10-16-2017

The Technology Requirements of the First Electronic Monitoring Agreement in US for Zappers, Phantomware, and Other Sales Suppression Devices

Richard Thompson Ainsworth
Boston University School of Law

Robert Chicoine

BU School of Law

THE TECHNOLOGY REQUIREMENTS OF THE FIRST ELECTRONIC MONITORING AGREEMENT IN US FOR ZAPPERS, PHANTOMWARE, AND OTHER SALES SUPPRESSION DEVICES

Boston University School of Law
Law & Economics Series Paper No. 18-15

July 2018

Richard T. Ainsworth
Robert J Chicoine

Boston University School of Law

Electronic copy available at: https://ssrn.com/abstract=3212262

THE TECHNOLOGY REQUIREMENTS OF THE FIRST ELECTRONIC MONITORING AGREEMENT IN US FOR ZAPPERS, PHANTOMWARE, AND OTHER SALES SUPPRESSION DEVICES

Richard T. Ainsworth
Robert J Chicoine

On August 30, 2017, a plea was entered in the case of case of *State of Washington v. Wong*, Wash. Super. Ct., No. 16-1-00179-0, and as a result the first electronic monitoring agreement of sales transactions in the US (the "Monitoring Agreement") was legislatively imposed on a retail business.

The Monitoring Agreement was negotiated between the State of Washington Department of Revenue (the "WA DOR") and the taxpayer over a period of several months and is comprised of two parts: the basic agreement, which covered the obligations and rights of the parties, and an appendix, which defines the scope of sales information to be monitored, and the technological means by which that information is gathered, secured from manipulation, and transmitted electronically to the DOR.

This paper focuses upon the technology requirements in this first-of-its-kind electronic monitoring agreement between a revenue authority and a taxpayer in the US. The basic agreement, which not only delineates the specific obligations of the taxpayer to provide the WA DOR with real time access to retail sales information, but also sets out various protections for the taxpayer, such as limitations on possible allegations of breach, rights to cure, and administrative adjudication of material disputes, all designed to protect the taxpayers right to continue in business, will be discussed in a separate follow-up article.

The problem this agreement seeks to address is sales suppression at the point of sale (POS). Not traditional sales suppression, or skimming with double tills, but sophisticated technology-assisted skimming. The specific targets are programs known as Zappers and Phantomware, which are used with POS systems or electronic cash registers (ECRs) to manipulate sales figures. Once installed, an electronic monitoring system will solve other types of suppression, like internal theft, open till, misuse of legitimate functions such as training mode, or voided transactions, but those frauds are not its immediate target.

Electronic monitoring of retail sales by taxing authorities is not unusual outside of the US. It has been used for decades to counteract Zappers and Phantomware, but never before has it been used in the US.[1]

Perhaps the best analogy to electronic monitoring of sales is the use of video cameras installed by businesses to monitor inventory theft. Electronic monitoring of POS systems or ECRs is simply using technology to watch in real-time for indications of suppression or

[1] Richard T. Ainsworth & Urs Hengartner, *Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud with Technology*, 57 CANADIAN TAX JOURNAL 715 (2009)(discussing anti-suppression systems in Quebec, Sweden, Greece, Brazil, Argentina, Belgium, Germany and Italy among others).

Electronic copy available at: https://ssrn.com/abstract=3212262

manipulation of the sales data that allows the sales tax paid by customers to go unreported by the shop owner.

ONLY IN WASHINGTON[2]

Twenty-five states have laws expressly prohibiting electronic sales suppression such as Zappers, Phantomware, and other suppression devices.[3] In *Wong* (the "Taxpayer"), the WA DOR prosecuted the use of a Profitek Zapper.[4] Other investigations continue to occur in Washington for suspected use of Zappers and Phantomware.

Financial penalties and criminal sanctions, including incarceration, are the punishments meted out in each of the twenty-five states. Washington's anti sales suppression statute is unique in two important respects: 1) it prohibits engaging in future business activity after conviction, and 2) a taxpayer is compelled to find an electronic monitoring solution which must be "acceptable to the department."

There is a three-part exception to the business prohibition provision, one part of which requires the Taxpayer to pay the tax liability "lawfully due" and another requires the installation of an electronic monitoring "acceptable to the department". The Washington statute provides:

> (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.[5]

Aside from the uncertainty of trying to timely satisfy requirements determined, in large part, by the discretion of the WA DOR i.e. the amount of tax legally due, the monitoring method acceptable to the WA DOR, and the terms of an agreement which the WA DOR will actually accept, practical technologic issues render the requirements of this provision far more difficult than they may first appear.[6]

---

[2] Details of this case in the context of the Washington statute are considered in Richard T. Ainsworth & Robert J. Chicoine, *Zappers, Phantomware and Other Sales Suppression Software in the State of Washington*, STATE TAX NOTES (forthcoming).

[3] A Zapper places sales suppression programming on a removable CD or memory stick, whereas Phantomware is suppression programming installed on a ECR/POS system. Their function is the same.

[4] For a discussion of the Profitek Zapper see: Richard T. Ainsworth, *Sales Suppression: The International Dimension*, 65 AMERICAN UNIVERSITY LAW REVIEW 1241 (2016).

[5] RCW 82.32.290(4)(b)

[6] The authors perceive a number of legal challenges to Washington's sales suppression statute, which are beyond the scope of this article.

Electronic copy available at: https://ssrn.com/abstract=3212262

There are two major hurdles: (a) the *security provider* should be independent of all point of sale *equipment providers* (the POS manufacturer, ECR manufacturer, printer manufacturer, or any distributors, or installers of this equipment), and (b) the third-party security provider needs to secure the *permission of a POS/ECR manufacturer to integrate* with the POS/ECR software, which will likely not occur.

Both of these difficulties have the same source. Almost all Zappers, Phantomware and other suppression devices are manufactured, sold, or provided to retailers by a member of the equipment-provider supply chain. It is rare today to find the manufacturer of a POS system directly producing and selling suppression software. It is far more common to find systems that are "open" to software "enhancements" of many kinds, and the real manufacturer of the Zapper or other device is the distributor, salesman, or system installer who has an interest in maximizing sales of the manufacturer's units to customers who are seeking suppression capabilities. This is simply how this marketplace works, and how these supply chains sell their product.

The involvement of the equipment supply chain in spreading technology-based sales suppression is common knowledge and can be documented globally. In the U.S., the clearest example is illustrated in New York where the Department of Taxation and Finance conducted a series of undercover sting operations. 95% of the sales people showing up to provide new ECR/POS systems to the undercover agents who were posing as restaurateurs offered suppression technology to help sell their equipment.[7]

Unlike Washington, which shifts the burden of finding a solution to the Taxpayer, all other jurisdictions that mandate electronic monitoring list on their web sites the "acceptable solutions." These jurisdictions compel ECR/POS equipment providers operating within their jurisdiction to cooperate with and allow the integration of the third-party security solutions. Take for example Quebec.[8] Revenue Quebec posts the name and model number of all acceptable ECRs and POS systems.
See: http://www.revenuquebec.ca/en/entreprises/obligationsparticulieres/restauration/systemes/default.aspx

With no regulations specifying what is and is not "acceptable," the Washington taxpayer must find, propose, and negotiate an acceptable solution, or go to the expense of challenging the statute and risk the right to continue business operations. Given that the international standard involves finding a third-party security provider who can integrate with an unrelated provider of ECR/POS equipment, the challenge is considerable.

---

[7] For a discussion of the sting operations see: Richard T. Ainsworth, *Sales Suppression as a Service, and the Apple Store Solution*, 73 STATE TAX NOTES 343 (August 4, 2014).

[8] There is no easy way to say this, but when it comes to anti-sales suppression technology the State of Washington should not be so far behind Quebec. Washington should at least be comparable. In Quebec, it is possible to visit any local cash register supplier to purchase a fully compliant POS. It does need to be registered and activated by the Quebec Revenue, but there is not much more to it for the taxpayer.

Electronic copy available at: https://ssrn.com/abstract=3212262

In the US context, we need to keep in mind the reality shown from the New York stings. This is a measure of the market. To stay in business a Washington taxpayer who is convicted under the statute is required to secure an arrangement with ECR/POS equipment providers that runs against established business practices. The practice is that manufacturers tend to make equipment that *can be* manipulated, and distribute it through salesmen and installers who are inclined to increase sales *by finding add-on technology* that will perform the data manipulations demanded by an owner. This gives the Taxpayer, who is searching for anti-suppression technology, a difficult problem. He needs to negotiate permission for a third-party security company to access and integrate with the manufacturer's ECR/POS system.

Getting access to proprietary systems is difficult, particularly a small restaurant. Although it may not be as difficult for a multi-location restaurant chain that can hold out the promise of purchasing many systems in exchange for cooperation on security features.

Because we were successful in negotiating agreements with both ECR/POS providers and third-party security providers, as well as the Washington State Department of Revenue and the Attorney General, the taxpayer and the defense team believe that it is in the interest of the community to publish the technology requirements within our Electronic Monitoring Agreement, and to provide an explanation of its provisions.

We have converted the technology requirements of the Monitoring Agreement into a universal form that can be referred to and used as a guide by others. The names of the taxpayers, the third-party security provider, the POS/ECR manufacturer, and the government revenue authority have been replaced with blanks and letters. The following appears, rather than the real names:

- Taxpayer = the name of the individual or business involved;
- X = the name and model number of the POS system involved;
- Y = the manufacturer of the POS system;
- Z = the name of the third-party security system to be installed in X with the permission of Y;
- State DOR = the name of the government revenue authority involved; and
- Citation to Statute = the applicable statutory provision granting authority to the State DOR to audit the business records.

Electronic copy available at: https://ssrn.com/abstract=3212262

Exhibit 1

ELECTRONIC MONITORING AGREEMENT

(Technical Requirements)

Between

_____(State)_____ DEPARTMENT OF REVENUE and

_____(Taxpayer)_____

Hardware, Software and data requirements:

A. Point of Sale System: _____X_____ POS system purchased from _____Y_____.

B. Electronic Monitoring Solution: _____Z____, a software-based security system, integrated with the _____X_____ POS system, will be configured to securely store all *sales information* on site, as well as transmit *sales information* to the __(State) ___ DOR.

    1. Per___(citation to Statute) _____, all records must be open for inspection and examination at any time by the department, upon reasonable notice, and must be kept and preserved for a period of __(number)___ years.

C. The ____Z_____ security system will encrypt the database(s) in which its collected information is stored, using one of the following industry standard symmetric encryption algorithms such as:

    1. AES,
    2. Triple DES,
    3. Blowfish or
    4. Twofish.

D. In relation to the sales, _____(Taxpayer)_____ will provide ____(State)_____ DOR.

    1. Monthly sales reports generated from the _____X_____ POS system and the back end financial system (if any).
    2. In addition to the monthly sales report, the monthly summary information will include, detailed information collected by ____Z_____ secure monitoring system.
        i. The information from ____Z_____ will include:
            1. Total Sales by day for month (Quantity and Amount)
            2. Total Sales by Item (Quantity and Amount)
            3. Total Discounts (Quantity and Amount)

Electronic copy available at: https://ssrn.com/abstract=3212262

4. Net Sales
5. Total Tax
6. Total Amount Accounted For (grand total)
7. Tender/Payment Breakdown (Quantity and Amount)
8. Taxable Total
9. Number of voids (Quantity and Amount)
10. Number of open tills (Quantity)
11. Check Count/Average (Quantity and Average)
12. Guest Count/Average (Quantity and Average)

3. The raw data collected by _____Z_____ will be provided electronically to ____(State)_____DOR in the native format.

E. Method for Transmitting the Data Files:

1. The files will be sent decrypted electronically to a secured Secure File Transfer (SFT) site provided by ____(State)____ DOR.
2. This data is due to ____(State)____ DOR no later than the 5th of each month
3. ____(State)____ DOR will provide a confirmation that the data was received no later than the 20th of each month.

F. _____Z_____ will contain functionality to print QR / Bar codes on each receipt.

1. The QR / Bar code data will contain:
   i. Unique identifier code for each sale from_____Z____.
   ii. Data from _____X_____ POS system includes at a minimum the following fields: Date, Subtotal, tax amount, tendered total, payment method
2. The QR / Bar code will be required on all original (completed sales) receipts.
3. The QR / Bar Code shall not be included on reprints and training mode sales receipts.
4. Software for reading the QR / Bar Code will be provided to ____(State)____ DOR.

G. _____Z_____ will record the times when systems are shut down and when they were restarted whether or not these are caused by power outages or other triggers.

H. ____Y_____ will provide ____(State)____ DOR:

Electronic copy available at: https://ssrn.com/abstract=3212262

1. User manual for the _____X_____ POS system (in English and _____).
2. Outline of database structure for _____Z_____ system.

I. ____Y____ will provide _____(Taxpayer)_____ with help-line assistance through telephone, e-mail and optionally on-line chat. It will:

1. Provide assistance to ____(State)____ DOR when questions arise concerning the operation of the system, when accessing data from the system, or data definitions
2. Provide assistance to _____(Taxpayer)_____ when notified of a software update whenever such an update requires modifications to the ____Y_____ security installation.

J. ____Y_____ will provide a technician who will be available on-site for a two-day period after full installation to demonstrate the system and train employees of the _____(Taxpayer)_____ restaurant, and members of the ____(State)____ DOR (if requested) in the operation of the system.

K. If the parties mutually agree that any additional information should be directly transferred to ____(State)____ DOR, _____(Taxpayer)_____ and / or _____(Taxpayer's Representative)_____ will inform _____Y_____ of the additional data that should be transferred. Every effort will be made by _____Y_____ to program _____Z_____ for updated compliance.

L. ____Y_____ will notify the _____(Taxpayer)_____ of any software updates needed to the security system installed at the _____(Taxpayer) _____.

M. _____Y_____ will test the POS system after security installation to assure:

1. Accuracy of records,
2. Encryption of sales data,
3. Ability of the _____Taxpayer_____ to deliver sales data to the ____(State)____ DOR on the schedule required.

Electronic copy available at: https://ssrn.com/abstract=3212262

COMMENTARY

The technical requirements within the Monitoring Agreement are formally part of the basic agreement between the Taxpayer and the WA DOR. Paragraphs A through M were negotiated over a period of several months by the Taxpayer and the DOR.

Neither the POS manufacturer, nor the firm providing the software that does the electronic monitoring are parties to the Monitoring Agreement, although the Taxpayer sought to do so. Nevertheless, because these third-parties were making promises to the Taxpayer that will be relied upon by both the Taxpayer and the DOR, it was deemed prudent to have them directly involved in drafting, and reviewing the Monitoring Agreement.

Paragraphs A and B. The opening sections identify the POS system (X) and make it clear that the POS system, manufactured by (Y), is independent of the software-based security system (Z). The DOR specifically rejected using InfoSpec/Profitek as the POS provider (Y), as did the Taxpayer.

Paragraph C. This paragraph promises that (Z) will apply "industry standard symmetric encryption." This is important because the provision is not time-limited. Industry standards in the technology field are continually moving. This Monitoring Agreement endures for five years. The Agreement permits flexibility to adjust the encryption methodology if necessary for the protection of both the Taxpayer and the WA DOR.

Paragraph D. This paragraph makes the hybrid nature of the security system apparent. D (1) expects that the POS system (X) will provide standard monthly sales reports. These reports are expected to be delivered through software-based security system (Z).

D (2) moves directly to the additional data-elements that will be transmitted by the software-based security system (Z). These data-elements are promised within the monthly reports referenced at D (1), but can be produced in real-time to conform to a demand under the statute reference at B(1).

The twelve data-elements promised exceed what is normally delivered by a top-of-the-line POS system including time-measures of the "open till" as well as some standard audit metrics Check Count/Average and Guest Count/Average. All of these measures can be provided in various aggregates and real-time.

D (3) specifies that the transmission to the DOR will be electronically performed in readable native format.

Paragraph E. Sets up the requirements for data transmission to the DOR with format specified at E (1) and date of transmission at E (2), as well as an acknowledgement of receipt requirement at E (3).

Electronic copy available at: https://ssrn.com/abstract=3212262

Paragraph F. Assures the WA DOR of wide ranging functionality in (Z) to print QR/Bar codes on each receipt issued F (1) with a unique identifier for each sale F (1) (i) and data retrieved from the POS (X) related to that transaction including date, subtotal, tax amount, tender total and payment method F (1) (ii).

This functionality has far ranging implications (and applications) if the WA DOR wants to pursue development in this area. It is common in this field (although the State of Washington did not seek full performance functionality during negotiations) for QR/ Bar code on a receipt to provide the DOR with real-time data of high audit value.

For example, an individual could make a purchase at an establishment, and with the receipt-in-hand be able to verify that the data for the purchase was secured by the POS (X), encrypted by the secure element (Z), transmitted to the DOR and confirm everything in real-time. Related functionality would allow an inspector to sit in an establishment with an iPhone application that would track in real-time the orders being processed as they were "rung up" on the POS (X), as well as any of the standard audit metrics and more, also in real-time. Thus, it would be possible to know that a cashier was operating with an open till in real-time, that is, while the inspector is standing in the restaurant, perhaps talking with the manager. This kind of functionality allows very brief, highly targeted real-time audits on location (where an auditor can see the real-time activity behind the numbers) or remotely (where an auditor can perform a reasonably comprehensive real-time audit from a distance).

Paragraph G. This paragraph requires (Z) to record power outages and system downtimes, with in most instances an identification of the trigger event.

Paragraph H. Concerns the provision of user manuals and an outline of the database structure that will be provided to the DOR by (Y).

Paragraph I. References the technology assistance that will be provided to both the DOR and the Taxpayer from the technology provider.

Paragraph J. References the onsite training that will be provided to both the DOR and the Taxpayer by the technology provider, including hands-on training with the actual system in place.

Paragraph K. Is a good faith catch-all provision that records a promise by (Y) to provide additional data capture, and transmission to all parties to the agreement upon notice of need.

Paragraph L. Contains a promise by (Y) to provide notification of system updates.

Electronic copy available at: https://ssrn.com/abstract=3212262

Paragraph M. Contains a promise by (Y) to the Taxpayer to test the entire system for accuracy, encryption, and transmission capabilities, that will be sufficient for the Taxpayer to meet statutory obligations under this electronic monitoring agreement.

CONCLUSION

These requirements are the technology heart of this first-of-its-kind electronic monitoring agreement for sales tax compliance in the US. It represents the end of a very long road for technology-based solutions to Zappers, Phantomware and other sales suppression devices in the US. Washington is taking a one-by-one, criminal enforcement approach to a very serious systemic tax problem. Something far more comprehensive is needed, but this is a beginning.

The WADOR and other state taxing jurisdictions have long been aware of the problems posed by Zappers and Phantomware. Over 10 years ago, Professor Ainsworth, one of the authors of this article, recommended an approach similar to the present one, but instead of being used under criminal statutes, it would be offered in the context of negotiating a settlement with problematical taxpayers. The design would be to bring them back into compliance with a carrot and a stick. The end result, but by a different path is the present Monitoring Agreement which will likely be the prototype for such agreements in the future.

Electronic copy available at: https://ssrn.com/abstract=3212262