taxnotes® international

Volume 89, Number 11 ■ March 12, 2018

Fighting Technology With Technology: Taking Aim at Electronic Sales Suppression

by Richard T. Ainsworth and Robert Chicoine

Reprinted from *Tax Notes International*, March 12, 2018, p. 1037

Fighting Technology With Technology: Taking Aim at Electronic Sales Suppression

by Richard T. Ainsworth and Robert Chicoine

Richard T. Ainsworth

Robert Chicoine

Richard T. Ainsworth is an adjunct professor at the Boston University graduate tax program and the New York University graduate tax program. Robert Chicoine is with Robert Chicoine Law in Seattle. Email: prof482@bu.edu, rjc@robertchicoinelaw.com

In this article, the authors examine how various countries combat the use of electronic sales suppression to commit tax fraud and demonstrate how these examples could be applied to improve Washington state's problematic electronic sales suppression enforcement model.

Electronic sales suppression (ESS) is a fraud that has been a prominent in North American retail business since at least 1996.[1] The first ESS case in the United States dates from 1981.[2] ESS is a global problem and is estimated to be present in 34 percent of Canadian,[3] 50 percent of German,[4] and 70 percent of Swedish[5] and Slovenian[6] businesses. It may be the case that you cannot leave home without encountering or participating in ESS.

ESS fraud is a generic term representing 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 allows the fraudster to collect the government's tax and not remit it; in other cases, the fraudster manipulates to the records to avoid paying the correct amount of tax.

The range of ESS frauds in a jurisdiction depends on the tax systems and the taxes that are the easiest targets. If the opportunity presents

[1] Email from Dave Bergeron (June 6, 2008) (on file with author). *See also* Bergeron, Pacific Region ECAS Conference, slide 3 (unpublished presentation, on file with author); Richard T. Ainsworth and Bergeron, "Zappers (automated sales suppression)," slide 6, New York Prosecutors Training Institute (July 31, 2008) (unpublished presentation, on file with author); Ainsworth, "Zappers and Phantomware: Are State Tax Administrators Listening Now?" *State Tax Notes*, July 14, 2008, p. 103; and Kevin Pratt, "Tax Evasion in an Electronic Environment — 'Zapping'" (presentation at the Federation of Tax Administrators Compliance Education Workshop, Louisville, Kentucky (Feb. 25-27, 2001)) (on file with author).

[2] *United States v. Leonard and 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, which began as a physical skimming operation, are preserved in federal sentencing appeals).

[3] Dean Beeby, "Taxman Finds Rampant Restaurant Fraud," *Globe and Mail*, Aug. 1, 2011. *See also* Canada Revenue Agency 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) (heavily redacted version on file with author).

[4] Unterrichtung durch den Bundesrechnungshof (Nov. 24, 2003); and Bemerkungen des Bundesrechnungshofes 2003 zur Haushalts — und Wirtschaftsführung (Einschlieblich der Feststellungen zur Jahreschung des Bundes 2002).

[5] Email correspondence with Bo Arvidsson, tax director of the Swedish Tax Agency (Feb. 19, 2010) (on file with author). Arvidsson later indicated that the 70 percent figure was conservative and the real number was closer to 80 percent, although that was not the official position of his agency.

[6] The Slovenian Tax Administration announced that in 1,150 cases in which receipts were photographed with cellphones and left on the tables of restaurants, 70 percent were tampered with by zappers. *See* "You Go to the Bar? Take the Bill," RTVSLO (Jan. 19, 2008) (Google translation, original in Slovenian).

itself, fraudsters will target two or more taxes that can be hit with a single stroke.[7] Income taxes, payroll taxes, customs duties, excise taxes on fuel and cigarettes, VAT, and retail sales taxes are all vulnerable. However, because the reward is so immediate, it is the transaction taxes — taxes in which the government's revenue is collected as part of the commercial exchange — that appear to be the technology fraudster's favorite target.

The common solution in all cases is digital security, or fighting technology with technology.[8] In the United States, ESS has funded common criminals, organized crime syndicates, and foreign and domestic terrorist organizations. U.S. suppression cases have involved celebrity chefs,[9] members of Congress,[10] the funding arm of Hezbollah,[11] grocery store chains,[12] restaurants,[13] bars and strip clubs,[14] and pizza parlors. For some reason, the United States has been slow in fighting ESS technology with technology.

Given that Washington state collects 47.3 percent of its revenue (excluding local government taxes) from the retail sales tax,[15] and that technology has been the backbone of the state's economy for years,[16] it is only natural that Washington would lead in this effort; however, the state still trails international efforts by a wide margin. The United States 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, as of January 1, the members of the Gulf Cooperation Council (Bahrain, Kuwait, Oman, Qatar, the United Arab Emirates, and Saudi Arabia).

The most common types of sales suppression technology are zappers and phantom-ware programming.[17] In some instances, sales suppression is a personal, hands-on service offered by installers or electronic cash register/point-of-sale (ECR/POS) sales representatives — sales suppression as a service (SSaaS).[18] Recently suppression has entered the dark cloud — a fully automated manipulation of sales data that takes place offshore and uses internet-based data transfers.[19]

I. Washington's Technological Response to ESS

Using the California statute as a template, 25 states[20] have responded to ESS by making it a

[7] For a discussion of dual ESS frauds from Denmark and Saudi Arabia, see Ainsworth and Musaad Alwohaibi, "The First Real-Time Blockchain VAT: The GCC Solves MTIC Fraud," *Tax Notes Int'l*, May 22, 2017, p. 695.

[8] Lauren Loricchio, "Connecticut Announces First Arrest for Zapper Sales Tax Fraud," *State Tax Notes*, July 31, 2017, p. 422 (quoting Connecticut Revenue Commissioner Kevin Sullivan as saying, "The real hope would be that there would be equal technology that would essentially. . . detect the presence" of ESS technology).

[9] *See* Daniel Gerzina, "Mayor No More? Tony Hu Planning to Sell Most of His Chinatown Restaurants," *Chicago Eater* (Feb. 16, 2015); *United States v. Hu Xiaojun*, Docket No. 1:16-cr-00316 (N.D. Ill. May 13, 2016); and Ainsworth, "Sales Suppression: The International Dimension," 65 *A.L. Rev.* 1241 (2016).

[10] Former U.S. Rep. Michael Grimm was convicted of manipulating the sales at his fast food restaurant, Healthalicious, from 2007 through 2010 and underreporting payroll by concealing off-the-books wages. *See* John Crudele, "Trolls and Perverts Hound a Reformer Off Facebook," *New York Post*, May 14, 2014; and *United States v. Grimm*, Case No. 14-cr-00248 (PKC) (E.D. N.Y. 2015).

[11] *See* U.S. Department of Justice release, "Financial Manager Sentenced to 18 Months for Tax Evasion" (May 15, 2007). The $20 million skimmed at the LaShish restaurant chain was used to finance Hezbollah terrorists in Lebanon. U.S. Department of Justice release, "Superseding Indictment Returned Against LaShish Owner" (May 30, 2007).

[12] *Leonard and Guthman*, 37 F.3d 32, which until recently was "the largest computer driven tax-evasion case in the nation," Treasury, IRS, *75 Years of Criminal Investigation History (1919-1994)*, at 146.

[13] Heather Cherone and Ariel Cheung, "Cesar's Restaurant Owner Charged With Failing to Report $1 Million in Sales," *DNAInfo Chicago*, Aug. 3, 2017.

[14] In an early sales suppression as a service (SSaaS) case, a Detroit computer consultant was employed by the owner of two strip clubs to visit them regularly and run a zapper program. The consultant had secured the program from programmers in Quebec. *See* U.S. Department of Justice release, "Michigan Software Salesman Pleads Guilty to Conspiracy to Defraud the Government" (Nov. 17, 2010); and *United States v. Faramso and Kramer*, Case 5:10-cr-20173-JCO-MKM (E.D. Mich. 2010).

[15] Washington State Department of Revenue, Research and Fiscal Analysis Division, "Tax Statistics 2016, Chart 1."

[16] Blanca Torres, "Washington State Ranks No. 1 for Combined Job and Wage Growth," *The Seattle Times*, Feb. 15, 2016.

[17] Ainsworth, "Zappers and Phantomware: The Need for Fraud Prevention Technology," *Tax Notes Int'l*, June 23, 2008, p. 1017; Ainsworth, "Zappers and Phantomware," *supra* note 1.

[18] Ainsworth, "Sales Suppression as a Service (SSaaS) and the Apple Store Solution," *State Tax Notes*, Aug. 4, 2014, p. 343.

[19] The dark cloud is a term coined for this discussion. We use it to describe an internet business that accepts data transmission from cash register systems, manipulates sales data with predetermined algorithms, and then returns the data to the systems. Dark clouds operate both on regular schedules or in real-time, and have appeared in New York and North Carolina.

[20] Ga. Code Ann. section 16-9-62; R.I. Gen. Laws section 44-19-42; Ala. Code section 40-29-121; W.Va. Code section 61-3-22a; 13 Vt. Stat. Ann. section 2032; Conn. Gen. Stat. Ann. section 12-428a; N.D. Cent. Code section 12.1-23-16; N.C. Gen. Stat. Ann. section 14-118.7; Tenn. Code Ann. section 39-14-704; Wash. Rev. Code Ann. section 82.32.670; 17 Me. Rev. Stat. Ann. section 909; Cal. Rev. & Tax. Code section 55363.5; Mich. Comp. Laws Ann. section 750.411w; Fla. Stat. Ann. section 213.295; Tex. Bus. & Com. Code section 326.002; La. Rev. Stat. section 47:1641.1; Ind. Code. section 35-43-5-4.6; 35 Ill. Comp. Stat. 105/14; Wyo. Stat. section 39-15-108; 72 Pa. Stat. section 7268; Minn. Stat. Ann. section 289A.63; 68 Okla. St. Ann. section 212.1; Utah Code Ann. section 76-6-1303; Ky. Rev. Stat. section 517.130; and S.D. Codified Laws section 10-59-57.

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"[21] 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."[22]

In some states, like Kentucky,[23] the criminal acts associated with ESS include only possession. Others, like Louisiana,[24] make it a crime to "create, design, manufacture, sell, purchase, lease, install, update, repair, service, transfer, use, possess or make available" such programs. Each of the 25 states criminalizes zappers and phantom-ware by name. Minnesota adds the catchall phrase "or similar device."[25] This language is unlikely to apply to SSaaS or dark cloud types of ESS fraud, because they are suppression services, not devices.

However, only Washington goes 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,[26] if they want to remain in business. This is a requirement to use security technology to fight fraud technology, and is comparable to most serious fraud prevention efforts around the world.

By implementing monitoring for specific offenders, rather than universally[27] or by market segment,[28] Washington has decided to move slowly, though in the correct direction. If nothing else, the state will have a pilot program with multiple businesses using many kinds of solutions, each one of which could expand to provide complete coverage throughout the state. There are no known plans for this, however, just the potential. Washington will be the only state to have hands-on experience interfacing with those security technologies, and it should be well placed to decide what to do if the problem is a serious as the international studies suggest it could be.

There is every indication that this is a serious situation. We have written on the flow of zappers into Washington from Vancouver, British Columbia, and from China.[29] There is 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 SSaaS or move into the dark cloud. Chasing technology fraudsters is like playing whack-a-mole — each time you push against the fraud it morphs and becomes more difficult to stop. Fraudsters will try to morph in a way that takes them outside the current statute.

We will examine three of the most serious challenges faced by the Washington statute. First is the lack of regulatory guidance on how to interpret the statute, with the most glaring omission being the lack of guidance on what methods of electronic monitoring are acceptable to the DOR. Second is the absence of a statutory requirement that ECR/POS retailers allow access to their systems by independent digital security firms so that the mandated electronic monitoring can be installed. Third is protection against excessive estimates and false positives. With 34 to 70 percent of the ECR/POS systems in the state likely vulnerable to ESS, and severe penalties for the mere possession of ESS technology, the statute must provide protections against inevitable false positives. There are taxpayers who the department will presume to be engaged in ESS fraud simply because they own ECR/POS systems that are known to be vulnerable to sales suppression.

[21] Cal. Rev. & Tax. Code section 7153.6(a).

[22] Cal. Rev. & Tax. Code section 7153.6(b).

[23] Ky. Rev. Stat. section 517.130 (1).

[24] La. Rev. Stat. section 47:1641.1(A)

[25] Minn. Stat. section 289A.63.

[26] Wash. Rev. Code Ann. section 82.32.290 (4)(b)(iii)

[27] Argentina, Brazil, China, Croatia, Greece, the Gulf Cooperation Council, Hungary, Indonesia, Italy, the Philippines, Portugal, Romania, Russia, Rwanda, South Korea, Taiwan, and Venezuela have a universal transactional security system.

[28] A market segment-based transactional security system is found in Austria, Belgium, Germany, the Netherlands, Ontario, Quebec, and Sweden.

[29] Ainsworth, "Sales Suppression: The International Dimension," 65 *Am. U. L. Rev.* 1241 (2016) (discussing the InfoSpec/Profitek zapper and POS system imported into Washington from Vancouver, British Columbia, and from China, and numerous other instances in the United States and Canada).

II. Difficulties With the Washington Statute

Based on our work with the Washington ESS statute, we believe the following three aspects of the Washington enforcement regime need to be addressed. In each of those 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 expand upon in further articles. This should be considered an initial and not a final statement on these issues.

A. Regulations

In 2013 Washington enacted S.B. 5715, codified at Wash. Rev. Code section 82.32.290, which prohibits ESS. Specifically, the statute makes it a crime 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."[30]

In four years, no substantive regulations have been issued, even though the statute's penalties are severe. ESS is a class C felony imposing up to five years' incarceration and a $10,000 fine, as well as termination of the business license unless a five-year electronic monitoring agreement is entered into with the DOR.[31] Regulations are even more important in this area because the topics 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.

Each of the operative terms in the statute needs clarification. For example, what does it mean to knowingly "possess" phantom-ware when it 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?"[32]

Consider the following hypothetical: Is it a violation of the statute when a business purchases an ECR/POS system that contains factory-installed phantom-ware, and the owner, who does not use the programming, later becomes aware through news reports that the system purchased long ago has this hidden program? Which of the significant phantom-ware penalties should apply to the business owner? And even though seizure 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 "the 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."[33]

There are more than 25 commonly marketed ECR/POS systems manufactured for sale in Washington that have factory-installed phantom-ware functionality. Iterations of most of the systems have been on the market for several decades. There are many more systems in which phantom-ware programming can be self-installed by someone with reasonable technological aptitude. The phantom-ware installation is easy because the manufacturer has left the back door unlocked and opened.

Thus, anyone owning one of those systems in Washington, whether they bought it themselves or purchased a business over the last 25 years with the equipment already installed, is violating the statute if they possess it knowing of its ESS functionality. Seizure of a business's ECR/POS system will effectively shutter the establishment until another ECR/POS system can be installed.

[30] Wash. Rev. Code Ann. section 82.32.290 (4)(a).

[31] Wash. Rev. Code Ann. section 82.32.290 (4)(c)(i).

[32] Wash. Rev. Code Ann. section 82.32.670 (7)(c) defines phantom-ware as:

> 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.

[33] Wash. Rev. Code Ann. section 82.32.670 (1)(b) and (b)(2).

Thus, this statute's enforcement provisions need to be softened. Amnesty regulations are needed. The business community should expect it.

B. International Examples

Rather than using domestic examples, we believe it is advisable where possible to move the discussion into the international sphere where there are also abundant examples of fraud. The following two examples will show the need for Washington regulations: the factory-installed phantom-ware at the Café Dudok in the Netherlands, and the phantom-ware that can be installed on three Casio-brand ECRs. This latter issue was discussed by European Commission's Fiscalis Committee Project Group 12.

1. Factory-Installed Phantom-Ware: Dudok

The Café Dudok used the factory-installed phantom-ware program in its Finishing Touch POS system, manufactured by Straight Systems B.V.[34] Straight Systems is a Netherlands company that specializes in single-service ECR systems, in which all hardware and software are developed in-house. The company website 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."[35]

The Dudok case discusses three software programs: Twenty/Twenty, Finishing Touch, and Tickview.exe. Twenty/Twenty was a U.S. touch-screen program that did not have a phantom-ware application. Straight Systems added the phantom-ware application to Twenty/Twenty and renamed the program Finishing Touch. With 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 can delete the whole ticket, for which the system records a "no sale" and the entire audit trail to the original data is eliminated.[36]

The phantom-ware program embedded in Finishing Touch was first used by Dudok to skim cash receipts during a Dutch revenue agency examination. The agency was suspicious that staff salary payments were being made under the table.[37] Testimony indicated that on the second day of the audit the managing director of Straight Systems visited Dudok and was approached by the owner-manager who explained that he was having difficulty accounting 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 explained that this was "a hidden menu option that, after enabling said option, allowed operators of catering establishments to delete cash register receipts from the system."[38] After this discussion, a Straight Systems employee visited Dudok to explain the application of the function, which Dudok later decided to use.[39] This case shows how a business can purchase a POS system with an embedded phantom-ware program without knowing about it. The purchase was most likely made based on commercial reputation, and the phantom-ware application was not a selling point.

Under the Washington statute, as soon as the owner learns that his POS system contains phantom-ware, the criminal provisions apply personally and to the corporate entity. Possession is not a question, only knowledge of the possession is. The operation of the statute may be too draconian if there is no flexibility in its application. For instance:

- What if the owner knew about but did not use the phantom-ware? If this was a new POS system an owner might hesitate to resolve the issue because it could mean replacing an expensive POS system.
- What if the night manager and not the owner learned about the phantom-ware?

[34] District Court of Rotterdam, LJN: AX6802 (June 2, 2006) (in Dutch, translation with author); judgment affirmed by the District Court of The Hague, LJN: BC5500 (Feb. 29, 2008) (in Dutch, translation with author).

[35] Straight Systems (in Dutch, translation with author).

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

[37] LJN: BC5500, at F3. Before using the phantom-ware installed on its system, Dudok's sales skimming system was amateurish. Entire sales records were deleted and records were reconstructed on spreadsheets. The examining agents did not trust the spreadsheets and asked for the POS records as confirmation. This led to the conversation during which Dudok was informed that it already had phantom-ware that might solve this problem installed in its system. Van der Zwet, personal email correspondence (May 28, 2008) (on file with author).

[38] LJN: AX6802, at Consideration of the Evidence (June 2, 2006).

[39] LJN: BC5500, at F3.

Can the owner and business be held liable if the night manager does not pass this information on (perhaps because he wants to embezzle funds from the business himself)?

- What if the owner's manual, which was left with the company's IT specialist, contained instructions explaining the hidden delete function? Can the owner be held criminally liable?
- What if the phantom-ware is discussed in online forums the IT staff visits? Can the owner be held criminally liable?

2. Self-Help Phantom-Ware: Casio TE-2000

The Fiscalis Committee Project Group 12 broke down numerous ECRs and presented detailed expositions on how to reset the ECR so that the system would suppress sales. Installing phantom-ware in a ECR/POS system is not that difficult.[40]

Under Washington law, if self-help phantom-ware is detected on an ECR/POS system, a criminal violation is almost assured, provided it can be determined who performed the installation. It would be exceedingly difficult for the installer to deny knowledge and possession of self-help phantom-ware. But consider the following hypotheticals:

- What if the self-help phantom-ware was installed by the distributor, and the business owner did not know about the programming?
- What if the equipment was purchased second-hand when the business changed hands? Does the statute require proof of who installed the self-help phantom-ware?
- What if a rogue night shift manager or the IT specialist installed the self-help phantom-ware? Is there a criminal violation?

All those questions lead to the observation that there needs to be something more than knowledge-plus-possession to activate criminal enforcement measures fairly. The software also needs to be used to defeat tax collection. The problem is that possession and use are separate acts under the Washington statute, and they need to be joined in some manner. This is a regulatory matter that Washington can address.

Aside from the absence of regulations, further difficulty for Washington state taxpayers is illustrated in the two examples above. Assume that the DOR uncovers two phantom-ware frauds, one using a POS system like Finishing Touch in Dudok, and the other using a self-help phantom-ware application like on the Casio TE-2000 POS machine.

As happened immediately after Dudok, the Washington DOR will likely open audits on any enterprises using Finishing Touch or a Casio TE-2000 system. Because the presence of phantom-ware is a certainty in a Finishing Touch POS system, any sales irregularities could quickly lead to a seizure of the system, effectively shutting down the business. Enterprises using the Casio might be suspect, but without a forensic analysis seizures would be unlikely. Regulations should try to level the playing field between those two types of phantom-ware 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 it is aware that Casio TE-2000 and Finishing Touch are suspect classes of POS systems. This is what the Fiscalis Committee Project Group was doing when it detailed the Casio's self-help phantom-ware procedures. Would the Washington DOR be willing to do the same?

Regulations for a fair enforcement system would include a discussion of the POS/ECR systems that the DOR is aware have factory-installed phantom-ware or systems that allow phantom-ware to be easily installed. A fully transparent regulatory structure would do what the Fiscalis Committee Project Group did and explain in detail how to activate the self-help phantom-ware structures. The business community would be alerted that audits would be conducted to find modified ECR/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 DOR. As it stands, the DOR has a statute that punishes severely, and some might argue unfairly, and that will achieve its policy objectives slowly and with great expense.

[40] *See* European Commission, Fiscalis Committee Project Group 12, Cash Register Project Group, Cash Register Good Practice Guide (Dec. 2006).

III. ECR/POS Access

Washington has no statute compelling ECR/POS retailers to allow access to their systems by independent digital security firms so that third-party electronic monitoring systems can be installed. Understanding why such a mandate is necessary requires an understanding of the economic forces that control the ECR/POS commercial marketplace and what real data security in the ECR/POS marketplace looks like.

A. Economic Forces in the ECR/POS Market

1. Traditional Data Security for Tax Purposes

Almost all traditional ECR/POS systems have data security mechanisms including:

- *Printed (paper) receipts.* The most traditional and visible security measure for recording sales is the printed receipt. If every sale is recorded with a 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 more.
- *Digital (emailed) receipts.* The electronic version of the paper receipts with the advantage that they are easier to aggregate.
- *X reports.* Standard reports produced by an ECR that provide a snapshot of the cash drawer balance. An X report is cumulative and never resets.
- *Z reports.* Standard reports produced by an ECR that are run to provide a final balance for the cash drawer. A Z report resets the cash drawer balance to $0.
- *Electronic journals.* Internal memory storage areas in the ECR/POS system that record the line-by-line details of all transactions completed. When an electronic journal's storage is nearly full, a warning will issue allowing the user to print the journal to prevent data loss. When the journal is completely full, either no additional transactions will be saved or the journal will begin to write over the old data.

2. Origin of Zappers and Phantom-Ware

Zappers and phantom-ware programs are products 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 phantom-ware that defeat the traditional security features installed within them.

Zappers and phantom-ware programs are both a threat and an opportunity to the distributors of ECR/POS systems. For example, they are a threat in the hands of an embezzling employee who might suppress sales for personal gain at the expense of the owner.[41] They are an opportunity when they accelerate the sale of new ECR/POS systems to businesses intent on suppressing sales.

The latter group appears to be dominant. In fact, during a 2009 New York undercover sting operation, in which revenue officers posed as restaurant owners looking to purchase new systems, 95 percent of the salespeople also pitched suppression software and services tailored to fit their ECR/POS systems. Many provided demonstrations on how the suppression mechanisms worked. The kinds of suppression offered included zappers, phantom-ware, and SSaaS.[42]

The salespeople represented national leaders in the ECR/POS marketplace. One firm had 400 clients in Connecticut, New Jersey, and New York City. A second had 1,200 New York City clients, performed 200 installations a year. A third firm had 1,100 New York City clients. A fourth was the top POS sales and installation firm in Pennsylvania with 40 employees in its New York office and more than 3,000 total clients.[43] They were all pitching suppression to sell their ECR/POS systems.

The pattern repeats itself internationally. In Canada, for example, zappers and phantom-ware are designed, manufactured, and marketed by same firms or individuals who make and sell the ECR/POS systems. Why would the United States be any different?

Four Canadian cases illustrate the marketplace. They involve both small firms with IT professionals who install and maintain a limited number of ECR/POS systems, and large

[41] *See* IRS, "Ex-Burger King Manager Sentenced in IRS Fraud Case for Skimming $180,000 in Cash" (Mar. 20, 2007) (relating the manual skimming fraud orchestrated by a Burger King night manager).

[42] Ainsworth, "Sales Suppression," *supra* note 18.

[43] *Id.*, at 344, notes 7 and 8.

multi-corporate enterprises with considerable international reach. Audio Lab LP, Michael Roy, and Luc Primeau are examples of the small players and InfoSpec/Profitek is a major multinational enterprise.

a. Audio Lab LP Inc. In April 2004 Revenu Québec 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.[44] The allegation was that the restaurant was using a zapper to delete sales records. The zapper was on a diskette used with the restaurant's computer system.[45] In April 2005 Revenu Québec announced that the director of San Antonio Grill pleaded guilty to using a zapper. The director, Apostolos Mandaltsis, was fined. A related company of similar name, Grill San Antonio in Repentigny, pleaded guilty to similar offences.[46]

In October 2005 Revenu Québec announced that it executed five more search warrants in Montreal and Laval regarding Audio Lab LP Inc.[47] The company was suspected of having developed and marketed a zapper that was compatible with its own restaurant cash register software, Softdine.[48] Softdine was the operating software in the cash registers at San Antonio Grill and Grill San Antonio. In 2007 Audio Lab pleaded guilty to 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."[49] In other words, it pleaded guilty to developing a zapper to add on to its own commercial software that it provided to restaurants for use in their POS systems. Press reports directly link this conviction to the Laval investigation.[50]

b. Michel Roy. Before the first Audio Lab warrants were issued, Revenu Québec had concluded an extensive investigation of 28 restaurants doing business under the name Stratos.[51] Each restaurant used zappers. To dispose of the excess cash from skimmed sales, a double billing system was put in place with suppliers (to conceal purchases made in cash) and wages were paid to employees in cash without being reported as income.[52]

The guilty pleas from this investigation came in waves — 19 companies pleaded guilty in September 2002, six more in October 2002, and four in March 2003. Press releases provided details of only the final 10 companies. The taxes and penalties for those companies totaled just over C $1.8 million, but the most important information from the news releases was that Revenu Québec searched 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."[53]

In April 2003 Michel Roy and his two sons, Danny and Miguel, were convicted of tax evasion.[54] Michel was the creator of the zapper that worked with Terminal Resto. He promoted it and made the sales. His sons installed the software and designed the fraud. Aggregate fraud penalties assessed against the Roys were nearly C $1.1 million.[55]

c. Luc Primeau. Revenu Québec announced in March 2003 that seven Patio Vidal restaurant franchises and a bar, La Tasca, in Gatineau, as well as another bar named O'Max in Masson-Angers, were convicted of adding zappers to their Microflash cash register software (later upgraded to a new version called Caracara).[56] Even though

[44] Revenu Québec release, "Le Ministère du Revenu Soupçonne le Restaurant Grill San Antonio de Laval d'Avoir Utilisé un Zapper" (Apr. 8, 2004) (on file with author).

[45] *Id.*

[46] *Id.*

[47] Revenu Québec release, "Revenu Québec Enquête sur un Concepteur de Logiciel de Point de Vente Soupçonné d'Avoir Conçu et Distribué un Camoufleur de Ventes" (Oct. 14, 2005) (translation on file with author).

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Revenu Québec release, "Tous les Restaurants Stratos Coupables de Fraude Fiscale en Lien Avec l'Utilisation du Zapper" (Mar. 18, 2003) (on file with author).

[52] *Id.*

[53] *Id.*

[54] Revenu Québec release, "Des Amendes de Plus de Un Million de Dollars — Un Père et Ses Deux Fils Condamnés Pour Fraude Fiscale en Lien Avec le Zapper" (May 2, 2003).

[55] *Id.*

[56] Revenu Québec release, "M. Marcel St-Louis de l'Outaouais Coupable de Fraude Fiscale Liée à l'Utilisation d'un Zapper" (Mar. 17, 2003).

guilty pleas were entered, a search warrant had already been executed against the designer of Microflash and Caracara because the software developer was suspected of also being the developer of the associated zapper program.[57]

In 2005 Primeau admitted using his software to assist those companies to evade C $435,000 in goods and services tax and Quebec sales tax (QST).[58] They skimmed $2.7 million in cash sales and Primeau was fined $20,000. However, Primeau was more than a zapper salesman; he also considered himself a provider of management services for which he charged a fee. Revenu Québec determined that not only did Primeau fail to report GST and QST of nearly $34,000 on his own zapper sales, but he also failed to report over $155,000 in services income for zapper management advice.[59]

d. InfoSpec/Profitek. Profitek is a leading POS software development company specializing the hospitality and retail industries. Founded in 1985 and based in Vancouver, British Columbia, 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 (later corrected), the Canada Revenue Authority was ineffective in the case it brought against the manufacturer,[60] but it was successful against the salesman (assessing C $3.3 million in sales and income taxes)[61] and the restaurants (assessing overdue taxes of $731,986).[62] Not surprisingly, the InfoSpec/Profitek POS system and zapper has shown up in the US.

In Seattle, the Washington attorney general investigated John Yin, a 64-year-old self-employed software salesman, and a restaurant owner who allegedly used a zapper Yin sold her. Yu-Ling Wong secured both the zapper and her POS system from Yin, who admitted to selling Profitek zappers to multiple business owners. Yin entered a plea that included restitution of $3.4 million in Washington sales taxes and federal income tax due from skimmed receipts.[63]

B. Real Data Security in the Modern Market

Real transactional data security comes in two forms. Either it is provided directly by the government and mandated for all businesses or businesses in a specific market segment as a condition of securing a business license,[64] or it is provided by independent third-party vendors who have no commercial interest in the manufacture, sale, or installation of ECR/POS systems. The Rwanda government mandates only that ECR/POS products can interface with a secure unit, which is also purchased by the taxpayer.[65]

1. Traditional Security in the Cloud

It is insufficient for an ECR/POS system provider to take 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 a technological embellishment, but 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.

[57] *Id.*

[58] Revenu Québec release, "Le Concepteur d'un Camoufleur de Ventes de Boucherville Plaide Coupable à Diverses Accusations Portées par le Fisc Québécois" (Oct. 26, 2005).

[59] *Id.*

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

[61] *R. v. Au*, 2011 B.C.S.C. 75, para. 1 (Can.).

[62] On May 1, 2013, the CRA announced that it had found the Profitek zappers in two Winnipeg, Manitoba, restaurants. "Foody Goody and Buffet Square Plead Guilty to Numerous Charges of Tax Evasion," *Metro News* (May 1, 2013).

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

[64] This is the case with Quebec, which commissioned a secure unit called the *module d'enregistrement des ventes*, known in English as the sales recording module. The module records and preserves on-site all tax-critical data produced by the ECR/POS system it is connected to. The government designed the module, controls its technology, and physically owns the units, which it provides to the taxpayer at no cost.

[65] The Rwandan approach is like Quebec's but the government does not own the secure units. VAT Law No. 37/2012 of Sept. 11, 2012, article 24, obliges all VAT-registered taxpayers in Rwanda to acquire and use an electronic business machine to issue tax invoices.

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 phantom-ware also work in real time. And if the ECR/POS system or the top-of-the-line printer company is invested in making sales by providing zappers and phantom-ware to its customers, then the marketplace will defeat the solution.

Those kinds of security solutions would not be secure, and should never be a method acceptable to the DOR under Wash. Rev. Code Ann. section 82.32.290 (4)(b)(iii). Those security solutions should not be acceptable once the real-time functionality of zappers and phantom-ware 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; manipulation remains highly possible.

Those types of security offerings are very close to the dark cloud, where data is transmitted to the cloud, manipulated, and then returned to the ECR/POS system. 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, and DOR real-time storage) will match, but all will be manipulated.

This is apparently what happened in a North Carolina case that arose during a partnership dispute involving sales suppression, tax fraud, and a partner's embezzlement.[66] Among the relevant issues are that it was a private embezzlement action between two partners that involved significant tax fraud. Although tax fraud was not the motivation for the sales suppression, it occurred, and in this instance the interests of the tax administration and the private businessperson aligned nicely. The fraud was partly uncovered by one partner, talking with other businesses in the area and finding out that they were suppressing sales through their ECR/POS systems. The same ECR/POS installer was involved in each business, and the data manipulation happened in the dark cloud, which the installer selected, rather than the cloud access storage provided by the manufacturer.

2. Government-Provided/Mandated Security

This is the approach taken by many jurisdictions, including Quebec and Rwanda. It accepts that technology has allowed significant opportunities for fraud to enter the highly corruptible transactional marketplace. Rather than expecting changes in the marketplace, this approach levels 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*;[67] in Rwanda the device is called an electronic business machine (EBM).[68] In both cases there was an immediate improvement in revenue. Quebec saw self-reported revenue increases of C $160 million, and C $1.3 million in fines during the first year of operation.[69] Rwanda saw an 8 percent revenue increase in the first six months and 20 percent in the first two years.[70]

3. Industry Standards

Washington has decided to put the burden of finding a monitoring system that is acceptable to the DOR on the taxpayer. This is a more difficult undertaking than it appears, largely because the industry-standard level of security requires access to the operating system of the taxpayer's ECR/POS system. A considerable degree of detail is needed to assure a tax authority that ECR/POS data is unaltered. The example below illustrates

[66] The North Carolina case is discussed in Ainsworth, "Sales Suppression," *supra* note 18, at 351-352. In it is fraud identical to that described by ECR/POS salesmen to the New York undercover investigators.

[67] Ainsworth and Urs Hengartner, "Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud With Technology," 57 *Can. Tax J.* 715 (2009).

[68] Eugene Kwibuka, "RRA: Use of EBM Will Soon Be Mandatory for Every Business," *The New Times,* Oct. 10, 2016.

[69] Revenu Québec release, "Tax Evasion in the Restaurant Industry: Revenu Québec Gives a Positive Assessment of the First Year of Implementation of MEV in the Food Sector" (Feb. 14, 2013).

[70] David Deputy and Goran Todorov, "Securing the Fisc via Digitization," FTA Technology Conference, Indianapolis (Aug. 2, 2017).

this complexity along with examples of the aggregate data reports that the third-party security system would need to prepare for the tax administration.

4. Transactional Example

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

1. A customer purchases a $1 hamburger. The sales tax rate in the jurisdiction is 10 percent.

2. The order is placed and the POS system captures the order. The third-party security system also captures and preserves this data.

3. As the hamburger is prepared, the customer offers $2 cash.

4. The cashier presses the cash button to complete the sale and takes $2. During this time:

   a. the POS system captures this data, marking it as a cash transaction;

   b. the third-party security system also captures and preserves this data and immediately notifies the tax authority about the transaction;

   c. the tax authority receives, retains, and records this data, and notifies the third-party security system that it has done so; and

   d. the third-party security system receives notification from the POS system that it has captured this data.

5. The data is now with the tax authority, the POS system, and the third-party security provider.

6. The third-party security system can store and encrypt what was ordered; the tax due; the aggregate cash payment; the date, time, and table number for the transaction; the check number; and the server's name or ID number.

7. Simultaneous with full encryption of the data, a verification response is generated of the encrypted files and placed on the bottom of the receipt in the form of a bar code.

8. Anyone can use the verification response (bar code) on the bottom of the receipt to immediately confirm that the receipt is valid, the data is complete and stored in the POS, and the data is complete and stored in the third-party security system's files.

5. Reports Prepared

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

- total sales by day, per month, indicating the quantity sold per item and the amounts charged;
- total discounts provided by day, per month, indicating both the quantity and the amounts provided per item;
- net sales by day, per month;
- total sales tax by day, per month;
- total amounts tendered by day, per month, divided by category of cash, credit, debit card, or other;
- total number of void transactions, no-sale transactions, and cash drawer openings by day, per month;
- total time the cash drawer is open, by day, per month, subdivided by duration in single incidents;
- total guest checks issued by day, per month, itemized by quantity purchased per check and average amounts purchased per check by day, per month; and
- total guest count per check, by day, per month, arranged in time sequence.

6. Third-Party Security

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.

In 2015 the POS market was a $13.31 billion, highly competitive industry focused on potential efficiencies in the cloud, but also concerned about security. One market researcher noted that "one of the key factors contributing to the market growth is the increased adoption of credit and debit

cards."[71] However, the firm said that "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." Finally, the firm said that cloud-based POS solutions would likely continue to grow because they "have various advantages over traditional solutions such as access to a service on demand, lower CapEx, reducing internal IT infrastructure, and others."[72]

We contacted the leading POS manufacturers used in the Washington restaurant and hospitality sector,[73] and major POS manufacturers overall.[74] They uniformly rejected the idea of cooperation with a third-party security provider without a government mandate. We asked for integration permission from either of the two major third-party security providers we located, one from Canada and the other from the EU.

The primary reason the POS vendors rejected cooperation was that they wanted to protect the security and integrity of their platforms. 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 its 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.

Second was that each POS provider had developed unique software that would need to be shared at some level with the third-party security firms. This was characterized as a commercial partnership proposal, which again did not make sense given the small market potential.

Third was that many of those companies offered their own cloud-based solutions that 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 the cloud as a solution. This response illustrates a fundamental disconnect. Many manufacturers leave a limited back door open in their POS systems for suppression of outbound data. They do this to allow their sales representatives and distributors room to respond favorably to the buyers' suppression demands. However, they work hard to close off outside access to their systems (inbound data) that could allow in malware or viruses. Their 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.

We were part of the litigation that reached the first agreement with the DOR for acceptable third-party monitoring under Wash. Rev. Code section 82.32.290(4)(b)(iii). Under the agreement, a recognized third-party electronic monitoring system has been integrated with an autonomous POS system. Whether such a solution is scalable is unknown. Numerous interested parties came together in this instance, but the solution would have been much easier if there was a state mandate that POS systems offered for sale in the state allow third-party security.

IV. Risks and Remedies in Washington

The Washington statute creates problems that can be roughly cataloged 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 identify problems and suggest regulatory remedies and opportunities to improve the state's response to ESS.

A. Excessive Estimates

One of the greatest enforcement difficulties with ESS fraud 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 unlikely that the tax administration would have access to them. Those books would not be made by a zapper, the function of which is

[71] Grand View Research, "Point of Sale (POS) Software Market Analysis, Market Size, Application Analysis, Regional Outlook, Competitive Strategies and Forecasts, 2016 to 2024" (report summary), Report ID 152 (undated).

[72] *Id.*

[73] *PC Magazine* ranks the top seven POS systems in the restaurant and hospitality industry as Square chip card reader, Aldelo POS Pro, PAR Brink POS, Posera Maitre'D POS, Revention POS, Action Systems Restaurant Manager, and Menusoft Systems Digital Dining. Evan Schuman, "The Best Point-of-Sale (POS) Systems of 2017," *PC Magazine*, July 19, 2017.

[74] See Webnexs POS, "15 Best POS Software Systems for Small Business," FinancesOnline (undated) for a list of the top 15 POS systems.

to delete data so completely that it leaves no trace of the data or the program that was used to delete it. The dark cloud and SSaaS can offer a second set of books, held offshore, as a service.

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 is on solid ground, and neither is likely to completely prove its sales figures. ESS penalties give the government leverage.

Zapper and phantom-ware cases, like all sales suppression cases, even those not based in technology, quickly dissolve into a battle of the estimates. For example, when there are no reliable sales figures, estimates are drawn from the ratio of cash to credit sales compared with industry and local averages. For restaurants, sales per square foot, per customer, per seat, or per table can be compared with the Restaurant Industry Operations Report of the National Restaurant Association or the IRS Market Segment Specialization Program's report for the Bars and Restaurants Audit Techniques Guide. The same reports can be used for a cost-of-goods-sold analysis.

All of these estimation approaches are imprecise, however, and this can create considerable anxiety for taxpayers and government auditors. However, under Washington statute, the presence of an ESS device strengthens the government's hand. The assessment is criminal, not merely civil. This results in larger tax loss estimates.

B. Disproportionate Penalties

Washington's ESS fraud penalties are disproportionate to its tax losses. If two individuals both suppress $100,000 in taxable sales, one using old-fashioned double tills and the other using technology, the second is punished far more severely. Why? The tax loss is the same, the type of fraud is the same, and the audits and related disputes will be similar. Only the method of accomplishing the fraud differs. Washington is punishing technology, not tax fraud. It needs to work with technology, not fight it.

Because of difficulties that inevitably flow from a sales suppression fact pattern, the state appears to be overreacting with its ESS penalties. Washington penalizes any person who knowingly possesses sales suppression software, even if it can be shown that the software has not been used and was not intended to be used. Instead of indexing ESS penalties to tax losses, Washington presumes tax losses and applies a set of uniform penalties regardless of the tax impact. The penalties are:

- five years' confinement in a state correctional institution and/or $10,000 fine;[75]
- seizure and forfeiture of ESS devices as well as any devices that used the ESS, or property that is traceable to ESS, including the business's ECR and POS systems;[76] and
- conditional loss of business permits unless taxes, penalties, fines, and interest are paid and a five-year electronic monitoring agreement is entered into with the DOR.[77]

The interlocking nature of those penalties make them particularly painful, can put an individual in a difficult position personally, and could easily cripple a business. This is especially true in situations in which the owner may be unaware that phantom-ware or zappers have been installed either because they were already on second-hand equipment or they were installed by a rogue employee. Those penalties seem better designed to leverage the government's position in an ESS estimate battle than to resolve the problem of data recovery from an ESS application. This seems to be what Washington did in its first four Profitek zapper cases.[78] As of February 2, 2017, in those cases, the assessed state tax was $73,324, $132,000, $80,000, and $149,811, respectively. The corresponding payments were $74,045, $511,832, $55,305, and $105,647.[79]

There is no explanation for the occasionally wide variance between assessed tax and paid tax, but one suspects the interplay between the traditional estimate battle and the potential punishments are used as negotiation leverage.

[75] Wash. Rev. Code section 9a.20.021(1)(c).

[76] Wash. Rev. Code section 82.32.670(1)(a).

[77] Wash. Rev. Code section 82.32.290(2)(a)(i).

[78] *See Yin*, Docket No. 2:16-cr-00314-RAJ.

[79] *Yin*, Government's Opposition to Defense Motion to Continue Sentencing for a Second Time, Attachment 2, Docket No. 2:16-cr-00314-RAJ (Apr. 11, 2017).

Evidence that the state negotiated away its penalty leverage to secure the assessed taxes is apparent in a critical enforcement omission. None of the Profitek zapper users was required to enter into a five-year written electronic monitoring agreement.[80] One suspects that a taxpayer in an ESS estimate battle that insists on its estimate and its total sales number will bear the full brunt of the state's penalty provisions.

C. Problem of False Positives

The nature of ESS fraud encourages tax authorities to act quickly. Tax administrations initiate massive sweeps, auditing all the businesses found on the customer lists of ECR/POS system installers, whenever those systems are found to be vulnerable to ESS fraud. The assumption is that if the POS installer sells zappers, or if the system he installs comes with embedded phantom-ware, then businesses with those POS systems are also likely to be using this technology.

Wash. Rev. Code section 82.32.290(4)(a) has a threshold lower than tax fraud. It does not require successful use of ESS technology. To knowingly possess an ESS device is sufficient for a class C felony, and seizure of ECR/POS systems is possible even without a warrant. Section 82.32.290(4)(a), therefore, invites aggressive action by auditors when proof of possession seems assured at the start of an audit and proof of use is not required. Mistakes would seem easy and there are no statutory exceptions. Whether possession is knowingly undertaken would seem to be the auditor's judgment call.

Washington's response to zappers can be illustrated by the case of John Yin — InfoSpec's Profitek salesman. He was the sole source for the Profitek zapper in the state for nearly a decade. Washington secured a search warrant for Yin's customer lists in July 2015 and he pleaded guilty 17 months later. Yin's plea was entered a mere three days after the information against him was filed in Seattle's federal district court.

By the time of Yin's sentencing, Washington had audited nine restaurants where he sold zappers. Bearing in mind that Washington had never found a zapper or a phantom-ware application before it accessed Yin's customer lists, the assessments are staggering — over $3.4 million in aggregate omitted sales taxes.[81] The U.S. attorney noted that when this figure was determined events were moving so quickly that "not all of the restaurants are aware of the audit results."[82] That's a fast-moving audit sweep!

The Profitek ESS system uses a zapper, which 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 by the buyer. The same is not true of phantom-ware applications that come preinstalled in a POS system. However, the Washington statute treats all ESS devices the same. What would have happened if Profitek was phantom-ware?

The essence of the Dudok case was the unknown possession of a phantom-ware program. There was no knowledge of the program's existence until Dudok's owner received a tutorial from the managing director of Straight Systems. This tutorial would be sufficient to secure a felony conviction under the Washington statute. However, the Netherlands requires proof that an ESS device is used to avoid a tax.

Nevertheless, once the Dutch authorities became aware that phantom-ware was embedded in the Finishing Touch POS system, they targeted every known purchaser of the system in the country. Visits were scheduled and audits were undertaken. There is no public tally of the amounts collected from the Dutch sweep of all known Finishing Touch POS systems, but Straight Systems was assessed a €100,000 fine and quickly left the POS market.[83]

D. Voluntarily Negotiated Agreements

ESS fraud rates in the United States are probably comparable to the rest of the world. This means that somewhere between 34 and 70 percent of the businesses in Washington either:

[80] Wash. Rev. Code section 82.32.290(4)(b)(iii).

[81] At an average 9 percent sales tax rate, this represents over $38 million in suppressed sales.

[82] *Yin*, Government's Sentencing Recommendation, at 9 n. 3, No. 2:16-cr-00314-RAJ, Apr. 14, 2017.

[83] *See* LJN: AX6802 (in Dutch, translation on file with author).

- use zappers, phantom-ware, SSaaS, or the dark cloud to suppress sales; or
- have ECR/POS systems that have a dormant version of ESS technology or are designed to accept later installation of ESS technology, even though they are not actively suppressing sales.

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 should encourage broad adoption of the solution, not using the solution as a cudgel to beat taxpayers into submission or threaten them with loss of their businesses if they do not comply. The only businesses allowed to participate in Washington's electronic monitoring system are felons. This does not seem right — all should be welcome into the monitoring system.

An information campaign on the ESS problem would be a good start. Monitoring agreements should be an easy sell to the public if it is explained that despite their paying a sufficient amount in taxes, rates will need to go up because businesses continue to siphon off the state's revenue. The normal response to this campaign by businesses that knowingly possess ESS technology would be to seek shelter. Shelter in the form of electronic monitoring should be widely available.

A halfway measure would provide taxpayers a way to clean their ECR/POS systems, and then certify that the system is not ESS-capable. This could be a registration and inspection program, like automobile inspections, and could be made part of the business licensing process. The difficulty with a program like this (as was adopted by Greece[84]) is that the state would need to acquire and maintain expertise on all the technology used in ECR/POS systems.

A preferable approach would be to adopt the Rwandan solution of the EBM. A business would purchase an EBM, which could easily cost less than $100. The business would then take the EBM with a sales data recorder, if one was not already embedded in the EBM, to any DOR branch office where it would be activated. The DOR officer would personalize the recorder, assign it to the taxpayer, and activate its keys for data encryption.

Under the EBM approach, the state would need to set up a small data center to receive the real-time data from all designated Washington businesses. It is common to start a program like this by market segment — restaurants being a common starting place. An artificial intelligence program — like that installed in Ceará, Brazil, by SmartCloud Inc. to perform VAT risk analysis — would be needed to analyze the data flows.[85]

E. Opportunity for Good-Faith Amnesty

Even with no changes in the statute and no effort to advertise the ESS problem to the public, there is a community of businesses — specifically restaurants — that might appreciate an amnesty program. An effective program would not only require that the business turn in its code, but also require enrollment in an electronic monitoring program.

The difficulty with amnesty in this area is that the individual coming forward is admitting to knowingly possessing an ESS device — a class C felony. Because Washington disconnects the tax fraud from the crime of possessing an ESS device, any discussion about the actual suppression is independent of the admission to the crime. As a result, only individuals who know there will be 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 phantom-ware, but who has never used it, will come forward. So too would the owner of a POS system that contains phantom-ware installed by an embezzling night manager.

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

[84] Ainsworth and Hengartner, *supra* note 67, at 715, 728-734 (providing a comparative assessment of fiscal tills in Greece, Quebec, and Germany).

[85] Michael W. Barnet, personal email communication (Sept. 14, 2016) (on file with author).

situation would only address 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.

V. Conclusion

The Washington statutes dealing with ESS, Wash. Rev. Code section 82.32.290(4) and section 82.32.670, operate with an exceedingly low threshold that criminalizes knowingly possessing "any automated sales suppression device or phantom-ware." Either the statute should be modified or regulations should be issued to clarify that the device or phantom-ware must be used to evade or avoid a tax. Knowingly possessing software is not tax fraud. Using software to evade or avoid a tax is.[86] Making this adjustment would increase the burden on auditors slightly because they would have to investigate the use of the software, but it would go a long way toward rationalizing and harmonizing tax enforcement around ESS. We regularly perform a software usage test in this context — it is not challenging.

Second, both statutes are far too limited and far too homogenized when explaining what they address. For example, those statutes appear to treat zappers and phantom-ware almost as synonymous, even though one involves placing suppression code on removable tangible property such as 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 easy for someone to unknowingly possess phantom-ware, whereas unknowingly possessing a zapper is unlikely. As a result, the Washington statute criminalizes many business owners who have older ECR/POS systems, because those systems commonly contained phantom-ware even though they may never have been used for suppression purposes.

Regulations need to provide a safe harbor for those business owners with a way they can cleanse their systems of offending programs without risking criminal sanctions. The general topic of ESS regulations is another area of concern — after four years on the books there is not a single regulation applying either of those statutes even though the ambiguities and questions about them are abundant.

Third, although Wash. Rev. Code section 82.32.290(4) (unlawful acts — penalties) and section 82.32.670 (seizure and forfeiture) purport to cover all ESSs, they deal with only two of the ESS permutations — zappers and phantom-ware. 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 interface with the business owner as services, but with an intensely technology-dependent structure. What is important for this discussion is that nothing — code, device, or other programming function — is possessed by the business owner. They are not devices.

Neither SSaaS nor the dark cloud permutations of ESS is covered by the Washington statutes. To capture them a phrase like "or other method of electronically suppressing sales" is needed. This problem is not unique to Washington. Many states and some foreign jurisdictions have language identical to Washington's. The few that do have a catchall phrase have focused it on other kinds of devices that can be possessed by the taxpayer and that will suppress sales.[87] Those ESS statutes do not include SSaaS performed by third-party technology and devices that are possessed by the third-party service provider but not the business

[86] *See* Cal. Rev. & Tax. Code section 55363.5(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.

Pennsylvania's statute uses the same language and Utah's is similar. Pa. Stat. 72 P.S. section 7268 and Utah Code Ann. section 76-6-1303(1). Kentucky criminalizes knowingly possessing "any device or software program that falsifies the business records created by a point-of-sale system." Ky. Rev. Stat. section 517.130(1).

[87] Most of the states with similar statutes also omit SSaaS and the dark cloud. Mich. Comp. Law Ann. section 750.411w(1) states: "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." See also Minn. Stat. Ann. section 289A.63, Subd. 12(a), which states: "A person who sells, purchases, installs, transfers, develops, manufactures, or uses an automated sales suppression device, zapper, or similar device knowing that the device is capable of being used to commit tax fraud or suppress sales is guilty of a felony."

owner. Generally, the statute fails to account for the speed at which technology changes and fraud methods mutate and migrate.

Fourth, and most importantly, the Washington statute is a hard-nosed enforcement statute that sees ESS as an aberration and a problem that needs to be confronted criminally. It does not see it as a long-established, deeply embedded — though highly improper — way of doing business that needs to be changed. The tax policy case here needs to be made clearly, honestly, and publicly. If even the lowest estimate of the ESS prevalence is applicable to Washington (the 34 percent of businesses estimate from Canada), then Washington has a systemic suppression problem. However, Washington has never commissioned an ESS study and no academic has volunteered to provide one as a civic service, so we are all operating blind.

Tax policy needs to facilitate a change, not freeze the problem in place. Harsh enforcement efforts sometimes make permanent what they hope to root out. They do this with traps (consider the unknowing possessor of phantom-ware) and limits on honest efforts to come clean. But more fundamentally, bad tax policy is one that identifies a problem, recognizes but does not adopt the solution, and instead chooses to punish violators severely with an unreasonably harsh mandate to adopt the 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 and is the proven way to stop ESS. This is what Washington has not adopted, although taxpayers may, as they are apprehended one by one for criminal violations, propose the international standard as part of a five-year monitoring agreement. This is simply not the way to conduct tax enforcement.

Technology must be used to stop technology-based suppression fraud. If Washington is unwilling or unable 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 have only those convicted of a class C felony allowed to enter into DOR monitoring agreement. 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 in a specific economic sector, join a real-time electronic monitoring program. ■