TAX FRAUD IN THE SALES TAX: ZAPPERS – WHAT ARE THEY? HOW CAN PUERTO RICO BLOCK THEM?

ARTICLE

RICHARD T. AINSWORTH*

INTRODUCTION

THE SALES AND USE TAX IS AN ESSENTIAL PART OF PUERTO RICO'S REVENUE profile. Effective only recently (November 15, 2006) the *Impuesto a las Ventas y Uso*

* Richard T. Ainsworth teaches Value Added Tax and Transfer Pricing at Boston University School of Law's Graduate Tax Program, and is Director of Government Relations (International) at ADP. He is the former Deputy Director of the International Tax Program at Harvard Law School.

(IVU)[1] was expected to raise between $2.3 and $1.05 billion annually,[2] and has already become the Commonwealth's fourth largest revenue source.[3] Actual revenue results for 2007-2008 came in at $1.1 billion,[4] which admittedly is closer to the low end than the high end of what is possible, but now that the tax is in place the next pressing question is how can its performance be improved?[5]

This paper supports recent efforts in Puerto Rico to use technology to improve IVU compliance and collection. It suggests that Puerto Rico is on the right

---

1 Law 117 of July 4, 2006, 13 LPRA § 9091-9098 (2009); Regulation 7249 of November 14, 2006, as amended.

2 GOVERNMENT DEVELOPMENT BANK FOR PUERTO RICO, FISCAL UPDATE 1 (April 10, 2006)(estimating $2.3 billion), *available at* http://www.gdb-pur.com/investors_resources/fiscal_updates/FiscalUpdate Apri106.pdf; Edwin R. Rios, Office of Economics and Financial Affairs, Treasury Department of Puerto Rico, Estimating Revenues – Puerto Rico – New Sales and Use Tax, Power Point Presentation at the 2007 Federation of Tax Administrators Revenue Estimation and Tax Research Conference (Sept. 18, 2007), *available at* http://www.taxadmin.org/ FTA/Meet/07rev_est/papers/edwin.pdf (estimating $826 million for just the Commonwealth 5.5% tax, and suggesting that the full estimate would be $1.05 billion). Although the reason for the wide disparity in revenue estimates is not apparent, part of the difference could be due to the 65% compliance rate that was assumed in the Puerto Rican Treasury study. If compliance were estimated at 100% the Treasury estimate would be $1.6 billion.

However, compliance appears to be much lower than this 65% estimate. A study conducted by the Puerto Rico Board of Accountancy [Colegio de Contadores Públicos Autorizados de Puerto Rico] indicated for the 19 months between December 2006 through June 2008 compliance was closer to 52%. *Hacienda y Municipio de San Juan inician tarea de cobro del IVU* [Finance and Municipality of San Juan start task of collecting the SUT], PRIMERA HORA, Nov. 10, 2009, http://www.primerahora.com/diario/noticia/politica/noticias/hacienda_y_municipio_de_san_juan_inician_tarea_de_cobro_del_ivu/343310.

Increased enforcement efforts (audit) are underway, as are suggestions for using cash register receipts in a lottery. This latter proposal is designed to encourage citizens to demand receipts that record the sales tax from business owners. Xavira Neggers Cresciono, *IVU-LOTO still in the works,* PUERTO RICO DAILY SUN, Feb. 12, 2010, http://www.prdailysun.com/index.php?page=news.article&id=126594381l.

3 OFFICE OF ECONOMIC AND FINANCIAL AFFAIRS OF THE TREASURY DEPARTMENT OF PUERTO RICO, SALES AND USE TAX COLLECTIONS IN FISCAL YEARS 07 AND 08 *(November 2006 – June 2008)* (indicating that the four largest revenue sources are: (1) Individual income tax, (2) Corporate income tax, (3) Non-resident income tax, (4) Sales and use tax).

4 The Treasury has provided a breakdown of the $1.1436 billion by sectors of the economy. Not surprisingly, the highest IVU revenue producers are in the hospitality industry (accommodation, food and establishments selling alcoholic beverages), followed closely by sales of general merchandise. DISTRIBUCIÓN DEL IMPUESTO DE VENTAS Y USO ESTATAL (IVU) POR CÓDIGO NAICS, AÑOS FISCALES 2007-2009 (2010) [DISTRIBUTION OF STATE SALES AND USE TAX BY NAICS CODE, FISCAL YEARS 2007-2009 (2010)], http://www.hacienda.gobierno.pr/downloads/xls/estadisticas/Recaudos_IVU_NAICS_2007-2009.pdf (in Spanish).

5 *Opinion: In Need of Resuscitation*, ECONOMIST.COM, Jan. 27, 2009, *available at* http://www.economist.com/node/13009687 (indicating that the Puerto Rican, "… fiscal deficit has risen to $3.2bn. Unless immediate corrective measures are put in place to boost revenue collection and cut spending, the administration [of Puerto Rico's new governor, Luis Fortuño] is set to run out of funds to meet payroll costs in the coming months.")

track as it considers adopting one or more of the software certification efforts underway globally to boost revenue results. It is not clear however, which way Puerto Rico is going.[6]

Puerto Rico would be well advised to cast its net broadly and to learn from what other jurisdictions are doing before it makes a firm commitment. There are technology solutions in Quebec, Greece, and Germany as well as many Latin American countries. At the current time Belgium is in exactly the same position as Puerto Rico – legislation in place to adopt technology, but no solution has been specified. Belgium has just completed a technical review of Swedish and German developments, and has encouraged third-party providers to blend technological solutions to meet its specific needs. Puerto Rico should consider the same approach. It should demand a solution that fits Puerto Rican needs; not bend Puerto Rican needs to off-the-shelf solutions.

The specific focus of this paper, however, is on stopping cash skimming frauds (the use of sales Zappers by businesses with electronic cash registers). It is important, however, to see this discussion as part of a wider movement to utilize certified technology to improve compliance and enhance revenue (without increasing rates), but an evaluation along the whole tax enforcement/technological interface is not possible in this paper.

It needs to be underscored that the IVU is a critically important revenue tool for more reasons than just gross revenue yields. Recent studies in the US indicate that sales and use taxes significantly reduce revenue volatility – that is, they provide a very reliable (stable) revenue stream.[7] Although it is too early to present similar evidence for Puerto Rico, as time passes the Commonwealth should expect to see this attribute of the IVU also. In the context of the current economic downturn then, both the revenue yield and the stability of the IVU should be pushing the performance goals for this tax to the forefront of fiscal policy debates.

I. TAX POLICY AGENDA

Two IVU issues should be at the top Puerto Rico's tax policy agenda: (1) should the Commonwealth adopt the Streamlined Sales and Use Tax Agreement

---

6 The Senate approved legislation requiring retail outlets to install electronic equipment to verify the sales subject to payment of the SUT, but it has not indicated the specific technological solution that to be adopted. Antonio R. Gómez, *Usarán tecnología para evitar evasión pago del IVU* [Using Technology to Prevent Avoidance of the SUT], PRIMERA HORA, Feb. 10, 2010, http://www.primerahora.com/diario/noticia/politica/noticias/usaran_tecnologia_para_evitar_evasion_pago_del_ivu/365088.

7 John L. Mikesell, *Dynamic Patterns in State Sales Tax Structures: Tax Policy Change and Convergence, 1979-2007*, 51 STATE TAX NOTES 175, 187 (2009) (indicating, for example, that without the sales tax the State of Maine would have the second highest revenue volatility ratio of all the states over the period from 1979 through 2000, but with the sales tax revenue streams are far more stable and predictable.)

(SSUTA)[8] and (2) how can Puerto Rico stem revenue losses from automated sales suppression software (Zappers). The first initiative would yield additional revenue of $200 million;[9] the second effort would likely yield an additional $170 million.[10] Both of these options approximate the amount of revenue that would be expected from a 1% increase in the IVU. This option was proposed as a "last re-

---

8 Streamlined Sales and Use Tax Agreement (2009), http://www.streamlinedsalestax.org/uploads/downloads/Archive/SSUTA/SSUTA%20As%20Amended%2009-30-09.pdf. The SSUTA contains statutory harmonization requirements and voluntary software certification regime. Under the SSUTA tax calculation software is certified by Member States. Businesses that use certified software (or that contract with trusted third-party providers that uses certified software) are insulated from liability for any errors in determining the proper tax. *See* SSUTA § 301 (voluntary registration); § 402A (amnesty rules); § 501 (certification provisions).

9 This estimate is an extrapolation based on revenue losses from e-commerce, mail-order, and telephone sales in States that have a GDP roughly equivalent to that in Puerto Rico. It assumes a 50% recovery of lost revenue based on a further assumption that commerce between the mainland and Puerto Rico is equally spread among the States, and further on the assumption that the 22 of the 45 States with a sales tax that are already members of the SST remain members of the SST. Using 2007 figures therefore, the (purchasing power parity adjusted) GDP for Puerto Rico ($72.03 billion) is bracketed by Hawaii ($61.53 billion) and New Mexico ($76.17 billion). Thus, assuming recoverable Puerto Rican sales tax losses from e-commerce and mail order sales through SST membership are roughly 50% of the midpoint between estimated Hawaiian losses ($359.2million) and the New Mexico losses ($440.2 million) or $399.7 million. DONALD BRUCE & WILLIAM FOX, CENTER FOR BUSINESS AND ECONOMIC RESEARCH, UNIVERSITY OF TENNESSEE, STATE AND LOCAL SALES TAX REVENUE LOSSES FROM E-COMMERCE: UPDATES ESTIMATES, Table 4: Combined State and Local Revenue Losses in 2006 (2001), *available at* http://cbaweb2a.bus.utk.edu/cber/ecomm/ecom0901.pdf. *See also* DONALD BRUCE, WILLIAM FOX, & LEANN LUNA, UNIVERSITY OF TENNESSEE, STATE AND LOCAL GOVERNMENT SALES TAX REVENUE LOSSES FROM ELECTRONIC COMMERCE (2009) (further updating the earlier work, but with statistical efforts focusing more narrowly on e-commerce, excluding mail order and other distance-sales tax losses, indicating in Table 4 that Hawaiian and New Mexico e-commerce-only losses in 2009 would be $106.8 million and $ 218.1 million.)

10 This rough estimate assumes that Zappers are as prevalent in the Puerto Rican economy as they are in Quebec where some of the most empirically accurate studies on Zappers have been conducted. It further assumes that because the Puerto Rican economy is only 40% as large as the Quebec economy, that Puerto Rican losses to this fraud would similarly be about 40% of the Quebec losses. Some caveats are appropriate: (1) because this is a technology-based fraud the level of economic development may suggest that the Quebec losses would be higher than the Puerto Rican losses, but (2) because the best Quebec studies were limited to the most abused sector – the restaurant industry, even though Zapper-based ECR frauds are common in grocery stores (USA, Netherlands, Brazil), hairdressing salons (France, Netherlands, Germany), and discount clothing stores (Australia) the full-economy revenue losses are much higher than the Quebec studies indicate, and (3) to the extent that the Puerto Rican economy is more dependent on the restaurant and hospitality sector than is the Quebec economy, then the Puerto Rican losses will again be higher than the losses measured in Quebec. To compare the Puerto Rican and Quebec economy and arrive at the 40% figure government statistic from Quebec were used. *See Québec ranks 22nd in terms of GDP per capita,* INSTUTUT DE LA STATISTIQUE QUEBEC, APRIL 5, 2007, http://www.stat.gouv.qc.ca/salle-presse/communiq/2007/avril/avril0705a_an.htm (the central authority for the production and dissemination of official statistical information for Quebec government departments and agencies) providing a statistically consistent measures for the GDP for Quebec ($230.6 billion) and Puerto Rico ($93.4 billion). On the government studies performed by Statistics Quebec determining revenue losses from fraud in the restaurant sector in excess of $425 million see the next section of this paper (40% x $425 million = $170 million).

sort" (*sólo en caso de ser absolutamente indispensable*) by the Puerto Rican Advisory Board on Fiscal and Economic Reconstruction.[11]

Even though Puerto Rico[12] may not be politically ready to join the twenty-two states[13] that are already full members of the SSUTA, this does not mean that the Commonwealth should not make preparations to join, nor should it ignore the second issue, the serious revenue threat posed to the IVU by automated sales suppression technology.

Preparing to join SSUTA would entail adopting all of the non-legislative SSUTA provisions. These provisions would include rules and procedures on software certification. Taking these steps only makes good sense if Puerto Rico decides to move forward with the statutory harmonization needed for full SSUTA membership.

Zappers (cash skimming software) are a different story. This technology, when added to modern electronic cash registers (ECRs), is a global problem. Germany, Brazil, Quebec, the Netherlands, and Sweden are among the many countries that have uncovered patterns of abuse and serious revenue losses from them. Although there are no published reports that Zappers have been found in Puerto Rico, it is very likely they are present. It seems that wherever ECRs are used to record sales, Zappers have been found to be removing selective cash sales and allowing businesses to siphon off revenue.

This paper is about the threat that Zappers pose to the strength and stability of the IVU, and how Puerto Rico can move against this threat today by extending the certification provisions of the SSUTA to ECRs. In other words, it is not necessary to join SSUTA to learn from it – although joining might not be such a bad idea.

II. SCOPE OF THE PROBLEM – STUDIES & CASES

A. Studies

The leading government studies of automated sales suppression are from Quebec and Germany. The UK reportedly completed a study in late 2009, how-

---

11 ADVISORY BOARD ON FISCAL AND ECONOMIC RECONSTRUCTION, REPORT TO THE GOVERNOR OF PUERTO RICO ABOUT FISCAL RECONSTRUCTION 41 (2009), http://www.fortaleza.gobierno.pr/CAREF-Informe%20Fiscal.pdf (in Spanish).

12 Puerto Rico, an Associate Member of the Streamlined Sales Tax, was admitted by a 13 to 0 vote of the governing board on April 19, 2006, but has yet to apply for full membership. Eric Parker, *Streamlined Governing Board OKs, Certified Service Provider Contract*, TAXANALYSTS.COM, Apr. 20, 2006, Doc. Num. 2006-7566; 2006 STT76-1.

13 The SSUTA was the product of the combined effort of 44 states and the District of Columbia. At present the 22 full-member states that are currently implementing the SST are: Aransas, Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Nebraska, Nevada, New Jersey, North Carolina, North Dakota, Oklahoma, Rhode Island, South Dakota, Vermont, Washington, West Virginia and Wyoming. Associate members are Ohio, Puerto Rico, Tennessee, and Utah.

ever, these results have not been made public. All of these studies focus on the restaurant sector. The German and Quebec studies both underscored the need for significant legislative reforms. Neither government has made the full studies available to the public, but a government-to-government exchange could be (and most likely should be) arranged. Summaries have been released, and the Quebec and German studies arrive at very similar conclusions.

1. Quebec

The government of Quebec conducted two studies. The first study gathered its subjects from the customer list of a known distributor/developer of automated sales suppression software. This investigation (the First Inspection Wave) examined 70 systems and uncovered 41 zappers.[14] A more statistically accurate investigation followed (the Second Inspection Wave). It was based on a random sample of businesses within the restaurant and hospitality industry. This survey, conducted by Finances Quebec, found that 16% of all sales went unreported.[15] This, of course, is a consumption tax as well as an income tax problem.

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

> Although the majority of restaurant owners 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 taxes and sales taxes. Tax losses in this sector are significant. Revenue Quebec estimates them at $425 million for the 2007-2008 fiscal year.[16]

---

14 Dave Bergeron & Richard Ainsworth, *Zappers (Automated Sales Suppression)* 12 (July 31, 2008) (Powerpoint presentation at the New York Prosecutors Training Institute (Syracuse, NY)) (on file with author).

15 *Id.* at 13 (but noting further that the 16% figure measures all skimming frauds, not just skimming with Zappers).

16 Press Release, 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*] (Jan. 28, 2008) *available at* http://www.revenu.gouv.qc.ca/fr/ministere/centre_information/communiques/autres/2008/28jan.aspx. *See also* accompanying powerpoint presentation Facturation obligatoire dans le secteur de la restauration, L'évasion fiscale au Québec, 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],* 3 (January 28, 2008) (in French) (on file with author, with translation).

Other things being equal,[17] because Puerto Rico's economy is roughly 40% the size of the Quebec economy, a similar study in Puerto Rico's restaurant sector might find tax losses to be in the $150 to $170 million range. This estimate could very well be low. Puerto Rico is in large measure a tourist-based economy, and this is reflected in the restaurant sector being the largest contributor of overall IVU revenues.[18]

2. Germany

The Interim Report of the German Working Group on Cash Registers indicated that the Group was "… aware of [technology-assisted] fraud amounting to 50% of companies cash receipts."[19] The Working Group did not separately quantify the kinds of *technology-assisted* fraud involved.

The Working Group's 50% observation is supported by a report made by the German Federal Audit Office (BHR) to the German Parliament in 2003. In this

---

17 Of course "other things" are not equal. Take for example the relative rate structures of Quebec and Puerto Rico. Because zappers reduce reported taxable income of businesses, and because these businesses tend to use these funds either to pay undeclared dividends or employee wages under the table, there is more than just a consumption tax comparison needed. In all of these taxes, the Puerto Rican rates are generally much higher than those in Quebec.

Consumption Tax: Puerto Rico's aggregate sales tax rate is 7% whereas Quebec's is 7.5%. However in the hospitality industry special rates apply in Puerto Rico. The same is not true in Quebec. In Puerto Rico hotels with casinos are subject to an 11% rate, which will include restaurant meals if the charge is part of hotel charge. Ley del Impuesto sobre el Canon por Ocupación de Habitación del Estado Libre Asociado de Puerto Rico [Room Occupation Tax Law of the Commonwealth of Puerto Rico], Ley Núm 272 de 9 de septiembre de 2003, 13 L.P.R.A. sec. 2271-2272(v) (2007 & Supp. 2008).

Corporate Income Tax: Quebec taxes corporate business at 11.9%, but there is a reduced rate for small businesses of 8%. DELOITTE, CORPORATE INCOME TAX RATES, CANADA, *available at* http://www.deloitte.com/view/en_CA/ca/services/tax/f54d9c14ef6e2210VgnVCM100000ba42f00aRCRD.htm (follow "Corporate income tax rates 2005-2012" hyperlink).

Corporate income tax rate in Puerto Rico is comprised of a base rate of 20%, plus a graduated surcharge in addition to the corporate income tax at rates that range from 15% to 19%, personal income tax rates in Puerto Rico progressive up to 33%, DELOITTE, INTERNATIONAL TAX: PUERTO RICO HIGHLIGHTS (2009), *available at* http://www.deloitte.com/view/en_GX/global/services/tax/international-tax/international-tax-and-business-guides/all-jurisdictions/index.htm (follow "Puerto Rico Highlights" hyperlink).

Personal Income Tax: Quebec taxes personal income between 16 and 24% (indexed with an inflation factor of 2.36%). KPMG, PERSONAL INCOME TAX RATES IN CANADA, *available at* https://www.kpmg.com/Ca/en/IssuesAndInsights/ArticlesPublications/Documents/2009_Federal%20and%20Prov%20Income%20Tax%20Rates%20-%204Q%202009.pdf (last visited Aug. 8, 2010).

18 DISTRIBUCIÓN DEL IMPUESTO DE VENTAS Y USO ESTATAL (IVU) POR CÓDIGO NAICS, AÑOS FISCALES 2007-2009, *supra* note 4.

19 WORKING GROUP ON CASH REGISTERS: INTERIM REPORT 5 (2005) (in German) (translation on file with author).

report the BHR appears to focus only on factory installed software.[20] The BHR concludes that the potential loss in Germany is in the billions of euro:

> The Federal Audit Office (BHR) has complained that later models of electronic cash registers and cash management systems now fail to meet the principles of correct accounting practice when it comes to recording transactions … The risk of tax fraud running into *many billions* [of euro] should not be underestimated in cash transactions.[21]

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

> One federal state is currently implementing a special "restaurant" initiative. Checks already made have led to average upward revisions of 46% of original turnover. A comparable initiative in another federal state resulted in over half the cases (54%) having upward revisions of 60% of declared turnover. Fraud amounting to 25% was detected in a fifth of the cases, and was as high as 5% in the remaining 26% of cases. A third federal state has found that around 45% of till receipts involving cash are subject to upward revisions ranging from 20% to 118%.[22]

Although restaurants are a popular venue for sales suppression software, it is clear from Dutch and Brazilian investigations that grocery and convenience stores, hairdressers and butcher shops also have very high concentrations of automated sales suppression. Because the sales tax does not reach as broadly as a Goods and Services Tax/ Value Added Tax (GST/VAT), this kind of technology-assisted fraud in Puerto Rico's grocery stores and hairdressing salons would impact the income tax more than the sales tax.[23]

---

20 *Id.* at 5 (listing the following attributes: (1) erasing all data entries, (2) resetting the zero counter, (3) unwarranted counter-entries, (4) unwarranted use of the training mode, and (5) suppressing the grand total memory.)

21 BRH comments 2003, No 54, Federal Parliament circular 15/2020 at 197-198 (Nov. 24, 2003) (in German) (original and translation on file with author).

22 *Id.* at 5.

23 This observation is corroborated in the 2010 study by the Colegio de Contadores Públicos Autorizados de Puerto Rico [Puerto Rico Board of Accountancy]. ANÁLISIS DEL DESEMPEÑO DEL IVU Y METODOLOGÍA PARA LA EVALUACIÓN DE LOS INCENTIVES CONTRIBUTIVOS [THE EXPERIENCE OF THE SUT AND SPECIAL TAX INCENTIVES] (in Spanish) (2009), http://www.colegiocpa.com/download.php?id=774. The graph on page 17 indicates that 80% of the collection of the IVU comes from businesses that are likely to make a large number of cash transactions.

B. US Cases

However, Zappers are a significant income tax problem. Consider the two large US zapper cases – Stew Leonard's Dairy and the La Shish Restaurants. Stew Leonard's Dairy was a $17 million zapper-assisted tax fraud in a chain of grocery stores located in Norwalk Connecticut. This ten-year fraud was uncovered by US Customs when cash was found in large denomination bills packed into vacation suitcases headed for St. Martin in the Caribbean.[24]

The La Shish case in Detroit Michigan was a $20 million zapper-assisted tax fraud at the thirteen-location La Shish restaurant chain. The owner, Talal Chahine, remains a fugitive from U.S. authorities (believed to be in Lebanon) with a warrant issued for his arrest.[25] This four-year fraud allegedly sent its proceeds in small denomination cashier's checks to fund Hezbollah terrorists.[26]

Both *Stew Leonard's Dairy* and the *La Shish* restaurant cases were federal income tax investigations.[27] Related state sales and income tax enforcement actions commenced after the federal investigations were well underway. In the Connecticut case the sales tax impact was minimal, but in the Michigan case it was significant.[28]

---

24 U.S. v. Leonard, 37 F.3d 32 (2d. Cir. 1994), *aff'd,* 67 F.3d 460 (2d. Cir. 1995) (although the tax case was settled, the details of the fraud are preserved in these federal sentencing appeals).

25 Press Release, U.S. Department of Justice, Eastern District of Michigan, La Shish Financial Manager Sentenced for 18 months for Tax Evasion (May 15, 2007) *available at* http://nefafoundation.org/miscellaneous/FeaturedDocs/U.S._v_Aouar_DOJPR_Sent.pdf.

26 Press Release, U.S. Department of Justice, Eastern District of Michigan, Superseding Indictment returned Against La Shish Owner (May 30, 2007) *available at* http://www.justice.gov/tax/usaopress/2007/txdv072007_5_30_chahine.pdf.

27 Waiting to follow federal zapper investigations may not be the optimal response to this fraud, because other than Stew Leonard's Dairy and the La Shish restaurants there are no other reported IRS investigations of zappers.

28 In the Stew Leonard's Dairy case U.S. Customs searched Stew Leonard Sr. in the spring of 1991, leading to the execution of search warrants on August 9, 1991 by special agents of the IRS Criminal Investigation Division. *Leonard,* 37 F.3d at 35; DEPT. OF THE TREAS., I. R. S. 75 YEARS OF CRIMINAL INVESTIGATION HISTORY (1919 – 1994) 145, *available at* http://www.thememoryhole.org/irs/irs_75_years.rtf (last visited Mar. 27, 2009). The State of Connecticut commenced its audit "… as a result of IRS actions, in February, 1992 …" Leonard v. Commissioner of Revenue Services, 264 Conn. 286, 289 (2003). On July 22, 1993 Stew Leonard pleaded guilty in the federal audit. The State's audit was nowhere near completion at this time. A final Connecticut determination was not rendered until February 27, 1996.

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

> Michigan law (Michigan Compiled Laws Section 205.28(1)(f)) prohibits divulging any facts or information obtained in connection with the administra-

Therefore, based on these studies and American cases, it seems reasonable to conclude that zappers may well be siphoning off many multiples of the estimated $200 million IVU revenue from the Puerto Rican Treasury.

III. SKIMMING WITH ZAPPERS AND PHANTOM-WARE

Skimming cash receipts is an old fashioned tax fraud; a fraud traditionally associated with small or medium sized enterprises. Large businesses with formalized internal control mechanisms, external accountants, and professional management structures do not normally engage in skimming,[29] although personal conversations with auditors from Revenue Quebec indicate that this may not be a solid assumption any more. Businesses that skim frequently keep two sets of books (one for the tax man, the other for the owner). In its simplest (non-technological) form there are two tills, and the cashier simply diverts some cash from selected sales into a secret drawer. A record of the diversion may be maintained, but it will be kept outside the formal accounting system. Businesses that skim rarely do so with credit card transactions precisely because these sales can be documented externally through the banking system. Skimming frauds thrive when the owner (or a close family member) is the cashier.[30]

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

> tion of a tax, or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the department for a tax administered by the department. According, we are unable to provide you with the information you seek.

Email from Michael Eschelbach, Administrative Law Specialist, Tax Policy Division, Michigan Department of Treasury, Feb. 4, 2008 (on file with author).

29 EU Commission, Fiscalis Committee Project Group 12, Cash Register Project Group, Cash Register Good Practice Guide ¶ 2.5 (Dec. 2006) (unpublished report, on file with author).

30 See for example the use of double tills to manually skim cash receipts in the UK at Aleef Garage Ltd. This was a £5.3 million tax fraud, and according to Steve Armitt, Group Leader HMRC Criminal Investigations indicated, "... the investigation was made all the more difficult because of the closed ranks of the employees involved some of whom were close family members ... [t]hose involved tried to make it as difficult as possible for the cheating to be discovered." HMRC News Release, Company Directors Jailed for £5 million Fraud 1 (Nov. 13, 2007) *available at* https://www.gnn.gov.uk/content/detail.asp?NewsAreaID=2&ReleaseID=330199 (last visited Mar. 23, 2009).

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

While Puerto Rico has uncovered no zappers or phantom-ware applications, the Province of Quebec (alone) has brought 230 cases to court.[31] In the early days Quebec was concerned that the software that facilitated this fraud was US made and was sold over the internet for $500.[32] Canadian subsidiaries of US companies were early providers.[33] However, the design and installation of this software became soon a "cottage industry" for local IT professionals.[34]

---

31 Roy Furchgott, *With Software, Till Tampering Is Hard To Find*, NEW YORK TIMES (August 29, 2008) indicating:

> [T]he Canadian province of Quebec may be the world leader in prosecuting zapper cases. Since 1997, zappers have figured in more than 230 investigations, according to the tax collecting body Revenue Québec, which has found an active market for the software. In making 713 searches of merchants, Revenue Québec found 31 zapper programs that worked on 13 cash register systems.

available at http://www.nytimes.com/2008/08/30/technology/30zapper.html?scp=1&sq=With%20Software,%20Till%20Tampering%20Is%20Hard%20to%20Find%20%20comments&st=cse (last visited May 12, 2009).

32 Craig Silverman, *Zapped!*, HOUR (Feb. 19, 2004) , http://www.hour.ca/news/brief.aspx?iIDArticle=783 (last visited Mar. 25, 2009).

33 Turcotte v. Quebec (Ministry of Revenue), [1998] CarswellQue 1041, [1998] R.D.F.Q. 110, (Superior Court of Quebec) (Can.). This case involved the MRQ investigation of Gamma Terminal, Inc., a wholly owned Canadian subsidiary of an American company, Gamma Micro Systems. This investigation began in 1997 and focused on the distribution of the Gamma Restaurant Management System. It eventually lead to a number of conviction of restaurants that used this system to delete sales records, including the companies 136530 Canada, Inc. and San Antonio's Grill. Press Release, Revenue Quebec, Deux sociétés coupables d'avoir utilisé un camoufleur de ventes dans des restaurants de Laval et de Repentigny [Two companies guilty of having used a camoufleur sales in restaurants in Laval and Repentigny] (April 25, 2005) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/25avril.asp (in French, translation on file with author) (last visited May 12, 2009).

34 Consider for example the cases of (1) Audio Lab LP; (2) Michael Roy; or that of (2) Luc Primeau.

Audio Lab LP: On April 8, 2004 Revenue Quebec announced that it executed four search warrants on the numbered company 9061-1184 Quebec Inc. which operated a restaurant under the name San Antonio Grill in Laval, Quebec. The allegation was that a "sales Zapper" (*camoufleur de ventes*) was used to delete sales records. The Zapper was on a diskette used in connection with the restaurant's

computer system. News Release, Revenue Quebec, Le ministère du Revenu soupçonne le restaurant Grill San Antonio de Laval d'avoir utilisé un zapper [Tax Evasion: The Ministry of Revenue Suspects the Restaurant Grill San Antonio de Laval of having used a Zapper] (Apr. 8, 2004) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2004/08avril.asp (in French only, last visited May 12, 2009). Next year, on April 25, 2005, Revenue Quebec announced that the director of San Antonio Grill pleaded guilty to using a Zapper. (The director, Mr. Apostolos Mandaltsis, was personally fined.) A related company of similar name, Grill San Antonio in Repentigny, also pleaded guilty to similar offences. News Release, Revenue Quebec, Deux sociétés coupables d'avoir utilisé un camoufleur de ventes dans des restaurants de Laval et de Repentigny [Two Companies Guilty of having used Zappers in Restaurants in Laval and Repentigny], *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/25avril.asp (in French only, last visited May 11, 2009). Later that year, on October 1, 2005, Revenue Quebec announced that it executed five more search warrants in Montreal and Laval with respect to Audio Lab LP, Inc. It was under suspicion of having developed and marketing a sales Zapper, software that was compatible with its own restaurant cash register software, Softdine. News Release, Revenue Quebec, Revenu Québec enquête sur un concepteur de logiciel de point de vente soupçonné d'avoir conçu et distribué un camoufleur de ventes [Revenue Quebec Investigation of a Software Designer Outlet Suspected of having Developed and Distributed Zappers] (Oct. 14, 2005) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/140ct(2).asp (in French only, last visited Ma 11, 2009). Softdine was the operating software in the cash registers at San Antonio's Grill in Laval, and at Grill San Antonio in Repentigny. On June 26, 2007 Audio Lab LP, Inc. pleaded guilty to charges of having, "… designed and marketed a computer program designed to alter, amend, delete, cancel or otherwise alter accounting data in sales records kept by means of a software that [Audio Lab LP] had designed and marketed." In other words, it pleaded guilty to developing a Zapper to "add-on" to its own commercial software (Softdine) that it provided to restaurants for use in their POS systems. Press reports directly link this conviction to the investigation begun at Grill San Antonio in Laval in 2004. News Release, Revenue Quebec, La société Audio L.P. inc. condamnée pour fraude fiscale [The Company Audio LP, Inc. Convicted of Tax Evasion] (Sept. 21, 2007) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2007/21sep.asp (in French only, last visited May 11, 2009).

Michael Roy: Before the first warrants were issued in Audio Lab LP Revenue Quebec had successfully brought to conclusion an extensive investigation of twenty-eight restaurants doing business under the name Stratos. Each of the restaurants in the Stratos chain used Zappers. To dispose of the excess cash from skimmed sales (1) a double billing system was put in place with suppliers (to conceal purchases made in cash), and (2) wages were paid to employees in cash (without being reported as income). The guilty pleas from this investigation came in waves – nineteen companies pleading guilty on September 26, 2002; another six pleading guilty on October 11, 2002, and the four remaining pleading guilty on March 21, 2003. Press releases provide details of only the final ten companies. In aggregate the taxes and penalties for these companies came to $1,816,070.90, but the real thrust of the news releases were that "… the Department has conducted searches in order to establish proof that the designer of the IT function associated with the cash register software Terminal Resto had participated in the scheme set up by restaurants in the Stratos chain." The breakdown is: $429,179.07 (GST) + $492,023.11 (PST) + $214,589.55 (federal penalties) + $625,028.89 (provincial penalties) + $55,250.28 (judicial fees). News Release, Revenue Quebec, Tous les restaurants Stratos coupables de fraude fiscale en lien avec l'utilisation du zapper [All Stratos Restaurants Convicted of Fraud in Connection with the use of a Zapper] (Mar. 18, 2003) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/18mars.asp (in French only, last visited May 11, 2009). That proof was forthcoming on April 25, 2003, when Mr. Michel Roy and his two sons Danny and Miguel were convicted of tax evasion. The father (Michel) was the creator of the Zapper that worked with Resto Terminal. He promoted it and made the sales. His sons (Miguel and Danny) installed the software and designed the civil fraud. Aggregate fraud penalties assessed against the Roys were $1,064,459. News Release, Revenue Quebec,

IV. SOLUTIONS – POLICY ORIENTATIONS

Globally, two policy orientations guide enforcement actions in this area – one approach is rules-based; the other is principles-based.[35] They are not mutually exclusive – degrees of blending are common. Rules-based jurisdictions adopt comprehensive and mandatory legislation regulating, and/or certifying cash registers. Jurisdictions taking this approach include Greece and Germany. These jurisdictions are classified generally as "fiscal till" or "fiscal memory" jurisdictions.

Principles-based jurisdictions rely on compliant taxpayers following the rules. Compliance is enforced with an enhanced audit regime. Comprehensive, multi-tax 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. Jurisdictions taking this approach in-

---

Des amendes de plus de un million de dollars - Un père et ses deux fils condamnés pour fraude fiscale en lien avec le zapper [Fines of more than One million dollars – A Father and his Two Sons convicted for Tax Evasion in connection with the Zapper (May 2, 2003) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/02mai.asp (in French only, last visited May 11, 2009).

Luc Primeau: Revenue Quebec announced on March 17, 2003 that seven Patio Vidal restaurant franchises and a bar, La Tasca, from Gatineau, Quebec as well as another bar named O'Max in Masson-Angers, Quebec were convicted of adding Zappers to their Microflash cash register software (later upgraded to a new version called Caracara). Even though guilty pleas were entered on March 14, 2003, a search warrant had already been executed the previous December against the designer of Microflash and Caracara, because the software developer was suspected of also being the developer of the associated Zapper program. News Release, Revenue Quebec, M. Marcel St-Louis de l'Outaouais coupable de fraude fiscale liée à l'utilisation d'un zapper [Mr. Marcel St. Louis de l'Outaouais Convicted of Tax Evasion related to the use of a Zapper] (Mar. 17, 2003) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/17mars.asp (in French only, last visited May 11 2009). On October 17, 2005 Luc Primeau admitted using his software to assist these companies to evade $435,000 in GST and QST. They skimming $2.7 million is cash sales. Mr. Primeau was fined $20,000 for his involvement. However, Mr. Primeau was more than a Zapper salesman, he considered himself a provider of management services (admittedly focused on how to "manage Zappers") for which he also charged a fee. Revenue Quebec determined that not only did Mr. Primeau fail to report GST and QST of $33,725.45 on his own sales (of Zappers), but he also failed to report income of $155,084.99 in services income Zapper management advice). News Release, Revenue Quebec, Le concepteur d'un camoufleur de ventes de Boucherville plaide coupable à diverses accusations portées par le fisc québécois [The Zapper Designer of Boucherville Pleads Guilty to Various Charges brought by Inland Revenue Quebec] (Oct. 26, 2005) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2005/26oct.asp (in French only, last visited May 11, 2009). The real reason Mr. Primeau did not report this income probably [no one really knows] had to do with the fact that he was being paid out of the $2.7 million in skimmed cash sales from the nine companies where he sold, installed and managed his Zappers. These funds probably needed to be kept "hidden" (to facilitate the overall success of the fraud), and in a sense represented his "share" of the skimmed profits.

35 EU Commission, Fiscalis Committee Project Group 12, Cash Register Project Group, Cash Register Good Practice Guide 5-6 (Dec. 2006) (unpublished report, on file with author).

clude the UK and the Netherlands. France has implemented a program of preventive audits that target technology providers.[36] A similar effort can be found in Quebec where the customer lists of audited technology providers have been used to roadmap later audits of businesses suspected of technology-assisted skimming.

Quebec is in transition between these policy orientations. Prior to January 28, 2008, Quebec was squarely with the group that preferred a principles-based approach. However, the Quebec Minister of Revenue, Jean-Marc Fournier, announced[37] that by late 2009 the MRQ will begin testing the *module d'enregistrement des ventes* (MEV).[38] The MEV will be used only in the restaurant sector. By 2010 or 2011 MEVs will be mandatory in all Quebec restaurants, where they will assure accuracy and retention of business records within electronic cash registers (ECRs).

The US is particularly hampered in its approach to zappers – federal income tax audits are not well coordinated with state and local retail sales tax audits. 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 Puerto Rico wanted to tackle this problem it could apply a uniquely American solution - blending rules and principles based solutions in a simple extension of SSUTA principles.[39] Under a SSUTA structure certified third party software providers (CSPs)[40] 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 the Commonwealth that ECRs were accurately recording sales, that the correct IVU was being collected by the business,

---

36 *Id.* at 6.

37 Revenue Quebec, Press Release, Jean-Marc Fornier, *Pour plus d'équité dans la restauration : il faut que ça se passe au-dessus de la table* [For more equity in the restaurant sector it is required that business is conducted above the table] (Jan. 28, 2008) *available at* http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/autres/2008/28jan.asp (last visited May 18, 2009, translation on file with author).

38 Jean-Marc Fornier, *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] 3 (January 28, 2008) (in French) (powerpoint presentation and translation on file with author).

39 Streamlined Sales and Use Tax Agreement (adopted November 12, 2002, amended November 19, 2003 and further amended November 16, 2004) § 203 (defining a CSP as "[a]n agent certified under the Agreement to perform all the seller's sales and use tax functions, other than the seller's obligation to remit tax on its own purchases.") *available at* http://www.streamlinedsalestax.org/uploads/downloads/Archive/SSUTA/SSUTA%20As%20Amended%2009-30-09.pdf.

40 *Id.,* at § 203 (defining a CSP as "[a]n agent certified under the Agreement to perform all the seller's sales and use tax functions, other than the seller's obligation to remit tax on its own purchases.")

and that it was properly remitted. At the same time the corporate income tax auditors could be assured that zappers were not being used to underreport income. Certification of the CSP could be undertaken by the Puerto Rican Treasury.

V. SOLUTIONS – PRESENT APPLICATIONS

The final part of this article will describe four solutions to the zapper problem. The traditional fiscal till solution (employed by Greece) will be contrasted with the traditional principles-based solution (employed by the Netherlands). Because Germany will conclude the development of a smart card this year, the German approach will be considered next. The final option is the SSUTA extension.

A. Greece: FECR, AFED Printers, and FESDs

Greece has had comprehensive, rules-based fiscal till legislation in place for over twenty years. Technical specifications for Fiscal Electronic Devices (FEDs) were published widely in 2004. These rules provide complete ECR data security.

All Greek ECRs are certified. It is illegal to operate a business with a non-certified cash register. All technical specifications for certification are set out in Greek law. It is a very simple matter for an auditor to determine if a specific ECR has been tampered with. Factory-installed phantom-ware must be removed before certification. If a self-help version of phantom-ware[41] is on the ECR it will either be blocked, or there will be a record of the manipulation so that its impact on revenues will be neutralized. Data from all transactions are preserved and SHA-1 encrypted in the fiscal memory. Use of an add-on zapper will be a violation of the licensing regulations, and it will be detected in the same manner as self-help phantom-ware.

Through the certification process the Ministry of Finance preserves a copy of all approved firmware. It is a simple matter to calculate a checksum value (CRC-32[42] or SHA-1) for the object code of the firmware. Auditors can then read the contents of the program memory of a certified ECR and determine if changes

---

41 For a discussion of self-help phantom-ware *see* Richard T. Ainsworth, *Zappers and Phantom-ware: The Need for Fraud Prevention Technology* (Boston Univ. School of Law Working Paper No. 08-20), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1139826.

42 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. Wesley Peterson & D. T. Brown, *Cyclic Codes for Error Detection,* 49 PROCEEDINGS INST. RADIO ENGINEERS 228 (1961).

have been made in the firmware (through phantom-ware or zappers) by comparing his reading with that of the file kept in the Ministry of Finance.

Twenty years of experience in this field has given the Greek tax administration a wealth of knowledge about ECR security, but it has resulted in a somewhat complex system when seen from the outside. A rough understanding of the Greek system requires the reader to distinguish among a number of acronyms – in addition to FEDs there are FECRs, AFED Printers, and FESDs.

Under Greek rules FEDs are divided into two categories: (a) fiscal electronic cash registers (FECR) which are accompanied by autonomous fiscal electronic device printers (AFED Printers), and (b) fiscal electronic signing devices (FESDs). The first are used *only* in B2C transactions; the second may be used in B2C or B2B transaction. Both digitally sign tax-related documents.

1. FECRs and AFED Printers.

Fiscal electronic cash register (FECR) is a term that includes ordinary standalone cash registers, and cash registers equipped with advanced connection capabilities (network or PC operated machines). Autonomous fiscal electronic device printers (AFED Printers) are fiscal printers that operate only via a connected computer. They have no keyboard or display terminal. They do more than just print receipts however. AFED Printers store and secure in their fiscal memory the data that has passed through them (revenue from sales, and taxes collected).[43]

Data from the electronic journal memory is signed by a secure hash algorithm (SHA-1).[44] This hash value is permanently safeguarded and stored in the fiscal memory. Daily sums (receipts and VAT amounts) are saved into the fiscal memory, cumulatively and on a daily basis. This function essentially preserves the X and the Z Reports along with the Electronic Journal.

---

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

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

2. FESDs

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

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

Presently, the cost of an FESD is between € 450 and € 650. Thus, a FESD alone can cost more than a FECR, and for this reason smaller businesses do not normally use FESDs to issue legal receipts.[46] Economies of scale also come into the picture because a single FESD can support many cash registers linked on a network. It can be installed remotely (even in another city), and need not be directly connected to the point of sale terminal.

The Greek experience is an important template for Puerto Rico. The Puerto Rican Advisory Board on Fiscal and Economic Reconstruction recommends that the Commonwealth adopt fiscal printers and a receipt lottery system. The lottery encourages consumers to demand receipts issued by the fiscal printer and thereby channels B2C sales through certified cash registers where the IVU will be recorded.[47]

It is not clear if the Advisory Board is considering a device like the AFED Printer, or like the FESD. The Board does suggest that the government will bear the costs of this system (unlike the Greek system which is a business cost), and it seems to suggest that the system would be adopted for B2C transactions even though there is a B2B component that also needs to be certified.

---

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

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

47 *See* ADVISORY BOARD ON FISCAL AND ECONOMIC RECONSTRUCTION, *supra* note 11, at 26.

B. The Netherlands: Comprehensive Traditional Audits

The Netherlands is a principles-based jurisdiction, relying only on traditional audits to detect sales suppression technology. Fiscal till jurisdictions, like Greece, also must rely on audits, but not to the same extent and certainly not with the comprehensive scope as the Dutch.

The Netherlands is clearly at the other extreme. 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 recordkeeping systems of all businesses (encrypting the memory of all ECRs and POS systems) just to catch a few fraudsters is avoided at all costs. Following a pure principle-based approach to enforcement, the Netherlands feels it can rely on good business practices and compliant tax payers.

Netherlands officials speak about performing "deep audits" – that is, audits that are not focused just 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.

The Netherlands has been successful with this approach. One of the best examples of how a comprehensive multi-tax audit can uncover data manipulations, and how this fraud is derivative of the symbiotic relationship that develops between SMEs and their ECR providers can be seen in the Grand Café Dudok case.[48] A *grand café* is a style of café that occupies a single large space welcoming a large amount of foot traffic and a large cash-based clientele, so it 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 Belastingdienst (Dutch IRS) was suspicious of the low wages reported, and thought that additional (unreported) compensation might be being distributed (under the table).[49] Testimony in the case indicated that on the second day of the payroll audit the managing director of Straight Systems BV visited Dudok where he was approached by the Dudok's

---

48 Rechtbank Rotterdam [District Court of Rotterdam], June 2, 2006, LJN: AX6802 (Neth.) *available at* http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AX6802 (in Dutch) (translation on file with author); appealed to the District Court of The Hague where the judgment is upheld, Feb. 29, 2008, LJN: BC5500 *available at* http://zoeken.rechtspraak.nl (in Dutch) (translation on file with author).

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

owner-manager. Straight Systems BV[50] supplied the Finishing Touch point-of-sale 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. The numbers did not "seem right" to the auditors, and they were requesting back-up data, something that 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. This was, "... a hidden menu option that, after enabling ..., allowed operators of catering establishments to delete cash register receipts from the system."[51] After this discussion "... an employee of [Straight Systems] visited [Dudok] and explained [and enabled] the application of the erase rule [or hidden delete function[52]], after which [Dudok] subsequently decided to start using [it] ..."[53] Ben B.G.A.M. van der Zwet, a government technology auditor observes:

> 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 detail 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. Because [the entrepreneur] was aware that once the POS records were audited the fraud would instantly be clear.

---

50 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." Straight Systems BV, http://www.straight.nl (last visited Mar. 24, 2009) (in Dutch, translation on file with author).

51 LJN: AX6802, at Consideration of the Evidence (Jun 2, 2006) (in Dutch) (translation on file with author). The case discusses three software programs: Twenty/Twenty; Finishing Touch; Tickview.exe. Twenty/Twenty was a US touch-screen program that did not have a phantom-ware application. Straight Systems BV added the phantom-ware application to Twenty/Twenty and renamed the program Finishing Touch. Using just this program you can view the sales ticket and change data. With a secret command the Tickview.exe program within Finishing Touch can be activated and the operator is asked if they would like to delete the whole ticket. If an affirmative response is given then the system records a "no sale" and the entire audit trail to the original data is eliminated. Email from Ben B.G.A.M. van der Zwet, (May 28, 2008) (on file with author).

52 The trial court in Rotterdam refers to the phantom-ware application as a "hidden delete function" whereas the appeals court in The Hague refers to the phantom-ware as "the erase rule."

53 LJN: BC5500, at F3.

> 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![54]

The court upheld criminal tax fraud determinations in the Dudok case under income, value added, and payroll taxes. Both the restaurant operator and the ECR/software provider were convicted. Other successful audit-intensive cases in the Netherlands include:

- Microcraft Software which developed Analyse (aka, 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 key strokes, and the user could then indicate a percentage of turnover that would be skimmed.[55]
- B&F Software and Computers B.V. developed *Beleids Informatie Systeem* (B.I.S.) for hairdressers and an add-on program for zapping cash sales through POS and client information systems. After entering a percent to skim the system selects customers to eliminate (for example male walk-ins without appointments paying cash without special services).[56]

Thus, it is clear that an intensive and comprehensive audit approach works against automated sales suppression devices. There are a number of sizeable cases in the Netherlands and a much larger number of cases in Quebec that demonstrate the effectiveness of this approach. It is, however, very labor intensive.

C. Germany: Embedding Smart Cards in ECRs

The German Working Group on Cash Registers, comprised of the highest-tier central and regional tax authorities, has been examining automated sales suppression (both phantom-ware and zapper applications) in use in the country.

---

54 E-mail from Ben B.G.A.M. van der Zwet to Richard T. Ainsworth (Apr. 16, 2008) (on file with author).

55 The prosecutor in the district of Arnhem v. Anonymous Defendant, Rechtbank Arnhem [District Court of Arnhem], 18 april 2005, LJN: AT5876, (in Dutch) (on file with author).

56 B&F Optics B.V., Rechtbank Amsterdam [District Court of Amsterdam], 11 augustus 2005, 13/120088-03 (Neth.) (in Dutch) (on file with author).

An Interim Report has been released.[57] The problem is deemed to be serious, and a technological solution is entering the final stages of testing.

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

Papers on encryption[58] by Dr. Norbert Zisky of the PTB convinced the German Working Group that encryption techniques had been sufficiently tested in secure communication settings with measuring instruments[59] that 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.[60] Included with the technical specifications for the signature smart card was a determination of the

---

57 *See* WORKING GROUP ON CASH REGISTERS, INTERIM REPORT, *supra* note 19.

58 Norbert Zisky, Manipulation Protection – Electronic Cash Registers and POS Systems, German Federal Standards Laboratory, Brunswick & Berlin (May 2005) (unpublished draft, on file with author); Norbert Zisky, Manipulationsschutz elektronischer Registrierkassen und Kassensysteme German Federal Standards Laboratory, Brunswick & Berlin (Mar. 15, 2004) (Ger.) (unpublished draft, on file with author). Since this early paper there have been a few modifications to Professor Zisky's proposal. The critical changes include:

> 1. The signature device (smart cards) distributed by the tax authorities will be personalized to the tax payer not to the cash register (cash box);
>
> 2. The signature device will have a set of dedicated sum storages which will be controlled by the signature device itself. It [will] generate the relevant data from the set of data to be signed. In the [case where there may be] a loss of signed data the tax authorities [will be] able to read the stored data from the smart card. The sum storages [are required] to read out periodically and [are required] to be stored after signing.
>
> 3. The receipts [must] contain all relevant data for the verification of the transaction (including the signature). These [receipts will be] exactly the same [as those] in the memory (from the point of view of data modeling). With the help of [the memory record] you are able to validate each receipt. Falsification of receipts [is] not possible. But there is a little problem [currently]: If you have the paper receipt you [will need] to type in every character into your computer by hand (or you may use a scanner). The manual test of receipts without technical support will be the exception, but it [will be] possible.

E-mail from Norbert Zisky to Richard T. Ainsworth (Feb. 15, 2008) (on file with author).

59 Luigi Lo Iacono, Christoph Rulans & Norbert Zisky, *Secure Transfer of Measurement Data in Open Systems*, 28 COMP. STANDARDS & INTERFACES 311 (2006); SELMA Project, http://www.selma-projekt.de (in German) (last visited Mar. 12, 2009).

60 The INSIKA project finished its work on schedule, although the time line for publication of the results has been pushed back. The results were demonstrated at a February 18, 2009 conference in Berlin.

data structures and formats, communication protocols and security analysis for the system.[61]

Based on 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 holding of sales data (or any other activity performed on a cash register) is secured through an encrypted hash total of the main data elements in the ECR. A secure electronic signature is issued for this data based on Public Key Infrastructure (PKI).

The essence of the German solution revolves around cryptography and smart card access to cryptographic data preserved within the cash register or POS system. When the revenue authority audits it can access the records of the cash register with a "key" to read the data and determine if there has been tampering.

The German solution is a fiscal till solution, but it is far more flexible and potentially more comprehensive than the Greek solution. The German mandate is for all ECRs and POS systems to be fitted 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, or each transaction, open or closed, (sale, refund, training session, voided sale, or temporary record) could be designated as a tax relevant and signed whenever entered into the ECR. It would not matter under the German system if there was no receipt (Greek and Quebec solutions are dependent on "legal receipts.") It would only matter that each sale be processed through an ECR or POS system, and for that system to be fitted with a smart card.

The government could conduct audits remotely, because the German solution is fully digital. A data feed could be taken directly from ECRs, or data could be transmitted through an e-mail attachment. The Greek solutions cannot do this.

The Greek and German solutions can also be distinguished based on "per unit" cost of implementation. The German solution is far and away the least expensive. Greece has concerns over the high costs of its solution. Under the Greek regime the entire cost is born 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 their solution to businesses for free, but the overall cost to the government is expected to be $55 million.[62]

---

61 Ben B.G.A.M. van der Zwet, Fiscal Obligations for Cash Registers in the Netherlands 10 (Feb. 1, 2008) (unpublished draft, on file with author).

62 Caroline Rodgers, *Québec va de l'avant pour stopper la fraude fiscale*, Hotels, Restaurants & Institutions, Feb. 12, 2008, *available at* http://www.hrimag.com/spip.php?article2771 (in French only, translations with author).

Dr. Zisky estimates a cost of 50 euro for the German smart card solution.[63] In fact, Vectron's prototype of the INSIKA smart card solution has an even lower cost estimate of a "single-unit end-user price of less than 25 euro."[64]

D. Blending Rules & Principles: Certification of Third Party Service Providers

Certification is the common thread among all zapper enforcement efforts. This is apparent if we step back from the details. In each instance, – the Greek, German and Dutch – 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 problems.

In the instance of rules-based jurisdictions the prospect of forcing all businesses to accept a government presence inside the recordkeeping 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* sales activity be certified through government oversight, just because *some* records are untrustworthy? In Greece, no business can be conducted without processing transactions through a government certified ECR.

Principles-based jurisdictions are much more "hands-off" 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 unpleasant for a small business 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 audit. Funding is rarely sufficient to secure the necessary audit teams and computer audit specialists.

---

63 E-mail from Norbert Zisky to Richard T. Ainsworth (February 19, 2008) (on file with author).

64 VECTRON SYSTEMS A.G., TAMPER-PROOF POS DATA FOR PROJECTGROEP ONDERZOEK ADMINISTRATIEVE SOFTWARE (2007), http://www.gbned.nl/downloads/xmllogistiek/poas/20071031%20Vectron.pdf; Norbert Zisky, Manipulation Protection – Electronic Cash Registers and POS Systems, German Federal Standards Laboratory, Brunswick & Berlin 5.7 (May 2005) (unpublished draft on file with author) (estimating 50 euros); Norbert Zisky, Manipulationsschutz elektronischer Registrierkassen und Kassensysteme, German Federal Standards Laboratory, Brunswick & Berlin (Mar. 15, 2004) (unpublished draft, on file with author).

Fortunately, there is another option – certification of intermediaries. This approach uses certified service providers (CSPs). CSPs are well known under the SSUTA, and can be a useful tool for jurisdictions, like Puerto Rico, that might seek to develop *less intrusive* and *less expensive* methods for combating automated sales suppression. Currently SSUTA 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 traditional CSP obligations to include certification *by the CSP* to the government that *the taxpayer's ECRs and POS systems* are free from zappers and phantom-ware would create a highly sophisticated, market-driven enforcement regime. Four questions need to be addressed: (1) how would a CSP get ECR and POS system data; (2) how would a CSP know the data it has is accurate; (3) what standards should the government use to certify a CSP's automated system – (in other words) what data does a tax authority want to be sure that a CSPs automated system captures so that it can trust the CSPs attestation of the accuracy of the taxpayer's system; and (4) what is the most efficient and cost effective way for a CSP to satisfy this standard?

1. How would a CSP get ECR and POS system data?

CSPs currently pull data directly from the ECR or POS system when they determine taxability under SSUTA. This data is stored in an independent (tamper-proof) audit file, and is used by taxpayer to draft the invoice (receipt). The CSP independently maintains this file to protect itself from liability.

2. How would a CSP know that the data it has is accurate (free from manipulation)?

This is a key question. 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. Every key stroke can be recorded, collected and encrypted on the smart card, and then transmitted to the CSP.[65] Questions about any transaction, or the business records associated with any ECR could then be directed to the CSP. Only in cases of fraud would it be neces-

---

65 E-mail from Norbert Zisky to Richard T. Ainsworth (Nov. 17, 2008) (on file with author):

> You are right. 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 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.

sary for the tax administration to approach the taxpayer. If suspicions were raised it would be in the self-interest of the CSP to assist the government in determining the truth.

Comprehensive ECR monitoring would be the result, but in this instance it would be the private sector monitoring the private sector,[66] and not an intrusive government oversight program stepping in to preserve business records.

> 3. What standards should the government use to certify a CSP's automated 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 principles-based jurisdiction, like the Dutch, would set down for all ECRs. In *Your Cash Register and the Fiscal Accounting Obligations*,[67] the Dutch Tax Authority lists the requirements for a business wishing to bring their ECRs or POS system into compliance with Dutch law. 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.
- Taking adequate measures to guard against subsequent alterations in a manner that will assure that data-integrity is maintained.

The Dutch requirements may not be difficult for larger businesses, but for SMEs (which is where phantom-ware and zappers are found) the requirements are burdensome. Ben B.G.A.M. van der Zwet confirms.

Hardly, any of the cash registers or Point of Sale systems by themselves complies 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.

---

66 Not only could all transactions (final and temporary) be tracked and e-signed by the German smart card, all of this could occur in real-time. However, because the data is collected by government authorities the German planners indicate that they, "… will have a strong resistance against this online tracking of transactions." E-mail from Norbert Zisky to Richard T. Ainsworth (Nov. 17, 2008) (on file with author). There is a Serbian proposal to do this, but it has not been well received. Milan Prokin, Technical and Functional Specification of Turnover Controllers *7 (undated) (*unpublished draft prepared for Fiscalis FPG 12 Cash Register Project Group, on file with author). Professor Prokin, 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 serves store all transaction data]."

67 BELASTINGDIENST, YOUR CASH REGISTER AND THE FISCAL ACCOUNTING OBLIGATIONS 7-9 (2007), http://download.belastingdienst.nl/belastingdienst/docs/your_cash_register_and_fiscal_accounting_obligations_on2001z1fdeng.pdf

- 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.[68]

Under the SSUTA model a service provider would not be certified unless it could assure tax authorities that its system accurately, completely, and automatically captures this data from the taxpayer's ECRs. With this data on hand the CSPs attestations would be highly credible.

> 4. What is the most efficient and cost effective way for a CSP to satisfy this standard?

The German smart card is the primer solution. It is far less expensive and captures far more data than any other option. The smart card is proven technology, and the CSP in a SSUTA context is a proven legal structure. Merging them in a CSP/smart card solution makes a great deal of sense.

SSUTA was born as an inexpensive, voluntary regime to streamlines sales tax compliance. It extends audit immunity to taxpayers who used CSPs, because the CSP is trusted by the government. A SSUTA-like system to prevent zappers and phantom-ware applications in ECRs could be made mandatory for all sectors of an economy or it could be applied only in high risk sectors or maybe it could be made mandatory only for those taxpayers who had previously been found to manipulate sales records. Even though mandatory for some the CSP option should remain open for all businesses. This would increase the pressure on those who do not use CSPs to maintain good records, and traditional audit resources could be more intensively focused on this subset.

CONCLUSION

Automated sales suppression is a global problem, and it will only grow in significance. Solutions to this problem run from very expensive fiscal till regimes to intensive commitments of specialized audit resources. It is difficult to believe that zappers are rampant throughout the world and not be present in Puerto Rico. Revenue losses may be in the hundreds of millions of dollars.

---

68 *Id*. at 2.

Fortunately, there is a cost-effective remedy – the CSP option. Puerto Rico has not become a full member of SSUTA, but that does not prevent it from taking an arrow from the SSUTA's quiver and directing it at the Zapper.

If Puerto Rico recognizes that Zappers are a problem, the immediate next step is to measure the extent of the automated sales suppression problem. This is a measure that probes more deeply than general revenue shortfalls. It is a study that targets a specific source of the shortfall. This is a measure of one particularly damaging type of tax fraud, not a general measure of overall non-compliance.

If this study returns results like Quebec's and Germany's, then one would expect to find that nearly 50% of all the Commonwealth's ECRs are infected with zappers or phantom-ware. One should also find that estimated aggregate revenue losses from this source alone will be in the neighborhood of 16% of total revenue (sales tax, business income tax, payroll taxes and personal income taxes combined).

Puerto Rico might also consider a visit to Belgium to discuss Belgian approaches to this problem. Belgium is assessing the latest European technological solutions. As of this writing (March 2010) Belgium is reviewing Swedish, and German approaches as well as some of the best private-sector solutions.

Belgium has reviewed the Swedish Board for Accreditation and Conformity Assessment (SWEDAC) certification standards that were completed in late 2009. It also completed an assessment of the smart-card solution developed by the INSIKA project of the German PTB. The PTB published technical specifications to its signature smart card in late 2009.[69] Data structures, formats, communications protocols and security analysis are all freely available.

Puerto Rico should also take note of the way Belgium encouraged tailor-made third-party solutions to meet its needs. For example, when BMC Inc. appeared before the Belgian revenue authority it responded to the Belgian request for an even better and more cost effective ECR security module by sending its eTax device into further development. BMC's eTax was already one of the few devices that met SWEDAC standards. It was certified by the Swedish tax administration on August 24, 2009.

However, when BMC made its presentations on March 4 and 5, 2010 it demonstrated a greatly enhanced eTax device – the Sales Data Controller (SDC). The SDC incorporates the INSIKA smart card into its protection profile. This new system meets German and Swedish demands for security. But BMC did not stop there. It went further. The new BMC system borrowed from the Quebec solution an ability to produce encrypted bar codes on receipts that can be read by a hand-held audit scanner.

---

69 Mathias Neuhaus, Jörg Wolff & Norbert Zisky, Proposal for an IT security standard for preventing tax fraud in cash registers, (Sep. 2009) (Information Security Solutions Europe conference papers) (unpublished, on file with author); Ben B.G.A.M. van der Zwet, Fiscal Obligations for Cash Registers in the Netherlands 10 (Feb. 1, 2008) (unpublished draft, on file with author).

The Belgian effort then, is a classic example of how a tax administration can use the marketplace to forge strategic partnerships that advance cutting-edge solutions. By controlling the specifications and insisting on free competition, Belgium feels confident that it will find a balanced (cost-effective/cutting-edge/optimally secure) solution. Puerto Rico should do the same. Belgium is casting the net broadly, considering a wide range of government and private-sector solutions. As technology advances, so too will the specifications and the certification standards.

> Belgium, at this point, is looking around for feasible technical solutions at reasonable cost for both taxpayer and government and [which will offer] the highest possible protection. ... The Belgian Government will make a choice and then publish the required technical specifications ... Whatever that choice will be [the field for providing cash register security] will be open for competition, in accordance with all EU rules of free competition.[70]

The benefits of this dynamic process are already evident. BMC's new Sales Data Controller (SDC) appears to incorporate the best attributes of the eTax module approved in Sweden, the INSIKA smart card, and Quebec's SRM. All receipts will contain a unique electronic signature for each record. The SDC will produce a transaction report containing all receipts identified by type and totals, dividing totals for each tax rate on both sales and refund amounts. It will preserve data and permit extraction only by the tax administration, which will have the decryption algorithm. Is this the best solution? The competition will tell us.

Puerto Rico would be well advised to follow this approach. It is in a unique position to merge the best European solutions (Swedish, German, Greek and Belgian) with the best American solutions (SSUTA and CSPs). Puerto Rico is well positioned to push the tax compliance answer in this field further.

---

70 E-mail from Jan C.A. de Loddere, Belgian Ministry of Finance, to Richard T. Ainsworth (Feb. 25, 2010) (on file with author).