SALES SUPPRESSION – THE INTERNATIONAL DIMENSION

[Draft March 27, 2016]
65 American University Law Review ____ (2016)
Annual Symposium: Taxing Remote Sales in the Digital Age

Richard T. Ainsworth

Transaction taxes are highly susceptible to technology fraud. This is an inevitable result of our heavy reliance on technology to document the transactions we tax. However, technology can be (and is) manipulated to defeat the collection of these taxes. Both the US retail sales tax (RST) and the value added tax (VAT) are vulnerable to technology-based fraud. This paper concerns sales suppression in the RST, and at the final (retail) stage of the VAT, the retail stage, which is where tax is collected from final consumers.

The modern electronic cash register (ECR)/ point of sale (POS) system is vulnerable. These devices are essentially a computer with programming molded to meet the commercial needs of a particular business. Although these devices are functionally similar across all retail establishments, the data engines that they operate on are not. In the US the dominant databases are MS SQL Server, MYSQL, and MS Access. All are Microsoft products. Unsurprisingly, the popularity of MS Windows some years back made Microsoft the "go to" database provider for developers seeking easy installations. Recently, and notably in Europe, open source POS systems based on Linux databases are becoming the more common. Furthermore, MS databases are not found in the new Apple iOS POS systems, or Square Register, which uses an open source PostgreSQL database. This paper will focus on a particular POS system (Profitek) manufactured in Vancouver, British Columbia (by InfoSpec), which uses an MS SQL server, and which can be purchased with a dedicated sales suppression device (the Profitek Zapper).

The cash register/POS market divides along database lines. The market further subdivides when attributes, like operator language preferences are considered. For example, Chinese restaurants with predominantly Chinese wait staff can be expected to prefer a POS system with Chinese language functionality, but a French restaurant with French-speaking wait staff would prefer a different system.

As a result, the market for POS systems is both niche and international, and so are sales suppression software applications. It is common therefore, to find that the person who sells an ECR/POS system to a business is the same person who can provide the business with the Zapper that will selectively suppress sales recorded in the system. Zappers are not universal. They are system-specific. Zappers and ECR/ POS systems travel together, and in some instances it is the elegance and effectiveness of the Zapper that may actually sell the system.[1] A high quality Zapper responds to suppression

[1] See: Richard T. Ainsworth, *Zappers and Phantomware: A Global Demand for Tax Fraud Technology*, 50 TAX NOTES INTERNATIONAL 1017 (June 23, 2008).

> Zappers and phantom-ware are programs that are added-on (zappers) or factory installed (phantom-ware) to modern ECRs or point-of-sale (POS) systems. Some

requests by going into the ECR/POS database and deleting selective sales, recalculating individual receipts, as well as the taxes due. It will re-order all sales slips, and adjust the internal ledger. It will then tell the operator how much "extra" cash in the till needs to be removed so that bank deposits will match the adjusted sales totals.

An application that effectively manipulates the digital records of a specific POS system will quickly travel across borders with the POS system it was designed for. Very quickly a Zapper initially developed for use in one jurisdiction can become a concern for a neighboring tax authority. Such is the case with the Profitek system sold by InfoSpec Systems Inc., and the zapper that was manufactured by the company to defeat its own recordkeeping functionality.

This paper follows the InfoSpec/Profitek system and its associated zapper as it migrated from the Canadian restaurant market into the US market. It notes the time-gap between the beginning of the audit cycle involved in the Canadian litigation (October 4, 2000) and the beginnings of the first two US investigations of the same company and the same zapper. The FBI is conducting a Chicago investigation (public documents began to appear October 21, 2014), and the Washington State Attorney General is conducting another (public documents began to appear July 13, 2015). If the InfoSpec/Profitek system and its associated zapper crossed the US/Canadian boarder about the time of the Canadian litigation this means that this fraud was present, but remained undetected in the US for approximately fifteen years. This is a long time for a fraud to remain hidden in the US market.

This paper suggests that once a zapper and a vulnerable POS system is identified by one tax authority, there is considerable value in sharing this information with other tax administrations (internationally). Effective solutions need to be shared.

THE CANADIAN FRAUD CASES

Canadian tax authorities brought cases against the company that made the Profitek Zapper (InfoSpec), the salesmen that sold them (David Au, for example), and the restaurants that used them (the Foody Goody Chinese Buffet Restaurant and the Buffet Square in Winnipeg, Manitoba, for example).

---

programs (zappers) have no legitimate purpose other than to facilitate cash skimming at the point-of-sale. Others programs (phantom-ware) may have legitimate (non-fraud) purposes, although these purposes are somewhat obscure (remote from normal business uses). Phantom-ware programs are frequently hidden (in the sense of not being disclosed in user manuals), making their use and even their existence difficult to detect on audit. With training a fraudster can skim cash receipts with phantom-ware as effectively as with a zapper.

Zappers are commonly temporary installations. A CD or memory stick containing a zapper is inserted into a POS system to reconstruct (delete, replace or supplement) ECR records from a network. Without a disclosure by the fraudster (or the distributor, or the zapper-developer) the use of a zapper is nearly impossible to detect. Traces of zapper use however, can be found when fraudsters are not careful.

Salesmen. The case against David Au, an InfoSpec salesperson, is characteristic of this aspect of Canadian enforcement efforts. Mr. Au pleaded guilty (December 16, 2010) to defrauding the public by selling Zappers to restaurant owners so that they could delete cash sales.[2] Mr. Au's sales territory was the Lower Mainland and elsewhere in British Columbia. Between October 4, 2000 and August 28, 2008 Mr. Au sold the Profitek system, along with the Zapper program to 23 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. On average, Mr. Au sold eight Zappers each year over an eight-year span.

At the time of his sentencing 14 of the 23 restaurants he had sold Zappers to had been fully audited. Over $14,000,000 in sales had been suppresses by these establishments, resulting in tax losses of $2,400,000 in federal income and $1,000,00 in Goods and Service Taxes (GST). Mr. Au not only sold the Profitek Zapper, he provided troubleshooting, technical support and servicing related to the Zapper under a services contract.

Mr. Au's Zapper was provided on a CD and cost an additional $1,500, of which $400 represented his commission. The Zapper was commonly paid for in cash and allegedly without a receipt being issued. Mr. Au was sentenced to two years and six months in jail.

Restaurants. InfoSpec is a Vancouver, British Columbia firm, but that did not confine the sales suppression fraud it facilitated to British Columbia. 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, 1,427 miles due east of Vancouver. Both of the eating establishments were Chinese – the Foody Goody Chinese Buffet, and the Buffet Square restaurant.

Aggregate overdue taxes and fines (amounting to $731,986[3]) were imposed after guilty pleas. A portion of this amount was specifically because the restaurants "…

---

[2] *R v. Au* 2011 BCSC 75 (January 24, 2011); 2011 CarswellBC 3862.

[3] The tax amounts evaded, and fines imposed were:

- **Foody Goody Chinese Buffet** – which pleaded guilty to evading:
  - Federal taxes for the years 2006-2008:
    - Income tax of $82,039, and
    - Goods and Services Tax (GST) of $62,581
  - Provincial taxes under the Manitoba *Tax Administration and Miscellaneous Taxes Act* for the years 2007-2009:
    - Income tax and retail sales tax of $106,064.
- **Buffet Square** – which pleaded guilty to evading:
  - Federal taxes for the years 2007-2009:
    - Income tax of $85,000, and
    - Goods and Services Tax (GST) of $47,734
  - Provincial taxes under the Manitoba *Tax Administration and Miscellaneous Taxes Act* for the years 2007-2008:
    - Income tax and retail sales tax of $60,614.

possess[ed] software that [was] designed to suppress electronic sales transaction."[4] These Zapper-specific fines were allowed under Manitoba statute.[5] At the time there was no comparable anti-Zapper law in place at the Canadian federal level.[6] Zapper-fines in each case equaled 100% of the Manitoba sales tax unreported, plus $500.

Manufacturer. The CRA also pursued InfoSpec, the company that manufactured the Profitek Zapper, and which hired the salesmen to sell it in tandem with its POS system. The Profitek POS system is customized for each customer's needs. Right-out-of-the-box, the Profitek system permits transactions to be voided, but does not allow them to be permanently deleted.

The Profitek Zapper (which also needs to be customized) allows a user to take the next step and completely delete selected sales transactions from sales records. As a result, the Profitek system (with a Zapper) will produce records that under-reports income and eliminates records of sales taxes that have been collected.

R v. InfoSpec Systems Inc.[7] is an appeal of the conviction of InfoSpec in the Supreme Court of British Columbia for defrauding the public ~~by~~ through its sales of the Profitek Zapper.[8] The appeal was allowed. The appellate court determined that the sale of a Zapper (standing alone) was not an act that reasonable people would consider to be

---

- **As Shareholders** – the individual shareholders also pleaded guilty to income tax evasion for amounts received as follows:
    - Joe Chung Chee Cheung $146,121
    - Andy Tsz-Wei Chung $53,271
    - Kenneth Wa Chung Ng $45,085
    - Gibson Mei-Chi Lam $46,477.

[4] Canadian Revenue Agency announcement (May 1, 2013) available at: www.cra.gc.ca/convictions. This announcement was formerly at: http://www.cra-arc.gc.ca/nwsrm/cnvctns/mb/mb130501-eng.html (http://www.cra-arc.gc.ca/nwsrm/cnvctns/mb/mb130501-eng.html) but it has recently been archived. A copy of the original posting is available from the author. See also: Winnipeg Restaurants Taste Tax Evasion Fines (May 13, 2013) at: http://www.knowledgebureau.com/index.php/news/category/tax-planning

[5] Manitoba *Tax Administration and Miscellaneous Taxes Act,* C.C.S.M. c. T2 provides at 18.1:

> 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.

[6] In its 21 March 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]." The proposals were effective January 1, 2014 and covered "the use, possession, acquisition, manufacture, development, sale, possession for sale, offer for sale or otherwise making available of [Electronic Suppression of Sales] software". See: Department of Finance, Budget 2013, *Annex 2: Tax Measures: Supplementary Information and Notices of Ways and Means Motions*.

[7] 2013 BCCA 333 (July 17, 2013).

[8] InfoSpec was charged in an indictment with one count of fraud over $5000.00, contrary to s. 380(1)(a) of the Criminal Code, R.S.C. 1985, c. C-46. It was also charged with four counts of evading income tax, contrary to s. 239(1)(b) of the Income Tax Act, R.S.C. 1985 (5th Supp.), c. 1 and four counts of evading Goods and Services Tax, contrary to s. 327(1)(b)(i) of the Excise Tax Act, R.S.C. 1985, c. E-15. InfoSpec was convicted only on the fraud count.

dishonest. As a result, there was neither fraud, ~~not~~ nor attempted fraud in this case. The court indicated:

> 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.[9]

This result is consistent with the tax assessment raised on the Manitoba restaurants considered above. In those cases Zapper-specific penalties were imposed only at the State level.[10] There was no comparable anti-Zapper law at the federal level.[11] As a result Minnesota Zapper-fines in each case equaled 100% of the Manitoba sales tax unreported, plus $500, but the federal fines were $0.00.

Although this decision was effectively overturned by the express prohibition of electronic sales suppression [ESS] software in the March 21, 2013 Budget announcement it has considerable relevance for the US and the states, many of whom find themselves in position analogous to that in the *InfoSpec Systems* case. The Canadian Federal Government proposed and then adopted, "… new administrative monetary penalties and criminal offences under the *Excise Tax Act* (GST/HST) and the *Income Tax Act* to combat [Electronic Sales Suppression] types of tax evasion." The changes were effective January 1, 2014. Offenses now include "… the use, possession, acquisition, manufacture, development, sale, possession for sale, offer for sale or otherwise making available of [Electronic Suppression of Sales] software."[12] The US States that have adopted anti-Zapper legislation largely follow the drafting of the Canadian statute, although the

---

[9] *InfoSpec*, 2013 BCCA 333 (July 17, 2013) at: 21-22 (emphasis added).

[10] Manitoba *Tax Administration and Miscellaneous Taxes Act,* C.C.S.M. c. T2 provides at 18.1:

> 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.

[11] In its 21 March 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]." The proposals were effective January 1, 2014 and covered "the use, possession, acquisition, manufacture, development, sale, possession for sale, offer for sale or otherwise making available of [Electronic Suppression of Sales] software". See: Department of Finance, Budget 2013, *Annex 2: Tax Measures: Supplementary Information and Notices of Ways and Means Motions*.

[12] Department of Finance, Budget 2013, *Annex 2: Tax Measures: Supplementary Information and Notices of Ways and Means Motions*, available at: http://www.cra-arc.gc.ca/gncy/bdgt/2013/qa08-eng.html.

monetary penalties in the US tend to be much lower.

The Canadian federal penalties have a progressive cast.[13] They allow a measured response to electronic sales suppression [ESS], with a clear distinction between the activities of salesmen and those of end-users. They are civil and criminal.

- Monetary penalties:
  - For use, possession or acquisition of ESS software:
    - $5,000 on the first infraction; and
    - $50,000 on any subsequent infraction.
  - For the manufacture, development, sale, possession for sale, offer for sale or otherwise making available ESS Software:
    - $10,000 on the first infraction; and
    - $100,000 on any subsequent infraction.
- Criminal penalties:
  - For the manufacture, development, sale, possession for sale, offer for sale or otherwise making available ESS Software:
    - On summary conviction, a fine of not less than $10,000 and not more than $500,000 or imprisonment for a term of not more than two years, or both; or
    - On conviction by indictment, a fine of not less than $1,000,000 or imprisonment for a term of not more than five years, or both.

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 US. This should have happened roughly sixteen years ago (2000), that is, about the time when the Profitek Zapper was first showing up in Canadian audits.

The most obvious target US jurisdiction for InfoSpec products would be Washington State. Seattle, Washington is 142 miles south of Vancouver, British Columbia, and considerably closer than Winnipeg, Manitoba. Nevertheless, the first public announcement by any US tax authority that the Profitek Zapper may have been in use in the US comes out of Chicago, Illinois, a full 2,202 miles east of the company's head offices (*In the Matter of the Search of Lao You Ju*).[14] The second announcement comes closer to home. It is out of Seattle, Washington (*State of Washington v. John Yin*).[15]

---

[13] The CRA conducted a nation-wide study of sales suppression, which led to these changes. See: 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). A redacted version of this document is available from the author.

[14] *Affidavit for Search Warrant*, US District Court, Northern District of Illinois, Eastern Division, Case 1:14-mc-00571 (October 21, 2014).

[15] *Affidavit for Search Warrant*, State of Washington, King County Superior Court, 15-1-12052-9 SEA (July 13, 2015).

The Chicago investigation is focused on several specific restaurants all owned by the same individual who ~~allegedly~~ may have used the Profitek Zapper. The Seattle investigation initially focused on an alleged Profitek Zapper salesman. The Seattle investigation has developed recently into a specific case against one alleged Profitek Zapper user who allegedly secured the Profitek Zapper from the identified salesman. Other cases in Seattle may follow.

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 bi-lingual advantage Chinese/English (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 B.C. (by TNet) 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*.[16]

Thus, similar to the litigation we have seen in Canada, there are signs that enforcement ~~litigation~~ is beginning in the US against restaurants that allegedly use Profitek Zappers (*Chicago's Search of Lao You Ju*) and the salesmen who are allegedly selling Profitek Zappers to them (*Washington's Search of John Yin*). We have yet to see evidence of an enforcement action against the manufacturer, InfoSpec Systems, but this may be just a matter of time.

U.S. Restaurants. On Tuesday, October 21, 2014 the Federal Bureau of Investigation (FBI) filed with US District Court Judge Jeffrey T. Gilbert of the Northern District of Illinois nine *Applications and Affidavits for Search Warrants*. The FBI wanted to search each of the nine Chicago restaurants owned by Hu Xiaojun.[17] The suspicion

---

[16] http://www.profitek.com/About/ (emphasis added).

[17] Hu Xiaojun is also known as Tony Hu, and as a "celebrity chef" has a sobriquet of the "Mayor of Chinatown" in Chicago. Daniel Gerzina, *Mayor No More? Tony Hu Planning to Sell Most of His Chinatown Restaurants*, EATER CHICAGO (February 16, 2015) *available at*: http://chicago.eater.com/2015/2/16/8046983/tony-hu-selling-most-chinatown-restaurants

was that Hu was systematically under-reporting income. The POS system at each restaurant was INFOSPEC SYSTEMS INC. MODEL PROFITEK RM SYSTEM V10.0.3.[18] It was the common system in use at Chinese restaurants in Chicago's Chinatown.[19]

Alleged violations include (a) conspiracy to commit tax fraud in violation of Title 18, United States Code, Section 371; (b) tax fraud in violation of Title 26, United States Code, Section 7206; and (c) wire fraud in violation of Title 18, Section 1343. No Illinois state violations were referenced.

In each of the nine cases the search warrant was formally *entered* in the court reporting system about six months after submission to the court.[20] The *entry* date was uniformly Monday, April 13, 2015. The *entry* is followed immediately with a *Motion to Seal the Search Warrant*, and an *Order Granting the Government's Motion to Seal.* The *entry* date for each of these documents is again Monday, April 13, 2015. There is a final

---

[18] See: paragraphs 42 & 43 of the *Application and Affidavit for Search Warrant,* in United States of America v. Lao You Ju, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago, Illinois, Docket No. 1:14-mc-00571 (N.D. Ill. Oct 21, 2014).

[19] The *Application and Affidavit for Search Warrant* recites the following at paragraph 43:

> The waiter [at the Lao Sze Chuan – Uptown restaurant on or about December 4, 2013] 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.

In footnote 10 attached to this sentence is the following:

> 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), Loa Beijing (Subject Business 4). Lao Shanghai (Subject Business 5), Loa Ma La (Subject Business 7), and Lao Yunnan (Subject Business 9) are located in the China Square mall.

[20] The nine cases are:

(1) United States of America v. Lao Shanghai, which is located at 2163 South China Place, Suite 1F, Chicago, Illinois, Docket No. 1:14-mc-00570 (N.D. Ill. Oct 21, 2014);

(2) United States of America v. Lao Yunnan, which is located at 2109 South China Place, Chicago, Illinois, Docket No. 1:14-mc-00574 (N.D. Ill. Oct 21, 2014);

(3) United States of America v. Lao Sze Chuan, which is located at 1331 West Ogden Avenue, Downers Grove, Illinois, Docket No. 1:14-mc-00566 (N.D. Ill. Oct 21, 2014);

(4) United States of America v. Lao Sze Chuan, which is located at 2172 South Archer Avenue, Chicago, Illinois, Docket No. 1:14-mc-00567 (N.D. Ill. Oct 21, 2014); (4) United States of America v. Lao Sze Chuan, which is located at 4832 North Broadway Street, Chicago, Illinois, Docket No. 1:14-mc-00568 (N.D. Ill. Oct 21, 2014);

(5) United States of America v. Lao Sze Chuan, which is located at 2172 South Archer Avenue, Chicago, Illinois, Docket No. 1:14-mc-00567 (N.D. Ill. Oct 21, 2014), Court Docket;

(6) United States of America v. Lao Ma La, which is located at 2017 South Wells Street, Chicago, Illinois, Docket No. 1:14-mc-00572 (N.D. Ill. Oct 21, 2014);

(7) United States of America v. Lao Hunan, which is located at 2230 South Wentworth Avenue, Chicago, Illinois, Docket No. 1:14-mc-00573 (N.D. Ill. Oct 21, 2014);

(8) United States of America v. Lao Beijing, which is located at 2138 South Archer Avenue, Chicago, Illinois, Docket No. 1:14-mc-00569 (N.D. Ill. Oct 21, 2014);

(9) United States of America v. Lao You Ju, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago, Illinois, Docket No. 1:14-mc-00580 (N.D. Ill. Oct 24, 2014) and United States of America v. Lao You Ju, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago, Illinois, Docket No. 1:14-mc-00571 (N.D. Ill. Oct 21, 2014).

entry in each of the nine cases – a final notice that each warrant was *Returned Executed.* The *entry* date is again Monday, April 13, 2015, although the execution date in each case is uniformly Friday, October 24, 2014.

There is one exception. The warrant in *United States of America v. Lao You Ju, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago Illinois* was issued twice. Once on October 21, 2014, and a second time on the date that each of the initial 9 warrants were *Returned Executed*, Friday, October 24, 2014. It appears that there may have been some difficulty with the execution of the first warrant, and the FBI asked the court for a second. The second warrant was *Returned Executed* on November 7, 2014. The use 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.[21] A reporter for the Chicago Sun-Times found the court's publication of the first warrant. This may have resulted in an unauthorized disclosure of confidential taxpayer information.

On Monday, April 27, 2015 the Chicago Sun-Times ran an article, *Feds Went to Chinatown looking for Food – and Fraud*. The basis of the article is the FBI allegations in the first search warrant on the Lao You Ju restaurant.[22]

In 110 pages the affidavit sets out the major arguments of ~~the~~ a tax case against all nine restaurants. The analysis ~~in all cases~~ revolves around an apparent "second set of books" constructed from intercepted e-mail attachments which are compared with the filing position on federal income tax returns and Illinois sales tax returns. Daily bank deposits are used to provide further contrast.

The FBI shows probable cause by demonstrating for example that the Lao Sze Chuan – Downers Grove restaurant apparently (and allegedly) suppressed roughly 40% of its sales from 2008-2010. The FBI compares the manager's spreadsheets of sales with the gross receipts filed on the federal corporate return.[23] The following chart appears at paragraph 55.

Lao Sze Chuan – Downers Grove restaurant

Year	Manager's Spreadsheet itemizing sales	IRS Form 1120 Gross receipts	IRS/annualized spreadsheet
2008	$938,461 (Feb – Dec)	$604,709	59.07%
2009	$2,066,382	$656,866	61.16%
2010	$722,212 (Jan – Aug)	$797,713	68.87%

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

[22] Personal communication with Jon Seidel, October 25, 2015 indicating 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, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago Illinois* search warrant filed on October 21, 2014. Mr. Seidel was of the impression that all of the warrants were publicly available. If so, that is no longer the case.

[23] Application and Affidavit for a Search Warrant, *United States of America v. Lao You Ju, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago Illinois,*

The FBI is clearly interested in cash sales. The strong suggestion in the warrant is that this category of sales had been systematically suppressed in each of the nine restaurants. 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.

From the tentative "second set of books" it constructs the FBI breaks down the amounts received into cash and credit card transactions. When these figures are compared with the monthly Illinois sales and use tax returns (Forms ST-1 and E911 Surcharge Returns), it appears that the tax returns are uniformly lower, suggesting suppression. To make its point even clearer the FBI further aligns monthly bank deposit data. For example, the average monthly deposit for Lao Sze Chuan was $230,812, but the average monthly receipt reported to the government was $214,995.[24] 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.[25] In addition, the bank records show that for month-after-month and for restaurant-after-restaurant no cash is deposited into corporate bank accounts, suggesting that a large portion of the (allegedly) suppressed sales are the cash transactions. The bank deposits on record are primarily credit card merchant account deposits.

There is no mention of a Profetek Zapper in the search Warrant.[26] However, given the presence of the Profitek POS system in each of the nine restaurants, knowledge of the prior litigation in Canada,[27] and the passage of anti-zapper legislation in Illinois, effective January 1, 2014, it is entirely possible that the real focus of the FBI's Search Warrant is to find a Profitek Zapper in Chicago.[28] If a Zapper was found by the FBI, and if it was used after January 1, 2014, then the state charges against Hu Xiaojun could be criminal.

On August 16, 2013 the Governor of Illinois signed into law Public Act 098-0352 which added the following provision to the law:

> 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.[29]

Under Illinois law, a class 3 felony is punishable by two to five years' imprisonment. An "extended term" class 3 felony is punishable by five to ten years in prison.[30]

---

[24] See: paragraph 93.
[25] See: paragraph 113.
[26] CBS Chicago, *Feds Raid Celebrity Chef Tony Hu's Restaurants in Tax Fraud Probe*, CBS (April 28, 2015) *available at*: http://chicago.cbslocal.com/2015/04/28/feds-raid-celebrity-chef-tony-hus-restaurants-in-tax-fraud-probe/
[27] *R v. Au,* 2011 BCSC 75 (January 24, 2011); the Foody Goody Chinese Buffet, and the Buffet Square restaurant guilty pleas of May 1, 2013; *R v. InfoSpec Systems Inc*., 2013 BCCA 333 (July 17, 2013)
[28] The Search Warrant only references that the State of Illinois Department of Revenue Publication 113 (October 2011), *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. See paragraph 41.
[29] 35 ILCS 105/14
[30] 730 Ill. Comp. Stat. §5/5-4.5-40.

Each of the ten cases (one each for Hu Xiaojun's nine restaurants, and a tenth additional case for the second warrant for the *Lao You Ju* restaurant) are now formally *Closed* in court records. There is no tax case in the public record. The FBI actions are considered "mysterious" in the local media.[31]

Hu Xiaojun is in the process of selling his restaurant and moving out of state. Lao Beijing was sold in January 2015. 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.[32]

The FBI was aware that Hu Xiaojun owned restaurants outside of the Chicago area, notably in Milford, Connecticut, and Las Vegas, Nevada.[33] No search warrants were issued at these locations. This is peculiar in light of the search warrant's comprehensive assessment of how Hu Xiaojun (allegedly) coordinated the tax manipulations remotely (through e-mail correspondence with managers and bookkeepers). There was concern with whether or not the InfoSpec systems worked with "cloud-based computing."[34]

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)."
>
> 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.[35]

---

[31] Staff reporters, *Mystery Behind Chinatown Raids Remains*, EATER CHICAGO (October 27, 2014) *available at*: http://chicago.eater.com/2014/10/27/7079837/mystery-behind-chinatown-raids-remains and Peter Frost, *What's Happening with Chinatown's Tony HU?* CRAIN'S CHICAGO BUSINESS (February 28, 2015) a*vailable at*: http://www.chicagobusiness.com/article/20150228/ISSUE01/302289982/whats-happening-with-chinatowns-tony-hu

[32] Daniel Gerzina, *Mayor No More? Tony Hu Planning to Sell Most of His Chinatown Restaurants*, EATER CHICAGO (February 16, 2015) *available at*: http://chicago.eater.com/2015/2/16/8046983/tony-hu-selling-most-chinatown-restaurants

[33] See: paragraph 6 note 2of the *Application and Affidavit for Search Warrant,* in United States of America v. Lao You Ju, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago, Illinois, Docket No. 1:14-mc-00571 (N.D. Ill. Oct 21, 2014).

[34] *Id*., at paragraph 45, note 13. Cloud-based manipulation has been found in other jurisdictions. Richard T. Ainsworth, *Sales Suppression as a Service and the Apple Store Solution*, 73 STATE TAX NOTES 343, 351-2 (August 4, 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).

[35] Peter Frost, *Tony Hu sells Lao Beijing*, CRAIN'S DINING CHICAGO (February 2, 2015) *available at*: http://www.chicagobusiness.com/article/20150202/BLOGS09/150209967/tony-hu-sells-lao-beijing

US Salesmen. Unlike the FBI in Chicago, when the Washington State Attorney General's Office became aware that restaurants in their jurisdiction were using InfoSpec's Profitek POS system with the Profitek Zapper, they secured a search warrant to investigate the salesman.[36] The search warrant was approved, and sealed. Much like the situation in Chicago, when the warrant was unsealed the local press became aware of the investigation. It was not long before reporters were writing on the investigation. Articles were published and investigative TV coverage of the story began.

The Washington Department of Revenue made a criminal referral to the Attorney General's Office. It was told by a taxpayer who was using a Profitek POS system that the Profitek Zapper had been used with the POS system "for many years" to suppress sales.[37] The taxpayer identified John Yin as the individual who sold the Profitek POS system, but "… did not admit that John Yin sold the accompanying Revenue Suppression USB drive …"[38] However, the affidavit makes it clear that "… this USB only works with Profitek POS Systems."[39]

The stage is now set for a search warrant. John Yin was the "… only licensed reseller of Profitek Software in Washington State …"[40] so, a warrant was needed to determine if Mr. Yin sold this Profitek Zapper. Has he sold Zappers to others? If so, how many and to whom? The Canadian *Au* case made it clear that Profitek POS salesmen were instructed to sell Profitek Zappers to clients as a service. When they did their commission was $400.

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. The search would be for copies of the Profitek Zapper, the customer list of all current and former Profitek clients, and income records. In the classic Zapper salesman case it is common for the salesman to also be an installer, a technology troubleshooter, and an all-purpose sales suppression service provider for Zapper customers under a services contract. The dominance of this "service model" is the real lesson learned from the undercover sting operations in New York which targeted sales suppression.[41]

The most well-known Zapper-salesman case dates back to 2002-03, and involves Michael Roy, a software developer with the Resto Terminal POS supplier in Quebec, his two sons, and 28 restaurants doing business under the name Stratos. 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.

---

[36] *Affidavit for Search Warrant, State of Washington v. John Yin,* King County Superior Court (July 13, 2015) Docket no. 15-613 (15-1-12052-9 SEA)
[37] *Id.*, at 3.
[38] *Id*., at 3.
[39] *Id.*, at 3.
[40] *Id.*, at 3.
[41] Richard T. Ainsworth, Sales Suppression as a Service and the Apple Store Solution, 73 State Tax Notes 343 (August 4, 2014).

Mr. Roy designed and developed a very effective Zapper that was specific to the Resto Terminal POS. 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. Aggregate fraud penalties assessed against the Roys were $1,064,459.[42] Statutory penalties for manufacture or sale of sales suppression technology applied. Income from the Roys "consulting business" was not reported, and (of course) sales of the Zapper were also not reported. Transactions were in cash. Essentially, the Roys designed their "business" to receive a percent of the suppressed sales at each location they "serviced."

Revenue Quebec published the aggregate fraud penalty and tax assessment against the first 10 Stratos restaurants ($1,816,070.90).[43] Final restaurant totals were not released at the time the Roys were sentenced. Revenue Quebec's press releases were not as interested in the restaurants as they were in the Roys. 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.

The Washington Attorney General and the Washington Department of Revenue seem to have learned the lesson of the Roys. The Washington State search warrant was issued against Mr. Yin, the Profitek salesman.[44]

This was not a lesson that the FBI had internalized in Chicago. Rather than pursuing the business that sold the Profitek POS system to Hu Xiaojun in Chicago, or the salesman who was directly involved in the sales, the FBI conducted searches of nine area restaurants suspected of using the Profitek Zapper. The FBI knew the name of the Profitek retailer in Chicago (Vision I Computers Inc.) and it knew the name of the salesman assigned to Hu Xiaojun's account (Wah Chu). No search warrants, civil or criminal cases can be found in the Chicago area involving either Vision I Computers Inc. or Mr. Wah Chu. The *Affidavit* recites the knowledge that the FBI had:

> Agents again observed [at the Lao Sze Chuan – Uptown] the "INFOSPEC SYSTEMS INC. MODEL PROFITEK RM SYSTEM V10.0.3" markings in the lower right hand corner of the monitor. The

---

[42] Revenue Quebec, News Release, Fines of more than One million dollars – A Father and his Two Sons convicted for Tax Evasion in connection with the Zapper (May 2, 2003) *formerly available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/02mai.asp (in French only, translation on file with author, *currently archived by Revenue Quebec*). See also: *Stratos Pizzeria - Amende de plus d'un million pour fraude fiscale en restauration* LA PRESSE MONTREAL (May 2, 2003) at A14 *available at*: http://collections.banq.qc.ca:81/lapresse/src/pages/2003/P2003-02/05/03/A/82812_20030503LPA14.pdf

[43] The available breakdown is: $429,179.07 (GST) + $492,023.11 (PST) + $214,589.55 (federal penalties) + $625,028.89 (provincial penalties) + $55,250.28 (judicial fees). Revenue Quebec, News Release, All Stratos Restaurants Convicted of Fraud in Connection with the use of a Zapper (Mar. 18, 2003) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2003/18mars.asp (in French only, translation on file with author).

[44] The Washington Attorney General alleged probable cause that 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.

> waiter then 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. [footnote 10 indicates that 5 of Hu Xiaojun's 9 restaurant are also located in the Chinatown mall: Lao Sze Chuan; Lao Beijing; Lao Shanghai; Lao Ma La; and Lao Yunnan].
>
> … an August 23, 2013 email from wah@visioni.com to tgguschina@gmail.com under the subject line "Proposals for 2 Restaurant POS" that included revised quotes for POS systems for the Lao Beijing (subject Business 4) and Lao Sze Chuan – Chinatown (Subject Business 2) restaurants. The body of the email included the following statement: " It will be the same setup as your Broadway location …" [footnote 12 inserted here indicates that this is a reference to the Lao Sze Chuan – Uptown restaurant at which the agents had previously observed were using the Profitek InfoSpec system]. The email had five attachments, including two proposals for POS systems for the Lao Beijing restaurant and two proposals for the Lao Sze Chuan – Chinatown restaurant. These four proposals were from a company identified as Vision I Computers, Inc. 2416 S. Canal Street, Chicago, IL 60616. … a January 14, 2014 email from wah@visioni.com … included a signature block of an individual named Wah Chu …
>
> Based on my training and experience and the training and experience of investigating agents with whom I have consulted, 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.[45]

The FBI does not seem to appreciate that the core problem in technology-assisted sales suppression are the salesmen, installers, and other "service providers," not the individual users. But even if the FBI is right, and the problem is the individual user of suppression technology, why did it not search the five other restaurants owned by Hu Xiaojun outside of Chicago's Chinatown.[46] If Hu Xiaojun is suppressing sales in nine Chinatown restaurants, why wouldn't he be suppressing sales in the five more remote restaurants? Technology-assisted sales suppression is not geographically constrained. It moves across and among jurisdictions both domestically and internationally. To stop this fraud the FBI needed to think like a technology person, not like a restaurateur who is skimming sales when he is at the cash register.

The FBI appears to think that sales suppression occurs locally – where the owner is located. The FBI appears to believe that the person engaged in the suppression fraud

[45] Paragraphs 43, 46-8 of the *Application and Affidavit for Search Warrant,* in United States of America v. Lao You Ju, which is located at 2002 South Wentworth Avenue, Unit 100, Chicago, Illinois, Docket No. 1:14-mc-00571 (N.D. Ill. Oct 21, 2014).

[46] Paragraph 6, footnote 2 of the *Application and Affidavit for Search Warrant,* lists 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.

must be present where the records are manipulated. Why else would the FBI memorialize a discussion with a Profitek employee who explained that the data for each restaurant is preserved on a local server? The *Affidavit* indicates:

> Investigating agents contacted an employee of Profitek familiar with the systems observed in Lao Hunnan (Subject Business 8) and Lao Sze Chuan – Uptown (Subject Business 3). The Profitek employee with whom the agents spoke explained that the subject POS system is based on a Microsoft SQL database and that the version of the InfoSpec system maintains a history of the sales transactions logged into the system on a server that is integrated into the point of sale system.

The *Affidavit* inserts footnote 11 at this point. It states:

> The Profetek employee explained that the InfoSpec system did not support cloud-based computing. Accordingly, data from each point of sale system is stored on a local server and not a remote system.

The use of a local server in each of Hu Xiaojun's fourteen restaurants does not mean that Hu Xiaojun could not have manipulated the records of any of those establishments remotely with a Profitek Zapper. If the 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.

In fact the FBI is currently involved in another case of sales suppression in seven IHOP restaurants in Ohio where the manipulation of records on a MICROS POS system was performed remotely (from the owners bedroom) with "Team Viewer" software.[47] The *Indictment* in that case states at paragraph 47:

> Tarek Elkafrrawi and M.K. directed the Point of Sale system remotely through the use of software that gave them full access and control of the Point of Sale system from their homes. Since approximately 2010-2011, Tarek Elkafrawi and M.K. have used software called "Team Viewer." This software was installed on the home computers of Tarek Elkafrawi and M.K. in 2010 and 2011, respectively, shortly after the latest MICROS system was installed on all IHOP computers.[48]

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 that spread the fraud. The restaurants or other retailers are of secondary importance.

Perhaps the Attorney General took the approach he did because the Washington statute directs the enforcement community to aggressively go after the salesmen. Like

---

[47] Federal Bureau of Investigation, Cleveland Division, US Attorney's Office, *Eighteen People Indicted for Roles in $3 Million* (May 23, 2012) *available at*: http://www.fbi.gov/cleveland/press-releases/2012/eighteen-people-indicted-for-roles-in-3-million-schemes-involving-seven-ihop-restaurants *Schemes Involving Seven IHOP Restaurants*

[48] United States of America v. Tarek Elkafrawi et al. District Court for the Northern District of Ohio, Western Division (case number 3:12CR 262).

Quebec, but unlike Illinois, Washington has penalty provisions that directly target the people who sell, install and service Zappers.

The Revised Code of Washington (RCW) at 82.32.290 dealing with Unlawful Acts – Penalties states (emphasis added):

> (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. …
>
> (4)(c)(ii) Any person violating the provisions of this subsection by *furnishing* an automated sales suppression device or phantom-ware to another person or by *updating* or *repairing* another person's automated sales suppression device or phantom-ware is, in addition to the punishments prescribed in chapter 9A.20 RCW, subject to a *mandatory fine* fixed by the court in an amount equal to the greater of *ten thousand dollars*, the *defendant's gain* from the commission of the crime, or the *state's loss* from the commission of the crime.
>
> For purposes of this subsection (4)(c)(ii), "loss" means the total of all taxes, penalties, and interest *certified by the department* to be due, as of the date of sentencing, as a result of any violation of the provisions of this subsection by a person using the automated sales suppression device or phantom-ware obtained from, or updated or repaired by, the defendant, which results in the defendant's conviction for violating the provisions of this subsection.

It is particularly RCW 82.32.290(4)(c)(ii) with its emphasis on furnishing, updating or repairing sales suppression software that is the key. It subjects an ~~this~~ individual to a penalty that is the greater of:

- $10,000
- the defendant's gain, or
- the state's loss

In the third prong, the Department of Revenue must *certify* the state's loss because it would not otherwise be publicly known due to taxpayer confidentiality rules. In the *Au* case for example, the state's loss from his sale of Profitek Zappers was $2,400,000 in federal income tax and $1,000,000 in Goods and Services Tax, and this was after audits had been completed on only 14 of the 23 firms Mr. Au ~~he~~ had sold Zappers to. Effectively, the third prong of the Washington penalty provision would make Mr. Au (and the manufacturer) a guarantor of total taxes lost.

If Mr. Au had been prosecuted under the Washington statute and if the final penalty is to be determined under the third prong of RCW 82.32.290(4)(c)(ii) his penalty would be calculated by aggregating the deficiencies of all 23 firms he sold Profitek Zappers to, and then 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.

One final note on the Profitek Zapper; the Zapper provided by Mr. Au was on a CD, and the Zapper provided by Mr. Yin was on a thumb drive. The current version of the Profitek Zapper is available online, and does not need to be installed locally. It can be accessed over the internet with a browser. In addition, Profitek offers an Online Ordering Module (OLO), which Profitek suggests can be used to enhance sales via the internet.[49] In this case both sales records and the Zapper would be located in the cloud, and considerably more difficult for an auditor to find.

CONCLUSION

Technology-assisted sales suppression fraud differs fundamentally from traditional tax fraud. The technology at the heart of this fraud needs to be dealt with directly, and most likely with counter-technology. The path we are on is an inevitable one.

We need to have either: (a) technology that efficiently reconstructs digital transaction records that have been suppressed,[50] or (b) security (technology that encrypts and saves) digital records at the time of their creation. The solution adopted in most jurisdictions is (b). Most effective enforcement regimes involve real-time secure transmission of encrypted transactional data to a central location[51] where high quality risk analysis can be performed with artificial intelligence (AI) in a deployment that assures taxpayer privacy.[52]

---

[49] See the assessment of Profitek in this software review: http://point-of-sale.softwareinsider.com/l/230/Profitek

[50] For example, a company called *iSeekDiscovery,* which is in the forensic data recovery and eDiscovery business promises to be able to recover suppressed data remotely. See: http://www.cybercrime-forensics.com/#!iseekdiscovery/c1naj

[51] A number of international companies specialize in data encryption of POS systems responding to government ficalization regulation. They include, for example, Data Tech International Ltd. (www.dti.rs) 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. Avatar Technologies Ltd, (www.avatar.ci) 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); enterprise resource planning systems (ERPs)]. APIS-IT d.o.o. http://www.fiscalization.hr/en/questions-and-answers The agency for IT system support and information technologies, APIS-IT ltd. is a company which works closely 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. Allagma Technologies Inc. (www.Allagma.com) 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.

[52] Richard T. Ainsworth, *Phishing and VAT Fraud in CO2 Permits: The Digital Invoice Customs Exchange Solution*, 77 TAX NOTES INTERNATIONAL 357, 367 (January 26, 2015) discussing the use of state of the art AI over streams of real-time data in Brazil that is sent to the Ministry of Finance for tax fraud risk analysis.

What we need to be concerned about is legislation like that in South Dakota allowing the DOR to seize automated sales suppression devices or Phantomware without a warrant. Section 5 of House Bill 1051 states:

> An automated sales suppression device or phantom-ware or any cash register or device containing an automated sales suppression device or phantom-ware is contraband and may be seized without a warrant by the secretary, agents or employees of the secretary, or any law enforcement officer of this state. The disposition of any property seized under this section shall be conducted pursuant to chapter 23A-37.[53]

Because 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,"[54] this provision would allow the warrantless seizure of a restaurant's POS system, for example. This would effectively close a business without a warrant. There is not even a requirement in the South Dakota proposal that the operator has *used* the sales suppression program before seizure.

The Washington statute seems to overreach also, but in a different direction. The Washington overreach points to the fundamental problem of traditional audit compliance regimes in the world of Zappers and Phantomware. Washington makes the salesmen and manufacturers of suppression devices a guarantor of the tax revenue "certified" by the DOR.

Once a Zapper or a Phantomware program has erased transactional data from a POS system, it is very difficult to reconstruct actual tax losses. We may know that a Zapper was used, but how much was taken? Traditional tax administration audit protocol falls back on estimates. Under the Washington statute the DOR is allowed to "certify" those estimates as "losses," and then demand that a statutory guarantor (the salesman, or the manufacturer) pay those estimates. This kind of overreaching makes the tax system seem unfair. 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? This is a question that will come front and center, if and when an action commences in Washington against InfoSpec.

The Washington Statute also points at solutions ~~in another direction also~~. This portion of the statute ~~direction~~ is closer to the international standard for dealing with Zappers and Phantomware. RCW 82.32.290(4)(a) & (b) states (emphasis added):

---

[53] House Bill 1051, section 5 which seeking to amend SD Codified L §10-59. 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. It was signed into law by the Governor on March 10, 2016. There is similar legislation pending in Minnesota HB 1825, *available at*: https://legiscan.com/MN/text/HF1825/id/1196718/Minnesota-2015-HF1825-Engrossed.pdf

[54] South Dakota House Bill 1051, section 1(3).

(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 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*.

What this provision does in (iii) is to mandate the international standard. The only problem with the Washington mandate is that it is limited to individuals convicted of violating the statute. 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.

Nevertheless, even after a limited adoption of a security solution in a state like Washington, it will be possible (after some time in operation) to determine actual losses at the restaurant level when AI is allowed to analyze frequency of guests and menu item selections. 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 a greatly reduced liability. The measure of losses determined by the AI could still be used a penalty in a separate actions against the salesman and the manufacturer.

Electronic sales suppression with Zappers and Phantomware is an international problem. The fraud technology crosses borders freely. We should be anxious to learn and share successes and failures. We should expect overreaching and pushback as we work out answers to this problem. Washington and South Dakota may be going too far in some respects, but if the focus remains on the technology we will be further along in our efforts to suppress sales suppression than if we engage in large scale traditional audits. The FBI may have learned that it missed its target in Chicago when it only went after Hu Xiaojun's Chinatown restaurants and missed the Zapper salesman, the local retail establishment that sold them and the foreign manufacturer that exported the fraud technology to the US.