Boston University School of Law
Scholarly Commons at Boston University School of Law

Faculty Scholarship

7-2018

Zappers, Phantomware and Other Sales Suppression Software in the State of Washington

Richard Thompson Ainsworth
Boston University School of Law

Robert Chicoine

Recommended Citation

Richard T. Ainsworth & Robert Chicoine, *Zappers, Phantomware and Other Sales Suppression Software in the State of Washington*, No. 18-14 Boston University School of Law, Law and Economics Research Paper (2018).
Available at: https://scholarship.law.bu.edu/faculty_scholarship/474

BU School of Law

ZAPPERS, PHANTOMWARE AND OTHER SALES SUPPRESSION SOFTWARE IN THE STATE OF WASHINGTON

Boston University School of Law
Law & Economics Series Paper No. 18-14

July 2018

Richard T. Ainsworth
Robert J Chicoine

Boston University School of Law

ZAPPERS, PHANTOMWARE AND OTHER SALES SUPPRESSION SOFTWARE IN THE STATE OF WASHINGTON

Richard T. Ainsworth
Robert J. Chicoine

Electronic sales suppression (ESS) is a fraud that has been a (prominent) feature of the North American retail business since at least 1996.[1] The first EES case in the US dates from 1981.[2] ESS is a global problem. Depending on the jurisdiction, and the research study consulted, ESS is estimated to be present in 34% (of Canadian),[3] 50% (of

[1] Personal e-mail communication with Dave Bergeron, June 6, 2008 (on file with author). Mr. Bergeron at the time was an information-technology analyst working on Zappers at Revenue Quebec since 2000 as part of a specialized unit of accountants and computer experts providing technical expertise to investigators at Revenue Quebec. He indicated:

> In 1996, Revenue Quebec detected and was made aware that some restaurants were using a Zapper. In 1997, a television reporter investigated and reported this phenomenon. In the fall of the same year, a departmental committee was implemented by our organization. Its mandate was to tackle the problem and seek out solutions.

See also: David Bergeron, *Pacific Region ECAS Conference* slide 3 (unpublished powerpoint presentation, on file with author) and Richard T. Ainsworth & Dave Bergeron, *Zappers (automated sales suppression)*, New York Prosecutors Training Institute (July 31, 2008) slide 6 (unpublished powerpoint presentation, on file with author). The Canadian Revenue Authority (CRA) did not uncover its first ESS case until 2006 in British Colombia, nearly a decade after Revenue Quebec. See also: Richard T. Ainsworth, *Zappers and Phantomware: Are the State Tax Administrators Listening Now?* 49 STATE TAX NOTES 103 (July 14, 2008) discussing the first Zapper presentation at the FTA in February 25-27, 2001 by Kevin Pratt of the CCRA discussing developments in Quebec five years ahead of the first Zapper found by the Canadian federal government, and outlining similar audits in Australia, the Netherlands, Sweden and the UK. It has been nearly two decades since Mr. Pratt's talk, and the State Tax Administrators are indeed "listening now." Kevin Pratt, *Tax Evasion in an Electronic Environment – "Zapping,* (power point presentation at the FTA Compliance Education Workshop, Louisville, Kentucky (Feb. 25-27, 2001) (on file with author).

[2] U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), *aff'd.* 67 F.3d 460 (2nd Cir. 1995) (although the tax case was settled, the details of the fraud are preserved in federal sentencing appeals). Notably, skimming of cash receipts began in the 1970's. This was a physical skimming operation. It was performed by the CFO, Barry Belardinelli who worked in the store's vault room where large bags of cash were received daily from the store's cash registers. The skimming was manually coordinated by Belardinelli with the amounts and days of the week when skimming would be performed designated by either Frank or Steven Guthman. In about 1981 or 1982 the skimming was automated. The court indicated that the automation was a Zapper (before the term "Zapper" was in use for this purpose:

> Frank Guthman instructed Jeffrey Pirhalla, a store computer programmer, to write a complex program [called the "Equity Program"] that reduced the store's sales and financial data by the amount of the skimmed cash and permanently altered the data from which the books and records were created. The program left no audit trail that it had run.

Leonard, 37 F.3d at 35.

[3] Elaine Thompson, *A third of Canada's Restaurants may be Ripping off the Taxman by Using Sophisticated Software Programs to hide their Sales*, (updated online by) Dean Beeby, *Taxman Finds Rampant Restaurant Fraud*, GLOBE AND MAIL (August 1, 2011) available at: http://www.theglobeandmail.com/news/national/taxman-finds-rampant-restaurant-fraud/article2116523/print/. The referenced study was secure by the author though an Access to Information Act request with a Canadian professor. It is available in redacted form. Electronic Commerce Compliance Division, High Risk Compliance Strategy Division, ELECTRONIC SUPPRESSION OF SALES (ESS) REPORT ON PHASE ONE OF CRA'S STRATEGY TO ADDRESS ESS (APRIL 1, 2008 TO MARCH 31, 2010 (June 17, 2010). This "heavily redacted" report is likely the same report secured by The Canadian Press under a

German – two studies),[4] and 70% (of Swedish[5] and Slovenian[6]) businesses. It may be the case today, that "you cannot leave home without" encountering (or participating in) ESS.[7]

ESS fraud is a generic term. It represents a large subset of technology-assisted tax frauds. In all cases the basic practice is to use technology to suppress records, allowing a fraudster to defeat a tax system by manipulating the digital tracking of his activities. In some cases, the manipulation will allow the fraudster to collect the government's tax and not remit it, in other cases the fraudster will avoid the government's assessment of a tax properly due with records that obscure the truth.

The range of ESS frauds that play out in any one jurisdiction is dependent on the tax systems present and the tax(es) that are the easiest targets. If the opportunity presents itself, fraudsters will target two or more taxes that can be "hit" with a single stroke.[8] Income taxes, payroll taxes, customs duties, excise taxes on fuel and cigarettes, VAT and retail sales taxes are all vulnerable. However, it is the transaction taxes; taxes where the

similar Access to Information Act request, and is the basis of the Thompson & Beeby article. That article referenced the 34% figure. This information was redacted from the copy sent to the author.

[4] The German study is available from the author in German: Unterrichtung durch den Bundesrechnungshof (Informing through the Federal Court of Auditors) 24 November 2003, BEMERKUNGEN DES BUNDESRECHNUNGSHOFES 2003 ZUR HAUSHALTS- UND WIRTSCHAFTSFÜHRUNG (EINSCHLIEßLICH DER FESTSTELLUNGEN ZUR JAHRESRECHNUNG DES BUNDES 2002) (Comments by the Federal Court of Auditors: For budget and economic management (Including the findings on the annual accounts of the Confederation 2002).

[5] Personal e-mail communication with Bo Arvidsson, Tax Director of the Swedish Tax Agency, February 19, 2010 (available with author) indicating:

> I [would] like to confirm that a study in Sweden during 2007 has shown that about 70 % of all cash registers used in Sweden was constructed for manipulation or had software that made it possible to manipulate the sum of the sale during a specific date. Our controls during the recent years have not given us information to revise our view of the percentage of manipulated registers.

In a later e-mail Mr. Arvidsson indicated that the 70% figure was conservative and the real number was closer to 80%, although that was not the official (for publication) position of his agency.

[6] The Slovenian Tax Administration (DURS) announced that in 1150 case where receipts were photographed with cell phones and left on the table of restaurants when leaving, that 70% were tampered with by Zappers. http://translate.google.com/translate?js=n&prev=_t&hl=en&ie=UTF-8&layout=2&eotf=1&sl=sl&tl=en&u=http%3A%2F%2Fwww.rtvslo.si%2Fgospodarstvo%2Fgreste-v-lokal-vzemite-racun%2F82132

[7] Because the Swedish and Slovenian studies talk about the scope of "identified vulnerable POS systems" and the Canadian and German studies talks about "POS systems used for ESS fraud," these studies can be placed together in aggregate to make the following statement:

> Global tax authorities have conducted serious multi-year studies of ESS frauds with retail POS systems and have determined that 70% to 80% of these POS systems are vulnerable to ESS with 34% to 50% of the businesses actually using these systems for ESS.

[8] For a detailed discussion of two dual ESS frauds (1) the Danish chocolate tax frauds which intersected with Danish missing trader VAT fraud, and (2) the Saudi cigarette smuggling frauds intersects with Saudi missing trader VAT frauds see: Richard T. Ainsworth & Mussad Alwohaibi, *The First Real-Time Blockchain VAT: The GCC Solves MTIC Fraud,* 86 TAX NOTES INTERNATIONAL 695 (May 22, 2017).

government's revenue is collected as part of the commercial exchange that appears to be the technology-fraudster's favorite target (largely because the reward is immediate).

The common solution in all cases is digital security, or fighting technology with technology.[9] In the US, ESS has funded common criminals, organized crime syndicates, foreign and domestic terrorist organizations. US suppression cases have involved celebrity chefs,[10] sitting members of Congress,[11] the funding arm of Hezbollah,[12] popular grocery store chains,[13] restaurants,[14] bars/ strip clubs,[15] and small owner-operated pizza

[9] The Connecticut Revenue Commissioner stated the same when Xiaoning Fan, owner of the Lao Sze Chuan restaurant in Milford Connecticut was arrested for use of a Zapper.

> Commissioner Kevin Sullivan agreed that the software is difficult to detect. "The real hope would be that there would be equal technology that would essentially . . . detect the presence. . . . It is available, but not many of us have it," he said.

Lauren Loricchio, *Connecticut Announces First Arrest for Zapper Sales Tax Fraud* 85 STATE TAX NOTES 422 (July 31, 2017).

[10] Hu Xiaojun, a "celebrity chef" also known as Tony Hu, is regarded as the "Mayor of Chinatown" in Chicago. Daniel Gerzina, *Mayor No More? Tony Hu Planning to Sell Most of His Chinatown Restaurants*, CHI. EATER (Feb. 16, 2015, 1:07 PM), *available a*t: https://chicago.eater.com/2015/2/16/8046983/tony-hu-selling-most-chinatown-restaurants; *United States v. Hu Xiaojun*, Docket No. 1:16-cr-00316 (N.D. Ill May 13, 2016). For a detailed discussion of this case, see: Richard T. Ainsworth, *Sales Suppression: The International Dimension*, 65 AMERICAN LAW REVIEW 1241 (2016).

[11] Congressman Michael Grimm (NY's 11th Congressional District), former Marine, former FBI agent, and accountant was convicted of manipulating the sales at his "Healthalicious" fast food restaurant from 2007 through 2010 as well as underreporting payroll by concealing off-the books wages from Payroll Processing Companies. It was not clear at the trial if Grimm's underreporting of more than $1 million was aided by a Zapper or Phantomware. John Crudele, *Trolls and Perverts Hound a Reformer Off Facebook*, NEW YORK POST (May 14, 2014). See: *United States v. Michael Grimm* (judgment) Case No. 14-cr-00248 (PKC) (E.D. N.Y., July 13, 2015).

[12] A $20 million skimming operation was uncovered at the LaShish restaurant chain in Michigan. See: Press Release, U.S. Dept. of Justice, Eastern District of Michigan, *LaShish Financial Manager Sentenced for 18 months for Tax Evasion* (May 15, 2007) *available at*: http://www.cybersafe.gov/tax/U.S.aopress/2007/txdv072007_5_15_ElAouar.pdf
The cash skimmed at the LaShish was used to finance Hezbollah terrorists in Lebanon. Press Release, U.S. Dept of Justice, Eastern District of Michigan, *Superseding Indictment returned Against LaShish Owner* (May 30, 2007) *available at*: http://www.justice.gov/tax/usaopress/2007/txdv072007_5_30_chahine.pdf

[13] U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), *aff'd.* 67 F.3d 460 (2nd Cir. 1995), which until recently was "… the largest criminal tax case in the history of Connecticut, … [and] the largest computer driven tax-evasion case in the nation," DEPT. OF THE TREAS., I. R. S. 75 YEARS OF CRIMINAL INVESTIGATION HISTORY (1919 – 1994) 146, *available at* http://www.thememoryhole.org/irs/irs_75_years.rtf

[14] Heather Cherone & Ariel Cheung, *Cesar's Restaurant Owner Charged With Failing to Report $1Million in Sales*, DNA INFO, CHICAGO (August 3, 2017) available at: https://www.dnainfo.com/chicago/20170803/lakeview/cesars-killer-margaritas-charged-tax-evasion;

[15] In a very early SSaaS case, Ted Kramer, a computer consultant in Detroit Michigan, was employed by the owner and co-defendant (Nicholas Forensa) of two "strip clubs" (Tycoon's Restaurant and BT's Restaurant) to visit the restaurants on a regular basis and run a Zapper program for the owner. The owner was not "comfortable" operating the reasonably complex program that Kramer had sold to him, called the Journal Sales Removal (JSR). Kramer had sold the JSR program to other businesses in the area. Kramer secured the JSR program from programmers in Quebec. Department of Justice, *Press Release Michigan Software Salesman Pleads Guilty To Conspiracy To Defraud The Government*, available at: http://www.justice.gov/tax/txdv101309.htm *United States v Nicholas J. Faramso & Theodore R. Kramer*, Case 5:10-cr-20173-JCO-MKM (Indictment) April 9, 2010 (E.D. Mich., S.D).

parlors.[16] The technological response in the US has been weak. For some reason, the US has been very slow in taking up the technology-with-technology fight.

Given that the State of Washington collects 47.3% of its revenue (not including local government taxes) from the retail sales tax,[17] and that technology has been the backbone of the State's economy for years,[18] it is only natural that Washington would take a US leadership position in this effort. Washington still trails by a wide margin the international efforts. The US has a lot to learn from jurisdictions like Belgium, Brazil, Canada (notably the provinces of Quebec and Ontario), China, Croatia, Italy, Russia, Rwanda, Sweden, and by January 1, 2018 each of the members of the Gulf Cooperation Council (the United Arab Emirates, Bahrain, Saudi Arabia, Oman, Qatar and Kuwait).

The most common types of sales suppression technology are Zappers and Phantomware programming.[19] In some instances, sales suppression is a personal (hands-on) service offered by installers or ECR/POS sales representatives. This is Sales Suppression as a Service or SSaaS.[20] Recently suppression has entered the Dark Cloud, a fully automated manipulation of sales data that (physically) takes place off shore and uses internet-based data transfers.[21]

WASHINGTON –
THE ONLY TECHNOLOGICAL RESPONSE TO ESS IN THE US

[16] Pizza restaurants have been a favorite Zapper location in Quebec. Assessments against them in the early days of Zapper enforcement activity in Quebec were abundant. For example, Konstantino Moutos was convicted for the second time of suppressing sales with a Zapper on December 21, 2007 at his Pizza City Restaurant. On May 4, 2007 the Thetford Town Pizza Restaurant and Nikolaos Triantafyllou was convicted of using a zapper to skim $1.9 million in Quebec Sales Tax (QST). On February 11, 2005 the Double Pizza in the Lasalle district of Montreal and was fined $10,000. On October 22, 2004 the Delight Pizza in Levis used a Zapper to delete sales and was fined $40,000. (case summaries in French, translations on file with author).

[17] Washington State Department of Revenue, Research and Fiscal Analysis Division, TAX STATISTICS 2016, Chart 1, *available at*: http://dor.wa.gov/Docs/Reports/2016/Tax_Statistics_2016/chart1.pdf

[18] Blanca Torres, *Washington State Ranks No. 1 for Combined Job and Wage Growth*, SEATTLE TIMES, (February 15, 2016) *available at*: http://www.seattletimes.com/business/economy/employment-and-wage-growth-in-washington-outpacing-other-states/; Washington Technology Industry Association, INFORMATION & COMMUNICATION TECHNOLOGY: ECONOMIC & FISCAL IMPACT STUDY (February, 2015) *available at*: https://www.scribd.com/document/257405449/ICT-Economic-Report-Executive-Summary-1

[19] Richard T. Ainsworth, *Zappers and Phantomware: The Need for Fraud Prevention Technology*, 50 TAX NOTES INTERNATIONAL 1017 (June 23, 2008); Richard T. Ainsworth, *Zappers and Phantomware: Are State Tax Administrators Listening Now?* 49 STATE TAX NOTES 103 (July 14, 2008)

[20] Richard T. Ainsworth, *Sales Suppression as a Service (SSaaS) and the Apple Store Solution*, 73 STATE TAX NOTES 343 (August 4, 2014).

[21] The Dark Cloud is a term coined for this discussion. As with the Phantomware term, there comes a time in this analytical effort where an activity is becoming common enough that a new term is needed. A Dark Cloud is an anonymous internet business which accepts data transmission from ECRs or POS systems, manipulates sales data with pre-determined algorithms on a specified schedule, and then returns the data to the systems from which it came. Dark Clouds operate both on a regular schedule (daily, weekly, monthly) or on a real-time basis. They have appeared in the New York and North Carolina markets. There is no evidence of Dark Clouds operating in the State of Washington (yet). The term is unrelated to and unintentionally borrowed from the old Japanese action role-playing video game *Dāku Kuraudo* developed by Level-5 and published by Sony Entertainment around 2000.

Using the California statute as a template (the statutes in most states are similar), as of this writing, twenty-five (25)[22] states have responded to ESS by making it a crime to "… purchase, install or use … any automated sales suppression device or zapper or phantom-ware with the intent to defeat or evade the determination of an amount due …"[23] as well as to "… sell purchase, install, transfer, or possess … any automated sales suppression device or zapper or phantom-ware with the knowledge that the sole purpose of the device is to defeat or evade the determination of an amount due …"[24]

In some states, like Kentucky[25] the list of criminal acts associated with ESS is short ("… possession …"), while in others, like Louisiana[26] the list of criminal acts is much longer ("… create, design, manufacture, sell, purchase, lease, install, update, repair, service, transfer, use, possess or make available …"). Each of the 25 states specifically criminalizes zappers, and phantom-ware by name. Minnesota, for example, adds a catch-all phrase "or similar device."[27] This language is unlikely to be sufficient to pull in SSaaS or Dark Cloud types of ESS fraud, because they are suppression services (not suppression devises).

However, of all the states, only Washington goes the next step beyond criminalization and requires businesses found to have used this technology to adopt "… electronic monitoring of the business's sales, by a method acceptable to the department [of Revenue],"[28] if they want to remain in business. This is a requirement to use security-technology to fight fraud-technology. It is an effort that is comparable to most serious prevention efforts around the world.

Implemented on a one-violator-by-one-violator basis, rather than universally[29] or even by market segment,[30] Washington has decided to move forward by "baby steps," but forward it is, and Washington is on the right track. If nothing else, Washington will

[22] **GEORGIA** Ga. Code Ann., § 16-9-62; **RHODE ISLAND** RI Gen. Laws 1956, § 44-19-42; **ALABAMA** Ala. Code 1975, § 40-29-121; **WEST VIRGINIA** W.Va. Code, § 61-3-22a; **VERMONT** 13 V.S.A. § 2032; **CONNECTICUT** C.G.S.A.§ 12-428a; **NORTH DAKOTA** NDCC, 12.1-23-16; **NORTH CAROLINA** N.C.G.S.A. § 14-118.7; **TENNESSEE** T.C.A. § 39-14-704; **WASHINGTON** RCWA 82.32.670; **MAINE** 17-A.M.R.S.A. §909; **CALIFORNIA** Cal. Rev. & Tax Code § 55363.5; **MICHIGAN** M.C.L.A. 750.411w; **FLORIDA** F.S.A. § 213.295; **TEXAS** V.T.C.A., BUS. & C. § 326.002; **LOUISIANA** LSA-R.S. 47:1641.1; **INDIANA** IC 35-43-5-4.6; **ILLINOIS** 35 ILCS 105/14; **WYOMING** W.S.1977 § 39-15-108; **PENNSYLVANIA** 72 P.S. § 7268; **MINNESOTA** M.S.A. § 289A.63; **OKLAHOMA** 68 Okl. St. Ann. § 212.1; **UTAH** U.C.A. 1953 § 76-6-1303; **KENTUCKY** KRS § 517.130; **SOUTH DAKOTA** SDCL § 10-59-57.

[23] CAL. REV. & TAX CODE §7153.6(a).

[24] CAL. REV. & TAX CODE §7153.6(b).

[25] KRS §517.130 (1).

[26] LSA-R.S.§47:1641.1(A)

[27] MN ST § 289A.63;

[28] RCWA §82.32.290 (4)(b)(iii)

[29] For example: a universal transactional security system is found in Argentina, Brazil, China, Croatia, Greece, GCC, Hungary, Indonesia, Italy, Philippines, Portugal, Romania, Russia, Rwanda, South Korea, Taiwan, and Venezuela.

[30] For example: a market segment based transactional security system is found in Austria, Belgium, Germany, Netherlands, Ontario, Quebec, Sweden

have a pilot program with multiple businesses using many different kinds of solutions, each one of which could expand throughout the state to provide complete coverage. There are no known plans for this in Washington, just the potential for it to develop. However, Washington will be the only state to have hands-on experience interfacing with these security technologies, and it should be well placed to decide what to do, if the problem is a serious in Washington as the international studies suggest it could be.

There is every indication that this level of seriousness is indeed the case. We have previously written on the flow of Zappers into Washington from Vancouver, Canada and China.[31] There is more than enough evidence that Washington is being buffeted with serious ESS fraud, and the more the DOR pushes against it, the more likely it is that the fraudsters will seek the services of professionals (SSaaS) or move deeply into the Dark Cloud to continue their fraud. This is a problem. Chasing technology fraudsters is like playing "Whack-a-Mole." Each time you push against the fraud it morphs, and becomes more difficult to stop, forcing the government to "step up" the technological pursuit. Fraudster will endeavor to morph in a manner that takes them outside the current statute.

In the following sections, we will examine three of the most serious challenges faced by the Washington statute:

(1) *regulations*: there is no regulatory guidance on how to apply and interpret the statute, with the most glaring omission being the lack of any guidance on what is "… a method [of electronic monitoring of the business's sales] acceptable to the department …";
(2) *ECR/POS access*: there is no statutory mandate compelling ECR/POS retailers in the State to allow access to their systems by independent digital security firms so that the mandated electronic monitoring can be installed; and
(3) *false positives protection*: with 34 to 70% of the ECR/POS systems in the state likely vulnerable to ESS, and the severe penalties for the mere "possession" of ESS technology, the statute needs to provide protections against inevitable false positives. There are taxpayers who the department will presume are engaged in ESS fraud simply because they own an ECR/POS system that is known to be vulnerable to technological sales suppression.

DIFFICULTIES WITH THE WASHINGTON STATUTE

Based on our work with the Washington ESS statute we believe the following three aspects need to be addressed by the State of Washington. They should be addressed in advance by any other state that may be considering the Washington example.

[31] Richard T. Ainsworth, *Sales Suppression: The International Dimension*, 65 AMERICAN UNIVERSITY LAW REVIEW 1241 (2016) (discussing in detail the Profitek/Infospec zapper and POS system imported from Vancouver and China into the State of Washington as well as a number of additional instances in the US and Canada).

A note of caution. In each of these categories the problems considered are illustrative, not comprehensive. For example, we do not consider every area where regulations are needed, just a few high-level areas that we will expanded upon in further articles. This should be considered a beginning not an ending statement on this issue in Washington.

Regulations

In 2013 the State of Washington enacted Senate Bill 5715, codified at RCW 82.32.290, which prohibits EES. Specifically, it declares that:

> It is unlawful for any person to knowingly *sell, purchase, install, transfer, manufacture, create, design, update, repair, use, possess, or otherwise make available*, in this state, any automated sales suppression device or phantom-ware.[32]

In four years, no substantive regulations have issued, even though the penalties imposed are severe – ESS is a class C felony imposing up to 5 years incarceration or $10,000 or both, as well as termination of the business license, unless an electronic monitoring agreement is entered into for five years with the department).[33] Regulations are all the more important in this area because the topics considered are both tax and technology related. It should not be assumed that the average tax practitioner is intuitively conversant in both fields, just as the average computer consultant would not be conversant in tax matters. Assistance here is an important government service.

Each of the twelve operative terms (italicized in the statute segment above) needs contextual clarification. For example, with respect to the term "possession," – what does it mean to "… knowingly … possess … phantom-ware …" when phantom-ware is a "… programming option that is hidden, preinstalled, or installed-at-a-later-time in the operating system of an electronic cash register or other point of sale system …?"[34]

Consider the following hypothetical. Is it a violation of the statute when a business purchases in year 2000 an ECR/POS which contains factory-installed Phantomware, and the owner who does not "use" the programming subsequently becomes aware (through news reports) that the system purchased long ago has this programming "hidden" within it?

- Does the $10,000/5 year incarceration penalty of a class C felony apply?
- Can the Department of Revenue now mandate "… the electronic monitoring of

[32] RCWA §82.32.290 (4)(a) (italics added).

[33] RCWA §82.32.290 (4)(c)(i).

[34] RCWA §82.32.670 (7)(c):

> "Phantom-ware" means a programming option that is hidden, preinstalled, or installed-at-a-later-time in the operating system of an electronic cash register or other point of sale device, or hardwired into the electronic cash register or other point of sale device, and that can be used to create a virtual second till or may eliminate or manipulate transaction reports that may or may not be preserved in digital formats to represent the true or manipulated record of transactions in the electronic cash register or other point of sale device.

the business's sales, by a method acceptable to the department, for five years at the business's expense?"[35] – simply because the business is now "knowingly" in "possession" of Phantomware in a violation of the statute?

- Because the Phantomware is embedded in the programming of the business ECR/POS, is the ECR/POS system "… contraband and … subject to forfeiture … by any agent of the department?"[36]
- Even though seizure which is normally conducted "… upon process issued by any superior court or district court having jurisdiction over the property" there are no protections offered against, "Seizure without process … if … [t]he department or the law enforcement officer has probable cause to believe that the property was used or is intended to be used in violation of RCW 82.32.290(4) and exigent circumstances exist making procurement of a search warrant impracticable."[37]

It is well known that there are in excess of 25 commonly marketed ECR/POS systems manufactured for North American sale, which are for sale in the State of Washington, *and which have factory-installed phantom-ware functionality*. Most of these systems, through various iterations, have been in the market for several decades. There are many more systems where phantom-ware programming can be self-installed by someone with reasonable technological aptitude. Self-installing Phantomware is a simple step-by-step process. We will explain how to do this below for a particular ECR commonly found in Washington. The phntomware installation is easy, because the manufacturer has "left the back door unlocked and opened." For some, it may appear that the light has also been left on with cookies on the mantel.

Thus, anyone owning one of these systems within the State of Washington (whether they bought it themselves or purchased a business over the last 25 years with the equipment already installed) is in violation of the statute, if they possess it *knowing* of its ESS functionality. Bearing in mind that seizure of a business's ECR/POS system will effectively shutter whatever establishment they are removed from (at least until another ECR/POS system can be installed), it is clear that this statute's enforcement provisions need to be softened. Amnesty regulations are needed. The business community should expect it.

International examples. Rather than employing domestic examples we feel it is advisable (wherever possible) to move the discussion into the international sphere where examples of the fraud are also abundant, and simply indicate that domestic analogues are readily available. This is an exceedingly business-sensitive topic, and we would like to get to the issues involved, not necessarily the businesses involved at this first pass through ESS in the State of Washington.

Two examples are developed below that will point for the need of regulations in the State of Washington: (1) the factory-installed Phantomware at The Grande Café

[35] RCWA §82.32.290 (4)(b)(iii).

[36] RCWA §82.32.670 (1)(a)

[37] RCWA §82.32.670 (1)(b) & (b)(2).

Dudok in Amsterdam, in the Netherlands, and (2) the "self-help" Phantomware that can be installed on a CASIO TE-2000, TE-4000 and TE-6000 ECR that was discussed by European Commission's Fiscalis Committee Project Group 12.

Factory-installed Phantomware at The Grande Café Dudok. The Grande Café Dudok used the factory-installed Phantomware program in its Finishing Touch point of sale system, manufactured by Straight Systems BV.[38] 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 the checkout's front office and back office systems."[39]

The *Dudok* 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 a user 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.[40]

The phantom-ware program embedded within Finishing Touch was first used by Dudok to skim cash receipts in the midst of a Dutch IRS examination. The IRS was initially concerned with staff salary. Payments were being made under the table, and the IRS was suspicious.[41] Testimony in the case indicated that on the second day of the IRS audit the managing director of Straight Systems BV visited Dudok where he was approached by the owner-manager. The owner-manager of Dudok explained that he was having difficulty accounting to the IRS for the turnover.

During this conversation, the Straight Systems managing director explained the existence of a "hidden delete" option in the Finishing Touch cash registers. The court indicated that this was, "… a hidden menu option that, after enabling said option,

[38] District Court of Rotterdam, LJN: AX6802 (Jun 2, 2006) *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 LJN: BC5500 (Feb. 29, 2008) *available at*: http://zoeken.rechtspraak.nl (in Dutch) (translation on file with author).

[39] *Available at:* http://www.straight.nl (in Dutch, translation on file with author).

[40] LJN: AX6802, at Consideration of the Evidence (Jun 2, 2006) (in Dutch) (translation on file with author). Confirmed by Ben B.G.A.M. van der Zwet, EDP-auditor/Accountant, Belastingdienst (personal e-mail correspondence May 28, 2008) (on file with author).

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

allowed operators of catering establishments to delete cash register receipts from the system."[42] After this discussion "… an employee of the defendant visited [Dudok] and explained the [technical] application of the erase rule [or hidden delete function[43]], after which [Dudok] subsequently decided to start using [it] …"[44]

The *Dudok* case shows how a business (owner-manager) can initially purchase a POS system with an embedded Phantomware program without knowing about it. The purchase is most likely made based on commercial reputation, and the Phantomware application is not a "selling point."

Under the Washington statute as soon as the owner-manager *knew* that his Finishing Touch POS contained Phantomware the criminal provisions applied personally and to the corporate entity. *Possession* is not a question, only *knowledge of the possession* is. The operation of the statute may be seen as too Draconian, if there is no flexibility in its application. A series of "what if's" are needed in regulations:

- "What if" the owner-manager "knew" but did not use the Phantomware? If this was a new POS system an owner might hesitate doing something about this situation because it might mean an expensive replacement of the POS system.
- "What if" the "night manager" not the owner-manager acquired this knowledge from the Straight Systems managing director. If the "night manager" does not pass this information on (perhaps because he wants to embezzle funds from the business himself) will this knowledge be attributed to the owner-manager and the business because the night manager is an employee under the "control" of the owner-manager?
- "What if" the owners-manual that was provided by Straight Systems contained instructions that would explain the "hidden delete" function, and the owner's manual was left with the Dudok's IT specialist, who may or may not have read the manual. Will this knowledge be attributed to the owner-manager or the company?
- "What if" none of the above happens, but this paper is circulated widely, is available on the internet, and becomes part of online discussion groups that the IT staff visits. Will this knowledge be attributed to the owner-manager?

[42] 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. Ben B.G.A.M. van der Zwet, (personal e-mail correspondence May 28, 2008) (on file with author).

[43] 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."

[44] LJN: BC5500, at F3.

Self-help Phantomware in the CASIO TE-2000.[45] The EU Commission's Fiscalis Committee Project Group 12 broke down a number of ECRs, and presented detailed expositions on how to re-set the ECR so that the system would suppress sales. The detail presented below may not be relevant to many, but the overall point should be relevant to anyone working on tax issues in this area. The materials associated with the next two charts can be skimmed.

Installing your own version of Phantomware in your own ECR/POS system is not that difficult. The discussion starts with the Z Report.

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

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

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

Code	**0**	**0**	**1**	**0**	**0**	**0**
Short hand identifier "D" = digit	D6	D5	D4	D3	D2	D1

We want to reconfigure the 0822 program. To do this in the CASIO TE-2000 the following steps are taken:

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

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

(a) D6 set to "0" indicates "print first and last consecutive numbers of the day."
(b) D5 set to "0" indicates three things:

[45] This discussion was taken from the EU's Fiscalis Committee Project Group 12, CASH REGISTER PROJECT GROUP, *Cash Register Good Practice Guide* (Dec. 2006) (on file with author).

a. "skip zero total lines on department and transaction read/reset report"
b. "skip zero total lines on PLU read/reset report"
c. "skip zero total lines on hourly sales report."

(c) D4 set to "1" indicates two things:

a. "print the sales ratio on read/reset report"
b. "do not suppress printing of the non-resettable grand total on the daily reports."

(d) D3 set to "0" indicates two things:

a. "suppress the printing of RF [refund] totals and RF count [both RF mode and RF key]"
b. "print tax rate with tax totalizer."

(e) D2 and D1 signify actions that are not relevant in this discussion

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

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

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

Code	**0**	**0**	**3**	**1**	**0**	**0**
Short hand identifier "D" = digit number	D6	D5	D4	D3	D2	D1

Once re-programmed, "[t]he daily read/reset reports printed in X and Z modes will not print the non-resettable grand total and refund transactions made in the RF mode and RF key."[46] The *Guide* runs two examples based on this re-programming. The first (using the "001000" code) shows:

- sales of 1,000 (500 + 250 + 250),

[46] *See supra* note 45, *Cash Register Good Practice Guide*, Appendix E, at 4.7.

- a refund of 250, and
- a cash-in-the-drawer total of 750.

The second (using the "003100" code) shows:

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

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

Under the Washington statute if self-help Phantomware is detected on an ECR/POS system a criminal violation is almost assured, provided we know who performed the self-help installation. It would be exceedingly difficult to deny knowledge and possession of Phantomware in a self-help fact pattern by the "programmer." But is the programmer the current owner of the ECR/POS system? Consider the following hypothetical permutations:

- What if the self-help Phantomware was installed by the distributor, and the business owner did not have knowledge of the programming? If so, then the whole set of "what if's" from the Dudok case applies again.
- What if the equipment was purchased second-hand when the business changed hands? Does the statute require proof of who actually installed the self-help Phantomware?
- What about the rogue "night shift" manager, or the inquisitive IT specialist? What if they installed the self-help Phantomware? Is there a criminal violation?

All of these questions lead to the observation that there needs to be something more than *knowledge* plus *possession* to fairly activate criminal enforcement measures. There seems to be a sense that some kind of "*proof of use*" is needed or perhaps some "proof that the *knowledge* and the *possession* were *used* to *defeat* the collection of a *tax*." The problem is that "possession" and "use" are separate acts under the Washington statute, and the sense is that they need to be joined in some manner. This is a regulatory matter that Washington can address.

Aside from the absence of regulations, there is a further difficulty for Washington State taxpayers apparent in the two examples above. Assume that the DOR uncovers two Phantomware frauds, one using a POS like Final Touch in the *Dudok* case, and the other using a self-help Phantomware application in a CASIO TE-2000 ECR.

As happened immediately after the *Dudok* case, the WA DOR (like the Dutch Belastingdienst) will likely open audits on any enterprises using a Final Touch or CASIO TE-2000 POS. Because the presence of Phantomware is a certainty in a Final Touch POS, any sales irregularities might quickly lead to a seizure of the POS, effectively shutting down the business. Enterprises using a CASIO TE-2000 might be suspect, but without a forensic analysis seizures would not be likely. Regulations should try to level the playing field between these two classes of Phantomware cases, and perhaps provide an amnesty program for businesses with known suspect systems.

However, to fairly activate an amnesty program the Washington DOR would need to publicly announce that they are aware that a CASIO TE-2000, or the Final Touch POS is a suspect class of POS systems. This is what the EU Commission's Fiscalis Committee Project Group 12 was doing when it detailed the CAIO TE-2000 self-help Phantomware procedures. Would the Washington DOR be willing to do the same?

A fair system of enforcement would put in the regulations a detailed discussion of all the POS/ECR systems that the DOR is aware of that have factory-installed Phantomware, as well as all of the systems that leave the "back door open and unlocked" to self-help Phantomware. A fully transparent regulatory structure would do what the EU Commission's Fiscalis Committee Project Group 12 did, and explain in detail how to activate the self-help Phantomware structures, and then alert the business community that audits would be conducted to find these modified ECER/POS systems.

If this were the case, then businesses that had (unknowingly) purchased suspect systems would likely "volunteer" to install third-party security "acceptable to the Department" in precisely the manner that the DOR has set for its policy objective in this area. As it stands now, the DOR has a Draconian statute that punishes severely, and some might argue unfairly, and that will achieve its policy objectives slowly and with great expense all around.

ECR/POS ACCESS

Washington has no statutory mandate compelling ECR/POS retailers in the State to allow access to their systems by independent digital security firms so that a third-party electronic monitoring system can be installed. Understanding why a mandate is necessary requires an understanding of (1) the economic forces that direct activity in the ECR/POS commercial marketplace, and (2) what real data security in the ECR/POS marketplace looks like.

(1) *The economic forces in the ECR/POS commercial marketplace*

Traditional ECR/POS data security for tax purposes. There are traditional data security mechanism in all modern ECR/POS systems. They are:

- **Printed (paper) receipts –** the most traditional and visible security measure for recording sales is the printed (paper) receipt. If every sale is recorded with a printed receipt, and if every receipt is collected, then by totaling all the receipt data an auditor can determine total sales, total cash received, total credit sales, and much more about the aggregate operations of the business.
- **Digital (e-mailed) receipts –** are simply the electronic version of the paper receipt. Their advantage is that they are easier to aggregate.

- **X Reports –** are standard reports produced by an ECR that are used to provide a "snap shot" of the cash drawer balance. An X Report is cumulative, and never resets. As a result, if a business only runs X Reports the data will build each day.
- **Z Reports –** are standard reports produced by an ECR, but they are run to provide a final balance for the cash drawer. A Z Report resets the cash drawer balance to $0.00 so that the next time the report is run a fresh balance is produced. Thus, if an X Report is run immediately after a Z report (without any new sales) the X Report will print with all zeros.
- **Electronic journals –** are internal memory storage areas in the ECR/POS that record the line-by-line details of all transactions completed on the system (all sales transactions, all reports run, even no-sale rings used to open the cash drawer). When an electronic journal's storage is nearly full a warning will issue allowing user to print the journal to prevent any loss of data. When the journal is completely full either no additional transactions will be saved, or the journal will begin to re-write over the old data.

Where do Zappers and Phantomware programs come from? It is quite clear that Zappers and Phantomware programs are a product of ECR/POS marketplace dynamics. There is a reason that many of the same individuals manufacture, sell, and distribute ECR/POS systems, as well as the Zappers and Phantomware programming that defeat the traditional security features installed within them.

Zappers and Phantomware programs are both a *commercial threat* and a *commercial opportunity* to the distributors of ECR/POS systems. They are a threat, for example, in the hands of an embezzling employee who might suppress sales for personal gain at the expense of the owner and the reputation of the POS/ECR manufacturer.[47] They are an opportunity when they accelerate the sale of new ECR/POS systems to businessman intent on suppressing sales.

The later group appears to be dominant. In fact, during the New York undercover sting operations, where revenue officers posed as restaurant owners looking to purchase new systems from March through September 2009, 95% of the salesmen made pitches to the revenue agents of suppression software and services tailored to fit their ECR/POS systems. Many provided demonstrations on how the suppression mechanisms worked. The NY undercover teams considered these demonstrations to be high-quality, free training sessions. The kinds of suppression offered ran the gambit from Zappers-to-Phantomware-to-SSaaS.[48]

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

[48] Richard T. Ainsworth, *Sales Suppression as a Service and the Apple Store Solution*, 73 STATE TAX NOTES 343 (August 4, 2014).

Many of the NY salesmen represented distributors that were national leaders in the ECR/POS marketplace. One firm had four-hundred clients in Connecticut, New Jersey, and NY city. A second firm had 1,200 clients just in NY city, performed two-hundred installations a year, and was in the top five for Aloha POS sales and installations nation-wide. A third firm had 1,100 NY city clients. A fourth was the top POS sales and installation firm in Pennsylvania with forty employees in their NY office, and over 3,000 clients overall.[49] They were all pitching suppression to sell their ECR/POS systems.

The same pattern repeats internationally. In Canada for example, Zappers and Phanomware are designed, manufactured, and marketed by same firms, or same individuals who make and sell the ECR/POS systems. Why would the commercial/economic dynamic be different in the US?

Four cases from Canada illustrate the marketplace. There are both small (boutique) firms with IT professionals that install and maintain a limited number of ECRs and POS systems, as well as large multi-corporate enterprises with considerable international reach involved. Audio Lab LP, Michael Roy and Luc Primeau are examples of the small players, InfoSpec/Profitek is a major multinational enterprise.

Audio Lab LP. On April 8, 2004 Revenue Quebec announced that it executed four search warrants on the numbered company 9061-1184 Quebec Inc. that operated a restaurant under the name San Antonio Grill in Laval, Quebec.[50] The allegation was that a “sales Zapper” (*camoufleur de ventes*) was used to delete sales records.[51] The Zapper was on a diskette used in connection with the restaurant’s computer system.[52]

Next year, on April 25, 2005, Revenue Quebec announced that the director of San Antonio Grill pleaded guilty to using a Zapper.[53] The director, Mr. Apostolos Mandaltsis, was personally fined.[54] A related company of similar name, Grill San Antonio in Repentigny, also pleaded guilty to similar offences.[55]

Later that year, on October 14, 2005, Revenue Quebec announced that it executed five more search warrants in Montreal and Laval with respect to Audio Lab LP, Inc.[56] It

[49] Id., at 344, ns. 7 & 8.
[50] Press Release, Revenu Québec, 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) (on file with author).
[51] *Id.*
[52] *Id.*
[53] Press Release, *supra* note 25.
[54] *Id.*
[55] *Id.*
[56] Press Release, Revenu Québec, 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/en/ministere/centre_information/communiques/ev-fisc/2005/14oct.aspx (translation on file with author).

was under suspicion of having developed and marketed a Zapper that was compatible with its own restaurant cash register software, Softdine.[57]

Softdine was the operating software in the cash registers at San Antonio's Grill in Laval, and at Grill San Antonio in Repentigny.[58] 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."[59] 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.[60]

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.[61] Each of the restaurants in the Stratos chain used Zappers.[62] 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).[63]

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 14, 2003.[64] Press releases provide details of only the final ten companies.[65] 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 also 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 chain Stratos."[66]

On April 25, 2003, Michel Roy and his two sons Danny and Miguel were convicted of tax evasion.[67] The father (Michel) was the creator of the Zapper that worked

[57] *Id.*
[58] Press Release, *supra* note 9.
[59] *Id.*
[60] *Id.*
[61] Press Release, Revenu Québec, 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) (on file with author).
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] Press Release, Revenu Québec, 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) (on file with author).

with Resto Terminal.[68] He promoted it and made the sales.[69] His sons (Miguel and Danny) installed the software and designed the civil fraud.[70] Aggregate fraud penalties assessed against the Roys were $1,064,459.[71]

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).[72] 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.[73]

On October 17, 2005 Luc Primeau admitted using his software to assist these companies to evade $435,000 in GST and QST.[74] They skimmed $2.7 million in cash sales, and Mr. Primeau was fined $20,000 for his involvement.[75] 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.[76] 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).[77]

InfoSpec/Profitek. Profitek is a leading software development company specializing in Point-of-Sale (POS) solutions for the Hospitality and Retail industries. Founded in 1985 and based in Vancouver, Canada, Profitek has three offices in Canada, two offices in China and a growing dealership network across North America. It has been ranked among the top 100 technology companies in British Columbia since 1999.

Canadian tax authorities brought cases against InfoSpec Systems, the company that makes the Profitek Zapper, a salesman who sold them, and two restaurants that used them. Because of deficiencies in the federal statute (that were later corrected) the CRA

[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] Press Release, Revenu Québec, 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) (on file with author).
[73] *Id.*
[74] Press Release, Revenu Quebéc, 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/fr/ministere/centre_information/communiques/ev-fisc/2005/26oct.aspx (translation on file with author).
[75] *Id.*
[76] *Id.*
[77] *Id.*

was ineffective in the case it brought against the manufacturer,[78] but was successful against the salesman (assessing responsibility for $3,300,000 in sales and income taxes),[79] and the restaurants (assessing overdue taxes of $731,986).[80] Not surprisingly, the InfoSpec/Profitek POS system and Zapper has shown up in the US.

In Seattle, the Washington Attorney General investigated an alleged Profitek Zapper salesman (John Yin), and a restaurant owner who allegedly used the Zapper he sold to her. Yu-Ling Wong secured both the Zapper and her POS system from Mr. Yin. Yin admitted to selling Profitek Zappers to multiple business owners, and was convicted. The sixty-four-year-old self-employed software salesman entered a plea that including restitution of $3,445,589 in Washington sales taxes and federal income tax due from skimmed receipts.[81] Other Seattle cases may follow.

(2) *Real data security in the contemporary ECR/POS marketplace*

Real transactional data security in today's ECR/POS marketplace comes in two forms, either (a) it is provided directly by the government and mandated for all businesses, (or for all businesses within a particular market segment) as a condition of securing a business license,[82] or (b) it is provided by fully independent third-party vendors who have no commercial interest in the manufacture, sale or installation of ECR/POS systems. The government mandates only that ECR/POS products have the ability to interface with a secure unit (which is also purchased by the taxpayer). [83]

[78] *R. v. InfoSpec Systems, Inc.*, 2013 B.C.C.A. 333 (Can.)

[79] *R. v. Au*, 2011 BCSC 75 ¶ 1 (Can.) Between October [4,] 2000 and August [28,] 2008, Mr. Au sold the Profitek system, along with the zapper program, to [twenty-three] known restaurant owners" who used it to delete "cash sales for the purpose of evading income and sales taxes. At the time of his sentencing, fourteen of the twenty-three restaurants to which he had sold zappers had been fully audited. Over $14,000,000 (Canadian) in sales had been suppressed by these establishments, resulting in tax losses of $2,400,000 in federal income tax and $1,000,000 in Goods and Service Taxes (GST).

[80] On May 1, 2013, the CRA announced that it had found the Profitek Zappers in two Winnipeg, Manitoba restaurants, 1438 miles east of Vancouver. Both establishments were Chinese— the Foody Goody Chinese Buffet and the Buffet Square. *Winnipeg Restauranteurs Taste Tax Evasion Fines*, KNOWLEDGE BUREAU (May 13, 2013), http://www.knowledgebureau.com/index.php/news/article/winnipeg-restauranteurs- ; *see Foody Goody and Buffet Square Plead Guilty to Numerous Charges of Tax Evasion*, METRO NEWS (May 1, 2013), http://www.metronews.ca/news/winnipeg.html

[81] *United States v. John Yin*, Case 2:16-cr-00314-RAJ (Government's Sentencing Recommendation) at 9 (April 14, 2017).

[82] This is the case with Quebec, which commissioned a secure unit called the *module d'enregistrement des ventes* (MEV). In English the unit is known as the sales recording module (SRM). The SRM records and preserves on site all tax-critical data, produced by the ECR/POS it is connected to. It digitally signs each receipt. The government designed the MEV, controls the technology within the MEV, and physically owns the units which it provides to the taxpayer at no cost. The MEV is manufactured for Revenue Quebec by AAEON Technologies (Taiwan), and distributed to installers/ resellers by IBM Canada. SRM installers are authorized by Revenue Quebec. SRM developers are in charge of developing adaptors to POS software to allow the units to interface properly and permit the SRM to function with a specific POS. SRM developers are also authorized by Revenue Quebec. At the architecture/Software level the principal partner that put the solution in place is CGI.

[83] The Rwandan approach is similar to Quebec's but the government does not "own" the secure units. VAT law No. 37/2012 of 09/11/2012, article 24 obliges all VAT registered taxpayers in Rwanda to acquire and use an electronic business machine (EBM) to issue tax invoices. There is no MEV. Instead, the

Traditional security in the Cloud. Needless to say, it is not sufficient for an ECR/POS system provider to take any one or more of the traditional security measures, encrypt the data, send it off to the cloud, and call this data security. Although there are many providers offering this service, it does not secure transactional data from manipulation. It is certainly a technology embellishment, but it is not much more. It cannot assure the government that the transactional data is complete and secure from manipulation, because the traditional security measures are not sufficiently secure to begin with.

For example, a firm making top-of-the-line-printers, might digitize each paper receipt, encrypt the data and send it to the cloud. An ECR/POS firm might do the same with X or Z Reports, or the entire Electronic Journal. Doing this in real-time is better than doing it daily, weekly or monthly, but the problem is that Zappers and Phantomware work in real-time too. Additionally, if the ECR/POS system or the top-of-the-line-printer is invested in making sales by providing Zappers and Phantomoware to their customers then the marketplace will defeat the solution.

These kinds of "security solutions" would not be secure, and should never be a "… method acceptable to the department …" under RCWA §82.32.290 (4)(b)(iii). These "security solutions" should not be acceptable once the real-time functionality of Zappers and Phantomware are factored into the equation. Provider-encrypted ECR/POS files, and provider-encrypted receipts from the attached printer sent to the provider-operated cloud are no better than the original documents. The manipulation possibility is still open.

These types of security offerings are very close to the Dark Cloud, where manipulation happens *after* data is transmitted to the cloud, manipulated, and then returned to the ECR/POS system to be preserved within the electronic memory of the device. The entire circuit can take less than a second. The manipulation can occur by algorithm. The transmission to the tax administration can occur in near real-time. All data records (electronic memory, cloud storage, DOR real-time storage) will match, but all will be manipulated. This is apparently what happened in a North Carolina case which arose during a partnership dispute that involved sales suppression, tax fraud, and a partner's embezzlement.[84] There are a number of interesting elements in this case which

government requires that ECR/POS units sold in the country be compliant and be able to connect to a certified Sales Data Recorder (SDC) which is a secure unit that processes and stores receipts. Thus, the connectivity of a CASIO POS would be tested, (when it passes it is a certified EBM) and it is listed as CIS compliant at: http://www.rra.gov.rw/index.php?id=302 A taxpayer could purchase any system on this list it wanted, but it would need to take it to a revenue office where the EBS would be activated and have the associated SDC personalized and assigned to the taxpayer.

[84] The North Carolina case is discussed in Richard T. Ainsworth, *Sales Suppression as a Service and the Apple Store Solution*, 73 STATE TAX NOTES 343, 351-2 (August 4, 2014). It is identical to the fraud described by ECR/POS salesmen to the NY undercover investigators in transcript 5 and transcript 6 of the NY stings. In these cases data on an Aldelo POS is manipulated with a LogMeIn program to access and manipulate data with a hidden delete function on the Aldelo POS. Warren Klomp, District Administrator, California Department of Taxes and Fees, is becoming famous for the term RDM (remote data manipulation) which is essentially is a clinical or functional description of the Dark Cloud. "What we have seen is the vendor logging on remotely and taking the data away, once manipulated it is put back. Not

tie back to issues covered above:

- it was a private embezzlement action between two partners (embezzlement is always a factor when considering sales suppression – things may not be as they initially appear);
- it involved significant tax fraud (although tax fraud was not the motivation for the sales suppression, it was a part of what happened, and in this instance the interests of the tax administration and the private business person align nicely);
- it was in part uncovered by one of the partners talking with other businesses in the area and finding out that the ECR/POS system in her business was the same as that used it their businesses, and that they were actively suppressing sales with it (sales suppression was active and somewhat openly discussed in the general business community);
- the same ECR/POS installer was involved in each of the businesses (the type of suppression was promoted by the installer/ salesman and appears to have been a "selling point" for his systems);
- that the data from all of their businesses was sent to the cloud where the manipulation happened (this is the Dark Cloud), and
- cloud access storage was provided by the ECR/POS manufacturer, but the installer switched clouds preferring a private cloud service located in California rather than the cloud offered (for free) as part of the purchase of the ECR/POS system (the ECR/POS manufacturer left an open and unlocked back door to the cloud that the installer used to facilitate fraud).

Government provided/ mandated security. This is the approach taken by many countries. Quebec, and Rwanda are examples. It is a policy position that accepts that technology has allowed significant opportunities for fraud to enter the transactional marketplace which is highly corruptible. Rather than expecting changes in the marketplace, these jurisdictions level the playing field directly. Each business, as a condition of receiving a business license, is required to install a government designed monitoring system.

In Quebec the monitoring device is call the *module d'enregistrement des vents* (MEV),[85] in Rwanda the device is called an Electronic Business Machine (EBM).[86] In both cases there was an immediate improvement in revenue. Quebec saw a self-reported revenue increases of $160 million and $1.3 million in fines during the first year of operation.[87] Rwanda saw a revenue increase of 8% in the first six months and 20% in the

exactly the cloud but transfer to another system." The Dark Cloud however, is more. It includes the fully automated, remote Zapper that works by remote algorithmic manipulation of data in real-time.

[85] Richard T. Ainsworth & Urs Hengartner, *Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud with Technology*, 57 CANADIAN TAX JOURNAL 715 (2009).

[86] Eugene Kwibuka, *RRA: Use of EBM will Soon be Mandatory for Every Business*, THE NEW TIMES (October 10, 2016) available at: http://www.newtimes.co.rw/section/article/2016-10-10/204315/

[87] Press Release, Revenue Quebec, *Tax Evasion in the Restaurant Industry: Revenue Quebec Gives a Positive Assessment of the First Year of Implementation of MEV in the Food Sector*, (February 14, 2013) available at: http://www.revenuquebec.ca/fr/salle-de-presse/default.aspx

first two years.[88] These are not the approaches taken by Washington State.

Third-party industry-standard secure monitoring. Washington has decided to put the burden of finding a monitoring system that is "acceptable to the department" on the taxpayer. It is a condition of remaining in business. This is a more difficult undertaking than it appears, largely because the level of security that is standard in the industry requires access to the operating system of the taxpayer's ECR/POS.

The degree of detail needed to assure a tax authority that ECR/POS data is untampered with is considerable. It is easier to see some of this complexity with an example, and then after the example consider the aggregate data reports that the third-party security system will need to prepare for the tax administration.

Transactional example. Assume the following transaction occurs at a restaurant where a POS is installed which is equipped with an industry-standard third-party security monitoring system. What is captured, preserved, and encrypted during this transaction?

1) A customer walks in to the restaurant and wants to purchase a $1.00 hamburger
2) The order is placed (and the tax rate is 10%)
    a) the POS system captures this order
    b) the third-party security also captures, and preserves this data
3) As the hamburger is prepared, the customer offers cash based on the lighted numbers on the cash register terminal of $1.10
4) When the cash is handed over the cashier presses the cash button to complete the sale and takes $2.00
    a) the POS system captures this data, marking it as a cash transaction;
    b) the third-party security also captures, and preserves this data;
    c) the third-party security immediately notifies the tax authority about the transaction in real-time;
    d) the tax authority receives, retains, and records this data, and notifies the third-party security system that it has done so
    e) the third-party security [at step 4(b) above] also received notification from the POS that the POS system has similarly capture this data. The data is now in three places:
        i) the Tax Authority
        ii) the POS system (on site)
        iii) the third-party security (on site and in the cloud)
5) The third-party security has the ability to store (and encrypt) the following data points:
    a) the hamburger order (item-by-item);
    b) the tax due and paid;
    c) the aggregate cash payment (the cash handed back to the customer in change can be found in the electronic journal, but is not relevant for security purposes);
    d) the date and time and table number of the transaction, and

[88] David Deputy & Goran Todorov, *Securing the Fisc via Digitization*, FTA TECHNOLOGY CONFERENCE, INDIANAPOLIS, INDIANA (August 2, 2017)

e) the check number, and the server's name or ID number

6) Simultaneous with full encryption of all the data (at 5, above) a verification response is generated of the encrypted files and placed on the bottom of the receipt (best representation is in the form of a bar code). [All of 4, 5, & 6 can be accomplished in milliseconds so the customer really only sees the receipt being printed as soon as cash is tendered.]
7) Anyone can use the verification response (bar code) on the bottom of the receipt to immediately confirm that:
   a) the receipt is valid;
   b) the data is complete and stored in the POS, and
   c) the data is complete and stored in the third-party security system's files.

Reports prepared. In addition to the individual transactional data which is collected, encrypted and transmitted to the tax administration in real-time, the following aggregate reports will be prepared:

1) Total sales by day, per month, indicating both the quantity sold, per item, and the amounts charged;
2) Total discounts provided by day, per month, indicating both the quantity, and the amounts provided per item;
3) Net sales, by day, per month;
4) Total sales tax, per day, per month;
5) Total amounts tendered, by day, per month divided by category of cash, credit, debit card or other category;
6) Total number of void transactions, no sale transactions, and cash drawer openings by day, per month;
7) Total time the cash drawer is open, by day, per month, subdivided by duration in single incidents;
8) Total guest checks issued by day, per month itemized by quantity purchased per check, and average amounts purchased per check by day, per month;
9) Total guest count per check, by day, per month arranged in time sequence.

Third-party security with no government mandate. Washington has decided to be a "pilot project" for third-party security without a government mandate that ECR/POS manufacturers cooperate. This model is untried elsewhere. We can confirm that it is a difficult path forward.

In 2015 the POS market was a $13.31 billion, highly competitive industry poised for considerable growth, focused on efficiencies in the cloud, but with considerable technology-based security concerns.

> One of the key factors contributing to the market growth is the increased adoption of credit and debit cards. Debit cards have overtaken cash … However, businesses still need to address the most sophisticated processing and security challenges posed by credit cards, as well as the growth of mobile payment options. Advancement in cloud-based POS solutions is expected to showcase significant opportunities in coming years. … Cloud computing POS solutions have various advantages over

traditional solutions such as access to a service on demand, lower CapEx, reducing internal IT infrastructure, and others.[89]

We have contacted each of the leading POS manufacturers in the Washington State restaurant and hospitality sector,[90] and well as the major POS manufacturers overall. [91] The response was nearly uniform. Cooperation with a third-party security provider without a government mandate to do so (as in Rwanda and Quebec) was rejected. We asked for integration permission with either of the two major third-party security providers we located, one from Canada, and the other from the EU.

The reasons for the rejection were consistent, and thoughtful. On occasion the request to assist the government fight fraud went through several levels of authority, but the answers were clear.

- The primary reason given was that the POS vendors wanted to protect the security and integrity of their platforms. In other words, it did not make sense for a major POS provider to engage in a one-off project that would generate a small amount of revenue, but potentially compromise the security of their whole system. Even though they were sure it could be worked out, the large risk that something could go wrong was not worth the small prize.
- A second commonly recited reason involved proprietary software. Each of these POS providers had developed unique software which would need to be shared at some level with the third-party security firms. This was characterized in their mind as a commercial partnership proposal, which again did not make sense given the small market potential.
- A third reason was that many of these companies offered their own cloud-based solutions which they felt were sufficiently user-secure. They said they were not convinced that Zappers and Phantomware were common, or more particularly that they could be used to alter the records in their POS systems, but if this was a concern taxpayers should use their cloud as a solution. This third response brings into focus a fundamental disconnect. Many manufacturers leave a limited back door open in their POS systems for suppression of outbound data. They do this to

[89] Research Staff, *Point of Sale (POS) Software Market Analysis, Market Size, Application Analysis, Regional Outlook, Competitive Strategies and Forecasts, 2016 to 2024*, GRAND VIEW RESEARCH, (Report Summary) Report ID 152, *available at*: http://www.grandviewresearch.com/industry-analysis/point-of-sale-pos-software-market

[90] PC Magazine bills itself as the complete guide to computers, phones, tablets and peripherals based on their testing and review of products and services. It globally ranks the top seven POS systems in the restaurant and hospitality industry as follows: (1) Square Chip Card Reader; (2) Aldelo POS Pro; (3) PAR Brink POS; (4) Posera Matre'D POS; (5) Revention POS; (6) Action Systems Restaurant Manafer; (7) Menusoft Systems Digital Dining. Evan Schuman, *The Best Point-of-Sale (POS) Systems of 2017*, PC MAGAZINE, *available at*: http://uk.pcmag.com/cloud-services/74663/guide/the-best-point-of-sale-pos-systems-of-2017 .

[91] The major US and EU independent review platform for B2B, SaaS and financial solutions ranked the top 15 POS solutions overall as: (1) Square Register; (2) Vend; (3) QuickBooks POS; (4) Salesforce Commerce Cloud; (5) FastSpring; (6) Shopify POS; (7) Skubana; (8) Erply; (9) Bindo POS; (10) Booker; (11) Toast POS; (12) Lightspeed Retail; (13) Miva Merchant; (14) TouchBistro; (15) Webnexs POS, r*15 Best POS Software Systems for Small Business*, FINANCESONLINE, available at: https://financesonline.com/15-best-pos-software-systems-business/

> allow their sales representatives and distributors room to respond favorably to the suppression demands of buyers. However, they work very hard to close off outside access to their systems (inbound data) which could bring with it malware or viruses. The sensitivity on this point is acute. Most advanced POS systems are also payment processing platforms, and the security requirements in this realm are exceedingly tight.

The authors have met the "… method acceptable to the department …" requirements of RCWA 82.32.290(4)(b)(iii) in a first-ever case applying the statute. A recognized third-party with an industry-standard electronic monitoring system has been integrated with an autonomous POS system. The statutory solution works, but whether or not it is scalable is a different question. A number of interested parties came together in this instance, but the solution would have been much easier to find if there was a state mandate that POS systems offered for sale within the state must allow third-party security.

WASHINGTON'S
EXCESSIVE ESTIMATES, DISPROPORTIONATE PENALTIES & FALSE POSITIVES
COULD BE TRANSFORMED INTO
NEGOTIATED MONITORING AGREEMENTS & GOOD FAITH AMNESTIES

The Washington statute creates problems that can be roughly catalogued as problems of excessive estimates, disproportionate penalties, and false positives. It also creates opportunities for voluntarily negotiated monitoring agreements and good faith amnesties. In the sections that follow we will identify problems and suggest regulatory remedies, as well as point to opportunities for improvement in the state's response to ESS.

Excessive estimates. One of the greatest enforcement difficulties with ESS frauds is that the actual tax losses are difficult (if not impossible) to prove. There is the *possibility* of a reliable second set of books, but if they exist it is not likely that the tax administration has access to them. Those books would not be made by a Zapper. As a general rule, Zappers and Phantomware do not make second-sets-of-books, their function is to delete data, and the best programs delete data so completely that they leave no trace of the program that was used to do it. The Dark Cloud and SSaaS can (and do) offer a second-sets-of-books as a service. They are held "off shore."

In an abundance of caution, most ESS assessments assert much larger deficiencies than an auditor can comfortably prove. However, once it is strongly suspected that sales have been suppressed neither the government nor the taxpayer have solid ground to stand on. Neither is likely to be successful in proving their sales figures in full. ESS penalties give the government leverage.

Zapper and Phantomware cases (like all sales suppression cases, even though not based in technology) quickly dissolve into a Battle-of-the-Estimates. For example, when there are no reliable sales figures, estimates of sales are drawn from the ratio of cash to credit sales compared to industry and local averages. At other times, in a restaurant case for example, sales per square foot, or sales per customer, or sales per seat (or table) can be compared with either (a) the Restaurant Industry Operations Report of the National Restaurant Association, or (b) the IRS Market Segment Specialization Program's report for Bars and Restaurants Audit Techniques Guide. The same reports can be used for a Cost of Goods Sold analysis.

None of these estimation approaches ever reach an accountant's level of precision. This can create considerable anxiety for both taxpayers and government auditors. However, in Washington, the presence of an ESS device under the statute strengthens the government's hand. The assessment is criminal, not merely civil. Larger (stronger) estimates of tax losses are the result.

Disproportionate penalties. Washington's ESS fraud penalties are disproportionate to the tax losses suffered. If two individuals both suppress $100,000 in taxable sales, one using old fashioned double tills, and the other using Zapping or Phantomware technology, the second is punished far more severely. Why? The tax loss is the same, the type of fraud is the same, the same Battle-of-the-Estimates will occur as the parties argue about the correct sales figure, only the method of accomplishing the fraud differs. Washington is punishing technology, not tax fraud. It needs to work with technology, not fight it.

The State of Washington appears to be overreacting with its imposition of ESS penalties. The source of the overreaction comes from difficulties everyone has with the Battle-of-the-Estimates that inevitably flows from any sales suppression fact pattern. Washington penalizes any person who *knowingly possesses* sales suppression software, even if it can be shown that the software has not been used nor was intended to be *used*.

Instead of indexing ESS penalties to tax losses, Washington presumes tax losses and applies a set of uniform, interlocking penalties regardless of the tax impact. The penalties are:

- Class C Felony[92]
    - 5 years confinement in a state correctional institution
    - and/or $10,000
- Seizure and forfeiture of ESS devices as well as any devices that used the ESS, or property that is traceable to ESS, including specifically the business's
    - Electronic Cash Registers, and
    - Point of Sales systems[93]
- Conditional loss of business permits, unless:
    - All taxes, penalties and interest is paid
    - All additional penalties and fines are paid
    - An electronic monitoring agreement acceptable to the Department is entered into between the taxpayer and the Department for 5 years.[94]

[92] RCW 9a.20.021(1)(c).

[93] RCW 82.32.670(1)(a)

[94] RCW 82.32.290(2)(a)(i)

The interlocking nature of these penalties make them particularly painful. These penalties put an individual, like those hypothesized in the text between notes 44 and 45 above, in a very difficult position.[95] The immediate forfeiture of a business' ECRs and POS system, coupled with the loss of a business license unless the demand for full payment of all taxes allegedly due, penalties and interest is satisfied along with the installation of an electronic monitoring system, could easily cripple a business. Not to mention a $10,000 fine and/or 5 years incarceration.

These interlocking penalties seem more designed for (or used to) leverage the government's position in an ESS Battle-of-the-Estimates, than they are designed to resolve the problem of data recovery from an ESS application. This seems to be what Washington has done in the first four Profitek Zapper cases it concluded. The US Attorney provided this information in the John Yin case.[96] As of February 2, 2017, Profitek Zapper cases #1, #2, #3, and #5 were assessed ("State Tax Due"): $73,324.00, $132,000.00, $80,000.00, and $149,811.00. The corresponding payments were ("State Tax Paid"): $74,045.15; $511,832.00; $55,304.79 and $105,647.39.[97]

There is no explanation for the occasionally wide variances between assessed tax and paid tax, but one strongly suspects the interplay between the traditional Battle-of-the-Estimates and the state's class C felony, seizure of ECR and POS equipment and business license revocation authority applied as negotiation leverage.

Evidence that the State "negotiated away" its penalty leverage to secure the taxes it assessed is apparent in a critical enforcement omission. None of the Profitek Zapper users (#1, #2, #3, and #5) were required to enter into a "… written agreement with the department for the electronic monitoring of the business's sales, by a method acceptable to the department, for five years at the business's expense."[98] One suspects that a taxpayer who insists on its estimate, its "total sales" number, in an ESS Battle-of-the-Estimates will bear the full brunt of the State's penalty provisions.

Problem of False Positives. The nature of ESS fraud encourages tax authorities to act fast, once they become aware of ESS. Tax administrations initiate massive sweeps, auditing all the businesses found on the customer lists of ECR/POS system installers,

[95] The three "types" of restaurant situations listed above are: (1) an owner, like owner of the Dudok, who has Phantomware installed unknowingly in his POS system by the distributor, who later finds out that it is in his system; (2) the second-hand purchase of equipment either directly, or through the acquisition of an ongoing concern with ECRs or POS systems, where Phantomware has been unknowingly installed by the prior owner, and which the current owner only becomes aware of later; (3) the owner whose technology-adept night manager has installed Phantomware to embezzle from the owner, the knowledge of which is attributed to the owner by virtue of his hiring and controlling this manager.

[96] *USA v. John Yin,* Docket No. 2:16-cr-00314-RAJ (W.D. WA)

[97] *USA v. John Yin*, Government's Opposition to Defense Motion to Continue Sentencing for a Second Time, Attachment 2, Docket No. 2:16-cr-00314-RAJ (W.D. WA) April 11, 2017. The attachment records four more Profitek Zapper cases: #4, #6, #7 and #8 with assessments of: $125,000.00; $87,997.00; $38,467.00; and $394,835.00 respectively. No state taxes are recorded as paid on these amounts as of the day of the US Attorney's Attachment 2.

[98] RCW 82.32.290(4)(b)(iii)

whenever those systems are found to be vulnerable to ESS fraud.[99] The assumption being, if the POS installer sells Zappers, or if the system he installs comes with embedded Phantomware, then it is likely that the businesses where he is installing POS systems are also likely to be using this technology to suppress sales.

RCW 82.32.290(4)(a) however, has a threshold lower than tax fraud. It does not require *use* of ESS technology, or even successful sales suppression. To be *knowingly in possession* of an ESS device is sufficient for a class C felony, and the seizure of ECRs and POS systems (seizures are possible even without a warrant). RCW 82.32.290(4)(a) therefore, invites aggressive action by auditors when proof of *possession* seems assured at the outset of an audit, and proof of *use* is not required at all. Mistakes would seem easy. There are no statutory exceptions. Whether or not a *possession* is *knowingly* undertaken would seem to be the auditor's judgement call.

To get a sense of Washington's response to an awareness that there are identified Zappers within the state, see the case of John Yin, the Profitek (POS) salesman for InfoSpec. He was the sole source for the Profitek Zapper in the State of Washington for nearly a decade. The State of Washington secured a search warrant on John Yin on July 13, 2015. It specifically targeted his customer lists. Yin's guilty plea was received 17 months later on Friday, December 2, 2016. Yin's plea was entered a mere three days after the Information against him was filed in the Seattle Federal District Court (Tuesday, November 29, 2016). In a sense, Yin's case was moving so fast, it was done almost before it started.

By the time of Yin's sentencing, the State of Washington had completed audits of nine restaurants where Yin sold Zappers. Bearing in mind that Washington had never found a Zapper or a Phantomware application before it got access to John Yin's customer lists, the aggregate assessment is staggering. $3,445,589.00 in omitted sales taxes were assessed.[100] The US Attorney noted at the time, that when this figure was determined events were moving so fast that "… not all of the restaurants are aware of the audit results."[101] That's a fast-moving audit sweep!

The Profitek ESS system uses a Zapper which John Yin sold separately to his POS customers. Although there is a risk of false positives in a Zapper case, it is unlikely that a separately purchased device would not be known about or used (at least once) by the buyer. The same is not true of Phantomware applications that come pre-installed in a POS system. However, the Washington statute treats all ESS devices the same. What would have happened if Profitek was Phantomware? The Dudok case provides a glimpse.

[99] For example, a tax agency may audit all of the POS installers in an area, and secure copies of their customer lists in this audit to build a file that can be accessed in case one of the clients is later found with ESS technology.

[100] At an average 9% sales tax rate this represents $38,284,322.00 in suppressed sales that the State of Washington was not previously aware of.

[101] *USA v. John Yin*, Government's Sentencing Recommendation, at 9 n. 3, Docket No. 2:16-cr-00314-RAJ (W.D. WA)) April 14, 2017.

The essence of the Dudok case is the *unknown possession* of a Phantomware program. There was no knowledge of the program's existence until Dudok's owner-manager received a tutorial from the managing director of Straight Systems B.V. This tutorial would be sufficient to seal a felony conviction under the Washington statute. However, in the Netherlands, the proof of *use* of an ESS device *to avoid a tax* is required.

Nevertheless, once the Dutch authorities became aware that Phantomware was embedded in the Finishing Touch POS system (just like the State of Washington became aware that Zappers were being sold with Profitek POS systems), they targeted every known purchaser of this system in the country. Visits were scheduled and audits were undertaken throughout. There is no public tally of the amounts collected from the Dutch sweep of all known Finishing Touch POS systems in use, but the net result was that Straight Systems B.V. was assessed a €100,000 fine and quickly left the POS market.[102]

Opportunity for voluntarily negotiated monitoring agreements. The reality of ESS fraud in the US is probably comparable to that in the rest of the world. This means that somewhere between 36% and 70% of the businesses in Washington are either:

- actively using Zappers, Phantomware, SSaaS, or the Dark Cloud to suppress sales, or
- that their ECR/POS systems either
  - have a dormant version of ESS technology within their system or
  - are favorably designed to accept a later installation of ESS technology

  even though they are not actively suppressing sales now.

Given that there is an international technology-based standard for dealing with ESS, Washington's approach of severely penalizing individuals who *knowingly possess* this technology overshoots its mark by a long shot

The law's design (instead) should encourage broad adoption of the solution, not use the solution as a cudgel to beat taxpayers into submission, or threaten them with loss of their business if they do not comply. Right now, the only businesses allowed to participate in Washington's electronic monitoring system are class C criminals. Somehow this does not seem right. The intent should be to welcome all businesses into the monitoring system.

An information campaign on the ESS problem would be a good first start. Monitoring agreements should be a fairly easy sell to the public at large if it is explained that in spite of the fact that they are paying a sufficient amount in taxes, the rates will need to go up because businesses will continue to syphon off the State's revenue unless monitoring agreements are more widely adopted. The normal business response to this campaign (at least by businesses that *knowingly possess* ESS technology) would be to seek shelter. Shelter should be provided. Electronic monitoring should be widely available.

[102] See: LJN AX6802 20060602, available at: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2006:AZ3100 (in Dutch, translation on file with author).

A half-way measure would be to provide taxpayers with a way to "clean" their ECR/POS systems, and then provide a certification that the system was not ESS-capable. This would be a registration and inspection program, similar to automobile inspections, and made part of the business licensing/re-licensing process. The difficulty with a program like this (similar to the one adopted by Greece[103]) is that the State would need to become an expert in all the technology used in all the ECR/POS systems in the state (and remain current on it).

A preferable approach would be to adopt the Rwandan solution of the Electronic Business Machine (EBM). A business would visit Home Depot, Target or Wal-Mart and select a EBM from the shelf, paying the standard price for a unit (it could easily be less that $100). The Business owner would then take the EBM (with an SDC, if one was not already embedded in the EBM) to any branch office of the DOR where it would be activated (for free). The DOR officer would use the EBM back office to personalize the Sales Data Recorder (SDC), assigning it to the taxpayer and activating keys for encryption of auditable data.

Under the EBM approach, the state would need to set up a data center (roughly the size and capacity of two good laptop computers) to receive the real-time data from all designated Washington businesses. It is common to start a program like this by "market segment." The restaurant sector is a common beginning sector. An artificial intelligence (AI) program similar to that put in place in Ceará, Brazil by SmartCloud Inc. to perform risk analysis for their VAT administration would be needed to risk-analyze the data flows.[104]

Opportunity for good faith amnesties. Even with no changes in the current statute, and with no effort made to advertise the ESS problem to the public there is a community of businesses with restaurants in the lead, but also bars, convenience stores, gas station and lumber yards not far behind who might appreciate an amnesty program. This would not be a program similar to turning in hand guns, because we are dealing with computer code not tangible property.

An effective amnesty would not just require that the business "turn-in the code," but also require enrollment in an electronic monitoring program (going forward).

[103] Richard T. Ainsworth & Urs Hengartner, *Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud with Technology* 57 CANADIAN TAX JOURNAL 715, 728-734 (2009). (providing a comparative assessment of "fiscal tills" in Greece, Quebec and Germany, and indicating that the Greek approach to Fiscal Electronic Devices (FED's) were published widely in 2004 under European Directive 98/34/EC. When considered as a whole, the Greek rules attempt to provide data security both when a pro-forma receipt is generated, and when the printer is being directed to issue the final receipt.)

[104] Michael W. Barnet, the head of Knowledge Engineering at SmartCloud Inc. indicates that the Ceará program, called CRex, scales linearly (that is, for more capacity you simply add more CPUs). Data for CRex with 1 CPU (2.53 GHz, 8 GB RAM, 8 Cores) gives it the capacity to import invoice data, store it, and perform risk analysis tests at a rate of 131,000 invoices (with 784,000 invoice items per invoice) in 220-270 seconds. This is a processing rate of 3,735 records/sec (or 1,172,790 bytes/sec). Ceará has allocated 16, 8-core machines to the CRex project. Personal e-mail communication (September 14, 2016) mbarnett@smartcloudinc.com (available with author).

The difficulty with any amnesty in this area is that the individual coming forward is admitting to *knowingly possessing* an EES device. This is an admission to a class C felony. Because Washington disconnects the *tax fraud* from the *crime of possessing* an ESS device, any discussion about the extent of the suppression (the actual tax amounts due) are independent of the admission to the crime. In other words, the Battle-of-the-Estimates will still occur.

As a result, only individuals who know that there will be very little dispute about the amount owned will come forward in an amnesty. For example, a person who (like the owner of the Dudok) *unknowingly* purchases a POS system with embedded Phantomware, but who has never used it, will come forward. So too will the owner of a POS system that contains Phantomware installed by an embezzling night manager.

Even here there may be complications if the DOR suspects a ruse to get clean bill of health. Then again, an amnesty might have value in the sale of a business where the new owner assumes no liability for prior taxes, but suspects that the ECR or POS system is ESS capable.

An amnesty in this situation would only be about the crime of *knowingly possessing* an ESS device. The new owner would want to avoid seizure of the equipment, and may want to participate in an electronic monitoring program (going forward).

CONCLUSION

The Washington statutes dealing with ESS, RCW 82.32.290(4) (unlawful acts – penalties) and RCA 82.32.670 (seizure and forfeiture), operate with an exceedingly low threshold, one that criminalizes "… knowingly … possess[ing] … any automated sales suppression device or phantom-ware." Either the statute should be modified, or regulations should be issued to make it clear that the device or phantom-ware must be "used" to evade or avoid a tax. "Knowing" or "possessing" software is not a crime, and it is not tax fraud. "[U]sing [software] to evade or avoid a tax" is.[105] Making this

[105] See the California statute which states at Cal. Rev. & T. Code §55363.5(a) (emphasis added):

> (a) Notwithstanding any other provision of this part, any person who purchases, installs, or uses in this state any automated sales suppression device or zapper or *with the intent to defeat or evade the determination of an amount collected pursuant to this part* is guilty of a misdemeanor.

The same language is used in Pennsylvania's statute. PA ST 72 P.S. § 7268. Utah statute is similar U.C.A. 1953 § 76-6-1303(1). See also Minnesota's statute in note 104. Kentucky has an original approach criminalizing "automated business record falsification devices" at KRS 517.130(1):

> A person is guilty of possession of an automated business record falsification device when he or she knowingly possesses any device or software program that falsifies the business records created by a point-of-sale system, such as any electronic device or computer system that keeps a register or supporting documents designed to record retail sales transaction information, by eliminating or manipulating true retail sales transaction information in order to represent a false record of transactions. These devices may also be referred to as "zappers" or "phantom-ware."

adjustment would increase the burden on auditors slightly as they would have to investigate the "use" of the software to avoid or evade a tax, but it would go a long way to rationalizing and harmonize tax enforcement around ESS. The authors regularly perform this test of software usage in this context. It is not a great challenge.

Secondly, both of these statutes are far too limited and far too homogenized when it comes to explaining what they are dealing with. For example, these statutes appear to treat Zappers and Phantomware almost as synonyms, even though one involves placing suppression code on removable tangible property (CDs or memory sticks) and the other writes suppression programming into the firmware or places it on the hard drive of an ECR/POS system. This is not a distinction without a difference. Placing suppression code in the firmware or on a hard drive makes it very easy for someone to be *unknowingly in possession* of ESS (Phantom-ware), whereas being *unknowingly in possession* of a Zapper is very unlikely. As a result, and as written, the Washington statute criminalizes many business owners who have older ECR/POS systems, because these systems commonly contained Phantomware, even though it may never have been used for suppression purposes.

Regulations need to provide a safe harbor for these business owners, as well as provide individuals similarly situated with a pathway through which they can appropriately cleanse their systems of offending programs (without risking criminal sanctions). The general topic of ESS regulations is another area of concern, one which this paper has not probed very deeply, but after four year on the books there is not one line of regulation applying to either of these statutes even though the ambiguities and questions about them are abundant.

Thirdly, although RCW 82.32.290(4) (unlawful acts – penalties) and RCA 82.32.670 (seizure and forfeiture) purport to cover all ESS, they really only deal with two of the ESS permutations - Zappers and Phantomware. At the present time there are four dominant strains of ESS each of which is deeply dependent on technology to suppress sales. The major ESS omissions are SSaaS and the Dark Cloud. Both of these interface with the business owner as services, but with an intensely technology-dependent backend structure. What is important for this discussion is that neither leave anything (code, device, or other programming function) in the possession of the business owner. They are not *devices*.

Neither SSaaS or the Dark Cloud permutations of ESS are within the ambit of the Washington statutes. To capture them a "catch-all" phrase like "or other method of electronically suppressing sales" is needed. This problem is not unique to Washington. Many, but not all of the other states (and some foreign jurisdictions) have language that is identical to Washington's. The few that do have a "catch-all" phrase have focused them on other kinds of *devices* that can be possessed by the taxpayer and which will suppress sales. These ESS statutes are not understanding that ESS can be a service performed by third-party technology, and any *devices* involved are possessed by the third-party service provider.[106]

Generally speaking, the statute fails to understand that we are a standing in a fast-flowing technology river which is being used for tax fraud. We may visit the same river several times during the year on our fishing expeditions, but *it is fundamentally not the same river* on each visit. Technology changes, fraud methods mutate and migrate. This is the game of "Whack-a-Mole" again. Washington, the state whose backbone is technology, should understand this almost intuitively.

Fourth, and most importantly, the Washington statute is a pure, hard-nosed enforcement statute that sees ESS as an aberration, a problem that needs to be confronted criminally. It does not see it as a long-established, deeply-embedded (although highly improper) way of doing business that needs to be changed.

There is a tax policy case here, and it needs to be made clearly, honestly, and publicly. If even the lowest estimate of the prevalence of ESS is applicable to Washington (the 36% of all businesses estimate out of Canada), then Washington has a systemic suppression problem. (In needs to be noted that Washington has never commissioned a study of ESS fraud within the state and no academic has volunteered to provide one as a civic service, so we are all operating somewhat blind here.)

Tax policy needs to facilitate a change, not freeze the problem in place. Harsh enforcement efforts sometimes have the effect of making permanent what they hope to root out. They do this with traps (consider the *unknowing possessor* of Phantomware) and limits on honest efforts to come clean (consider the *absence of amnesties* in the law). But more fundamentally, bad tax policy is one which identifies a problem, recognizes but does not adopt the solution, and instead chooses to punish violators severely (with an unreasonable harsh mandate to adopt the very same solution without state assistance to get it working).

There is a way to do this right – but it requires state action. The way is through real-time secure data capture and transmission to the tax administration. This is the international standard. This is the proven way to stop ESS. This is what Washington has not adopted, although taxpayers may (one-by-one) as they are apprehended for criminal violations of the statute, propose the international standard as part of "… a written agreement with the department for the electronic monitoring of the business's sales, by a

[106] Most of the other 25 states with similar statutes use the same language and have the same problem omitting SSaaS and the Dark Cloud, but see Michigan's law M.C.L.A. §750.411w(1) (emphasis added):

> (1) A person shall not knowingly sell, purchase, install, transfer, or possess in this state any automated sales suppression device or zapper, phantom-ware, *or a skimming device*.

Minnesota's statute has a catch-all phrase, but limits it to "devices." MN ST § 289A.63, Subd 12(a):

> A person who sells, purchases, installs, transfers, develops, manufactures, or uses an automated sales suppression device, zapper, *or similar device* knowing that the device or is capable of being used to commit tax fraud or suppress sales is guilty of a felony

method acceptable to the department, for five years at the business's expense."[107] This is simply not the way to do the tax enforcement business.

Technology must be used to stop technology-based suppression fraud. If Washington is not willing or able to take the road marked out by the international community, if it is insistent on a criminal penalty approach to solving ESS, then it needs to at least recognize that *it is not effective tax policy to* ***only have those convicted*** *of a class C felony allowed to enter into a monitoring agreement with the tax administration*. If Washington is serious about stopping ESS by imposing penalties, then it needs to create an avenue for voluntary participation in the electronic monitoring program, maybe in exchange for reduced penalties (or some other incentive).

The real solution however is to mandate that all businesses, or all businesses within a particular economic sector (restaurants, for example), must join the real-time electronic monitoring program.

[107] TCW 82.32.670 (4)(b)(iii)