SALES SUPPRESSION: THE INTERNATIONAL DIMENSION

Boston University School of Law
Law & Economics Paper No. 16-39

65 AM. U. L. REV. 1241 (2016)

Richard T. Ainsworth
Boston University School of Law

SALES SUPPRESSION: THE INTERNATIONAL DIMENSION

RICHARD T. AINSWORTH[*]

TABLE OF CONTENTS

INTRODUCTION

Sales transaction taxes are highly susceptible to technology fraud,[1] which is an inevitable result of today's widespread reliance on

[*] Richard T. Ainsworth is the Director of the Graduate Tax Program at the Boston University School of Law, and an Adjunct Professor at the Graduate Tax Program, NYU School of Law.

[1] *See* John Crudele, *Finally! NY Tax Cops Wise Up, Start Busting Sales Tax "Zappers"*, N.Y. POST (June 8, 2015, 9:55 PM), http://nypost.com/2015/06/08/after-years-of-warning-state-finally-notices-sales-tax-zappers (theorizing that transaction tax fraud may have cost the state of New York "billions in lost sales tax"). In 2009, the New York state tax collector conducted a sting operation that targeted companies that manufacture the point of sale (POS) devices containing sales-suppression software (also called zappers) that facilitate the transaction fraud. *Id.* The state tax collector found that of the twenty-six companies that manufacture such devices, twenty-five of them offered to help those conducting the sting operation evade taxes. *Id.*

technology to document taxed transactions.[2] Technology can be (and is) manipulated to defeat the collection of these taxes.[3] Both the U.S. retail sales tax (RST) and the European value added tax (VAT) are vulnerable to technology-based fraud.[4] This Article concerns sales suppression—intentionally not recording sales—in the RST, and at the final stage of the VAT, the retail stage, when tax is collected from final consumers.

The modern electronic cash register (ECR)/point of sale (POS) system is vulnerable to fraud.[5] These devices are essentially computers with programming that is molded to meet the commercial needs of any particular business.[6] Although these devices are functionally similar across all retail establishments, the data engines on which they operate are not.[7] In the United States, the dominant

[2] *See* Steven Aldrich, *Point-of-Sale System Basics for Retailers*, ENTREPRENEUR, http://www.entrepreneur.com/article/77960 (explaining that computerized POS systems have "grown in popularity over conventional cash registers" because they not only ring up sales, but also "amass vital, real-time information about" a business's customers and inventory).

[3] *See, e.g.*, United States v. Leonard, 37 F.3d 32, 35 (2d Cir. 1994) (involving defendants who utilized a computer program to alter a store's sales data, allowing them to successfully skim over $17.1 million over a ten-year period). "Skimming" is a method for concealing revenue. *See* Richard Thompson Ainsworth, *Automated Sales Suppression (Zappers): A Real Threat to Pennsylvania's Sales and Use Tax*, 8 PITT. TAX REV. 29, 33 (2010) (explaining the "simplest (nontechnological) form" of skimming involves diverting cash from sales into a secret drawer).

[4] *See* Ainsworth, *supra* note 3, at 38 (discussing how a man named Talal Chahine and his wife, Elfat El Aouar, were able to electronically skim more than $20 million from their Detroit restaurant chain over a four year period).

[5] *See* Chris Poulin, *What Retailers Need to Learn from the Target Breach to Protect Against Similar Attacks*, SECURITY INTELLIGENCE (updated Feb. 20, 2014), https://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers (recounting that hackers stole "the personal and financial information of approximately 110 million people" from Target and that it is likely that the attackers compromised the store's POS systems to gain access to this private data).

[6] *See* WES WHITTEKER, SANS INST., POINT OF SALE (POS) SYSTEMS AND SECURITY 3 (Oct. 2014), https://www.sans.org/reading-room/whitepapers/bestprac/point-sale-pos-systems-security-35357 (explaining that POS technology has existed since the late 1900's with the advent of the first mechanical cash register in 1879). In the late 1980's, POS technology was drastically overhauled with the advent of modern day personal computer technology. *Id.* An example of a current POS device "would be the check-out counter at a retail or grocery store." *Id.*

[7] *See DB-Engines Ranking*, DB-ENGINES, http://db-engines.com/en/ranking (last visited May 17, 2016) (ranking some 264 different database management systems or database engines that help run POS technology).

databases are MS SQL Server, MS Access, and MySQL;[8] the first two are Microsoft products and the last is an Oracle product.[9] Unsurprisingly, the popularity of Microsoft ("MS") Windows made Microsoft the "go-to" database provider for developers seeking easy installations.[10] Recently, and most notably in Europe, open source[11] POS systems based on Linux, a competing operating system, are becoming more common than Microsoft databases.[12] Furthermore, MS databases are not found in the new Apple iOS POS systems or Square Register, which uses an open source PostgreSQL database.[13] This Article will focus on a particular POS system called Profitek,

[8] *See id.* (ranking POS data engines by popularity, with MySQL ranked second, Microsoft SQL Server ranked third, and Microsoft Access ranked seventh out of a total of 264 engines); *see also DB-Engines Ranking-Trend Popularity*, DB-ENGINES, http://db-engines.com/en/ranking_trend (last visited May 17, 2016) (calculating MySQL, Microsoft SQL Server, and Microsoft Access as some of the most popular database engines over time).

[9] *MySQL Editions*, MYSQL, http://www.mysql.com/products (last visited May 17, 2016); *SQL Server 2014 & the Data Platform*, MICROSOFT, https://www.microsoft.com/en-us/server-cloud/products/sql-server (last visited May 17, 2016); *Access*, MICROSOFT, https://products.office.com/en-us/access?legRedir=true&CorrelationId=0da4117d-7af0-49f0-b001-2918c366e7d1 (last visited May 17, 2016).

[10] *See* Roy Furchgott, *With Software, Till Tampering Is Hard to Find*, N.Y. TIMES (Aug. 29, 2008), http://www.nytimes.com/2008/08/30/technology/30zapper.html (finding that eighty-five percent of all POS systems run on Microsoft ("MS") Windows systems).

[11] Open source refers to computer software with its source code made available (with a license) in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose. Thus, the Apple systems are closed, and the Linux systems are open, and can be more easily updated or enhanced. *What Is Linux?*, LINUX.COM, https://www.linux.com/what-is-linux (last visited May 17, 2016).

[12] *See* Seamus Quinn, *Europeans Like it Bigger, Newer and with More Linux*, POWERWIRE (Mar. 19. 2015), http://powerwire.eu/europeans-like-it-bigger-newer-and-with-more-linux (indicating that an IBM i (IBM's operating system) marketplace survey revealed that Europe uses Linux more than North America does). The survey's results showed that "56.6% of European Power i users [were] . . . running Linux" compared to only 42.7% of users in the United States. *Id.*

[13] *See Compare iPad POS Software*, SOFTWARE ADVICE, http://www.softwareadvice.com/retail/ipad-pos-comparison/?more=true#more (last visited May 17, 2016) (comparing 124 software systems that can be run on Apple's POS system, and not listing any MS databases); *see also* Steve Olenski, *Are iPad POS Systems the Future for Retailers?*, FORBES (Sept. 26 2013, 1:37 PM), http://www.forbes.com/sites/steveolenski/2013/09/26/are-ipad-pos-systems-the-future-for-retailers/#42e73af42115 (describing how retailers and restaurants are moving towards Apple POS systems using the iPad instead of cash registers); *Serious about Security*, SQUARE SECURITY, https://squareup.com/security (last visited May 17, 2016) (indicating that Square uses its own POS software).

manufactured in Vancouver by InfoSpec, which uses an MS SQL server, and can be purchased with a dedicated sales suppression device—the Profitek Zapper.[14]

The cash register/POS market divides along database lines[15] and the market further subdivides when attributes such as operator language preferences are considered.[16] For example, Chinese restaurants with predominantly Chinese employees will prefer a POS system with Chinese language functionality, but a French restaurant with French-speaking employees would prefer a different system with a French language functionality.[17]

As a result, the market for POS systems is both niche and international, and so are sales suppression software applications.[18] It is common, therefore, to find that the same person who sells an ECR/POS system is also able to provide the business with the zapper that can suppress sales recorded in that specific system.[19] Zappers are not universal, but rather are system-specific.[20] Zappers and ECR/POS systems travel together, and, in some instances, the zapper's elegance

[14] *See* Ian Mulgrew, *Richmond Company that Sold Software to Help Restaurants Avoid Taxes Acquitted*, VANCOUVER SUN (July 16, 2013), www.vancouversun.com/technology/mulgrew+richmond+company+that+sold+software+help+restaurants+avoid+taxes+acquitted/8673669/story.html (reporting outcome of case in which InfoSpec was charged with fraud for selling Zapper software for its POS systems).

[15] *See* Furchgott, *supra* note 10 (noting that consulting firm Frost & Sullivan calculated that eight-five percent of POS systems run on Windows).

[16] *See Chinese Restaurant POS System*, POS NATION, https://posnation.com/chinese-sushi-pos-system (last visited May 17, 2016) (explaining that POS Nation's POS system has a second language feature that allowed receipts to be printed in either English or Chinese because such a feature is "essential for Chinese speaking chefs and staff").

[17] *See id.*; *see also EPOS Multi-Lingual, English, French & Spanish in One Software*, EPOS SOFTWARE & SYS. BLOG, http://possystemblog.com/epos-multi-lingual-english-french-spanish-one-software (last visited May 17, 2016) (explaining that the PosBill POS system offers multiple language preferences).

[18] *See* Furchgott, *supra* note 10 (indicating that fraudsters have used automated sales suppression devices, or zappers, all around the world, specifically in Germany, Sweden, Brazil, Australia, France, Canada, the United States, and the Netherlands).

[19] *See id.*

[20] *See* Ainsworth, *supra* note 3, at 33 (noting that zappers are cash skimming software applications; further explaining that zappers are programming options added to POS networks and are "carried on memory sticks, removable CDs or . . . accessed through an [I]nternet link," so, because they are not "integrated into operating systems," they are hard to detect). Throughout this Article, zappers are referenced as both a generic software and as the specific Profitek Zapper manufactured by InfoSpec.

and effectiveness may actually be the most compelling feature.[21] A high quality zapper responds to suppression requests by entering the ECR/POS database and deleting selective sales, as well as recalculating individual receipts and the taxes due.[22] It will re-order all sales slips and adjust the internal ledger, which informs the operator how much extra cash is in the till to withdraw so that bank deposits will match the adjusted sales totals.[23]

An application that effectively manipulates the digital records of a specific POS system will quickly travel to other countries and states with the associated POS system for which it was designed.[24] Therefore, zappers initially developed on short notice for use in one jurisdiction can quickly become a concern for a neighboring tax authority. Such is the case with the Profitek POS system, sold and created by InfoSpec Systems Inc., and the zapper manufactured by the same company to defeat its own recordkeeping functionality.[25]

This Article follows the InfoSpec/Profitek system and its associated zapper as it migrated from the Canadian restaurant market into the U.S. market. It describes the time-gap between the beginning of the audit cycle involved in the InfoSpec/Profitek litigation in Canada—

[21] *See* Richard T. Ainsworth, *Zappers and Phantomware: The Need for Fraud Prevention Technology*, 50 TAX NOTES INT'L 1017, 1018 (2008). Zappers and phantomware are software that can either be factory installed or added on to ECR and POS systems post-sale. *Id.* While zappers "have no legitimate purpose other than to facilitate cash skimming at the point of sale," phantomware can be used for legitimate purposes—although these purposes remain somewhat obscure. *Id.* Phantomware are not disclosed in user manuals; therefore, they are difficult to detect even during an audit. *Id.* Moreover, a fraudster can use phantomware to engage in skimming with the proper training. *Id.* Zappers are also difficult to detect because they are usually contained on an external device that the fraudster connects to the POS system; however, they can be detected if not used carefully. *Id.*

[22] *Id.*

[23] *Id.*

[24] *See* Furchgott, *supra* note 10 (clarifying that zappers were found to have been used all across the world from Germany to the United States).

[25] *See About Profitek*, PROFITEK, http://www.profitek.com/About (last visited May 17, 2016) (explaining that Profitek specializes in POS software for the hospitality and retail industry); *InfoSpec Systems Inc.: About Company*, FIBRE2FASHION.COM, http://softwaresolutions.fibre2fashion.com/company/infospec (last visited May 17, 2016) (stating that InfoSpec Systems is the developer of Profitek and Profitek's POS systems); *Selling Tax-Evasion Software Is Legal, B.C. Court of Appeal Rules*, THE GLOBE & MAIL (last updated July 18, 2013, 11:14 AM), http://www.theglobeandmail.com/technology/tech-news/not-fraud-to-sell-tax-evasion-software-bc-court-of-appeal-rules/article13295953 (discussing that InfoSpec Systems manufactured a zapper for use on their own POS system).

October 4, 2000[26]—and the beginning of the first two U.S. investigations involving the same company and the same zapper—in 2014 and 2015. The Federal Bureau of Investigation (FBI) is conducting an investigation in Chicago (public documents began to appear October 21, 2014), and the Washington State Attorney General is conducting another investigation (public documents began to appear July 13, 2015).[27] If the InfoSpec/Profitek system and its associated zapper crossed the U.S./Canadian border during the Canadian litigation, it would mean that this fraud was present and remained undetected in the United States for approximately fifteen years. This is a long time for fraud to remain hidden in the U.S. market.

This Article suggests that once a zapper and a vulnerable POS system are identified by one tax authority, there is considerable value in sharing this information with other tax administrations. There is no point in reinventing the wheel. This kind of tax enforcement and information sharing is commonplace among tax administrations. For example, when the IRS became serious about combatting refund fraud, it rolled out a technology-intensive pilot program to test the capability of W-2 Verification Codes on filed W-2s.[28] The authenticity of the Form W-2 data included with the Form 1040 was examined with technology during the 2016 filing season.[29] This approach to verifying the tax reporting of critical wage data had long been championed in the VAT, but in the context of invoice verification.[30] Thus, the U.S. pilot is a similar income tax application of a previously successful VAT enforcement effort. Similar sharing of information

[26] *See Selling Tax-Evasion Software Is Legal, B.C. Court of Appeal Rules*, *supra* note 25 ("The case dates back to an eight-year period between Oct. 4, 2000 and Aug. 28, 2008.").

[27] *See* Affidavit for Search Warrant at 3, State v. Yin, No. 15-1-12052-9 (Sup. Ct. King Co. Wash. July 13, 2015) (indicating the likelihood that the defendant sold a Profitek POS system and zapper to a Washington restaurant owner); *see also* Amy Clancy, *Bellevue Restaurant Owner Charged in Tax Fraud Case*, *KIRO-TV* (Feb. 6, 2016, 9:51 AM), http://www.kiro7.com/news/kiro-news-app/restaurants-cheating-washington-taxpayers-out-of-millions/61479512 (discussing the tax fraud case against a restaurant owner, Wong, and her use of a zapper to hide taxable income (here, retail sales tax) by essentially erasing it from her transaction log to avoid paying state sales tax in the state of Washington).

[28] *IRS Tests W-2 Verification Code for Filing Season 2016*, IRS, https://www.irs.gov/Individuals/IRS-Tests-W-2-Verification-Code (last visited May 17, 2016).

[29] *Id.*; *IRS Starts Anti-Fraud Program Using Codes Input by Payroll Processors to Verify W-2s*, BNA, http://www.bna.com/IRS-starts-anti-fraud-program-n57982059210 (last visited May 17, 2016).

[30] Richard T. Ainsworth, *Real-Time Solution to Refund Fraud: VAT Lessons from Belgium, Brazil, and Quebec*, 66 TAX NOTES INT'L 533, 534 (2012).

will surely help enforcement efforts when a zapper is identified in a commonly used POS system.

I. THE CANADIAN FRAUD CASES

Canadian tax authorities brought cases against InfoSpec Systems, the company that made the Profitek Zapper, the salesman who sold them, and the restaurants that used them, including the Foody Goody Chinese Buffet Restaurant and the Buffet Square in Winnipeg, Manitoba.[31]

A. Salesmen

The prosecution and subsequent conviction of David Au, an Infospec salesman, illustrates the Canadian enforcement effort aimed at curbing the use of zappers to avoid paying sales tax.

Mr. Au pled guilty on December 16, 2010, to defrauding the public by selling zappers to restaurant owners.[32] "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" that were due to provincial and federal governments.[33] Mr. Au's sales territory was the Lower Mainland and elsewhere in British Columbia.[34] On average, Mr. Au sold eight zappers each year over an eight-year span.[35]

At the time of his sentencing, fourteen of the twenty-three restaurants to which he had sold zappers had been fully audited.[36] 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).[37] Mr. Au not

[31] *See* Nelson Bennet, *Richmond Company Fined $100K for Tax Evasion Software*, BUS. VANCOUVER (July 24, 2012, 11:00 PM), https://www.biv.com/article/2012/7/richmond-company-fined-100k-for-tax-evasion-softwa (reporting on the outcomes of cases against InfoSpec and David Au); Alexandra Paul, *Tax Software's Maker not Guilty; Eateries Are*, WINNIPEG FREE PRESS (July 19, 2013 1:00 AM), http://www.winnipegfreepress.com/business/tax-softwares-maker-not-guilty-eateries-are-216117151.html (stating that the owners of Foody Goody and Buffet Square pled guilty to tax evasion in 2007–2009 and 2006–2008, and providing background information about the court case).

[32] R v. Au, 2011 B.C.S.C. 75 ¶ 1 (Can.).

[33] *Id.* ¶ 4.

[34] *Id.* ¶ 3.

[35] *Id.* ¶ 11.

[36] *Id.* ¶ 27.

[37] *Id.*

only sold the Profitek Zapper, but he also provided the purchaser with troubleshooting, technical support, and servicing related to the zapper, as opposed to Profitek's customer support.[38] After his customers purchased the Profitek POS, Mr. Au would offer the zapper on a CD for an additional $1500, $400 of which represented his commission.[39] Customers commonly paid for the zapper in cash and allegedly did not receive a receipt.[40] The court sentenced Mr. Au to thirty months in jail.[41]

B. Restaurants

The Profitek Zapper traveled so well in Canada that on May 1, 2013, the Canadian Revenue Authority (CRA) announced that it had found the Profitek Zappers in two Winnipeg, Manitoba restaurants, 1438 miles east of Vancouver.[42] Both establishments were Chinese—the Foody Goody Chinese Buffet and the Buffet Square.[43]

Aggregate overdue taxes and fines, amounting to $731,986 were imposed after the owners entered guilty pleas.[44] A portion of the fine was specifically imposed because the restaurants "possess[ed] software [that was] designed to suppress electronic sales transactions."[45] These zapper-specific fines were authorized under the relevant Manitoba statute.[46] At the time there was no comparable

[38] *Id.* ¶ 5.

[39] *Id.* ¶ 11.

[40] R v. InfoSpec Sys. Inc., 2013 B.C.C.A. 333, ¶ 14 (Can.).

[41] R v. Au, 2011 B.C.S.C. 75 ¶ 33.

[42] *See* Paul, *supra* note 31 ("The case with the two very different outcomes played out in two courtrooms thousands of kilometers apart in different jurisdictions."); Winnipeg, Manitoba is 2314 kilometers (1438 miles) from Vancouver, British Columbia. DISTANCE CANADA, http://www.distancecanada.com (select "Manitoba (MB)" under the "Select from State" tab, then select "Winnipeg" from the "Select City" tab; then select "British Columbia (BC)" from the "Select to State" tab; finally, select "Vancouver" from the "Select City" tab).

[43] *See Buffet Square*, YELP, http://www.yelp.com/biz/buffet-square-winnipeg (last visited May 17, 2016); *Foody Goody Chinese Buffet Restaurant*, FACEBOOK, https://www.facebook.com/pages/Foody-Goody-Chinese-Buffet-Restaurant/132782873412925 (last visited May 17, 2016).

[44] *Winnipeg Restauranteurs Taste Tax Evasion Fines*, KNOWLEDGE BUREAU (May 13, 2013), http://www.knowledgebureau.com/index.php/news/article/winnipeg-restauranteurs-taste-tax-evasion-fines; *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/2013/05/01/foody-goody-and-buffet-square-plead-guilty-to-numerous-charges-of-tax-evasion.html.

[45] *Winnipeg Restauranteurs Taste Tax Evasion Fines*, *supra* note 44.

[46] *Id.* The Manitoba Tax Administration and Miscellaneous Taxes Act, R.S.M. 1987, c. R.150, § 18.1 (2016), provides:

anti-zapper law in place at the Canadian federal level.[47] Zapper-fines in each case equaled 100% of the restaurant owners' unreported Manitoba sales tax, plus $500.[48]

C. Manufacturer

The CRA also pursued InfoSpec, a Vancouver company that manufactured the Profitek POS system and zapper and hired the salesmen to sell the two as a bundle.[49] InfoSpec did not confine its distribution of its sales suppression technology to British Columbia.[50] InfoSpec customizes the Profitek POS system based on each customer's needs.[51] Right out of the box, the Profitek system permits customers to void transactions, but does not allow them to permanently delete the transactions from the system.[52]

The Profitek Zapper is also customized so that it works with the customer's specific Profitek system.[53] Once installed, the zapper allows a user to completely delete selected sales transactions from the

> No person shall possess, use, sell or offer to sell, update, upgrade or maintain software that is designed for, or is capable of,
>
> (a) suppressing the creation of electronic records of sale transactions that a taxpayer is required to keep under this Act; or
>
> (b) modifying, hiding, or deleting such records without keeping the original data and providing a ready means of access to them.

[47] In its March 21, 2013 budget announcement, the Canadian Federal Government proposed "new administrative monetary penalties and criminal offences under the *Excise Tax Act* (i.e., in respect of GST/HST) and the *Income Tax Act* to combat this type of tax evasion [evasion through sales manipulation software]." CAN. DEP'T OF FIN., JOBS, GROWTH, AND LONG-TERM PROSPERITY: ECONOMIC ACTION PLAN 2013, at 381 (2013), http://www.budget.gc.ca/2013/doc/plan/budget2013-eng.pdf. The proposals became effective January 1, 2014 and created new criminal offenses "[f]or the use, possession, acquisition, manufacture, development, sale, possession for sale, offer for sale or otherwise making available of [Electronic Suppression of Sales] software." *Id.* at 382.

[48] *See* R.S.M. 1987, c. R.150, § 76(2), (4)–(5) (2016) (setting the minimum fine for a first-time offender guilty of tax evasion at $500, and requiring an additional fine for the amount of tax sought to be evaded).

[49] *See* Matthew McClearn, *Clamping Down on High-Tech Tax Evaders*, CANADIAN BUS. (Oct. 18, 2013), http://www.canadianbusiness.com/economy/clamping-down-on-high-tech-tax-evaders (discussing the Canada Revenue Agency's (CRA) prosecution of InfoSpec).

[50] *See* Paul, *supra* note 31 (stating that InfoSpec sold its Profitek POS system and accompanying zapper to restaurants in Winnipeg).

[51] R v. InfoSpec Sys. Inc., 2013 B.C.C.A. 333, para. 6 (Can.).

[52] *Id.*

[53] *Id.* para. 7.

sales records.[54] As a result, the Profitek system, with a zapper, will produce records that under-report income and will eliminate records of sales taxes collected by the user.[55]

R v. InfoSpec Systems Inc.[56] is an appeal from InfoSpec's conviction in the Supreme Court of British Columbia for defrauding the public through its sales of the Profitek Zapper.[57] The appellate court determined that the sale of a zapper, standing alone, was not an act that reasonable people would consider dishonest.[58] As a result, there was neither fraud nor attempted fraud in this case.[59] The court stated:

> It is noteworthy that *the law does not prohibit the making, possession, or sale of a zapper.* As InfoSpec points out, the *Criminal Code* contains a number of provisions that criminalize the possession, making, or selling of certain things capable of being used to commit crimes. . . . I do not accept the Crown's submission that InfoSpec "engaged in a course of dealings that was by its very nature dishonest." InfoSpec participated in commercial transactions involving the sale of a computer program that is not prohibited by law; the restaurants got what they paid for. Whatever reasonable people might think about the propriety of such a sale, I am unable to say they would consider the vendor to have acted dishonestly. *If Parliament considers a prohibition on zappers necessary to thwart tax evasion, then it is open to it to enact a provision* similar to those to which I have just referred.[60]

This holding is consistent with the tax assessment raised on the Manitoba restaurants considered above.[61] In those cases, zapper-specific penalties were imposed only at the provincial level[62] because there was no comparable anti-zapper law at the federal level.[63] As a result,

[54] *Id.*

[55] *Id.*

[56] 2013 B.C.C.A. 333 (Can.).

[57] *See id.* paras. 10–11 (explaining that the Crown charged InfoSpec with one count of fraud over $5000 under section 380(1)(a) of the Criminal Code, R.S.C. 1985, c. C-46; four counts of evading income tax under section 239(1)(b) of the Income Tax Act, R.S.C. 1985 (5th Supp.), c. 1; and four counts of evading the Goods and Services Tax under section 327(1)(b)(i) of the Excise Tax Act, R.S.C. 1985, c. E-15, but that the court only convicted InfoSpec on the fraud count).

[58] *Id.* para. 24.

[59] *Id.*

[60] *Id.* paras. 21–22 (emphasis added).

[61] *See Winnipeg Restauranteurs Taste Tax Evasion Fines*, *supra* note 44.

[62] *See supra* note 46 (quoting from the relevant Manitoba tax law imposed on the restaurant owners).

[63] *InfoSpec Sys. Inc.*, 2013 B.C.C.A. 333, para. 21.

Manitoba zapper-fines in each case equaled 100% of the unreported Manitoba sales tax, plus $500, but the federal fines were zero.[64]

Although this decision was effectively rendered irrelevant by the express prohibition of electronic sales suppression (ESS) software in the March 21, 2013 Budget announcement,[65] it has considerable relevance for the United States and the individual states, many of which find themselves in a position analogous to that in *InfoSpec Systems*.[66] As a result of this holding, the Canadian Federal Government proposed and adopted "new administrative monetary penalties and criminal offences under the *Excise Tax Act* . . . and the *Income Tax Act* to combat [ESS] tax evasion."[67] Offenses now include "the use, possession, acquisition, manufacture, development, sale, possession for sale, offer for sale or otherwise making available of ESS software."[68]

The Canadian federal penalties have a progressive cast.[69] The penalties allow a measured response to ESS, with a clear distinction between the activities of salesmen and end-users.[70] They are both civil and criminal.[71] Civil penalties include relatively moderate fines, while criminal penalties include heavy fines and jail time.

Civil penalties for the use or possession of ESS are $5,000 for a first offence, $50,000 for subsequent offenses, and double for selling or manufacturing ESS. Criminal penalties for sale or manufacture of

[64] *See supra* note 48 and accompanying text.

[65] CAN. DEP'T OF FIN., *supra* note 47, at 381–82.

[66] *See* Furchgott, *supra* note 10 (explaining that zapper software may be a growing problem in the United States because only two zapper cases have been prosecuted by U.S. authorities, but the technology exists and instances of its use in the United States are likely going unnoticed).

[67] CAN. DEP'T OF FIN., *supra* note 47, at 381 (indicating that the changes were effective January 1, 2014).

[68] *Id.* at 382.

[69] *See* R.S.M. 1987, c. R.150, § 76(4)–(5) (2016) (raising both fines and prison time for second and subsequent offenses effective January 1, 2014). The Canada Revenue Agency (CRA) conducted a nation-wide study of sales suppression, which led to the new laws. *See* CRA 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 (2010) (redacted version on file with author).

[70] *See* CAN. DEP'T OF FIN., *supra* note 47, at 381 (assessing twice the fines for the manufacture or sale of zapper software as for possession, acquisition, or use of the software).

[71] *Id.* at 381–82 (listing the new monetary penalties and criminal offenses).

ESS include up to $1,000,000 in fines and five years in prison.[72] The U.S. states that have adopted anti-zapper legislation largely follow the language of the Canadian statute, although the monetary penalties in the United States tend to be much lower.[73]

II. THE AMERICAN FRAUD CASES

It would be surprising if InfoSpec's Profitek POS system and related Profitek Zapper had *not* crossed the international border and entered the United States. InfoSpec does not characterize itself as a purely Canadian company. It sees itself as an international provider of POS systems that is fully operational in North America with a distinct bilingual advantage for Chinese/English users, as well as any other language supported by Windows. The company's web site explains:

> 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.
>
> Profitek is unique in providing dedicated POS software suites for the Hospitality and Retail sectors. Mixed hospitality and retail environments such as museums, zoos, campuses, or any organization with both retail and food service operations are ideal candidates for Profitek's solutions.
>
> Profitek was the first POS solution in North America to provide dual language operation. *The software displays and prints in any second language supported by Windows and allows viewing and printing of orders and receipts in either language, based on the preference of each user.*[74]

Given Profitek's international scope, its zappers should have been found in the United States roughly sixteen years ago in 2000, when the Profitek Zapper was first surfacing in Canadian audits.[75] The migration of high-tech tax evasion software across the Canadian border presents new challenges to U.S. tax enforcement officials.

The most obvious targeted U.S. jurisdiction for InfoSpec products would be Washington State. Seattle, Washington is 142 miles south of

[72] R.S.C. 1985, c. 1 (5th Supp.), § 239.1(2)–(3); *see also* CAN. DEP'T OF FIN., *supra* note 47, at 381–82.

[73] CAL. REV. & TAX CODE § 7153.6(2)(A) (West 2016).

[74] *About Profitek*, PROFITEK, http://www.profitek.com/About (last visited May 17, 2016) (emphasis added).

[75] *See* Furchgott, *supra* note 10 (noting that Quebec's tax agency reported a case of zapper software sales in the year 2000).

Vancouver, British Columbia, and is considerably closer than Winnipeg, Manitoba. Nevertheless, the first public announcement by any U.S. tax authority that the Profitek Zapper may have been used in the United States came out of Chicago, Illinois, a full 2202 miles east of the company's head offices.[76] The second public announcement comes from Seattle, Washington, which is much closer to Vancouver than to Chicago.[77]

The Chicago investigation is focused on several specific restaurants all owned by the same individual who may have used the Profitek Zapper.[78] All of the restaurants used the model INFOSPEC SYSTEMS INC. MODEL PROFITEK RM SYSTEM V10.0.3 and an accompanying Zapper.[79] Hu Xiaojun had an ownership interest in all the restaurants, which were all located in the China Square Mall.[80]

In Seattle, the Washington Attorney General's investigation initially focused on an alleged Profitek Zapper salesman.[81] However, the focus has recently turned to one alleged Profitek Zapper-user who allegedly secured the Profitek Zapper from the previously identified salesman.[82] The case involved a restaurant owner named Yu-Ling Wong who had been suppressing sales tax information for three years.[83] After investigators discovered the tax fraud, they questioned Wong, who pointed them to John Yin, a sixty-four-year-old self-employed software salesman.[84] Yin admitted to selling Profitek Zapper software.[85] Other cases in Seattle may follow.

Thus, similar to the litigation in Canada, there are signs that enforcement litigation is beginning in the United States against restaurants that may have used Profitek Zappers in Chicago and the salesmen who are allegedly selling Profitek Zappers in Washington. There is yet to be any evidence of an enforcement action against the manufacturer, InfoSpec Systems, but this may be just a matter of time.

[76] Application and Affidavit for a Search Warrant ¶ 43, United States v. Lao You Ju, No. 1:14-mc-00571 (Oct. 21, 2014 N.D. Ill.) [hereinafter Ju Search Warrant Affidavit].

[77] Affidavit for Search Warrant, State v. Yin, No. 15-1-12052-9 SEA (July 13, 2015 King Cty. Super. Ct. Was.) [hereinafter Yin Search Warrant Affidavit].

[78] Ju Search Warrant Affidavit, *supra* note 76, ¶¶ 42–43.

[79] *Id.*

[80] *Id.* ¶¶ 3–6.

[81] Yin Search Warrant Affidavit, *supra* note 77, at 1, 3.

[82] Information, State v. Wong, No. 16-1-00179-0 (King Cty. Sup. Ct. Was. Feb. 5, 2016) (accusing Yu-Ling Wong of unlawful use of sales suppression software).

[83] *Id.* at 2.

[84] Yin Search Warrant Affidavit, *supra* note 77, at 3.

[85] *Id.* at 4.

A. U.S. Restaurants

On Tuesday, October 21, 2014, the FBI filed nine Applications and Affidavits for Search Warrants with U.S. Magistrate Judge Jeffrey T. Gilbert of the Northern District of Illinois.[86] The FBI wanted to search each of the nine Chicago restaurants owned by Hu Xiaojun,[87] on the grounds that Hu was systematically under-reporting income.[88] The POS system at each restaurant was "INFOSPEC SYSTEMS INC. MODEL PROFITEK RM SYSTEM V10.0.3,"[89] which was the most common system in use at Chinese restaurants in Chicago's Chinatown.[90] Alleged violations included (a) conspiracy to commit tax fraud in violation of 18 U.S.C. § 371; (b) tax fraud in violation of 26 U.S.C. § 7206; and (c) wire fraud in violation of 18 U.S.C. § 1343.[91] No Illinois state violations were referenced.[92] In each of the nine cases, the search warrant was (1) formally entered, (2) sealed upon motion by the Government, and (3) marked *Returned Executed* in the court reporting system on April 13, 2015.[93] However, the execution date for the warrant in each case was October 21, 2014.[94]

[86] *See* sources cited *infra* note 93; *see also* Ju Search Warrant Affidavit, *supra* note 76, at 1 (listing a Federal Bureau of Investigation (FBI) special agent as the applicant).

[87] 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), http://chicago.eater.com/2015/2/16/8046983/tony-hu-selling-most-chinatown-restaurants.

[88] Peter Frost, *Tony Hu Probed for Suspected Conspiracy, Tax Fraud and Wire Fraud*, CRAIN'S CHIC. BUS. (Apr. 28, 2015), http://www.chicagobusiness.com/article/20150428/BLOGS09/150429783/tony-hu-probed-for-suspected-conspiracy-tax-fraud-and-wire-fraud.

[89] Ju Search Warrant Affidavit, *supra* note 76, ¶¶ 42–43.

[90] *See id.* ¶ 43 ("The waiter [at the Lao Sze Chuan—Uptown restaurant] . . . told the agents that a number of Chinese restaurants utilized the same system, which was obtained from what the employee described as a company located in the Chinatown Square mall."); *see also id.* ¶ 43 n.10 ("The Chinatown Square mall is located in Chicago's Chinatown neighborhood. A number of the Tony Gourmet Group restaurants, including Lao Sze Chuan (Subject Business 2), Lao Beijing (Subject Business 4), Lao Shanghai (Subject Business 5), Lao Ma La (Subject Business 7), and Lao Yunnan (Subject Business 9), are located within the China [sic] Square mall.").

[91] *Id.* at 1.

[92] *Id.*

[93] The nine cases are:
(1) United States v. Lao Shanghai, No. 1:14-mc-00570 (N.D. Ill. Oct. 21, 2014);
(2) United States v. Lao Yunnan, No. 1:14-mc-00574 (N.D. Ill. Oct. 21, 2014);
(3) United States v. Lao Sze Chuan, No. 1:14-mc-00566 (N.D. Ill. Oct. 21, 2014);
(4) United States v. Lao Sze Chuan, No. 1:14-mc-00567 (N.D. Ill. Oct. 21, 2014);

There is one case that does not follow this timeline. The court issued two warrants in *United States v. Lao You Ju*: one on October 21, 2014, and one on October 24, 2014.[95] The latter date was the same date that each of the initial nine warrants were "*Returned Executed*" as indicated on the court dockets.[96] The issuance of a second warrant seems to have allowed the first warrant on the Lao You Ju restaurant to enter the public record on Friday, April 13, 2015, perhaps because the second warrant request opened a second case against the restaurant.[97] A reporter for the Chicago Sun-Times found the court's publication of the first warrant, and the paper ran an article on Monday, April 27, 2015, focusing on the FBI allegations in the first search warrant on the Lao You Ju restaurant.[98]

In 110 pages, the affidavit sets out the major arguments of the tax fraud case against all nine restaurants.[99] The analysis revolves around an apparent "second set of books" constructed from intercepted e-mail attachments. The FBI compared the information with the restaurants' filing positions on federal income tax returns and Illinois sales tax returns.[100] Monthly bank deposits provided further contrast.[101]

The FBI asserted probable cause that the restaurants underreported their gross income by demonstrating, for example, that the Lao Sze Chuan—Downers Grove restaurant allegedly suppressed roughly forty percent of its sales from 2008 to 2010.[102] To

(5) United States v. Lao Sze Chuan, No. 1:14-mc-00568 (N.D. Ill. Oct. 21, 2014);
(6) United States v. Lao Ma La, No. 1:14-mc-00572 (N.D. Ill. Oct. 21, 2014);
(7) United States v. Lao Hunan, No. 1:14-mc-00573 (N.D. Ill. Oct. 21, 2014);
(8) United States v. Lao Beijing, No. 1:14-mc-00569 (N.D. Ill. Oct. 21, 2014);
(9) United States v. Lao You Ju, No. 1:14-mc-00580 (N.D. Ill. Oct. 24, 2014); United States v. Lao You Ju, No. 1:14-mc-00571 (N.D. Ill. Oct. 21, 2014).

[94] *See* sources cited *supra* note 93.

[95] United States v. Lao You Ju, No. 1:14-mc-00580 (N.D. Ill. Oct. 24, 2014); United States v. Lao You Ju, No. 1:14-mc-00571 (N.D. Ill. Oct. 21, 2014).

[96] *Id.*

[97] When the second search warrant was issued, the court assigned a second docket number.

[98] Jon Seidel, *Feds Went to Chinatown Looking for Food—and Fraud*, CHI. SUN-TIMES (Apr. 27, 2015, 5:29 PM), http://chicago.suntimes.com/news/feds-went-to-chinatown-looking-for-food-and-fraud. Personal communication with Jon Seidel on October 25, 2015 indicates that his story was based on "case number 14-MC-571 in the Northern District of Illinois," which is the *United States of America v. Lao You Ju* search warrant filed on October 21, 2014.

[99] *See generally* Ju Search Warrant Affidavit, *supra* note 76.

[100] *Id.* ¶¶ 4, 9, 39, 52–55, 58–71.

[101] *Id.* ¶¶ 88, 93, 97, 104, 108, 113, 120, 131, 140.

[102] *Id.* ¶¶ 52–55.

do this, the FBI compared the manager's spreadsheets of sales with the gross receipts filed on the federal corporate return.[103]

The FBI is clearly interested in cash sales.[104] The warrant strongly suggests that each of the nine restaurants systematically suppressed cash sales. Undercover agents went to each restaurant, purchased meals with cash, and secured a receipt that indicated payment for the meal and payment of the Illinois sales and use tax that was included in the charge.[105]

In constructing the tentative "second set of books," the FBI broke down the amounts received into cash and credit card transactions.[106] When these figures were compared with the restaurants' monthly Illinois sales and use tax returns from Forms ST-1 and E911 Surcharge Return, it appeared that the amounts declared on the tax returns were uniformly lower, suggesting suppression.[107] To make its point even clearer, the FBI further aligned monthly bank deposit data.[108] For example, the average monthly deposit for Lao Sze Chuan was $230,812, but the average monthly receipt reported on Illinois Form ST-1 was $214,995.[109] Similarly, the average monthly deposit for Lao You Ju was $94,330, but the average monthly receipts reported on Illinois Form ST-1 was $82,468.[110] In addition, the bank records show that for month after month and for restaurant after restaurant, no cash was deposited into corporate bank accounts, suggesting that a large portion of the (allegedly) suppressed sales were the cash transactions.[111] The bank deposits on record are primarily credit card merchant account deposits.[112]

There is no mention of a Profitek Zapper in the search warrant.[113] However, given the presence of the Profitek POS system in each of the nine restaurants,[114] knowledge of the prior litigation in Canada,[115]

[103] *Id.* ¶ 55 (containing a chart showing that the restaurant reported gross sales figures below actual sales figures).

[104] *Id.* ¶ 4.

[105] *Id.* ¶¶ 87, 96, 103, 107, 112, 119, 130, 139.

[106] *Id.* ¶¶ 84–85, 89–90, 94, 98, 105, 109, 117, 128, 137.

[107] *See id.* ¶¶ 57–58, 60–61, 63–64, 66–67, 69–70, 72–73, 75–76, 78–79, 81–83, 93, 97, 104, 108, 113, 120, 131, 140.

[108] *Id.* ¶¶ 88, 93, 97, 104, 108, 113, 120, 131, 140.

[109] *Id.* ¶ 93.

[110] *Id.* ¶ 113.

[111] *Id.* ¶¶ 88, 93–94, 97, 104, 108, 113, 120, 131, 140.

[112] *Id.* ¶¶ 85, 90, 94, 101, 105, 110, 117, 128, 137.

[113] *See generally id.*

[114] *Id.* ¶¶ 42–43.

and the passage of anti-zapper legislation in Illinois,[116] it is entirely possible that the FBI might have been using the Chicago investigations to find a Profitek Zapper in Chicago.[117] If the FBI found a zapper, and if any of the nine restaurants used the zapper after January 1, 2014, then the state charges against Hu Xiaojun could be criminal.[118]

On August 16, 2013, the Governor of Illinois signed into law Public Act 098-0352, which made the knowing sale, purchase, installation, use, or transfer of zappers a Class 3 felony.[119]

Under Illinois law, a Class 3 felony is punishable by two to five years' imprisonment.[120] An "extended term" Class 3 felony is punishable by five to ten years in prison.[121] Despite the criminal statute, each of the ten cases—one against each of Hu Xiaojun's nine restaurants including an additional case for the second warrant for the Lao You Ju restaurant—are now formally *closed* in court records.[122] Consequently, there is no tax case in the public record. The FBI actions were considered "mysterious" in the local media.[123] Hu Xiaojun was in the process of selling his restaurant and moving out of

[115] R v. Au, 2011 B.C.S.C. 75 (Can.); R v. InfoSpec Sys. Inc., 2013 BCCA 333 (Can.); *see* sources cited *supra* note 44 (reporting about the fines imposed on the Canadian restaurants after they pled guilty).

[116] 35 ILL. COMP. STAT. 105 / 14 (2014) (effective Jan. 1, 2014).

[117] The Search Warrant only references that the State of Illinois Department of Revenue Publication 113 from October 2011, titled Retailer's Overview of Sales and Use Tax and Prepaid Wireless E911 Surcharge, requires that retailers keep "the cash register tapes and other data that provide a daily record of the gross amount of sales" for three and a half years after the date they file an ST-1 return. Ju Search Warrant Affidavit, *supra* note 76, ¶ 41.

[118] 35 ILL. COMP. STAT. 105 / 14. Illinois passed legislation effective January 1, 2014 that made zapper use a Class 3 felony. *Id.*

[119] 2013 Ill. Laws 4556 (codified at 35 ILL. COMP. STAT. 105 / 14) ("Any person who knowingly sells, purchases, installs, transfers, possesses, uses, or accesses any automated sales suppression device, zapper, or phantom-ware in this State is guilty of a Class 3 felony.").

[120] 730 ILL. COMP. STAT. 5 / 5-4.5-40(a) (2016).

[121] *Id.*

[122] *See* sources cited *supra* note 93.

[123] *Mystery Behind Chinatown Raids Remains*, EATER CHI. (Oct. 27, 2014, 4:01 PM), http://chicago.eater.com/2014/10/27/7079837/mystery-behind-chinatown-raids-remains (reporting that Hu Xiaojun did not know why the searches occurred, but that his Lao You Ju restaurant was back open); Peter Frost, *What's Happening with Chinatown's Tony Hu?*, CRAIN'S CHI. BUS. (Feb. 28, 2015), http://www.chicagobusiness.com/article/20150228/ISSUE01/302289982/whats-happening-with-chinatowns-tony-hu.

state.[124] Lao Beijing was sold in January 2015.[125] Lao Hunan, Lao Yunnan, Lao Shanghai, and Lao Ma La were up for sale in February 2015, and contracts for their transfer had been signed.[126]

The FBI was also aware that Hu Xiaojun owned restaurants outside of the Chicago area, notably in Milford, Connecticut and Las Vegas, Nevada.[127] The FBI did not obtain search warrants for either of these locations. The FBI's failure to issue search warrants is peculiar in light of the comprehensive assessment of how Hu Xiaojun allegedly coordinated the tax manipulations remotely through e-mail correspondence with managers and bookkeepers.[128] There was concern about whether or not the InfoSpec systems worked with "cloud-based computing."[129]

The mystery surrounding Hu Xiaojun's involvement in sales suppression has been put to rest with his guilty plea to felony fraud and money laundering charges alleging that he hid more than $9 million in cash receipts avoiding over $1.1 million in Illinois sales taxes.[130] The guilty plea came three days after the information.[131] There is no mention of a zapper in the information, which simply records that "defendant Hu modified the restaurants' sales records and caused the restaurants' sales records to be modified in order to conceal cash transactions that had occurred at the restaurants."[132]

[124] Although he resisted the characterization, Hu Xiaojun appears to many to be leaving town: "It's just rumors. A lot of people think I'm leaving Chinatown, but that's not true," he said. "I am thinking a lot about the future, and I plan to pay more attention to (growing the) Lao Sze Chuan (brand)." Peter Frost, *Tony Hu Sells Lao Beijing*, CRAIN'S DINING CHI. (Feb. 2, 2015), http://www.chicagobusiness.com/article/20150202/BLOGS09/150209967/tony-hu-sells-lao-beijing ("Hu said he's been spending much of his time at Lao Sze Chuan Downtown, which opened Dec. 18 in the Shops at North Bridge at 520 N. Michigan Ave. He said he's also entertaining offers to expand to Houston, San Francisco, Los Angeles and New York.").

[125] Gerzina, *supra* note 87.

[126] *Id.*

[127] Ju Search Warrant Affidavit, *supra* note 76, ¶ 6 n.2.

[128] *See id.* ¶¶ 2 n.1, 38, 52–89, 98–99, 109–27, 132–36, 156–64, 169.

[129] *See id.* ¶ 45, n.11. Other jurisdictions have found cloud-based manipulations. Richard T. Ainsworth, *Sales Suppression as a Service and the Apple Store Solution*, 73 ST. TAX NOTES 343, 351–52 (2014) (referencing manipulations on the Aldelo POS system installed by one partner to (allegedly) embezzle funds from the other partner of a North Carolina business through a cloud installation located in California).

[130] Plea Agreement ¶¶ 5, 6.a, United States v. Hu Xiaojun, No. 1:16-cr-00316 (N.D. Ill. May 16, 2016).

[131] *Id.* (entering Hu's guilty plea on May 16, 2016); Information, Unites States v. Hu Xiaojun, No. 1:16-cr-00316 (N.D. Ill. May 13, 2016) [hereinafter Hu Xiaojun Information] (formally charging Hu on May 13, 2016).

[132] Hu Xiaojun Information, *supra* note 131, at ¶ 5.

B. U.S. Salesmen

Unlike the FBI in Chicago, when the Washington State Attorney General's Office learned that restaurants in their jurisdiction were using InfoSpec's Profitek POS system with the Profitek Zapper, it secured a search warrant to investigate the salesman.[133] The search warrant was approved and sealed,[134] but much like the warrant in Chicago, which was unsealed, the local press began writing about it as soon as they learned of the investigation.[135] Articles were published and investigative TV coverage of the story began.[136]

The Attorney General's Office was able to obtain the warrant because the Washington Department of Revenue issued a criminal referral to the Attorney General's Office.[137] A taxpayer who was using a Profitek POS system informed them that the Profitek Zapper had been used with the POS system "for many years" to suppress sales.[138] The taxpayer identified John Yin as the individual who sold the Profitek POS system but "did not admit that John Yin sold her the accompanying Revenue Suppression USB drive."[139] However, the affidavit confirms that "this USB only works with Profitek POS Systems."[140]

Furthermore, John Yin was the "only licensed reseller of Profitek Software in Washington State,"[141] so a warrant was needed to determine whether John Yin sold this Profitek Zapper to others.[142] Did he sell it to others? If so, how many and to whom? The Canadian case, *R v. Au*,[143] confirmed that Profitek POS salesmen were

[133] Yin Search Warrant Affidavit, *supra* note 77.

[134] There is a stamp on the top of the Yin Search Warrant Affidavit, *supra* note 77, that says "SEALED." This Article's author's personal communication with the reporter who broke the story revealed that she was at the court house on Monday morning looking for anything that might have become "unsealed" over the weekend and she found this search warrant. The norm is for documents to be sealed for sixty days.

[135] Matt Day, *Bellevue Restaurant Accused of Tax Cheating*, SEATTLE TIMES (last updated Feb. 8, 2016, 2:41 PM), http://www.seattletimes.com/business/technology/bellevue-restaurant-accused-of-tax-cheating (reporting that investigators searched Yin's residence).

[136] *See, e.g.*, Amy Clancy, *Bellevue Restaurant Owner Charged in Tax Fraud Case*, KIRO7 (last updated Feb. 6, 2016, 9:51 AM), http://www.kiro7.com/news/kiro-news-app/restaurants-cheating-washington-taxpayers-out-of-millions/61479512.

[137] Yin Search Warrant Affidavit, *supra* note 77, at 3.

[138] *Id.*

[139] *Id.*

[140] *Id.*

[141] *Id.* at 4.

[142] *See id.* at 7–11.

[143] 2011 B.C.S.C. 75 (Can.).

instructed to sell Profitek Zappers to clients as a service, and when they did, their commission was $400.[144]

The Attorney General's Office needed to search John Yin's home, his automobile, all the technology devices he had, and all the records he kept.[145] The scope of the search would include copies of the Profitek Zapper, the customer list of all current and former Profitek clients, and income records.[146] In the classic zapper salesman case, it is common for the salesman to also install, troubleshoot, and provide all-purpose sales suppression services for zapper customers.[147] The dominance of this "service model" is the real lesson learned from several undercover sting operations that occurred in New York that targeted sales suppression.[148]

A well-known zapper-salesman case provides a great example of how this type of fraud develops and operates. Michael Roy, a software developer with the Resto Terminal POS supplier in Quebec, with the help of his two sons, aided twenty-eight restaurants commit sales suppression frauds in 2002 and 2003.[149] During the day, Mr. Roy worked on system software for Resto Terminal POS, but in the evening, he developed a zapper that would defeat the system's record retention system.[150] Mr. Roy designed and developed a very effective zapper that was specific to the Resto Terminal POS.[151] His two sons, Miguel and Danny, opened a small consulting business where they installed their father's zapper software and assisted restaurants in committing sales suppression frauds.[152]

In addition to statutory penalties for the manufacture or retail of sales suppression technology, the aggregate fraud penalties assessed against the Roys were $1,064,459.[153] Income from the Roys'

[144] *Id.* ¶¶ 10–11.

[145] Yin Search Warrant Affidavit, *supra* note 77, at 14.

[146] *Id.* at Attachment B.

[147] Ainsworth, *supra* note 129, at 347.

[148] *Id.*

[149] Richard Ainsworth, *Mass. Zappers—Collecting the Sales Tax that Has Already Been Paid*, (B.U. Sch. Law, Working Paper No. 09-28, 2009); *Fines of More Than One Million Dollars—A Father and His Two Sons Convicted for Tax Evasion in Connection with the Zapper*, REVENU QUÉBEC (May 2, 2003) (on file with author); *Stratos Pizzeria - Amende de Plus d'Un Million pour Fraude Fiscale en Restauration,* LA PRESSE MONTREAL (May 2, 2003) at A14, http://collections.banq.qc.ca:81/lapresse/src/pages/2003/P2003-02/05/03/A/82812_20030503LPA14.pdf.

[150] *See Fines of More than One Million Dollars*, *supra* note 149.

[151] *Id.*

[152] *See id.*

[153] *See id.*

"consulting business" was not reported, and, of course, sales of the zapper were also not reported.[154] Instead, to avoid reporting requirements, transactions were in cash.[155] Essentially, the Roys designed their "business" to receive a percentage of the suppressed sales at each location they "serviced."[156]

Revenue Quebec published the aggregate fraud penalty and tax assessment against the first ten Stratos restaurants, which accumulated to $1,816,070.90.[157] By the time the Roys were sentenced, final restaurant totals were not released.[158] In its press releases, Revenue Quebec was not as interested in the restaurants as it was in the Roys.[159] Revenue Quebec had come to appreciate that it was the salesmen, the installers, and the service providers, more so than the immediate restaurant users, who were at the heart of the sales suppression problem.[160]

Fortunately, the Washington Attorney General and the Washington Department of Revenue seem to have learned a lesson from the Roys. The Washington State search warrant was issued against John Yin, the Profitek salesman, rather than the restaurants.[161]

Unfortunately, unlike the Washington State Attorney General, the FBI in Chicago did not internalize the lesson from the Roys. Rather than pursuing the business that sold the Profitek POS system or the salesman who was directly involved in the sales, the FBI conducted searches of nine area restaurants suspected of using the Profitek Zapper.[162] The FBI knew the name of the Profitek retailer in Chicago, Vision I Computers Inc., and the name of the salesman assigned to Hu Xiaojun's account, Wah Chu.[163] There are currently

[154] *All Stratos Restaurants Convicted of Fraud in Connection with the use of a Zapper*, REVENUE QUEBEC (Mar. 18, 2003) (on file with author).

[155] *Id.*

[156] *Id.*

[157] The available breakdown is as follows: $429,179.07 (GST) + $492,023.11 (PST) + $214,589.55 (federal penalties) + $625,028.89 (provincial penalties) + $55,250.28 (judicial fees). *Id.*

[158] *Id.*

[159] *Id.*

[160] *Id.*

[161] *See* Yin Search Warrant Affidavit, *supra* note 77, at 2 (alleging that probable cause existed that John Yin "committed the crimes of Theft in the first degree (RCW 9A.56.030), Filing of False Tax Returns (RCW 82.32.090) and Unlawful Acts (RCW 82.32.090) during the years 2010 through [2015]").

[162] *See* Ju Search Warrant Affidavit, *supra* note 76 ¶ 3 (focusing its investigation on the businesses using the Zapper rather than the Zapper salesman).

[163] *Id.* ¶ 48.

no pending search warrants or civil or criminal charges involving either Vision I Computers Inc. or Mr. Wah Chu in the Chicago area.

Indeed, the FBI incorrectly focused on the restaurants despite finding information that could lead to the salesman.[164] The affidavit demonstrated that restaurant employees informed agents that "a number of Chinese restaurants utilized the same [Profitek] system, which was obtained from . . . a company located in the Chinatown Square mall."[165] Additionally, the FBI found an email indicating that the salesman set up at least four locations with the same POS system.[166] Further, the affidavit recognized that "it is not uncommon that retail businesses that operate from multiple locations with the same or common management and ownership often utilize the same or similar POS systems."[167]

The FBI does not seem to appreciate that the core problem in technology-assisted sales suppression are the salesmen, installers, and other "service providers," rather than the individual users.[168] Even if the FBI is right, and the central problem is the individual user of suppression technology, then it should have pursued Hu Xiaojun's five other restaurants outside of Chicago's Chinatown.[169] If Hu Xiaojun is suppressing sales in nine Chinatown restaurants, why would he not be suppressing sales in his other five more remote restaurants? Technology-assisted sales suppression is not geographically constrained.[170] As noted, it moves across and among jurisdictions both domestically and internationally.[171] To stop this fraud, the FBI needed to think like a technology expert, not like a restaurateur who is skimming sales when he is at the cash register.[172]

[164] *Id.* ¶¶ 43, 48 (indicating that the Lao Sze Chuan, Lao Beijing, Lao Shanghai, Lao Ma La, and Lao Yunnan restaurants were located in the Chinatown mall). Note 10, *supra*, indicates that five of Hu Xiaojun's nine restaurants are also located in the Chinatown mall: Lao Sze Chuan; Lao Beijing; Lao Shanghai; Lao Ma La; and Lao Yunnan. *Id.* ¶ 43 n.10.

[165] *Id.* ¶ 43.

[166] *Id.* ¶ 47.

[167] *Id.* ¶ 49.

[168] *See supra* notes 149–60 and accompanying text (discussing the salience of two cases where the investigation focused on the salesman rather than the restaurants involved).

[169] *See* Ju Search Warrant Affidavit, *supra* note 76, ¶ 6 n.2 (listing the following restaurants outside of Chicago's Chinatown: (1) the Lao Sze Chuan in Milford Connecticut; (2) the Lao Sze Chuan in Evanston, Illinois; (3) the Lao 18 in Chicago's River North neighborhood; (4) the Lao Sze Chuan in Skokie, Illinois, and (5) Lao Sze Chuan at the Palms in Las Vegas, Nevada).

[170] *See infra* notes 173–79 and accompanying text (expounding on the capability of committing sales suppression fraud remotely).

[171] *See id.*

[172] *See id.*

The FBI's investigation was too narrow, focusing on the notion that sales suppression occurs locally—where the owner is located.[173] The FBI appears to believe that the person engaged in the suppression fraud must be present where the records are manipulated.[174] This is evident through the FBI's fixation on its discussion with a Profitek employee who explained that the data for each restaurant is preserved on a local server. The employee explained that the POS system "maintains a history of the sales transactions . . . on a server that is integrated into the point of sale system," so the "data from each point of sale system is stored on a local server and not a remote system."[175]

Hu Xiaojun used a local server in each of his fourteen restaurants, but this does not mean that he could not have manipulated the records of any of those establishments remotely with a Profitek Zapper.[176] If a Profitek Zapper was installed at the remote restaurants, Hu Xiaojun could access each server with "Team Viewer" software and manipulate the records from a safe distance.[177]

In fact, the FBI is currently involved in another sales suppression case involving seven IHOP restaurants in Ohio where the manipulation of records on a MICROS POS system was performed remotely, from the owner's bedroom, with "Team Viewer" software.[178] The Indictment in that case indicates that the owners began remotely manipulating the POS systems shortly after installing the newest MICROS POS system on the IHOP computers.[179]

As previously illustrated, the Washington Attorney General appears to have a sharper focus on the sales suppression problem than the FBI. When zappers become common in a community, it is imperative to find the salesmen, installers, and service providers who spread the fraud.[180] The restaurants or other retailers are of secondary

[173] *See* Ju Search Warrant Affidavit, *supra* note 76, ¶ 45 (focusing the investigation on the fact that the fraud was maintained on a local server rather than committed remotely).

[174] *See id.*

[175] *See id.* ¶ 45 & n.11.

[176] *See infra* notes 178–79 and accompanying text (discussing a scenario where an individual remotely manipulated records with a Profitek Zapper).

[177] *See id.*

[178] *Eighteen People Indicted for Roles in $3 Million Schemes Involving Seven IHOP Restaurants*, FBI (May 23, 2012), http://www.fbi.gov/cleveland/press-releases/2012/eighteen-people-indicted-for-roles-in-3-million-schemes-involving-seven-ihop-restaurants.

[179] Indictment ¶ 47, United States v. Elkafrawi, No. 3:12CR 262, 2012 WL 8303904 (N.D. Ohio May 22, 2012).

[180] *See* Penelope Lemov, *Sales Tax Zapped by Zappers*, GOVERNING (May 10, 2012), http://www.governing.com/columns/public-finance/col-sales-tax-zapped-tax-zappers.html (arguing that because the salesman proactively offers a product that is

importance.[181] Perhaps the Attorney General took the approach he did because the Washington statute directs the enforcement community to aggressively go after the salesmen.[182] Like Quebec, but unlike Illinois, Washington has penalty provisions that directly target the people who sell, install, and service zappers.[183]

The Revised Code of Washington section 82.32.290 makes it unlawful to possess, sell, or service any sales suppression device.[184] It enforces an additional penalty against individuals who provide and service the devices.[185] The defendant may also be required to pay the state an amount equal to the sales taxes that were fraudulently withheld.[186]

It is particularly section 82.32.290(4)(c)(ii), with its emphasis on furnishing, updating, or repairing sales suppression software that is the key. It subjects an individual to a penalty that is the greater of (1) $10,000, (2) the defendant's gain from the commission of the crime, or (3) the state's loss from the commission of the crime.

With regards to the statute's third prong, the Washington Department of Revenue must *certify* the state's loss because of taxpayer confidentiality rules.[187] In *Au*, for example, the state's loss from Au's sale of Profitek Zappers was $2,400,000 in federal income tax and $1,000,000 in Goods and Services Tax.[188] This calculation was generated after audits had been completed on only fourteen of the twenty-three firms to whom Mr. Au had sold zappers.[189] Effectively, the third prong of the Washington penalty provision would make Mr. Au and the zapper manufacturer guarantors of total taxes lost.[190]

If Mr. Au was prosecuted under the Washington statute and if the final penalty was determined under the third prong of section 82.32.290(4)(c)(ii), then his penalty would be calculated by

extremely difficult to detect, the fault does not lie with the individual restaurant owner, who could be put out of business if other nearby businesses utilize the zapper).

[181] *Id.*

[182] *See* WASH. REV. CODE § 82.32.290(4)(a), (c)(ii) (2013) (creating harsher penalties for the individual who manufactures or provides the device).

[183] *Id.* § 4(a).

[184] *Id.*

[185] *Id.*

[186] *Id.* § 4(c)(ii).

[187] *See id.* ("'[L]oss' means the total of all taxes, penalties, and interest certified by the department.").

[188] *See* R. v. Au, 2011 B.C.S.C. 75, ¶ 4 (Can.) (calculating the defendant's mandatory fine based on the state's loss from his crime).

[189] *Id.*

[190] *See* WASH. REV. CODE § 82.32.290(4)(c)(ii) (noting that a state's loss is "the total of all taxes, penalties, and interest certified by the department to be due").

aggregating the deficiencies of all twenty-three firms he sold Profitek Zappers to and then by netting out the amounts actually remitted. The final amount could be more or less than the $3,400,000 already determined, but it could not be less than $10,000.[191]

III. LESSONS LEARNED

Technology-assisted sales suppression fraud differs fundamentally from traditional tax fraud.[192] The technology at the heart of this fraud needs to be dealt with directly, and most likely with counter-technology.[193] With regards to the zapper provided by Mr. Au, it was on a CD, and the zapper provided by Mr. Yin was on a thumb drive.[194] The current version of the Profitek Zapper is available online and does not require local installation.[195] Additionally, Profitek offers an Online Ordering Module (OLO), which Profitek suggests can be used to enhance sales via the internet.[196] In this type of situation, both sales records and the zapper would be located in the cloud, making it considerably more difficult for an auditor to find. As technology advances, technology-assisted sales suppression will also inevitably increase.

Enforcement agencies need to develop and employ either: (a) technology that efficiently reconstructs digital transaction records that have been suppressed[197] or (b) security software, technology that

[191] *See id.* (stating that the penalty shall be the greater of $10,000, the defendant's gain, or the state's loss).

[192] *See* Devlin Barrett & John D. McKinnon, *Identity Theft Triggers a Surge in Tax Fraud*, WALL ST. J. (Feb. 23, 2014, 8:49 PM), http://www.wsj.com/articles/SB10001424052702304834704579401411935878556 (describing traditional tax fraud as fraud involving individuals lying about their income or deductions, not requiring the use of complex technology, as opposed to technological sales suppression fraud in which a fake tax document is created).

[193] *See* ELECTRONIC SALES SUPPRESSION: A THREAT TO TAX REVENUES, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT 4, 35, 38 (2013) [hereinafter ELECTRONIC SALES SUPPRESSION], http://www.oecd.org/ctp/crime/ElectronicSalesSuppression.pdf (suggesting that tax administrations should attempt to improve detection and counter-measures and "invest in acquiring the skills and tools to audit and investigate POS systems").

[194] R v. Au, 2011 B.C.S.C. 75, ¶ 7 (Can.); Yin Search Warrant Affidavit, *supra* note 77, at 3.

[195] The author's personal communication (by telephone) with members of the Washington Department of Revenue who were conducting the investigation revealed this information.

[196] For an assessment of Profitek, see *Profitek*, SOFTWAREINSIDER, http://point-of-sale.softwareinsider.com/l/230/Profitek (last visited May 17, 2016).

[197] For example, a company called iSeekDiscovery that is in the forensic data recovery and eDiscovery business promises to be able to recover suppressed data

encrypts and saves digital records at the time of their creation.[198] Most jurisdictions have adopted solution (b).[199] The most effective enforcement regimes involve real-time secure transmission of encrypted transactional data to a central location[200] where artificial intelligence (AI) conducts a high quality risk analysis in a deployment that assures taxpayer privacy.[201]

The primary concern is legislation like House Bill 1051 in South Dakota, which allows the State's Department of Revenue (DOR) to seize automated sales suppression devices or phantomware without a

remotely. *iSeekDiscovery*, CYBER CRIME FORENSICS, http://www.cybercrime-forensics.com/#!iseekdiscovery/c1naj (last visited May 17, 2016).

[198] *See Certified Invoicing System (CIS)*, DATA TECH INT'L, http://dti.rs/wp-content/uploads/2015/06/Document-2015.pdf (describing technology that assists in preventing tax fraud by creating and maintaining evidence of transactions and providing "reliable documentation of transaction that is . . . highly secure").

[199] *See generally* Bethany Ansorge, Note, *Software Assisted Sales Skimming—Under Reporting Receipts*, 36 MICH. TAX LAW. 46 (2010) (discussing different jurisdictional approaches to the zapper problem).

[200] *See* Richard Ainsworth, *California Zappers: A Proposal for California's Commission on the 21st Century Economy*, (B.U. Sch. of Law, Working Paper No. 09-01, 2009). A number of international companies specialize in data encryption of POS systems responding to government fiscalization regulation, including, for example, Data Tech International Ltd. (DTI). DTI is based in Serbia. DTI's main activity is solution development and consultancy. It assists and advises governments combating tax frauds with commercially available technology. *Certified Invoicing System*, DATA TECH INT'L, http://dti.rs/wp-content/uploads/2015/06/Document-2015.pdf. Avatar Technologies Ltd. is based in Portugal. It partners with the Suisse group SGS - SOCIETE Genérale de Surveillance and the South African GVG - Global Voice Group. Avatar's main activity involved the development and distribution of regulator-compliant products (electronic cash registers (ECRs); point of sale systems (POSs); and enterprise resource planning systems (ERPs)). *About Avatar*, AVATAR TECHS., http://www.avatar-technologies.com/about (last visited May 17, 2016). APIS-IT is the agency for IT system support and information technologies, and it also works in conjunction with the Republic of Croatia and the City of Zagreb. They have developed very complex IT support systems for the City of Zagreb, and the Tax and Customs Administrations of the Ministry of Finance in the Republic of Croatia. *Questions & Answers*, FISCALIZATION.HR, http://www.fiscalization.hr/en/questions-and-answers (last visited May 17, 2016). Allagma Technologies Inc., based in Montreal, Canada, has considerable experience with data encryption in ECRs and POS systems for Revenue Quebec. Although the Quebec model does not send encrypted data to the Ministry of Finance (the data is kept secure on site), Allagma has offered to provide this service if Revenue Quebec moves in this direction. *What Did They Ask*, ALLAGMA TECHS., http://www.allagma.com/what-did-they-ask-STOP.shtml (last visited May 17, 2016).

[201] *See* Richard T. Ainsworth, *Phishing and VAT Fraud in CO2 Permits: The Digital Invoice Customs Exchange Solution*, 77 TAX NOTES INT'L 357, 367 (2015) (discussing the use of state of the art artificial intelligence (AI) over streams of real-time data in Brazil that is sent to the Ministry of Finance for tax fraud risk analysis).

warrant.[202] Section 5 empowers the state to seize, without a warrant, "any cash register or device containing an automated sales suppression device or phantom-ware."[203] Section 1 of the bill states that phantomware is "a programming option embedded in the operating system or hardwired into the electronic cash register that can be used to create a false till, or eliminate or manipulate transaction data before it is entered in the original till."[204]

The South Dakota provision would therefore allow the warrantless seizure of a restaurant's POS system.[205] Seizure of an establishment's POS system could effectively close a business without a warrant.[206] There is not even a requirement in the South Dakota proposal that the operator must have *used* the sales suppression program before seizure.[207]

The Washington statute seems to also overreach, but in a different direction.[208] This overreach reflects a fundamental problem in "bottom-up" traditional audit compliance in the digital world of zappers and phantomware.[209] In this realm of traditional audits, critical audit data has been removed "from the top" forcing considerable reconstruction through estimates.[210] Once technology fraud is suspected the audit needs to quickly move to the top of the technology chain. The audit needs to follow the technology from the local establishment (restaurant), to the technology salesman/distributor, and back to the manufacturer/originator of

[202] *See* H.R. 1051, 2016 Leg., 91st Sess. (S.D. 2016) (prohibiting the use of sales suppression devices).

[203] Section 5 of the Bill sought to amend section 10-59 of South Dakota's Code. *Id.* This bill passed the House Tax Committee 13-1, went through the House floor without a "no" vote, and on February 29, 2016 passed the Senate 35-0. The bill was approved and signed by the Governor on March 10, 2016. *House Bill 1051*, SOUTH DAKOTA LEGISLATURE, http://legis.sd.gov/legislative_session/bills/Bill.aspx?Bill=1051&Session=2016 (last visited May 17, 2016).

[204] H.R. 1051.

[205] *Id.*

[206] Though a business could maintain its operations without the POS system, the loss of the system would be to the business's great detriment. *See With vs. Without*, GREAT LAKES BUS. SYS., http://mjssm.ca/with-vs-without-retail (last visited May 17, 2016) (comparing the benefits of using a POS system versus the difficulty in operating without the POS system).

[207] H.R. 1051.

[208] *See* WASH. REV. CODE § 82.32.290(4)(c)(ii) (2015) (penalizing the manufacturers and sellers of the sales suppression device by imposing high mandatory fines).

[209] *See* ELECTRONIC SALES SUPPRESSION, *supra* note 193, at 5 (describing the problem of reconstructing data when evidence of the transaction has been suppressed).

[210] *See id.* at 10 ("Detailed business process information is needed in order to carry out an audit on the completeness of reported sales.").

the technology as quickly as possible to get a sense of the scope and the true locus of the problem.[211] The enforcing statute needs to support this effort, but the lack of evidence and quantification creates significant challenges. In the realm of combatting sales suppression, statutes tend to border on strict liability, and reach for denials of any right to conduct any business if an individual is tainted with technology fraud.[212] Furthermore, the Washington statute makes the salesmen and manufacturers of suppression devices guarantors of the tax revenue "certified" by the DOR.[213]

Once a zapper or a phantomware program has erased transactional data from a POS system, reconstructing actual tax losses is very difficult.[214] Traditional tax administration audit protocol, for example, falls back on estimates.[215] Under the Washington statute, the DOR is allowed to "certif[y]" those estimates as "loss[es]," and then demand that a statutory guarantor, such as the salesman or the manufacturer, pay those estimates.[216] This kind of overreaching makes the tax system seem unfair. The following questions will arise if Washington State brings an action against InfoSpec: How can the "guarantor" question the DOR's certification if that process is cloaked in taxpayer confidentiality? How does the salesman or manufacturer of a suppression device know the extent of the losses incurred by the state? Can the certification be challenged?

The Washington Statute also points at solutions in another direction.[217] The Revised Code of Washington, section 82.32.290(4)(a) and (b) states:

> (4)(a) 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 . . . .
>
> (b) It is unlawful for any person who has been convicted of violating this section to engage in business, or participate in any

[211] *See id.* at 29 (indicating that by targeting the zapper and phantomware suppliers, "it is possible to obtain client lists and identify the users of the software," as well as hone in on effective auditing and investigating techniques).

[212] *See* § 82.32.290(4)(a)–(b).

[213] § 82.32.290(4)(c)(ii).

[214] *See* ELECTRONIC SALES SUPPRESSION, *supra* note 193, at 5 (discussing the difficulty of finding the hidden transactions).

[215] *See* Theresa Esparza et al., *Sales Tax Audit Best Practices*, TAX ADVISER (July 1, 2012), http://www.thetaxadviser.com/issues/2012/jul/esparza-july.html (explaining that sales tax audits have been utilized to estimate correct amounts of sales taxes).

[216] § 82.32.290(4)(c)(ii).

[217] § 82.32.290(4)(a)–(b).

> business as an owner, officer, director, partner, trustee, member, or manager of the business, unless:
>
> (i) All taxes, penalties, and interest lawfully due are paid;
>
> (ii) The person pays in full all penalties and fines imposed on the person for violating this section; and
>
> (iii) The person, if the person is engaging in business subject to tax under this title, or the business in which the person participates, *enters 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.*[218]

Subsection (iii) is closer to the international standard for dealing with zappers and phantomware.[219] The only problem with the Washington mandate is that it is limited to individuals convicted of violating the statute.[220] It would be far better for this solution to be adopted universally, or even voluntarily, with the support of business groups trying to reduce the incidence of employee theft or franchise holder embezzlement as was the case with the seven IHOP franchises in Ohio.[221]

Nevertheless, even after a limited adoption of a security solution like that in Washington State, it will be possible (after some time in operation) to determine actual losses at the restaurant level when states employ AI to analyze frequency of guests and menu item selections.[222] With these figures, the DOR could reasonably estimate the state's "losses." It might even be possible to use an amnesty at the retail level to "sign-up" volunteer retailers who would "come clean" and help the state measure the losses in exchange for significantly reduced liability. The losses measured by the AI could still be used as a penalty in separate actions against the salesman and the manufacturer.

[218] *Id.* (emphasis added).

[219] *Id.*; *see* Sara Womble, *GTP Director Richard Ainsworth on the $20 Billion Tax Fraud States Are Overlooking*, B.U. LAW NEWS (Nov. 19, 2014), http://www.bu.edu/law/2014/11/19/gtp-director-richard-ainsworth-on-the-20-billion-tax-fraud-states-are-overlooking (providing the example of Rwanda's government, which has required that all business owners must utilize an Electronic Business Machine, which creates and forwards a daily electronic report to the tax administration).

[220] § 82.32.290(4)(a)–(b).

[221] *See Eighteen People Indicted for Roles in $3 Million Schemes Involving Seven IHOP Restaurants*, *supra* note 178 (describing the indictment of individuals who used sales suppression devices to evade taxes).

[222] *See* Ainsworth, *supra* note 201, at 367 (explaining how Smartcloud's AI can identify questionable transactions that indicate fraud).

Electronic sales suppression with zappers and phantomware is an international problem.[223] The fraud technology crosses borders freely.[224] To combat the problem of highly mobile technology fraud, international and domestic tax authorities must share successes and failures, though government overreach during this process is likely to occur. Washington and South Dakota may be going too far in some respects, but if the focus remains on technology, the focus will be further along to suppress sales suppression than the alternative approach through large scale traditional audits.[225] Did the FBI miss a zapper in Chicago? Most likely we will never know. The FBI may have learned that it missed its target in Chicago when it only went after Hu Xiaojun's Chinatown restaurants. There was no case developed against a zapper salesman, the local retail establishment that might have sold them, or the foreign manufacturer that would have exported the fraud technology to the United States.[226]

CONCLUSION

Technology-based sales suppression (zappers, phantomware, and cloud-based manipulation) is a threat to transaction tax revenue that is exceedingly difficult to detect, much less prevent, without the assistance of data security.[227] Although it may be overreaching, in part, the State of Washington is certainly on the right track with its requirement that a "person [convicted of a violation] . . . 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."[228] Through this provision, the State of Washington will most likely bring data security, common in foreign VAT jurisdictions, into a small segment of its retail sales tax enforcement effort.[229] More needs to be done.

[223] *See* Linda K. Enghagen, *Rendering unto Caesar that Which Is Caesar's: States Respond to High Tech Tax Evasion with New Criminal Laws*, HOSPITALITY LAW, at 4 (Dec. 21, 2015), http://hospitalitylawyer.com/wp-content/uploads/Manuscript-25-Enghagen-final.pdf (discussing how countries worldwide have attempted to tackle the problem of sales suppression devices).

[224] *See id.* at 4, 17 (noting that the problem is of international proportions, suggesting that the devices have slowly crossed the borders into other jurisdictions).

[225] *See* ELECTRONIC SALES SUPPRESSION, *supra* note 193, at 3, 4, 38 (arguing that developing better technology is essential to countering the zapper threat).

[226] *See supra* Part II.A.

[227] *See supra* note 20 and accompanying text.

[228] WASH. REV. CODE § 82.32.290(4)(b)(iii) (2015).

[229] *See* Ainsworth, *supra* note 30, at 534 (explaining that VAT jurisdictions have expended considerable resources in combatting tax fraud).

Technology-based sales suppression is global. It is not merely a local phenomenon. It is a business, not the technology hobby of a restaurateur (or other businessman).

Finely tuned suppression techniques follow the distribution network of specific POS systems.[230] Because POS systems are marketed globally so too are the devices that defeat the honest recordkeeping functionality within them.[231] Government auditors have an exceedingly difficult time when the records presented to them are the product of sophisticated manipulation. Reconstruction is difficult.

If manipulation is suspected, there are firms that can detect and re-establish records reasonably well.[232] Then again, the preferred solution is for a taxing authority to adopt solutions like the Sales Recording Module designed by Revenue Quebec,[233] and have it installed by a trusted third-party installer like Allagma Technologies, which assisted the Quebec government.[234]

This course of action, however, only gets the auditing process back to where it was before the technological manipulation. The next necessary step is to stream encrypted transaction data back to the tax administration and have AI, like that being installed on three continents by Smart Cloud, identify where the auditor needs to focus.[235]

[230] *See* Ainsworth, *supra* note 21, at 1018.

[231] *Id.*

[232] *See supra* note 197 and accompanying text.

[233] *Acquisition of an SRM*, REVENU QUEBEC, http://www.revenuquebec.ca/en/entreprises/obligationsparticulieres/restauration/mev/default.aspx (last visited May 17, 2016) (explaining that the sales recording module connects to a POS system and independently records sales transaction data).

[234] *See Ask Us First*, ALLAGMA TECHS., http://www.allagma.com/what-did-they-ask-STOP.shtml (last visited May 17, 2016) (stating that Allagma is "one of the leaders in Canada in POS system implementation and maintenance," and that it will test and implement new technologies for businesses); *Sales Recording Module (SRM)*, SIMPLE MENU RESTAURANT TOUCHSCREEN POINT OF SALE SOFTWARE, http://www.simplemenu.ca/sales-recording-module.cfm (last visited May 17, 2016) ("Allagma is authorised as an official Sales Recording Module (SRM) installer registered with the Revenu Québec.").

[235] *See* Ainsworth, *supra* note 201, at 367 (explaining how Smart Cloud's AI can identify questionable transactions that indicate fraud); Company, SMART CLOUD, http://www.smartcloudinc.com/#!about/ct07 (last visited May 17, 2016).