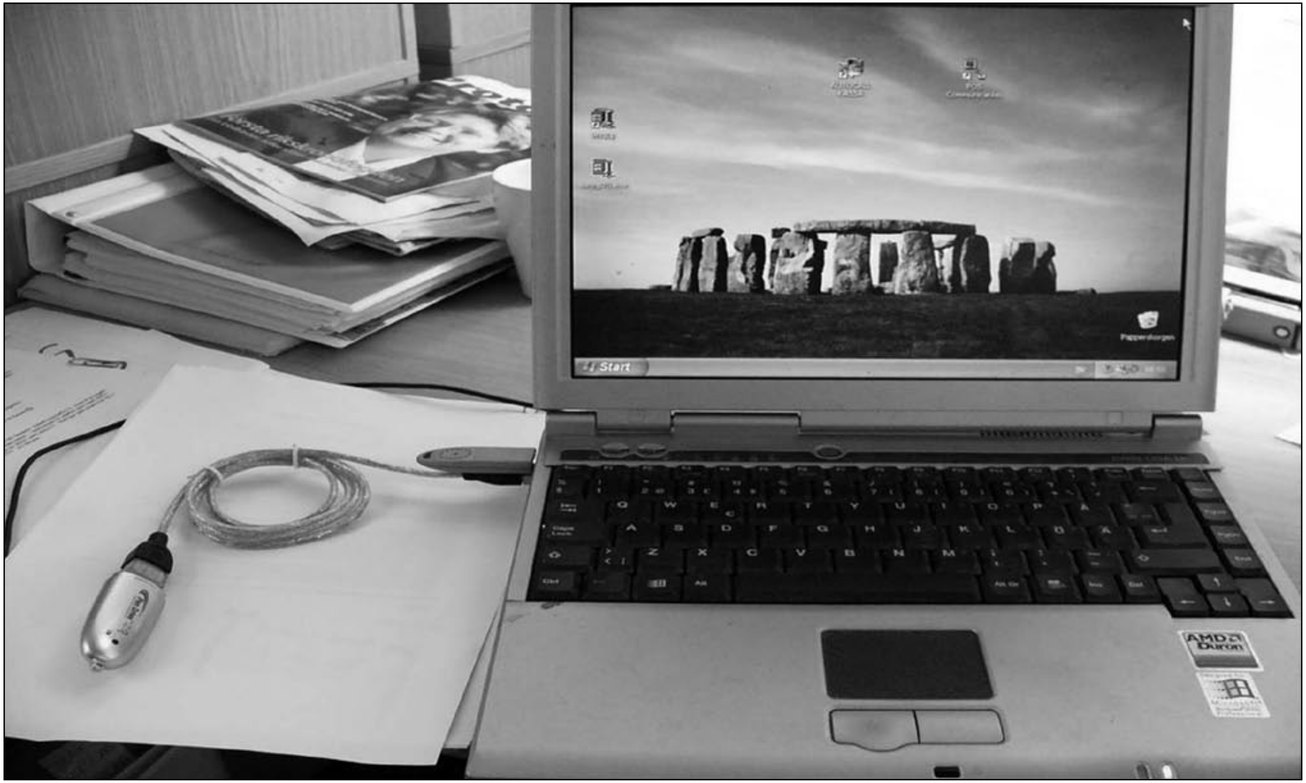
[6] European Commission, Directorate-General Taxation and Customs Union, Fiscalis Committee Project Group 12, Cash Register Project Group, "Cash Register Good Practice Guide," December 2006, 5-6 (unpublished report on file with R.T.A.).

FIGURE 1 **Old-Style Zapper, Hard-Wired into Electronic Cash Register**



This is an old-style zapper, which has been hard-wired into the electronic cash register (ECR) and is therefore easy to detect. The picture shows the top of the ECR removed; the large white arrow points to the device. (Reproduced by permission of the government of Quebec.)

FIGURE 2 Modern Zapper Using Memory Stick



This is a more modern zapper, which is a memory stick ("dongle") that is inserted into the back-office computer system that collects data from the business's electronic cash registers. (Reproduced by permission of the government of Sweden.)

jurisdictions adopt comprehensive and mandatory legislation regulating and/or certifying cash registers. Jurisdictions taking this approach include Greece and Germany. With the adoption of the SRM, Quebec will also fall within this group. These jurisdictions are classified generally as "fiscal till" (also called "fiscal memory") jurisdictions.

Principles-based jurisdictions rely on compliant taxpayers following the rules. Compliance is enforced with an enhanced audit regime. Comprehensive multitax audits (the simultaneous examination of income, consumption, and employment returns) are performed by teams that include computer audit specialists. Audits are frequently unannounced and preceded by undercover investigations that collect data to be verified.[7] Jurisdictions taking this approach include the United Kingdom, Canada, and the Netherlands. France has implemented a program of preventive audits that target technology providers.[8] A similar effort can be found in Quebec, where the customer lists of audited technology providers have been used to map later audits of businesses suspected of technology-assisted skimming.[9] Prior to the adoption of the SRM, Quebec fell squarely within a principles-based classification. Moving forward, Quebec will merge both approaches, even though it appears that the Canada Revenue Agency (CRA) will continue to pursue only principles-based enforcement techniques.[10]

[7] For example, the recent Canadian investigation in British Columbia into the alleged distribution of sales suppression software by InfoSpec Systems Inc. involved an eight-month undercover investigation by the Royal Canadian Mounted Police (RCMP). During this phase of the operation, undercover RCMP officers posed as potential buyers of sales suppression software. This evidence supported allegations that InfoSpec Systems Inc. knowingly provided restaurants with zappers. Canada Revenue Agency, "Charges Laid in Large-Scale Tax Fraud Investigation," *News Release*, December 10, 2008 (online: http://www.cra-arc.gc.ca/nwsrm/rlss/2008/m12/nr081210-eng.html).

[8] "Cash Register Good Practice Guide," supra note 6, at 6. This is the approach that the CRA took in the InfoSpec Systems investigation. Targeting the software program (Profitek) "documents, CDs, computer files, sales notebooks, an electronic calendar, e-mail and other client lists," the CRA was able to conduct a nationwide investigation, which (according to the *Vancouver Sun*) is "continuing and [CRA officials] expect more charges to be laid." Hansen, supra note 5.

[9] For example, see the investigation of Audio Lab LP: Revenu Québec, "Revenu Québec enquête sur un concepteur de logiciel de point de vente soupçonné d'avoir conçu et distribué un camoufleur de ventes" ["Revenu Québec Investigation of a Software Designer Outlet Suspected of Having Developed and Distributed Zappers"], *Communiqué de presse*, October 14, 2005 (online: http://www.revenu.gouv.qc.ca/en/ministere/centre_information/communiques/ev-fisc/2005/14oct.aspx) (translation on file with R.T.A.); and the investigation of Michael Roy reported in Revenu Québec, "Fines of More than One Million Dollars—A Father and His Two Sons Convicted for Tax Evasion in Connection with the Zapper," *News Release*, May 2, 2003 (online: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/02mai.asp) (on file with R.T.A.).

[10] In its recent *Tax Alert* dealing with sales suppression software, the CRA emphasized that it has "over 5,000 employees dedicated to finding unreported business income and ensuring that the proper amount of taxes is paid, even when sales records are missing." *Tax Alert*, supra note 5.

It would be very helpful if a comparative cross-methodology analysis of the various approaches could be presented (rules-based with and without technology versus principles-based with and without a comprehensive audit). We need to quantify the compliance improvement against the cost of getting that compliance. Unfortunately, most of the technology solutions are in prototype. Perhaps Quebec (as it measures the effectiveness of moving from traditional audit alone to technology and audit) will have good measures in a few years.

Amid all the international concern, it is notable that the United States does not have a coordinated zapper enforcement effort. In fact, the United States has uncovered only two zappers, one at Stew Leonard's Dairy in Norwalk, Connecticut, where $17 million in cash was skimmed,[11] and the other at the La Shish restaurant chain in Detroit, Michigan, where cash sales totalling $20 million were zapped and allegedly sent to Hezbollah in Lebanon.[12] The reason for this low enforcement rate is that the US authorities are hampered in their approach to zappers. Federal income tax audits are not coordinated with state and local retail sales tax audits, so the audits are not comprehensive in the Dutch sense. In addition, federal computer audit specialists are not normally assigned to audits of small and medium-sized enterprises (SMEs), and this is where the zappers are.

Nevertheless, if the United States became serious about this problem, it might have a unique blend of rules- and principles-based solutions in an extension of the Streamlined Sales and Use Tax Agreement[13] (SSUTA). Under the SSUTA, certified third-party software providers (CSPs)[14] could be tasked with assuring ECR accuracy. Not only is the SSUTA legal framework operational, but at present levels of technology, a CSP could readily assure states that the correct retail sales tax was being collected and remitted. At the same time, it could assure federal authorities that zappers were not being used to underreport income. CSPs indemnify both sides

[11] The *Leonard* case came about when a US customs officer inspected a suitcase carried by Mr. Leonard on one of his trips to St. Martin: *United States v. Leonard*, 37 F. 3d 32, at 35 (2d Cir. 1994); aff'd. 67 F. 3d 460 (2d Cir. 1995). Details of the tax fraud are preserved in the appeals of the sentence.

[12] United States, Department of Justice, Eastern District of Michigan, "La Shish Financial Manager Sentenced to 18 Months in Prison for Tax Evasion," *Press Release*, May 15, 2007 (online: http://nefafoundation.org/miscellaneous/FeaturedDocs/U.S._v_Aouar_DOJPR_Sent.pdf). The La Shish fraud apparently came to light as a result of the owner's failure to file a tax return. "Authorities declined to comment on how the reported crime was discovered, but according to court records, Mr. Chahine failed to file a tax return in 2003": Roy Furchgott, "With Software, Till Tampering Is Hard To Find," *New York Times*, August 20, 2008 (online: http://www.nytimes.com/2008/08/30/technology/30zapper.html).

[13] Streamlined Sales Tax Governing Board, Streamlined Sales and Use Tax Agreement, adopted November 12, 2002, amended November 19, 2003, and further amended November 16, 2004 (herein referred to as "the SSUTA").

[14] See SSUTA section 230, defining a certified software provider as "[a]n agent certified under the Agreement to perform all the seller's sales and use tax functions, other than the seller's obligation to remit tax on its own purchases" (online: http://www.streamlinedsalestax.org/uploads/downloads/Archive/SSUTA/SSUTA%20As%20Amended%2009-30-09.pdf).

(government and taxpayer) against loss.[15] Certification of the CSP would need to be undertaken jointly (by state and federal agencies), as would oversight of their operation. Quebec has not considered an SSUTA/CSP solution, but it might need to look at this option if it plans to extend the SRM outside the restaurant sector.

STRUCTURE OF OUR ARGUMENT

This article moves beyond a discussion of the variety of sales suppression programs in use—zappers and phantomware.[16] It goes beyond a discussion of the economic impact that this kind of fraud has on local businesses,[17] and sidesteps a speculative inquiry into where the money from this fraud ultimately goes—into the business or into the owner's pockets.[18] Those matters have been considered elsewhere. Our concern here is on enforcement efforts, particularly the SRM. The intent is to assess

[15] Under the SSUTA, a CSP needs to provide a surety bond to receive a contract from the governing board. Some enterprises will also take out an insurance policy.

[16] For discussion of these programs and possible countermeasures, see Richard T. Ainsworth, "Zappers and Phantomware: The Need for Fraud Prevention Technology" (2008) vol. 50, no. 12 *Tax Notes International* 1017-29; Richard Thompson Ainsworth, "Zappers and Phantomware: Are State Tax Administrators Listening Now?" (July 14, 2008) vol. 49 *State Tax Notes* 103-15; Richard Thompson Ainsworth, "Zappers: Technology-Assisted Tax Fraud, SSUTA, and the Encryption Solutions" (2008) vol. 61, no. 4 *The Tax Lawyer* 1075-1110; and Richard T. Ainsworth and Hiroki Akioka, "Electronic Tax Fraud—Are There 'Sales Zappers' in Japan?" (2009) vol. 11 *Kansai University Review of Economics* 1-34.

[17] There is evidence that the presence of a zapper in the local economy has a direct competitive impact on other businesses in the area, as well as an impact on enterprises that sell ECRs to retailing businesses. In a personal e-mail communication, February 11, 2008 (on file with R.T.A.), Michael O'Sullivan (a hearing officer in the State of Connecticut Department of Revenue) indicated, "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. We directed the individual to our special investigation section." The same observation has been made by German investigators: "Till manufacturers confirm that customers enquire about such [sales suppression] functions [in ECRs], and that they influence customer purchasing decisions." See the German Working Group on Cash Registers, *Interim Report*, March 16, 2005, citing BRH comments 2003, no. 54, Federal Parliament circular 15/2020, November 24, 2003 (original, in German, and translation on file with R.T.A.).

[18] The economics of where the money from skimming goes is difficult to assess. It most likely depends on the personal motivations of the fraudster. For example, in the skimming fraud at Aleef Garage newsstand/convenience stores in the United Kingdom, the skimmed funds went to under-the-table payments to more than 250 workers. Because regular wages were very low, allowing employees to qualify for welfare, cash from skimming became a necessary supplement for worker retention. HM Revenue & Customs, "Company Directors Jailed for £5 million Fraud," *News Release*, November 13, 2007 (online: http://nds.coi.gov.uk/clientmicrosite/Content/Detail.aspx?ClientId=257&NewsAreaId=2&ReleaseID=330199&SubjectId=36). Then

the anticipated workability and effectiveness of the SRM solution by contrasting it with solutions adopted or under development in other jurisdictions.

We will first present a rough schematic of how a zapper facilitates a skimming fraud. Then we will consider three rules-based enforcement approaches—the Greek "fiscal electronic devices" (FEDs), the Quebec SRMs, and the German "smart cards." Next we will examine the Dutch principles-based approach, which is also favoured by the United Kingdom. Finally, we will consider how CSPs in an SSUTA framework could be used to achieve similar outcomes under a blended rules-based/principles-based approach. Comparisons will be made throughout.

SCHEMATIC OF SKIMMING WITH ZAPPERS

There are six basic steps that occur in a sales transaction when a customer makes a cash purchase from a business using an ECR:

1. A consumer identifies goods or services for purchase.
2. A cashier, waiter, or other sales associate creates a pro forma bill[19] and presents it to the consumer for approval.[20] (This step is not always present.)
3. The consumer approves and offers to pay in cash,[21] and the pro forma bill is finalized (agreed upon).
4. The cashier "rings up" the sale in the ECR, which generates an itemized record of each good or service sold.

again, as noted above, in the La Shish fraud in Detroit, a zapper was used to skim cash and (allegedly) send it to fund Hezbollah terrorists in Lebanon. United States, Department of Justice, Eastern District of Michigan, "Superseding Indictment Returned Against La Shish Owner," *Press Release*, May 30, 2007 (online: http://www.justice.gov/tax/usaopress/2007/txdv072007_5_30_chahine.pdf). In yet another instance, this time in the Australian case *Regina v. Ronen and Ors*, 2005 NSWSC 991, the zappers installed in a used-clothing store provided funds that were wired to the owner's personal overseas bank accounts.

[19] This may occur by scanning a bar code, directly entering a PLU (price look up) number, or entering the name of an item (perhaps by pressing a touch screen).

[20] In a restaurant, if a customer orders directly (and only) from the menu presented by the waiter, the pro forma bill may be first drafted in pencil and then transferred to a digital ordering system associated with the ECR. In other instances, a customer may initially order a drink and an appetizer and then place additional orders for food and drink throughout the evening. The waiter will keep a running tally of the bill. It would be common in this case to present one or more pro forma bills at various times to keep the customer aware of the total amount due.

In a grocery store context, an itemized pro forma billing is frequently visible on an LCD screen that the cashier and the customer can see as items are run through a scanner. Some supermarkets today equip their shoppers with a hand scanner to pre-scan all purchases before arriving at the checkout. All modern ECRs have the capability to present this pro forma bill both formally and informally. The important point is that the pro forma bill can be changed before the sale is "rung up." Changes occur as a result of the customer and the operator acting in concert.

[21] Zappers target cash sales because credit, debit, cheque, or bank transfer transactions leave an audit trail.

5. The ECR then directs the printer to issue a paper receipt (invoice) for the customer. Under the SRM (and other fiscal till systems), this is to be a very detailed receipt, which will include
   a. a list of the items purchased;
   b. a price for each item;
   c. a taxability determination for each item;
   d. a segregated tax amount for each of the taxed items (in instances where all items at an establishment are taxed, and taxed at the same rate—as they would be at a restaurant, for example—this function will be performed in aggregate);
   e. the amount of cash tendered;
   f. the net amount returned to the customer in change;
   g. the date and time of purchase;
   h. the name, address, and identification number of the vendor; and
   i. the receipt (invoice) number of the transaction.
6. At the end of the day, a series of electronic reports is generated, based on transactions sent through the ECR.[22] These reports are relied on by compliance auditors. The reports are
   a. the daily Z report (with reset functionality);[23]
   b. the X report;[24] and
   c. the electronic journal.[25]

[22] It is important to note that the fraud we are addressing is a "backroom" issue. We are not so much concerned with the falsification of immediate real-time records as with the alteration of records at the end of the day. See infra note 26 and the related text for further details of this practice.

[23] One of the most important functions of a cash register is to record the details of daily transactions—sales, taxes collected, media totals, discounts, voids, and more. The report printed at the end of the day or shift that contains this information, and resets the record 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 report is a once-only report for a set period of time. Many cash registers have a Z2 feature that allows Z reports to be added together. When an operator "Z2's them out," these reports are erased 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.

[24] X reports are identical in information and time span to 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.

[25] See "Cash Register Good Practice Guide," supra note 6, appendix G, at paragraph 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 report—it is not a recap of the day's sales. The electronic journal tape is supposed to be a continuous, step-by-step record of every transaction made. 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 electronic cash register industry since the beginning. It can be used to check the Z report.

If, after step 6, a zapper is inserted in the ECR, or in the point-of-sale (POS) system, a seventh step is added to the sequence. The zapper allows the user to eliminate from the ECR and the enterprise's business records all traces of (some or all) cash sales without fear of leaving a digital record of the manipulation (assuming the absence of an anti-fraud device). Phantomware applications would do the same thing, except that their programming is embedded in the ECR's operating system, not temporarily added and then removed from the ECR.

At this point, the customer has in his hands an accurate receipt (from step 5), but (at the end of the day) the zapper will rewrite the internal memory of this receipt in the ECR—including the records in the Z report, the X report, and the electronic journal. This rewriting creates a new sales profile within the ECR. Selected cash sales are omitted. For example, in ticket files (the digital record of specific invoices issued in sequence), the file would be renumbered if an entire ticket were eliminated. If only some items are removed from some tickets, or if the price of an item is changed on a specific ticket, the amounts due will be recalculated (and a new tax due determined). The altered ticket files will now confirm the altered Z report, X report, and electronic journal. The ECR's records will not match customer receipts, but the records of the ECR will be internally consistent.[26]

Thus, one of the common (traditional audit) approaches to detecting a zapper is for an audit team to visit an establishment suspected of using a sales suppression device (in advance of the audit), make cash purchases, save the receipts, and then try to match the receipts with the digital files in the ECR. This is in fact how Revenu Québec uncovered its first zapper in 1996.[27]

The next thing to notice is that it is easy to skim sales without zapping. This can be done at step 2, but it requires collusion between the vendor and the customer. A consumer tendering cash could be orally offered a lower price (perhaps a tax-free

[26] Anti-fraud technology such as Quebec's SRM and Germany's smart cards (discussed below) is not designed to eliminate all skimming but only to preserve the records of the transactions that make it to step 5. The problem of the zapper has not been the real-time skimming fraud that occurs at the cash register as the customer pays, but the fraud that occurs in the backroom after the restaurant has closed for the evening. At this point, the zapper goes in and manipulates the records to allow the fraudster to make them look "good." There is commonly some strategy that the fraudster uses to make receipts normal. Thus, a zapper would be used on a night when an exceptionally large amount of cash had been taken in. If the average daily cash take was, say, 1,000 euros or dollars, and in one day 10,000 was received, then it would be a good target day for a zapper. However, a day when cash received was low (500, for example) would not be a good target day. Information provided in personal e-mail communications with Marc Simard, September 15, 2009 and Norbert Zisky, November 18, 2008 (both on file with R.T.A.). Marc Simard is the directeur de la recherche en technologies liées au contrôle fiscal, Revenu Québec; Norbert Zisky is with Germany's National Metrology Institute, or PTB (Physikalisch-Technische Bundesanstalt).

[27] Ainsworth, "Zappers and Phantomware: Are State Tax Administrators Listening Now?," supra note 16, at 104, note 5.

price) when the pro forma invoice is drafted. If the customer agrees, the sale is simply not "rung up." As a result, no record of the actual (finalized) transaction will appear in the daily Z report or the X report.

It is possible that the electronic journal might preserve a "trace" of the original transaction (if the pro forma was drafted with the assistance of the ECR). The transaction would appear as an aborted sale. It would look to the auditor as if the customer had declined the purchase when she saw the pro forma invoice. In a restaurant context, multiple aborted sales might raise suspicions, because normally the meal would already have been consumed. However, in a grocery or convenience store, a hairdresser's, or a butcher's shop, where the custom might be to discuss a transaction based on a pro forma invoice, aborted sales might not suggest that anything is amiss.

Some fiscal till jurisdictions try to block frauds at step 2 by preserving each keystroke in the electronic journal. These jurisdictions certify each ECR. Tamper-proof electronic journals are made a requirement of certification.

Another thing to notice is that there is a period of time (after the sale is completed at step 3 and before the zapper is inserted) when the records within the ECR are complete and accurate. This period lasts at least up to step 5—the point where the ECR directs the printer to issue an invoice for the customer. These records need to be accurate because the customer will demand an accurate invoice.

As a result, many fiscal till jurisdictions focus on preserving tamper-proof invoices, and the sequencing of those invoices at step 5. This is what the SRM does. The SRM makes every receipt useful for checking the ECR. For example, even a credit card transaction (which was not tampered with) can provide evidence of manipulation, if an auditor can tell that the receipt was renumbered. The SRM will indicate that some other receipt further up the chain is missing, and an auditor would then begin the search for the missing cash transactions.

Principles-based jurisdictions focus on this same point, step 5, but they need to directly find an altered receipt. Without an SRM (or similar device that uses select data on the receipt to derive a signature that is printed on the receipt), it is difficult to tell if a sequence of receipts has been manipulated. This makes pre-audit cash purchases and saved receipts a critical component of a principles-based auditor's workplan. Traces of a zapper can also be found by computer specialists examining the electronic journal as well as the X and Z reports produced at step 6.

A final thing to notice is that all critical elements of the tax return (at least all elements that would be derived from a specific ECR) are available at step 5. The items purchased (step 5a), the price charged (step 5b), the taxability determination (step 5c), and the tax collected per item or per invoice (step 5d) are all available. In addition, the customer has paid the tax.

Thus, it is entirely possible that fiscal till jurisdictions could require real-time pro forma returns based on these figures. They could also require real-time remission of the tax. In a retail sales tax jurisdiction, the vendor might be required to remit the entire return and payment. In a value-added tax (VAT) jurisdiction, the remittance would represent only the output portion of the return. The input VAT credits (deductions) would need to be gathered from other files.

FISCAL TILLS: GREECE, QUEBEC, AND GERMANY

In addition to Greece, Quebec, and Germany, fiscal till jurisdictions include Argentina, Brazil, Bulgaria, Italy, Latvia, Lithuania, Poland, Russia, Turkey, and Venezuela.[28] The discussion that follows sets the Greek and German regimes alongside Quebec's SRM in order to illuminate the attributes of this new anti-fraud technology.

Greece: Fiscal Electronic Devices (FECRs, AFED Printers, and FESDs)

Greece has had comprehensive, rules-based fiscal till legislation in place for over 20 years. Technical specifications for fiscal electronic devices, or FEDs, were published widely in 2004.[29] When considered as a whole, these rules attempt to provide data security at both step 2 and step 5 of the transaction sequence. In other words, the Greek approach is to secure data when the pro forma receipt is being generated, and when the printer is being directed to issue the final receipt.

Under Greek rules, FEDs are divided into two categories: (1) fiscal electronic cash registers (FECRs), which are accompanied by autonomous fiscal electronic device printers (AFED printers); and (2) fiscal electronic signing devices (FESDs). The first are used *only* in B2C transactions; the second may be used in either B2C or B2B transactions. Both preserve digital "fingerprints"[30] of data from tax-related documents.

[28] See "Cash Register Good Practice Guide," supra note 6, appendix D, at paragraph 1.

[29] A European directive (98/34/EC of June 22, 2998) requires that whenever a member state adopts new technical rules, specifications, or legal requirements, that state is obliged to announce this to the European Union before the rules take effect. According to this directive, there is a minimum standstill period of three months. During this period, any member state (or the European Commission) has the right to express a "detailed opinion." The issuance of a detailed opinion extends the standstill period for another three months, allowing for 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 European Union but also among the larger community of ECR manufacturers and distributors. The rules are available in Greek and in official translations in English, French, and German, and can be accessed on the Internet: "Codification of/Addenda to Technical Specifications for Inland-Revenue Approved Registers and Systems (Operating Procedures)" (online: http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=pisa_notif_overview&iYear=2004&inum=135&lang=EN&sNLang=EN).

[30] At this point, it is necessary to define two key terms in the language of cryptography: "digital fingerprint" and "digital signature." A digital fingerprint is a string of characters computed with a cryptographic (or open mathematical one-way) function applied to a particular set of data. It is of constant size (20 bytes is common) and collusion-resistant (that is, it is very unlikely that two data sets with the identical fingerprint can be found). A digital signature is different. It is computed by a cryptographic function that is applied to the digital fingerprint; thus, it is a step removed from the original data. In addition, a digital signature makes use of a private key (known only to the entity computing the signature) and a public key (available to anyone). Anyone can take the public key and use it to determine whether the entity used the corresponding private key to create the digital signature.

It is important to recognize this distinction because the Greek system (in formal documents, names of equipment, and public presentations) frequently uses the term "signature" in reference

FECRs and AFED Printers

"Fiscal electronic cash register" is a term that includes ordinary stand-alone cash registers and cash registers equipped with advanced connection capabilities (network or PC-operated machines). "Autonomous fiscal electronic device printers" are fiscal printers that operate only via a connected computer. They have no keyboard or display terminal. They do more than just print receipts, however. AFED printers store and secure in their fiscal memory the data that have passed through them (revenue from sales, taxes collected, etc.).[31]

to the production and storage of digital fingerprints. Thus, the FESD (fiscal electronic signing device) produces and stores digital fingerprints, not digital signatures, although the name of the device might suggest otherwise. Greece's contribution to the "Cash Register Good Practice Guide," supra note 6, appendix D, at paragraph 4.2.15, uses both terms interchangeably:

> The FESD receives this data, processes it with a special security algorithm (SHA-1) that creates a hash value (*sign*) and sends the result of this processing back to the connected computer. The hash value, which represents a sequence of characters and digits is the unique electronic *digital "fingerprint"* of the data of the slip being issued. Furthermore the FESD saves this hash value into [its] own working daily memory and issues a relevant slip. . . . The supporting software of the FESD which is located in the connected computer receives this "unique summary—*signature*" i.e. hash value and prints it along with the other data of the issued slip. . . . [At] the end of the day the FESD processes all the stored hash values of the working daily memory, produces a general daily hash value of all "summaries—*signatures*" of the day, issues a "Z" day report slip, on which the general day hash value is written. . . . The computer software receives this unique general "day summary—*signature*" hash value and saves it in a special electronic file. . . . [There is also] a Daily Fiscal *Signing* Record Report Slip—"Z" (DFSRRS) [and] Daily Summary—*Signature* Slip—(DSSS) [emphasis added].

See also the PowerPoint presentation of Panos Zafiropoulos at the November 2007 EU Fiscalis Exchange Program, "Safeguarding Electronic Tax Data: Data Locking, 'Fiscal' Electronic Signing Devices," 3, 7, 8, and 10 (on file with R.T.A.) (discussing the "e-sign" process, "previous day whole signature," "day whole signature," "formation of the signature string," "signature string (trace)," and "safeguarding e-signature traces," where in each instance the discussion is about digital fingerprints, not digital signatures); and "Codification of/Addenda to Technical Specifications," supra note 29, paragraphs 5.5 and 5.8 (statutory discussion of "signing" process, but meaning "fingerprinting") in the same context as above. Panos Zafiropoulos represents the Greek revenue authority on the Fiscalis Committee's Cash Register Project Group. See infra note 32 and the related text for further explanation of the secure hash algorithm (SHA-1).

[31] The FECR and AFED printer must be equipped with either a two-roll paper printing station, or a one-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 programmable ROM—read only memory—(EPROM or PROM) chip that is securely placed within the fiscal cash register. It is in this memory that all important fiscal data are stored. EJ memory is either pluggable/unpluggable or fixed. It resides in the fiscal device and is always a flash memory. See "Codification of/Addenda to Technical Specifications," supra note 29, at paragraph 2.11. In a personal e-mail communication, August 10, 2009 (on file with R.T.A.),

A digital fingerprint of the data from the electronic journal memory (EJ memory) is computed with a secure hash algorithm (SHA-1).[32] This hash value is permanently safeguarded[33] and stored in the fiscal memory. Daily sums (receipts and VAT amounts) are saved into the fiscal memory, cumulatively and on a daily basis. This function essentially preserves the X and the Z reports along with the electronic journal with digital fingerprints.[34] Disconnecting any Greek device (in an effort to prevent a transaction from being recorded, or to switch devices) will seal the device

Panos Zafiropoulos confirmed, "The type of fiscal memory is ROM based, but what it [sic] is used is [a] One-Time Programmable (OTP) ROM or UV Erasable Programmable (EP) ROM chip. This is why this chip shall be protected and covered by special epoxy glue, in such manner that [it] is impossible to take it out (or replace it) without breaking/destroying the case cover (the enclosure) of the Fiscal Electronic Device."

Security for the fiscal memory is provided by placing the circuits in a special box that is placed in a specially modulated receptacle; the box is an integral part of the machine. As described by Zafiropoulos, this fiscal memory box is clamped and sealed with an epoxy resin in such a way that removal of the tax memory box is impossible without destroying the cover. The preservation of data is independent of any power source. "Cash Register Good Practice Guide," supra note 6, appendix D, at paragraphs 4.1, 4.2.14, and 4.3.6; and "Codification of/Addenda to Technical Specifications," supra note 29, at paragraphs 2.11.4 (including a technical diagram of the sealed box) and 2.17 (specifying the casing, casing elements, and casing seals).

[32] The secure hash algorithm (SHA-1) was developed by the US National Institute of Standards and Technology. SHA-1 is a widely accepted cryptographic hash function. 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, these data are the values on the printed receipt). SHA-1 is described in detail in the *Federal Information Processing Standards Publication* 180-2, "Announcing the Secure HASH Standard," August 1, 2002 (online: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf).

[33] "Cash Register Good Practice Guide," supra note 6, appendix D, at paragraphs 4.3.1 and 4.3.2, specifies the physical security precautions taken:

> **4.3.1. Special security screw**
>
> Access to the inside of the FCR [fiscal cash register] is protected by a special security screw connecting the upper part of the FCR with the lower part. This screw is fitted in a . . . part of the mechanism cover [that is visible to the client]. Access to the inside of the FCR is impossible without the removal of the protective screw. For the sealing a designated material is used (ex. Lead seal), which does not tolerate scrapings and it is carried out in such a way as to make [it] impossible to remove it without destroying it.
>
> **4.3.2. Authorized technicians - Access control code**
>
> Opening and re-sealing can be carried out only by an authorized technician of the suitability license holder, employed for the repairing of malfunctions. The FED firmware controls, through a *special algorithm—access code-password*, the access of authorized technicians to it [emphasis in original].

[34] See ibid., appendix D, at paragraph 4.2.15, discussing the daily fiscal signing record report slip—"Z" (DFSRRS) and the daily summary—signature slip (DSSS). See also, ibid., a discussion of the periodical summary of memory reading slip (PSMRS), which is also preserved: "Note: The keeping of the stored filed of required data of the signing process is regulated by the same conditions as the keeping of the electronic journal, mentioned earlier." Note that the reference to "the signing process" should instead read "digital fingerprinting process."

in less than 30 seconds; an illegal receipt message will print and will be recorded on the tax data Z register; and after 10 disconnect/reconnect efforts, the device will automatically shut down.[35] This process ties in closely with a penalty regime (applied against manufacturers/distributors of ECRs and retailers) that aims to deter the sale or use of uncertified devices.[36] An authorized technician with an access control code will be needed to restore the device.[37]

The cost of FECRs varies from €200-250 to €800-1,000, depending on the manufacturer.[38] Every manufacturer, developer, or importer of an ECR into Greece must seek approval for each specific model that it intends to sell in the Greek market.[39] A licence to sell a specific ECR is issued by a special technical (interparty)[40] body (committee) and will be issued only when the ECR conforms to all statutory technical specifications.[41] 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 licence is sought. The committee has the authority to examine any additional data (including experience in the field, business solvency, creditworthiness, and the technical capacity of personnel), and the authority to recall and cancel licences in cases where material changes have been made in systems or in the conditions under which the licence was granted.

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

[35] "Codification of/Addenda to Technical Specifications," supra note 29, chapter 3, at paragraph 7.10, disconnection (discussing blocking of the device [7.10.2]; records of the disconnection retained [7.10.3]; the less-than-30-seconds rule [7.10.4]; what happens to a transaction that is in process when the disconnection occurs [7.10.5]; and records kept in the Z register [7.10.6]).

[36] "Cash Register Good Practice Guide," supra note 6, appendix D, at paragraph 4.2.1.

[37] See supra note 33, paragraph 4.3.2.

[38] Panos Zafiropoulos, personal e-mail communication, February 24, 2008 (on file with R.T.A.).

[39] 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 and 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 6, appendix D, at paragraph 4.1.

[40] An interparty body under Greek rules is a committee, each member of which 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.

[41] Technical specifications 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 the National Technical University of Athens (NTUA). The NTUA is also assigned by the committee to perform all the necessary evaluation tests on carried samples of FECRs.

a visual inspection of the machine and by matching the licence number on the machine with a given receipt.

FESDs

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

FESDs are designed for B2B applications. They are used primarily to compute a digital fingerprint[42] of critical tax data that is then printed on the invoice. FESDs can be used for any tax document, including a final retail receipt. The FESD is connected to the business's computer system via a dedicated port (RS-232; Ethernet RJ-45; USB). A driver must be installed to allow the computer system to interface with the FESD. Essentially, the FESD functions as a virtual printer, allowing the back-office software (ERP system or accounting software package) to function normally. However, every tax document required to be recorded is diverted through the interface to the FESD, where a digital fingerprint is created (the SHA-1 algorithm is applied) and a fingerprint is transmitted to (and printed on) each document. The whole-day fingerprint is permanently saved in the FESD's fiscal memory.[43] This preserves all data on the document in detail.[44]

Currently, the cost of an FESD is between €450 and €650; thus, an FESD alone can cost more than an FECR. For this reason, smaller businesses do not normally use FESDs to issue legal receipts.[45] 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 POS terminal.

An FESD owner is obligated to preserve fingerprinted 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 a new fingerprint against the existing ones secured within the FESD's fiscal memory.

[42] "Cash Register Good Practice Guide," supra note 6, appendix D, at paragraph 4.2.15, discussing this process as "signing" the receipt, by which it means that the fingerprint is being attached to the invoice. The PowerPoint presentation by Zafiropoulos, "Safeguarding Electronic Tax Data," supra note 30, at 2, 3, 7, and 10, describes this as an e-signing process.

[43] From a hardware and a security perspective, there is very little difference between an AFED printer (with an electronic journal) and an FESD.

[44] Panos Zafiropoulos, personal e-mail communication, February 24, 2008, item D (on file with R.T.A.).

[45] In an effort to mitigate the cost of FESDs, the tax law allows owners to depreciate these devices as fixed assets over three years. There is also a government loan program to assist in the purchase of all FEDs (FECRs, AFED printers, and FESDs). The interest on these loans is subsidized at 3 percent.

How FECRs with AFED Printers and FESDs Defeat Zappers and Phantomware

Because FECRs are certified for compliance with all technical specifications set out in Greek law—a law that is supported and updated regularly by the research laboratories of the National Technical University of Athens—it is a very simple matter to determine whether a specific ECR has been tampered with.

Factory-installed phantomware must be removed before certification. If a self-help version of phantomware[46] is on the ECR, either it will be blocked, or there will be a record of the manipulation so that its impact on revenues will be neutralized. Only true data from real transactions will be preserved and fingerprinted with SHA-1 in the fiscal memory. Use of an add-on zapper will be a violation of the licensing regulations. It will be detected in the same manner as self-help phantomware. Severe penalties apply, but detection does require an audit.

Through the certification process,[47] the Ministry of Finance preserves a copy of all approved firmware. According to the ministry,[48] it is a simple matter to calculate a checksum value (CRC-32[49] 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

[46] For a discussion of self-help phantomware, see Ainsworth, "Zappers and Phantomware: The Need for Fraud Prevention Technology," supra note 16.

[47] Over 400 different types of ECRs and POS systems have been certified to date: Panos Zafiropoulos, personal e-mail communication, May 28, 2008 (on file with R.T.A.). The certification process means that

> a fiscal cash register and its functionality is compliant with the given set of technical requirements, [and that it has been] tested and finally approved. A copy of its firmware (the object code) is laid down during the approval process. A checksum value (CRC-32 or SHA-1) is also calculated for the object file of that firmware.
>
> Anyone whenever he wants (let's say an auditor for audit purposes) can read the content of the program memory of a tested machine and easily understand if there are any changes comparing it with the object file which is originally kept in the competent department. This is a process that of course can be done, but requires a little bit more [effort] and more qualified staff.

Panos Zafiropoulos, personal e-mail communication, July 22, 2008 (on file with R.T.A.). The requirements for the testing are set out in the "Codification of/Addenda to Technical Specifications," supra note 29.

[48] Panos Zafiropoulos, personal e-mail communication, July 22, 2008 (on file with R.T.A.).

[49] 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 and D.T. Brown, "Cyclic Codes for Error Detection," (1961) vol. 49, no. 1 *Proceedings of the Institute of Radio Engineers* 228-35. Although CRC-32 may not be fully secure, because the same hash value could be generated with different data, circumventing the CRC is probably (1) beyond the technical skill of most

determine whether changes have been made in the firmware (through phantomware 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 phantomware applications nor zapper installations are effective when an FESD is installed. The FESD will fingerprint each document and preserve a trace in the fiscal memory of the device. Deletion or manipulation of the records associated with cash receipts is no longer possible without detection.

Thus, if a Greek vendor produces a pro forma receipt through an ECR, the details of the receipt will be recorded in the electronic journal. If the ECR is an FECR, these data enter the electronic journal, and when the AFED printer is set up to capture the data, they will be fingerprinted with a secure hash algorithm (SHA-1). This feature makes it possible to identify enterprises that have routinely offered customers lower prices in exchange for voiding the pro forma invoice at step 2. This would not be possible with FESDs. FESDs are virtual printers, and if data are not being sent to a printer, an FESD will have no need to e-sign it.

Both of the Greek solutions are very effective at step 5 enforcement. If a receipt is printed, both the FECR with an AFED printer solution and the FESD solution will assure tax authorities that the tax collected on cash transactions has been recorded. It is important to note, however, that all of these efforts are directed only at accurate record retention. Returns must still be prepared and filed, and payments remitted for the taxes due or collected, and the revenue authority still needs to audit to ensure compliance. Admittedly, this audit should be easier, but it is still needed.[50]

SMEs, and (2) very high risk for the manufacturer, who would find that all machines already sold and installed in Greece would lose their certification.

Exclusive reliance on the CRC-32 may not be well placed today. The CRC-32 was designed to deal with noise in transmission channels. It was not designed to deal with malicious people (see, for example, Axelle Apvrille, "Trash CRC32," June 9, 2009, *Fortiguard Blog* (online: http://blog.fortinet.com/tag/crc32/). Given the CRC-32 value of a particular firmware, it is easy to produce some other (maybe malicious) firmware with the same CRC-32 value. For example, the Web site for *CRC32 Compensation Tools/Library* (online: http://www.cr0.org/progs/crctools/) offers a tool that takes a file (for example, malicious firmware), an offset in the file, and a target CRC-32 value (for example, CRC-32 value of certified firmware). If we take the value returned by the tool and insert it into the file at the given offset, the CRC-32 of the file will now equal the target CRC-32 value.

Considering the availability of these tools, the Ministry of Finance should not believe that an attack is beyond the skill of most SME owners. Even if this were the case, the owner would not have to perform this attack himself; there could be a third-party supplier with the technical expertise to make and install the malicious firmware. Thus, using only the CRC-32 for ensuring the integrity of the firmware is not secure. However, the Ministry of Finance also has a copy of the actual firmware, not just its CRC-32 value, on file. The ministry should always compare the firmware itself. For SHA-1, comparing the fingerprints is sufficient. In addition, physical anti-tampering mechanisms used by the Greek ministry make it difficult for a third party to replace the firmware.

[50] See Zafiropoulos, "Safeguarding Electronic Tax Data," supra note 30, at 12.

Quebec: SRMs

Quebec is responding to sales suppression fraud much as Greece has responded, but on both a more limited and a technologically more sophisticated scale.[51] Where the Greek solution is based on digital fingerprints, Quebec goes further and provides data security through digital signatures. Quebec has determined that technological assistance is necessary because there are not sufficient audit resources to handle the estimated 500 new cases each year, involving close to 10,000 delinquent vendors.[52]

Compared with the Greek approach, the Quebec solution (set to be fully rolled out between 2010 and 2011) is limited in two respects: (1) its scope is limited to the restaurant sector, and (2) its range is limited to an FESD-like solution. Quebec has specifically rejected the "FECR with an AFED printer" type of solution.[53] Like Greece, Quebec approaches the sales suppression problem from an adequacy of business records perspective. But also like the principles-based jurisdictions (the United Kingdom and the Netherlands), Quebec supplements technology solutions with very aggressive traditional audits.

The first major legislative response to zappers in Quebec came in June 2000, when bookkeeping and record-keeping requirements were enacted specifying that electronically stored data, together with the means to read such data, formed part of a Quebec business's regular bookkeeping obligations.[54] Because zappers make digital records unreliable, it was then easy to specifically prohibit the design, manufacture, installation, sale, or lease of zappers in the province.[55] The latter is a presumption-of-use rule: it provides that whenever Revenu Québec finds a zapper, it is allowed to presume that the zapper was used to suppress sales.[56]

The business records that Quebec was primarily concerned about were the Z and X reports and the electronic journal, as well as all of the digital supporting files that

[51] Quebec performed two empirical studies of the zapper problem. The first was conducted soon after the June 2000 legislative reforms came into effect. It was a "bookkeeping and records" audit conducted on 70 enterprises. It uncovered 41 zappers. Soon thereafter, the second, more scientific study ("Tax Evasion in Quebec," supra note 4) was conducted. The use of statistical sampling techniques made this second study more accurate and authoritative. Dave Bergeron, personal e-mail communication, June 6, 2008 (on file with R.T.A.). Dave Bergeron is an IT specialist who, since 2000, has been working on zappers as part of a specialized audit unit at Revenu Québec.

[52] Gilles Bernard, "Solution for the Under-Reporting of Income in the Restaurant Sector, 2," PowerPoint presentation at the Federation of Tax Administrators Annual Conference held in Denver, Colorado on June 2, 2009 (on file with R.T.A.).

[53] The alternative of certifying ECRs and mandating the use of a device similar to an AFED printer was considered and expressly rejected for cost (as well as other technological and enforcement-based) reasons. Personal e-mail communications from Dave Bergeron, November 18, 2008 and Marc Simard, September 15, 2009 (both on file with R.T.A.).

[54] Act Respecting the Ministry of Revenue, RSQ, c. M-31, sections 34 and 35.

[55] Ibid., section 34.2.

[56] Ibid., section 34.1.

were kept in an ECR or POS system. These are the records that reside within an ECR at step 5. They are presumed accurate because these records are the basis of the data sent to the printer to produce the customer's receipt.

This brings Quebec to the place where all fiscal till jurisdictions end up—the legislatively defined "legal receipt." The legal receipt is the central enforcement document in all fiscal till jurisdictions. Quebec is no exception; it requires that all restaurant sales must be accompanied by a receipt, and then further specifies that this receipt must pass through the SRM, where it is e-signed.[57]

Penalties for not issuing a legal receipt are serious. Quebec's 2006-7 budget summarized the penalties as follows:

> 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.[58]

The legal receipt can be a very effective tool against skimming by collusion with the customer (step 2 skimming). If an establishment conspires with its customers to charge a lesser amount in exchange for engaging in cash transactions unaccompanied by a formal receipt, the restaurant operator is in violation of the legal receipt rule. If surveillance detects the fraud, penalties will apply. There is a variant of this fraud that is troubling, because it does not involve direct collusion with the customer; instead, the operator or owner produces Xeroxed, scanned, or otherwise duplicated valid receipts.[59] These remain among the frauds that can only be detected (at present) by traditional audits, and they are the reason for the high monetary penalties attached to the failure to provide a legal receipt.

For example, if a pizza shop's most common order is a single large pepperoni pizza, it would be possible to issue one receipt for this pizza early in the day (the ECR would print the order, price, tax, date, time, and name of the establishment correctly). If this receipt was reproduced and given to every customer who ordered the same pizza that day (without ringing each subsequent sale through the ECR), the cash received could be skimmed and the customer would have an apparently valid

[57] RSQ, c. T-0.1, section 425. The requirement for legal receipts is found in several other fiscal till jurisdictions, including Hungary, Greece, Finland, Portugal, Denmark, and Latvia. See "Cash Register Good Practice Guide," supra note 6, appendix A, at paragraphs 1.3.1.1 to 1.3.1.5, and appendix D, at paragraphs 3.2.1 and 4.2.6.

[58] Québec, Ministère des Finances, 2006-2007 Budget, Additional Information on the Budgetary Measures, March 23, 2006, 145.

[59] Bernard, supra note 52, indicated that "[i]f the signed invoice is returned to the POS, it is possible to develop a program that re-uses signed invoices in specific circumstances. The net effect is equivalent to using a Zapper."

receipt. The telltale sign of this fraud is the time code on the receipt. An auditor suspecting this fraud would need to order a pepperoni pizza at, say, 5:00 p.m. and notice that the receipt indicated a sale at 8:00 a.m. If the receipt passed through the SRM, it would also have apparently accurate bar codes—although Revenu Québec indicates that a hand-held scanner (discussed below) will be able to check for this fraud by comparing time stamps.

Revenu Québec unveiled its plans for the SRM pilot project in January 2008. A prototype was demonstrated at the annual conference of the Federation of Tax Administrators (FTA) in Denver, Colorado on June 2, 2009.[60] The pilot program began in November 2009. Participating restaurants must install the SRM microcomputer between their ECR or POS system and receipt printer.[61] The SRM will receive data[62] from specified transactions (the drafting of guest checks, register receipts, or credit notes). From the extracted data the SRM will produce a digital fingerprint and a digital signature of the fingerprint, which will then be transmitted to the printer.[63] Hand-held readers (used by auditors) do not use public key infrastructure (PKI)[64] to

[60] Physically, the prototype SRM was a relatively small (2 × 1 × 6-inch) metal box, connected to the printer and the ECR by standard cables.

[61] Participation in the pilot project is voluntary. After the pilot project has ended, mandatory installation of the device in restaurants throughout Quebec will take place gradually during 2010 and 2011.

[62] Revenu Québec will not disclose the data elements that are selected for signing. This information is "confidential for security reasons." Marc Simard, personal e-mail communication, August 10, 2009 (on file with R.T.A.).

[63] In a personal e-mail communication, August 7, 2009 (on file with R.T.A.), Marc Simard explained:

> In addition to ensure the integrity of the information presented on the receipt, the solution designed by Revenu Québec ensures that the bar-code scanned by the [hand-held] reader is produced by the certificate delivered by [Revenu Québec] to the specific MEV [SRM] which generates this signature. The signature is produced by a combination of SHA-256 and ECC-224.
>
> This method uses a certificate which includes a public and a private key issued for each MEV [SRM] with information that identifies the MEV [SRM] and the restaurant.
>
> We choose the elliptic curve algorithm (ECC) to reduce the length of the result (to be converted to a barcode) and to maintain a good strength. The efficiency of ECC is well-known, since it provides similar cryptographic strength as RSA but uses shorter keys. For our case, ECC with a 224-bit key size provides similar strength to RSA with a 2048-bit size (see NIST-800-57 http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf).

[64] Public key infrastructure (PKI) is a set of hardware and software procedures used to create, manage, store, distribute, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority. The user identity must be unique for each certificate authority. The binding is established through the registration and issuance process, which, depending on the level of assurance that the binding has, may be carried out by software at the central authority, or under human supervision.

verify that any receipt under question was actually produced by a specific SRM (as does the German solution).[65] With the SRM, it is the "SRM certificate" that performs this function.[66]

The digital signature will then be printed on the receipt from which it was derived. The digital signature, the digital fingerprint, and the recorded data will all be preserved within the fiscal memory of the SRM for seven years.[67] Restaurants will be required to submit sales summaries, generated by the SRM, when they submit their tax declarations.

The Quebec government believes that the SRM will

- permit restaurant [patrons] to verify that the taxes they pay are properly recorded and assure them that these funds will be remitted to the State;
- facilitate the intervention of Revenue Quebec in cases where a receipt is not issued or recorded [step 2 skimming] or where attempts are made with zappers or phantomware to manipulate the data on the receipt [step 7 skimming];
- allow Revenue Quebec to easily verify whether or not a specific receipt has been recorded;
- 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.[68]

A critical difference between the Greek and the Quebec approaches is that under the Greek system, it is not necessary to have multiple FESDs in an establishment that networks multiple ECRs—a grocery store or a large restaurant, for example. Although a single SRM might have been used in a similar manner, to e-sign receipts for multiple ECRs, this was deemed to be a security risk by Quebec authorities. Thus, an SRM has a one-to-one relationship with the receipt printer (but not necessarily with each

[65] The value of the hand-held reader to auditors cannot be overestimated. When Quebec's use of a bar-code scanner was demonstrated in June 2009 at the FTA's annual conference, the response of the German representatives, for example, was very positive. Subsequent correspondence suggested that Germany may emulate this technique:

> In our [Germany's] solution we print the digital signature [on] the receipt. If you want to verify the receipt you have to type all data of receipt including the signature [into a PC]. It takes a long time because you will make input errors. [If] . . . you test it, you will find out that this is not a good practice. . . . I [have used] a pencil scanner. . . . It works [well] and you are much faster. You can also use a normal scanner with OCR. We are testing different solutions. . . . If we use barcodes we have to have a barcode scanner.

Norbert Zisky, personal e-mail communication, August 10, 2009 (on file with R.T.A.).

[66] "*The MEV [SRM] certificate* [is used] to verify that the receipt was produced by a specific MEV [SRM]. . . . [S]ales summaries are generated and signed by the MEV [SRM]." Marc Simard, personal e-mail communication, September 15, 2009 (on file with R.T.A.).

[67] Supra note 2, slides 6 through 8.

[68] Ibid., slide 12.

ECR).[69] This difference has a significant financial impact when the estimated $650 cost of each SRM is factored into the equation.

Steps have been taken to prevent tampering with the SRM once it is installed. The SRM is physically secure within a sealed metal case that cannot be broken into without leaving a trace.[70] The SRM does not come with a backup power source. Unless restaurateurs already have a backup power source for their ECRs, the SRM will not operate in cases of power outage, and the outage will leave a record of disconnection and reconnection in the SRM. Thus, Revenu Québec will be alerted to conduct appropriate inspections whenever disconnection of the SRM occurs, regardless of the cause.[71]

The Quebec government has promised to shoulder the $55 million cost of providing SRMs to restaurants,[72] but there is no discussion in Quebec about extending SRM applications outside the restaurant sector. This is the case even though automated sales suppression technology is not confined to restaurant fraud.[73] It also appears that very small restaurants may not be required to use SRMs.[74]

[69] Information presented when the SRM was announced (supra note 2, slide 7), showing one SRM connected to either a single ECR or a POS system, was ambiguous in this regard, and did not reflect the intended one-to-one relationship. A personal conversation with Dave Bergeron on August 11, 2008 clarified this point.

[70] We wondered how easy it would be for an auditor to detect a physical invasion of the SRM. There are no publicly available (detailed) responses on this point from Revenu Québec. This question may be too close to the government's security concerns to be answered in great detail, but correspondence with the ministry on this point states that "safety seals [will be used] to detect attempts to physically break into the MEV [SRM]." Marc Simard, personal e-mail communication, September 15, 2009 (on file with R.T.A.). In addition, from appearances (a prototype was made available for inspection at the June 2009 FTA conference), the SRM appears to be very secure. At the FTA conference and other venues, Revenu Québec has been very clear that any attempt to physically break into the SRM will be detected. Similar safeguards have been built into technological solutions adopted in Greece, Germany, and other fiscal till jurisdictions.

[71] With regard to electrical disconnections, what happens if a restaurant simply decides to disconnect the SRM from its power source and make some sales with the printer directly connected to the ECR (bypassing the SRM)? Revenu Québec has indicated that this issue falls into the audit area. With the SRM's ability to detect disconnections, ministry officials feel confident that efforts to defeat the device in this manner will be identifiable; the subsequent reconnection would also be recorded. Marc Simard, personal e-mail communication, September 15, 2009 (on file with R.T.A.). Unlike the Greek system, which will automatically shut down the ECR after it registers a specified number of attempted disconnections and reconnections, the SRM does not appear to do the same.

[72] Supra note 3.

[73] For example, zappers have been found in grocery stores in the United States and the Netherlands, in clothing establishments in Australia, and in hairdressing salons in France.

[74] Supra note 58, at 144-45, indicating that the obligation of a restaurant to use SRMs will be dependent on whether the restaurant is required to remit a receipt to customers. That requirement is not expected to be universal, but instead will likely be defined and limited by regulation.

SRMs, however, are not the end of the story. Quebec's view is that SRMs will not eliminate the need for traditional audit enforcement; rather, the SRM will supplement or extend the traditional audit.[75] SRMs will integrate into traditional audit strategies in three ways:

1. they will be the basis for pre-audit investigation;
2. they will provide for rapid, digitally efficient confirmation of compliance with business record requirements; and
3. they will bring efficiencies to formal audits by standardizing record formats.

With respect to the first item, although immediately after the March 23, 2006 budget speech, inspection of books and accounts continued as before, once the SRM is in place Revenu Québec will accelerate the use of (non-audit) inspection teams.[76] These inspectors are charged with making unannounced visits to restaurants, to inspect books and records and to take backup copies of ECR and POS programs in their search for zappers and other frauds. These teams are made up of an auditor and a computer specialist. With SRMs, these inspectors will be able to more quickly identify the irregularities that would warrant transferring a case for formal audit or criminal investigation.[77]

With respect to the second item, the digital fingerprint and signature envisioned for the SRM is not the same as the alphanumeric hash value (SHA-1) that is printed on the legal receipt in Greece.[78] The SRM prints a bar code that can be read by a pocket computer through an integrated optical scanner. The bar code will immediately verify that a receipt is a "legal receipt," certified by a government-issued SRM, and that both income and consumption tax amounts have been properly recorded in the firm's business records.[79] The hand-held scanner is a critical (and globally unique) tool in Revenu Québec's effort to increase the effectiveness of its audits.[80]

[75] Supra note 2, slide 12.

[76] In *Québec (Sous-ministre du Revenu) c. Paré*, 2004 CanLII 39110 (Que. CA), Revenu Québec inspection teams had used warrants to search for zappers within the Squirrel computerized cash register system to which the defendant held exclusive distribution rights, even though the inspection did not rise to the level of a formal audit.

[77] Richard T. Ainsworth and Dave Bergeron, "Zappers: Automated Sales Suppression," New York Prosecutor's Training Institute, Syracuse, NY, July 31, 2008 (PowerPoint presentation, on file with R.T.A.).

[78] For example, Zafiropoulos, "Safeguarding Electronic Tax Data," supra note 30, at 7, presented the following signature string as a representative example of the e-signing script that would be found on a receipt issued by a Greek FESD: D5A63F82962AB37886F975820883A76415DB614E 0459 00083592 0410030925 EZI03013095.

[79] Supra note 2, slide 12.

[80] Could a complete audit of an establishment be performed with an SRM and a hand-held scanner? Revenu Québec indicates that the hand-held scanner is not intended to be used for this purpose. Marc Simard, personal e-mail communication, September 15, 2009 (on file with

With respect to the third item, the SRM will make traditional audits more efficient by standardizing the data flows from ECRs and POS systems in use throughout the province. It will no longer be necessary to have subspecialists in particular ECRs available to assist Revenu Québec auditors, because the SRM will standardize the data that an auditor will need to download onto a laptop computer in order to perform an audit.[81]

Germany: Smart Cards Embedded in ECRs

The German Working Group on Cash Registers, representing the highest-tier central and regional tax authorities, has been examining automated sales suppression technology (both phantomware and zapper applications) in use in the country. An interim report has been released.[82] The problem is deemed to be serious, and a technological solution is entering the final stages of testing.

The German solution involves storing critical data from sales transactions on smart cards securely embedded in ECRs. The German National Metrology Institute (Physikalisch-Technische Bundesanstalt [PTB]) is the home of the INSIKA project (Integrierte Sicherheitslösung für Kassensysteme—Integrated Security Solutions for Cash Registers). INSIKA began work on prototypes of the smart card solution in 2008.

Papers on digital signatures by Norbert Zisky of the PTB[83] convinced the working group that signing techniques had been sufficiently tested in secure communication

R.T.A.). Simard explains that the SRM (and the scanner) is part of a four-part fraud prevention strategy (based in large part on the determination that the fraud problem is much larger than zappers alone, and that a much broader effort is needed). The four-part strategy comprises the following steps:

(1) The restaurateur is obliged to remit a paper receipt or invoice to the client. This is the key to confirming that an economic transaction has occurred between a business and its customers. In most cases where income is not declared, hidden transactions were not recorded in the electronic cash register (ECR).
(2) Restaurateurs must produce invoices using an MEV [SRM] approved by Revenu Québec, which forces them to keep records.
(3) Revenu Québec will step up its inspection activities to ensure that the two above measures are adhered to. Note that the MEV [SRM] will allow us to redesign and speed up the inspection process and determine more efficiently whether or not a restaurant is complying with the law. Without such inspections, businesses seeking to mask income would simply not [record] transactions in the cash register, regardless of the control mechanisms in place (Greek or German solution, MEV [SRM], etc.).
(4) The general public is made aware of restaurateurs' obligation to remit an invoice to their customers, in order to re-establish fiscal equity and fair competition.

[81] Bernard, supra note 52.

[82] German Working Group on Cash Registers, *Interim Report*, supra note 17.

[83] Norbert Zisky, "Manipulationsschutz elektronischer Registrierkassen und Kassensysteme" ["Manipulation Protection—Electronic Cash Registers and POS Systems"], German Federal Standards Laboratory, Brunswick and Berlin (May 2005) (unpublished draft on file with R.T.A.);

settings with measuring instruments[84] that they could form the basis of a solution to zappers.

The INSIKA project was charged with completing the technical specifications for a signature smart card by the summer of 2008.[85] The work was completed in February 2009. Included with the technical specifications for the signature smart card is a determination of the data structures and formats, communication protocols, and security analysis for the system. The final results of the project were published at

and (March 15, 2004) (unpublished draft, translation on file with R.T.A.). Since these early papers, there have been several modifications to Zisky's proposal. The critical changes include the following:

> 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 [be] 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, February 15, 2008 (on file with R.T.A.).

[84] See Luigi Lo Iacono, Christoph Rulans, and Norbert Zisky, "Secure Transfer of Measurement Data in Open Systems" (2006) vol. 28, no. 3 *Computer Standards & Interfaces* 311-26; and the Secure Electronic Measurement Data Exchange (SELMA) Project (online: http://www.selma-project.de/) (in German). For a brief description of SELMA, see infra note 128 and the related text.

[85] Regarding the timeline for the completion and implementation of the project, Norbert Zisky indicated in mid-summer 2008:

> 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 [of 2008]. 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 [mandatory] use will be January 1st 2012 or 2013.

Personal e-mail communication, July 10, 2008 (on file with R.T.A.).

Further delays were encountered, but by mid-2009 the technical specifications for the smart card were completed and posted on the Internet at http://www.insika.de/ (in German only; an English translation is expected). At about the time that Quebec's SRM will be undergoing a pilot test (November to December 2009), so too will the German smart card. Norbert Zisky, personal e-mail communication, July 22, 2009 (on file with R.T.A.).

the Information Security Solutions Europe conference in the fall of 2009, and are available on the INSIKA Web site.[86]

On the basis of the recommendations of the working group, Vectron Systems AG developed (and is currently demonstrating) a privately developed prototype of the German solution. Under the Vectron prototype, every record that holds sales data (or any other activity performed on an ECR) is secured through a digital summary fingerprint of the main data elements in the ECR. A secure electronic signature is issued for this digital fingerprint based on PKI.[87]

The essence of the German solution revolves around cryptography and smart card access to cryptographic data preserved within the ECR or POS system. If the revenue authority audits, it can access ECR records using a key to read the data and determine whether there has been tampering. As described by Zisky,

> [t]he fiscally relevant data records can be examined both locally and after their transmission over various communication channels[. Processes will be] fully automatic with respect to their integrity and authenticity. For the electronic signature of the revenue [office] 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[s] themselves. . . .
>
> In the case of the marking procedure [the signing 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.[88]

The German solution is a fiscal till solution, but it is far more flexible than the Greek solution. It is substantively similar to Quebec's SRM;[89] however, the German mandate is broader. Where Quebec is concerned with only the restaurant sector, the German proposal is for all ECRs and POS systems to be fitted (at the business's

[86] Mathias Neuhaus, Jörg Wolff, and Norbert Zisky, "Proposal for an IT Security Standard for Preventing Tax Fraud in Cash Registers," paper presented at the Information Security Solutions Europe conference held at The Hague, October 6-8, 2009 (copy on file with R.T.A.).

[87] The German solution does not anticipate that auditors will use hand-held readers, nor will bar codes appear on receipts. Instead, auditors will use laptop computers and enter the alphanumeric code printed on the bottom of a receipt to confirm the integrity and accuracy of the receipt. (See supra note 64 for a description of PKI.)

[88] Norbert Zisky, "Manipulation Protection," supra note 83, at paragraphs 5.2 and 5.3.

[89] Norbert Zisky, personal e-mail communication, August 10, 2009 (on file with R.T.A.): "Quebec's device generates real digital signatures. . . . They store the signatures of each transaction inside the box. So the general approach of both solutions is very similar."

expense) with a smart card containing a crypto processor that e-signs designated "tax-relevant data." With this device, the entire electronic journal could be signed on a regular basis;[90] or each transaction, whether open or closed (sale, refund, training session, voided sale, or temporary record), could be designated as tax-relevant and signed whenever entered into the ECR. It would not matter under the German system if no receipt was issued, but auditing individual transactions would be more difficult.[91] It would matter only that each transaction be registered in an ECR or POS system that was fitted with a smart card.

Because the German solution is fully digital, the revenue authority will be able to conduct its audits of businesses remotely. A data feed may be taken directly from ECRs, or data may be transmitted through an e-mail attachment. The Greek solutions can do this, but the Quebec SRM cannot. The SRM presents data and security in digital format, but the expansion of audit capability to include remote audits has been rejected by Revenu Québec on policy and privacy grounds.[92]

There is a nagging question about the possibility that malicious software could be added to an ECR that has been fitted with a smart card.[93] The same question arises

[90] With the SRM, the electronic journal of transactions is signed by the device. Marc Simard, personal e-mail communication, September 15, 2009 (on file with R.T.A.).

[91] However, German legislation is pending that will require the issuance of a legal receipt, along with other legislation that will implement the smart card solution. This legislation has not been acted upon.

[92] Dave Bergeron, personal e-mail communication, November 20, 2008 (on file with R.T.A.), on the rejection of remote audits performed by linking to the taxpayer's SRM. It is questionable whether Revenu Québec is dealing with a real privacy concern here, or merely with the appearance of an intrusion on a protected privacy interest. There should be little that should be considered confidential in the bulk transmission of itemized business records setting out daily sales of goods or services, provided that those sales are not further associated with an individual—that is, an unsuspecting customer. It is the retention of a *customer's* personally identifiable information (PII) in business records that is a privacy concern. If not handled properly, this may lead to an unauthorized government intrusion into private lives. See Neil M. Richards and Daniel J. Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) vol. 96, no. 1 *Georgetown Law Journal* 123-82, discussing the origins and different development paths of privacy law in the United States and the United Kingdom—the United States with an individualistic understanding and the United Kingdom with a relational understanding—and indicating that unauthorized disclosure of PII within business records is central to both. Nevertheless, it is common in the transaction tax context to put protections in place whenever third-party access to tax data is contemplated. For example, section 321 of the SSUTA, supra note 13, restricts retention of PII by CSPs performing tax calculations.

[93] Under the German solution, each keystroke providing data that are destined for the smart card is assigned a number by the smart card itself. Missing data can be identified by looking for a break in the sequencing. This, however, does not answer the concern; it only pushes the hypothetical back in time, so that the malicious software intervenes before the assignment of a number. In a personal e-mail communication, August 6, 2009 (on file with R.T.A.), Norbert Zisky confirmed the assignment of the numbers under the German solution: "Each set of data which will be sent to the smart card for signing will be added with a sequence number generated by the smart card itself. This is the most important part of our solution. Therefore we developed a new smart card package with this functionality."

with Quebec's SRM. If software were designed to intercept data (entered into the ECR) that was destined for the smart card—for example, any sales of a particular beer, or any sales of beer in excess of the number of people at a table—would this defeat the system? This is a step 2, not a step 5, fraud. A valid receipt will not be issued under either the German or the Quebec solution. The German response to this hypothetical is similar to that of Quebec: because this fraud happens in real time (at the cash register) and not at the end of the day in the backroom, it is an activity that remains in the realm of traditional audit.[94] Brazil encountered exactly this problem in 2007 in *Operação Tesouro* (Operation Treasure-Hunt).[95]

However, under the Greek solution, where it is the ECR itself that is certified and not an add-on microprocessor (Quebec) or an add-on smart card (Germany), this fraud would be uncovered. The Greek approach directly certifies the programming within the ECR, and provides a machine-specific testing mechanism.[96]

The Greek, Quebec, and German solutions can also be distinguished on the basis of the "per-unit" cost of implementation. The German solution is far and away the least expensive. Both Greece and Quebec have responded to the high costs of their solutions. Under the Greek regime, the entire cost is borne by business, although the government does provide tax breaks (accelerated depreciation) and financial assistance (low-interest loans) to assist with hardware purchases. Quebec, on the other hand, plans to provide the SRM to businesses free of charge.

Zisky identified the low cost of the German solution, estimated at about €50 per ECR, as one of its key features:

> In . . . this approach . . . for the protection of electronic cash registers and POS systems against the manipulation of stored data [t]he large advantage . . . consists of the reaching of a comparatively high level of protection with only small hardware and software expenditures in the POS system being necessary.[97]

He itemized the components of the €50 estimate as follows:

> The additional costs per ECR are the result of [the] cost for the smart card (signature device), approx. 7-8 Euros, and for integration of the smart card to the 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 [part] of tax authorities some

[94] Norbert Zisky, personal e-mail communication, August 10, 2009 (on file with R.T.A.): "An auditor [should] see [this fraud] in realtime because no valid signature is printed on the receipt. It is the same problem [when] the tax payer does not use the ECR every time and puts the money in his trouser pocket directly."

[95] See infra note 102 and the related text.

[96] See supra note 47.

[97] Zisky, "Manipulation Protection," supra note 83, at paragraph 5.1, and paragraph 5.7 (estimating €50).

> 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 [a] base of more than 100,000 cards because they will be ordered by a central authority.[98]

Vectron's prototype of the INSIKA smart card solution has an even lower cost estimate—a "[s]ingle-unit end-user price [of] less than €25."[99]

The Role of Audits in Fiscal Till Jurisdictions

All fiscal till jurisdictions continue to rely on audits to detect fraud. The technological solutions discussed above—whether FECRs, AFED printers, FESDs, SRMs, or smart cards—do not replace auditing; they only make auditing easier. Thus, Quebec announced an increase in the use of inspection teams in tandem with the announcement that SRMs would soon be deployed. The SRM itself is designed with an auditor's eye. It harmonizes data feeds from widely diverse ECRs, and it translates the digital signatures on receipts into bar codes so that they can be scanned with hand-held optical readers.

Germany's assessment of the situation is similar to Quebec's. Germany believes that fraud technology has advanced so far that success with traditional audits is virtually impossible without a secure technological record. In a comment directed to the Federal Ministry of Finance on November 24, 2003, the German Federal Audit Office (Bundesrechnungshof [BRH]) warned that

> *[t]he latest generation of cash registers and cash register systems makes it impossible for tax authorities to detect fraudulent declarations of cash receipts. In these systems, data that have been entered, as well as system-generated register and control data can be secretly tampered with. This leads to a high risk of lost taxes that cannot be overestimated. This situation must change immediately. . . .*
>
> The analysis reveals that auditors and tax investigators have constantly discovered fraudulent manipulations of cash registers and the data they store. However, such manipulations could only be discovered in older generations of electronic cash registers and cash register systems.
>
> Verification of data has become extremely difficult since the introduction of new cash registers and cash register systems.[100]

Brazil's experience with ECR manipulation reinforces the German and Quebec assessments. Reliance on technology alone to block manipulation is not sufficient. No matter how much security is placed over digital records, an audit is necessary.

[98] Norbert Zisky, personal e-mail communication, February 19, 2008 (on file with R.T.A.).

[99] Vectron Systems AG, "Tamper-Proof POS Data: Projectgroep Onderzoek Administratieve Software," October 31, 2007, 30 (online: http://www.gbned.nl/downloads/xmllogistiek/poas/20071031%20Vectron.pdf).

[100] BRH comments 2003, no. 54, supra note 17, at 197-98 (emphasis in original).

Brazil requires that a "black box" be attached to each ECR. The device secures the electronic journal and can only be accessed by the tax administration. But as the 2007 criminal audit of all the supermarkets in Belém (*Operação Caixa 2*—Operation Second Register) demonstrates, fraudsters intent on skimming will find a way to get into the black box.[101] Similarly, in 2007, *Operação Tesouro* (Operation Treasure-Hunt) demonstrated that fraudsters have been successful in tampering with the black box through malicious software. This operation, conducted in the state of Bahia, uncovered over 300 food service establishments that used software to manipulate data *before* it was sent to the black box.[102]

[101] "Operação Caixa 2" (Operation Second Register), conducted by the Brazilian Federal Revenue service, began on October 1, 2007. In the early stages, it involved 50 fiscal auditors, 20 tax analysts, and 20 support personnel (police units) operating in 10 teams in the city of Belém. On the first day of the operation, five companies (supermarkets) were raided, 175 recording machines were confiscated, and 60 were found to have irregularities. In addition, 17 suppliers were searched. On the second day, four more supermarkets were raided in Capanema, and two more in Bragança were searched. "The fiscal auditor and coordinator of this activity, José Renato Gomes, affirms that yesterday's work is essential for finding out whether this kind of fraud is all coming from Belém, from the corporations supplying the equipment, or if it is being set up and carried out outside the State." "Receita Federal fiscaliza supermarcados em Belém" ["Federal Revenue Service Investigates Supermarkets in Belém"], *Plantao Online Edition*, October 1, 2007; "Receita Federal dá prosseguimento à Operação Caixa 2" ["Federal Reserve Gives the Go-Ahead to Operation Caixa 2"], *Plantao Online Edition*, October 3, 2007; and "Operação Caixa 2 divulga balance hoje" ["Operation Caixa 2 To Release Results Today"], *Plantao Online Edition*, October 18, 2007 (online: http://www.orm.com.br/plantao/comentar.asp?id_noticia=290720) (in Portuguese—sequence of posting on the federal government Web page; translations on file with R.T.A.).

[102] "Operação Tesouro" (Operation Treasure-Hunt) in the state of Bahia is described as follows:

> [S]even businessmen from the bar and restaurant sector, as well as the owners of two information sector businesses, namely Networks and Stella Systems, [have been] accused of being responsible for the development of a tax evasion software program. . . . [The operation involved] 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. . . .[T]hese businessmen have been withholding nearly 40% of their companies' turnover. . . . [T]he Colibri software, developed by Networks, is a database program for commercial automation, commonly used by bars, restaurants and luncheonettes. The fraud consists in the use of the program with a certain configuration permitting the deactivation of the Receipt Issuing Device (ECF), and thus keeping the machine from issuing a receipt during payment for sales of products or services.

"Technological fraud?..Bahia::Fraude:Sonegação Fiscal Leva sete Empresários para a Prisão Terça-feira" ["Technological Fraud? Bahia: Fraud: Seven Businessmen Imprisoned for Illegal Withholding of Taxes"], *Journal da Midia*, October 2, 2007 (online: http://www.jornaldamidia.com.br/noticias/2007/10/02/Bahia/Sonegacao_fiscal_leva_sete_empres.shtml) (translation on file with R.T.A.).

The experience of Greece, however, appears to stand in contrast to the Brazilian as well as the German and Quebec assessments. Even though regular audits of FECRs, AFED printers, and FECDs are conducted by Greek authorities, no significant enforcement actions involving ECRs have reached the courts, or can be referenced by tax officials.[103] In light of the 20 years of certification experience that Greece has with ECRs, one might have expected things to be different. It is not clear whether this is a case of false confidence in technology, a case of superior technology, or a case of a superior deterrence profile, but in light of the Brazilian investigations, the Greek approach needs to be considered carefully. Is the direct certification of an ECR, with the willingness and demonstrated ability to go in and check for programmatic modifications, a significant deterrent?[104]

COMPREHENSIVE AUDIT: THE NETHERLANDS

The Netherlands is at the other extreme of the technology/traditional audit continuum. The Dutch are convinced that audits alone are sufficient. They reject fiscal till technology. The fundamental emphasis in the Netherlands is on detailed, comprehensive, and technologically penetrating audits. Direct government intrusion into the record-keeping systems of all businesses just to catch fraudsters is avoided at all costs. Following a pure principles-based approach to enforcement, the Netherlands believes that it can rely on good business practices and compliant taxpayers.

However, Netherlands officials speak about performing "deep audits"—that is, audits that are not focused solely on the sales records in the ECR. A deep audit considers businesses comprehensively; it looks at income taxes, consumption taxes, and employment taxes simultaneously, and with heavy stress on the interrelationships among taxes. Ben B.G.A.M. van der Zwet, lead auditor for technology compliance, has described the Dutch approach as follows:

> The Dutch Tax Authority is convinced that the appropriate approach is to use principle based laws in this area. This method involves maintaining the law by stimulating the compliance of taxpayers. It is premised on a belief that we should be working from a starting point of trust to get compliance, or to provide explanations.
>
> With respect to the problem of auditability and the completeness of sales for enterprises with sizable over-the-counter payments, the Dutch Tax Authority has decided to work to improve voluntary compliance.
>
> The Dutch Tax Authority is cooperating with software developers, suppliers and manufacturers of cash registers, branch organizations, and larger companies.[105]

[103] According to Panos Zafiropoulos, "[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." Personal e-mail communication, May 10, 2008 (on file with R.T.A.).

[104] There is considerable interest in the Greek system in other countries. Kenya has adopted it, and at the time of writing (August 2009), the Greek approach was also being adopted in Kosovo. Panos Zafiropoulos, personal e-mail communication, August 10, 2008 (on file with R.T.A.).

[105] Ben B.G.A.M. van der Zwet, "Note: Draft 20080201—Fiscal Obligations for Cash Registers in the Netherlands," February 1, 2008 (unpublished draft on file with R.T.A.).

The Netherlands has been successful with this approach. One of the best examples of how a comprehensive multitax audit can uncover data manipulations is the café Dudok case.[106] The Dudok case also illustrates the connection between sales suppression fraud and the symbiotic relationship that develops between SMEs and their ECR providers. The case involved a Dutch "grand café"—a style of café with spacious facilities, which welcomes drop-in customers and has a large cash-based clientele. This type of operation is an ideal business for skimming.

Dudok skimmed cash receipts with a primitive zapper and used a portion of the cash to pay employees under the table. The Dutch revenue authorities (Belastingdienst) were suspicious of the low wages reported and thought that additional, unreported compensation might be being distributed to employees.[107] Testimony in the case indicated that on the second day of the payroll audit, the managing director of Straight Systems BV[108] visited Dudok, where he was approached by the café's owner-manager. Straight Systems BV supplied the Finishing Touch POS cash registers that were used by Dudok. The owner-manager explained that he was having difficulty accounting to the Belastingdienst for the wages that were being reported, in part because the auditors were also questioning the turnover that was reported. The numbers did not "seem right" to the auditors, and they were requesting backup data. The owner-manager was worried that this would lead them to the primitive zapper he was using.

The managing director of Straight Systems explained the existence of a more sophisticated zapper, a "hidden delete" option already embedded in the Finishing Touch cash registers. Essentially, the embedded device was "a hidden menu option that, after enabling . . . , allowed operators of catering establishments to delete cash register receipts from the system."[109] After this discussion, an employee of Straight

[106] District Court of Rotterdam, LJN: AX6802 (June 2, 2006) (online: http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AX6802) (in Dutch, translation on file with R.T.A.); appealed to the District Court of The Hague where the judgment was upheld, LJN: BC5500 (February 29, 2008) (online: http://zoeken.rechtspraak.nl) (in Dutch; translation on file with R.T.A.).

[107] LJN: BC5500, supra note 106, at F3. Prior to using the phantomware 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 Excel spreadsheets. The examining agents did not trust the spreadsheets and asked for the POS records as a backup to confirm what they were being shown on the audit. Ben B.G.A.M. van der Zwet, personal e-mail correspondence, May 28, 2008 (on file with R.T.A.).

[108] 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" (online: http://www.straight.nl) (in Dutch; translation on file with R.T.A.).

[109] LJN: AX6802, supra note 106, at "Consideration of the Evidence" (in Dutch; translation on file with R.T.A.). The case discusses three software programs: Twenty/Twenty, Finishing Touch, and Tickview.exe. Twenty/Twenty was a US touch-screen program that did not have a

Systems visited Dudok, and explained and enabled the application of the erase rule (the hidden delete function).[110] Subsequently, the café's owner-manager decided to start using the option.[111] Nevertheless, as van der Zwet recounts, the fraud was uncovered by the Belastingdienst auditors:

> The most interesting thing about [Dudok] is that the discovery of the fraud was completely the benefit of a good and thorough tax audit. Based on our principle based law, tax officers were not satisfied getting the total reports and MS excel work-pages with total sales etc. They wanted the [detailed] information of the POS. The tax officers persisted in their efforts to get the detailed information. This forced the entrepreneur to ask the POS supplier to help him out. . . . [He] was aware that once the POS records were audited the fraud would instantly be clear.
>
> Straight Systems was helpful by installing an additional hidden feature of the POS system. Records in the POS could [now] be deleted and the records renumbered so that no gaps would appear.
>
> A thorough investigation of the tampered databases revealed the deleting of the records anyway. So this was not simple bad luck [for the taxpayer] but a good audit job of the Tax administration![112]

The court upheld criminal tax fraud determinations in the Dudok case in respect of unreported income, value-added, and payroll taxes. Both the restaurant operator and the ECR/software provider were convicted.

Two other successful audit-intensive cases in the Netherlands are notable, both of which involved software enabling fraud:

- Microcraft Software developed Analyse (also known as CX Analyse and Retail) as a management information system for grocery stores, butchers, and bakers. It worked off a combination of ECRs and grocery scales. The zapper could be started with a hidden combination of keystrokes, and the user could then indicate a percentage of turnover that would be skimmed.[113]
- B&F Software and Computers B.V. developed *Beleids Informatie Systeem* (BIS) for hairdressers and an add-on program for zapping cash sales through POS and

phantomware application. Straight Systems BV added the phantomware 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 he would like to delete the whole ticket. If an affirmative response is given, 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 communication, May 28, 2008 (on file with R.T.A.).

[110] The trial court in Rotterdam refers to the phantomware application as a "hidden delete function," whereas the appeals court in The Hague refers to the phantomware as "the erase rule."

[111] LJN: BC5500, supra note 106, at F3.

[112] Ben B.G.A.M. van der Zwet, personal e-mail communication, April 16, 2008 (on file with R.T.A.).

[113] See Case LJN: AT5876, District Court of Arnhem, July 27, 2005 (in Dutch; translation on file with R.T.A.).

> client information systems. After the operator entered the percentage to be skimmed, the system selected the categories of transactions to be eliminated (for example, male walk-in customers paying cash without special services).[114]

Given the success of the Dutch authorities in prosecuting such cases, it is clear that an intensive and comprehensive audit approach works against automated sales suppression devices. There are a number of sizable cases in the Netherlands, and a much larger number of cases in Quebec, that demonstrate the effectiveness of this approach. Quebec, however, unlike the Netherlands, is convinced that more than an audit is needed. The SRM is a rules-based supplement to the audit effort.[115]

The United Kingdom has indicated that it shares the Netherlands' opinion,[116] and would prefer to avoid universal fiscal till solutions. However, a recent national pilot study of 941 UK enterprises has uncovered clear evidence of tax fraud involving phantomware. Given the apparent scope of this fraud (which has not been fully analyzed as of this writing), the United Kingdom may change its position on the use of fiscal till technology.[117]

BLENDING RULES AND PRINCIPLES: CERTIFICATION OF THIRD-PARTY SERVICE PROVIDERS

Certification is the common thread among all the zapper enforcement efforts considered above. This is apparent if we step back from the details. In each instance—Greece, Quebec, Germany, and the Netherlands—the tax authorities responded to the threat of automated sales suppression in the same manner: they all looked for certification of digital records. Rules-based jurisdictions imposed *external* certification regimes to force businesses to keep trustworthy records; principles-based jurisdictions induced businesses to develop their own *internal* (self-)certification regime. In all cases, however, it is the reliability of digital records that is the main concern—and in all cases, the question is whether the certification is trusted. Both approaches work. But neither approach (rules-based nor principles-based) comes without costs and problems.

In rules-based jurisdictions, the prospect of forcing all businesses to accept a government presence inside the record-keeping function of private enterprises—the fiscal till solution—is considered by some to be far too intrusive. The observation is that this remedy is overly broad, and needs to be more focused. Why should *all*

[114] *B&F Optics BV*, District Court of Amsterdam, August 11, 2005 (in Dutch; translation on file with R.T.A.).

[115] The Quebec approach is to have the SRM together with specialized inspection teams and a significant public awareness program. Supra note 2, slide 5.

[116] See "Cash Register Good Practice Guide," supra note 6, at paragraph 1.4.4 and appendix E.

[117] Jennifer Mitchell (HM Revenue & Customs, Local Compliance, SME Interventions), personal e-mail communication, November 26, 2008 (on file with R.T.A.).

sales activity be certified through government oversight, just because *some* records are untrustworthy? In Quebec, the government's SRM minicomputer must be placed between every ECR and printer in every restaurant (except perhaps some small restaurants). In Germany, every ECR will be required to install a tamper-resistant, government-issued smart card that can be configured to record, sign, and transmit all data processed by the ECR. In Greece, no business can be conducted without processing transactions through a government-certified FECR or FESD.

Principles-based jurisdictions prefer a "hands-off" approach, at least initially. Moral factors and good business practices are relied upon to make digital records trustworthy. Unfortunately, this solution requires oversight, and the oversight that works is an audit program that is both comprehensive and technologically intensive. Even though it is more than inconvenient for a small business to have to respond to these kinds of audits, the real problem is not the complaints of the business owners; it is the fiscal demands placed on the revenue authority that must conduct the audits. Funding is rarely sufficient to secure the necessary audit teams and computer audit specialists.

Fortunately, there is another option—certification of intermediaries. This approach is used in the United States with CSPs (certified service providers) under the SSUTA.[118] The SSUTA can be a useful template for jurisdictions seeking to develop less intrusive and less expensive methods for combatting automated sales suppression. Currently, CSPs perform all consumption-tax compliance functions for their clients. They determine taxability and the correct rates. They prepare and file returns, make tax payments, and immunize the taxpayer from liability for errors (except taxpayer fraud).

Extending the CSP's obligations to include certification by the CSP to the government that the taxpayer's ECRs and POS systems are free from zappers and phantomware would create a new enforcement regime. Four questions need to be addressed:

1. How does a CSP get ECR and POS system data?
2. How can a CSP be sure that the data it has are accurate?
3. What standards should the government use to certify a CSP's automated system? In other words, what data does a tax authority need in order to be sure that it can trust the CSP's attestation to the accuracy of the taxpayer's system?
4. What is the most efficient and cost-effective way for a CSP to satisfy the government's standards?

Possible responses to these questions are provided below.

1. How Does a CSP Get ECR and POS System Data?

CSPs currently pull data directly from the ECR or POS system to determine taxability at step 4 of the transaction sequence. The data are stored in an independent

[118] See supra notes 13 to 15 and the related text.

(tamper-proof) audit file before they are used by the taxpayer to draft the invoice (receipt). The CSP maintains this file to protect itself from liability.

Unlike fiscal till solutions, which preserve data that are sent to the printer from step 5 (procedures a through d) or from step 6 (when the data are recorded in the X or Z reports or the electronic journal), the CSP is actually involved in generating the critical data sets. In real time, the CSP determines the taxability of transactions, calculates the tax, and passes this information back to the ECR. This event has a three-way data check:

1. The customer is demanding an accurate receipt, and the CSP and the business (the vendor-taxpayer) must produce it.
2. The business (which has the primary obligation to collect and correctly remit the tax) is demanding that the CSP perform this tax function accurately.
3. The CSP (which is assuming all the tax-compliance obligations of the business, including remission of taxes from funds provided by the business) is motivated to be accurate (to detect any fraud) because it has liability for any errors in the calculation and remittance of tax, and must compensate the tax authority for such errors out of its own funds.

With a CSP-based system, a "legal receipt" is not required. It could be mandated to combat fraud occurring outside the ECR, or maybe as a further tool against consumer-business collusions, but it is not necessary for the CSP. It is likely that the revenue authority would demand a legal receipt to facilitate audit checks.

The SSUTA is a voluntary system. However, there are strong incentives to participate. Businesses participate to get relief from regular audit, relief from penalties for tax calculation errors, and relief from additional taxes (penalties and interest) that stem either from late changes in laws or errors in taxability determinations.[119] CSPs participate for commercial reasons: fees for service from the business-client or the state,[120] and money-movement benefits. These incentives are offset by a shift in tax liability to the CSP if it makes errors. Only fraud by the business-client (the taxpayer)[121] removes this liability.[122] All CSPs insure against the risk of their own errors (so there is always a fund out of which missing taxes can be paid). They are also required to post a bond before receiving certification, and they are permitted to retain confidential transactional data in order to defend themselves, if necessary.

[119] SSUTA, supra note 13, at section 9(a).

[120] Ibid., at sections 601 to 603 (providing that the government may enter into contracts with a CSP to compensate the service provider directly on the basis of taxable transactions processed, or a percentage of instances where sellers without nexus volunteer to collect sales taxes that they are not otherwise obligated to collect).

[121] A CSP is also relieved from liability for charging and collecting the incorrect amount of tax if that error is caused by erroneous data provided by a member state on tax rates, boundaries, or taxing jurisdiction assignments, or if it is based on erroneous data provided by the member state in the taxability matrix. SSUTA, supra note 13, at sections 328 and 331.

[122] Ibid., at section 9(a).

2. How Can a CSP Be Sure That the Data It Has Are Accurate (Free from Manipulation)?

Ensuring the accuracy of the data relied upon is key to the SSUTA approach. In our view, the most effective way to do this is to adopt the German smart card in the private sector. The German smart card can be configured to sign every event—completed sales, temporary records, refunds, test modes, open or partially completed transactions. Thus, every keystroke could be recorded, collected, and signed on the smart card, and then transmitted to the CSP.[123] The tax authority could then direct questions about any transaction, or about the business records associated with any ECR, to the CSP. Only in cases of fraud would it be necessary for the tax authority to approach the taxpayer-client. If suspicions were raised, it would be in the self-interest of the CSP to assist the government in determining the truth.

Use of a smart card would be a form of comprehensive ECR monitoring, but the private sector would be monitoring the private sector, in contrast to an intrusive government oversight program.[124] For additional protection, it is likely that a CSP would also adopt the Greek security regime; that is, it would take steps to certify each specific ECR, and then keep a digital record of the programming of each machine that could be confirmed in the manner of a Greek audit.[125]

3. What Standards Should the Government Use To Certify a CSP's Automated System?

What data does a tax authority need in order to be sure that it can trust the CSP's attestation to the accuracy of the taxpayer's system?

The data preservation standards that a CSP would need to meet if it were to certify the accuracy of business records in an ECR should be the same standards that a

[123] In a personal e-mail communication, November 17, 2008 (on file with R.T.A.), Norbert Zisky confirmed, "If I get the data in Berlin from an ECR in Boston I am able to check the integrity (whether the data is unchanged against the original data) and the authenticity (whether the signature belongs either to the ECR or [to] the tax payer). The kind of authentication depends on the operational concept of the tax body. In principle every transaction [final sales (step 5) and temporary transaction (step 2)] could be transferred to the auditor or a remote server."

[124] Not only could all transactions (final and temporary) be tracked and e-signed by the German smart card, but all of this could occur in real time. However, the German planners have indicated that, because the data are collected by government authorities, businesses "will have a strong resistance against this online tracking of transactions." Norbert Zisky, personal e-mail communication, November 17, 2008 (on file with R.T.A.). There is a Serbian proposal to do this, but it has not been well received. Milan Prokin, "Technical and Functional Specification of Turnover Controllers—Draft Prepared for Fiscalis FPG 12 Cash Register Project Group" (undated; on file with R.T.A.), 7. Prokin (of the Faculty of Electrical Engineering, Belgrade) proposes a system whereby "[a]ll 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 servers store all transaction data]."

[125] See supra note 47 and the related text.

principles-based jurisdiction, like the Netherlands, would set down for all ECRs. In a guide to businesses outlining their fiscal accounting obligations, the Dutch tax authority lists the requirements that a business must meet in order to bring its ECRs or POS system into compliance with Dutch law.[126] They include

- detailed records available for the tax auditor if and when required,
- electronic preservation of the details of transactions,
- preservation of a complete audit trail, and
- adequate measures to guard against subsequent alterations in a manner that will ensure that data integrity is maintained.

The Dutch requirements may not be difficult for larger businesses to meet, but for SMEs (which is where phantomware and zappers are found), the requirements are burdensome. Van der Zwet confirms:

> Hardly any of the cash registers or Point of Sale systems by themselves [comply] with the requirements set out by the Dutch Tax Authority. With larger companies this omission can be compensated for with adequate internal control measures. Without similar internal control efforts, SMEs that may be willing to comply with Dutch fiscal obligations will fail in their attempts.
>
> - Data needs to be stored electronically.
> - Facilities have to be implemented to export data to digital data carriers.
> - Settings of the software and the adequate database structures must support a proper audit trail.
> - Measures must be taken to assure the reliability of retained data.[127]

Under the SSUTA model, a third-party service provider could not be certified unless it could assure tax authorities that its system accurately, completely, and automatically captured the required data from the taxpayer's ECRs. With these data on hand, the CSP's attestations would be highly credible.

4. What Is the Most Efficient and Cost-Effective Way for a CSP To Satisfy the Government's Standards?

Combining the smart card with the SSUTA approach appears to be the best solution. It is far less expensive than any other option; it uses proven technology, and the CSP in an SSUTA context is a proven legal structure. But there is also a strong argument for blending in the Greek approach to ECR certification, as well as the Quebec SRM's

[126] Belastingdienst, *Your Cash Register and the Fiscal Accounting Obligations* (The Hague: Belastingdienst, 2007) (online: http://www.gbned.nl/downloads/xmllogistiek/poas/Your%20cash%20register%20and%20the%20fiscal%20accounting%20obligations.pdf), paragraph 6, "Checklist for Cash Registers."

[127] Van der Zwet, supra note 105, at 4.

bar-code reader. Merging attributes of all three systems, a CSP vehicle makes a great deal of sense.

The only competing option is for the government to become the vehicle for implementation. However, even the German research teams working on the smart card project concede that direct government involvement compromises the effectiveness of the solution.

The German smart card solution comes from successful research in legal metrology, specifically the SELMA (Secure Electronic Measurement Data Exchange) project. The immediate goal of SELMA was to ". . . ensure the secure transfer of measured *energy data* from decentralized meters to the authorized users via open networks."[128] SELMA succeeded. The project leaders summarized SELMA as follows:

> SELMA . . . developed a security architecture to establish trust in the electronic transfer of data from the meter to data acquisition systems and further to the customers. The introduced security mechanisms are based on asymmetric cryptography and more specifically on digital signatures that enable the signed measurement data to be verified and authenticated in conjunction with a suitable key management. Particular security units have been created that contain the necessary security mechanisms.
>
> The SELMA architecture represents a best practice solution of strong cryptographic mechanisms to secure a wide range of metrology applications and is compatible with appropriate European directives and guidelines.[129]

SELMA looked at natural gas meters. The SELMA solution assured multiple parties (traders, distributors, owners of distribution networks, and consumers) that remotely monitored meters were accurate. On the basis of the assumption that ECRs and POS systems are only a different kind of meter recording a different kind of data flow, the SELMA researchers suggested that the same solution could apply in this new context as well. The INSIKA project (described earlier in this article) was launched in 2008 to consider this application.

There are two critical differences between SELMA and INSIKA: (1) the INSIKA data represent confidential tax information (not natural gas measurements), and (2) the group of interested parties includes the government (whereas only private parties are involved in gas metering). The researchers soon became aware that businesses were strongly resistant to online tracking of transactions by the government.[130] As a result, the SELMA solution was not able to be fully implemented in INSIKA. Zisky noted:

> The realtime, central collection of very large amounts of data is already being carried out today in different sectors of the economy. One example worth mentioning is the area of special contract customers for power supply. Of approximately 300,000 special

[128] Iacono et al., supra note 84, at 312-13 (emphasis added).

[129] Ibid. Also see the online source for the SELMA project, supra note 84.

[130] See supra note 124, quoting from personal e-mail communication with Norbert Zisky.

> contract customers, energy amounts recorded in intervals of 15 minutes are read out daily and stored centrally. These data, relevant to calibration law, provide the basis for the monthly billing. For the sake of completeness, the following should also be mentioned: work is currently being done towards securing measurement data cryptographically.
>
> *The decisive difference between the example of energy data transfer and the realtime, central recording of tax-relevant data consists in the fact that the data must be collected by the authorities, rather than by a contracting partner.*[131]

Simply put, even when there is "nothing to hide," there are real privacy concerns when the government gets too intrusive.[132]

These are the same issues that confronted the SSUTA. The real-time collection of tax data by the government was not acceptable to business, but the collection of such data was acceptable when a third party did it. Thus, the issue changed. Now, the question was whether the government could trust the third party as much as the taxpayer did (rather than whether the government should be trusted to collect the data directly). The SSUTA answer was that, yes, the government could trust a third party, but only if the third party's systems were certified.[133] (Similarly, the Dutch tax authority was concerned with finding a way to encourage voluntary compliance by taxpayers, rather than imposing too much government control over private business records.)

The SSUTA was born as an inexpensive, voluntary regime to streamline sales tax compliance. It extends audit immunity to taxpayers who use CSPs, because the CSP is trusted by the government. An SSUTA type of system to prevent zappers and phantomware applications in ECRs could be made mandatory for all sectors of an economy. Alternatively, it could be applied only in high-risk sectors, or it could perhaps be made mandatory only for those taxpayers who had previously been found to manipulate sales records. Even if it were only mandatory for some taxpayers, participation in the system should remain an option for all businesses. This would increase the pressure on those who do not use CSPs to maintain good records. Traditional audit resources could be more intensively focused on this subset.

CONCLUSION: ASSESSING QUEBEC'S SRM

With the SRM currently in operation in a select number of restaurants on a volunteer basis, it seems appropriate to offer an assessment of how effective the SRM could prove to be, in light of the experience with anti-fraud initiatives in other jurisdictions. There are five critical observations.

[131] Zisky, "Manipulation Protection," supra note 83, 10-11 (emphasis added).

[132] Daniel J. Solove, "'I've Got Nothing To Hide' and Other Misunderstandings of Privacy" (2007) vol. 44, no. 4 *San Diego Law Review* 745-72.

[133] There is a related issue of trust involving consumers. It was necessary to add a provision to the SSUTA to protect personally identifiable information (PII) from disclosure when it was in the hands of the trusted third party. See supra note 92.

1. The SRM will work. Coupled with a significant audit effort, the SRM will most likely be an effective zapper and phantomware deterrent in the Quebec restaurant sector. There are several reasons for this:
   a. the SRM is similar to the very effective FESD and FECR with AFED printer that has been in use in Greece for over 20 years;
   b. the SRM deployment is accompanied by a commitment to increase pre-audit investigators who will refer suspected fraudsters for full audits; and
   c. the SRM will facilitate rapid pre-audit investigations by embedding bar codes on each receipt that will verify that it is "legal."

   All of these factors bode well for the workability, effectiveness, and ultimately the success of the SRM.
2. The SRM is expensive. Quebec estimates that the SRM will cost approximately $650 per unit, an expense that will be borne entirely by the Quebec government. The estimated cost for full deployment of the SRM throughout the restaurant sector is $55 million. These costs approximate the Greek costs, but are 10 times the per-unit cost of the German smart card, and they present Quebec with a scalability problem. In other words, if Quebec wants to eventually extend the SRM throughout the economy, instead of focusing on a single sector, the magnitude of these expenses might force the government to either limit its financial support (as is the case in Greece) or move to a device modelled on the German smart card. Because zappers and phantomware are not confined to the restaurant sector, the scalability of the SRM solution needs to be considered in advance of full implementation.
3. The SRM is an invoice-based solution. Quebec, like Greece and Germany, designed its solution around the invoice (receipt), and passed laws mandating that a legal receipt must be given in each sale. This requirement raises concerns about too much government in private business: Why should *every* sale need to be accompanied by an SRM-signed receipt when profits from only *some* sales are skimmed? However, this intervention into private business relationships is a necessary part of the enforcement regime, because the invoice is the trigger that sets the whole data security process in motion. Factoring in some Dutch concerns and looking more closely at a CSP/smart card solution might have some merit.
4. Extending a mandatory SRM solution outside the restaurant sector may be difficult. Indeed, the fact that some restaurants have agreed to participate in the SRM pilot project on a voluntary basis does not mean that the SRM will be widely accepted throughout the restaurant sector. Could the government impose mandatory use of the device throughout the economy? Quebec's empirical work supports a restaurant initiative, but audit results in the Netherlands (as well as some early cases in Quebec) suggest that the problem is much more widespread; grocery stores, convenience stores, and hairdressers are all suspect. In Germany, there is considerable resistance to the smart card precisely because it is being considered for the whole economy. Quebec's single-sector approach is unusual and may ultimately prove to be unstable,

because it will not solve the whole problem, and it treats businesses unequally. Business incentives may be helpful in this effort, and by offering them, Quebec would be taking a page from the principles-based jurisdictions. The SSUTA model highlights the incentives that have worked in the United States.

5. The SRM is not a real-time solution.[134] There is nothing in the SRM, in the German smart card proposal, or in the Greek system that accelerates audit, return filing, or tax remission into real time. Real-time compliance is very possible with certified systems, but this would require adoption of a CSP/smart card solution. It is an intriguing thought that the CSP/smart card would not only stop skimming frauds with zappers and phantomware, but also bring tax compliance into real time.[135]

APPENDIX COMPARISON OF SOLUTIONS IN THE FIVE JURISDICTIONS—A GRAPHIC SUMMARY

Admittedly, there is a considerable amount of material in our comparative assessment of zapper prevention efforts, and a lot of it is highly technical. If we keep in mind that the effort here has focused on technological solutions to backroom (not real-time) skimming of cash sales,[136] there are some fundamental comparative

[134] However, if one considers the entire Quebec effort—the use of the SRM with hand-held scanners in conjunction with enhanced monitoring of restaurants by inspection teams—it is likely that Quebec comes closer to a real-time enforcement effort than other jurisdictions. (Although this is not a formal real-time audit, it may well result in real-time enforcement.)

[135] Use of a CSP solution would not (in the opinion of Revenu Québec) be effective in preventing all types of fraud. For this reason, Revenu Québec remains committed to very substantive audits (along the lines of the Dutch approach) in conjunction with the SRM. Marc Simard indicates that "a CSP-type solution (including certification of computer systems), would not be at all effective in combating other types of schemes such as failure to record invoices and the absence of invoices. As explained earlier, the restaurateur may decide not to use this system to record sales, even if he has a certified system. It is therefore quite likely that with this type of solution, restaurateurs will continue using other tax-evasion methods, which might even replace the use of zappers. Revenu Québec's solution, which is more comprehensive, requires that an invoice issued by the MEV [SRM] be remitted to the customer, ensuring that the sales amount is recorded in the system. Customer awareness, combined with on-site inspections, will play an important role in ensuring the effectiveness of this solution." Marc Simard, personal e-mail communication, September 15, 2009 (on file with R.T.A.).

[136] Real-time skimming runs the range from situations where the owner simply chooses not to ring a sale through an ECR (and puts the cash directly in his pocket), to situations where the owner produces copies of common receipts and uses the copies of a single receipt multiple times (and then puts the cash in his pocket). There are a whole series of frauds that can occur directly at the ECR. Some of them do involve technology. A hidden switch could activate a program in the ECR on an individual transaction basis and prevent the ECR from functioning (so that cash could be put directly in an owner's pocket). All of these real-time frauds rely on the owner (or a trusted associate) being the clerk at the ECR. These frauds tend to occur in very small businesses (so-called Mom and Pop establishments), because stealing receipts from

points—costs, the nature of the security, and special features—that can provide handles to assist analysis of the several options.

Costs run from approximately $650 to $50 (€1,000 to €30), with the expense being borne by the taxpayer (Greece) or the government (Quebec), or on occasion by a third-party service provider (the United States). Adoption of these security devices is (or will be) either mandatory (Quebec, Greece, and Germany) or voluntary (the United States). Mandatory adoption can be limited to a specific market segment (Quebec).

Security features can be provided through digital fingerprints alone (Greece) or through combining a digital fingerprint and a digital signature (Quebec and Germany). There are remote auditing possibilities (Germany), as well as hand-held scanning options that can be utilized to assist traditional auditors in compliance efforts (Quebec).

the government is one thing, but instructing employees in the art of stealing receipts from the business is quite another matter.

The critical point with zapper technology is that these devices allow fraud to move out from behind the ECR and into the backroom. It allows the fraud to migrate up the business chain—from the single Mom and Pop stores into the medium-sized or multistore chains of commonly owned businesses. With a zapper, an owner can put employees at the ECR, insist that they ring sales accurately, but late at night eliminate selected cash sales from the business records. It is this second level of fraud (more serious, involving larger businesses, and encompassing larger aggregate sales totals) that the SRM (and the other technological solutions) is aimed at. The SRM alone will not stop skimming frauds. It is especially bad at detecting real-time skimming. Audits are still necessary, but the SRM gives Revenu Québec a hand-held scanning device that (along with the requirement that a legal receipt must always be issued) goes a long way toward addressing these additional concerns.

Summary of Features of Anti-Skimming Solutions in Five Jurisdictions

Jurisdiction	Cost	Cost paid by	Mandatory/voluntary	Security	Special features
Quebec					
SRM	$650 per ECR	Government	Mandatory in restaurant sector	Digital fingerprint and digital signature	Hand-held bar-code reader
Greece					
FECR, AFED printer	€200-250 to €800-1,000[a]	Taxpayer	Mandatory with every ECR in the country	Digital fingerprint	Multiple ECRs can be connected to single device
FESD	€400-650 per machine[b]				
Germany					
Smart card	€30-50 per machine[c]	Undecided	Mandatory with all new ECRs in the country	Digital fingerprint and digital signature	Will allow remote auditing
Netherlands					
Comprehensive audit	Unknown (deemed to be prohibitive by the Netherlands and Germany)	Government	Random/risk-selected audit	Not applicable	Not applicable
United States					
CSP and SSUTA	Fee determined by marketplace based on size of taxpayer's business and services needed	Government[d] or taxpayer	Voluntary	Dependent on system adopted	Trusted third party

[a] Cost of FECR with AFED printer, low-end and high-end; used only for B2C transactions.

[b] Cost of FESD used for B2B and B2C transactions, and presumes the existence of an ECR or POS system.

[c] Assumes that the smart card is inserted into a new ECR.

[d] Incentive provided under the SSUTA to get *some* taxpayers to use a CSP; in such cases, government assumes all costs. Otherwise, cost of a CSP is borne entirely by the taxpayer.