12-2019

# Washington's 'Cutting-Edge' Technology Solution to Combating Sales Tax Fraud: Real-Time Data (Now), Real-Time Remittance in the Future

Richard Thompson Ainsworth

Robert Chicoine

Andrew Leahey

Sunder Gee

# WASHINGTON'S "CUTTING-EDGE" TECHNOLOGY SOLUTION TO COMBATTING SALES TAX FRAUD: REAL-TIME DATA (NOW), REAL-TIME REMITTANCE IN THE FUTURE

Richard T. Ainsworth
Robert J. Chicoine
Andrew Leahey
Sunder Gee

Globally, consumption tax compliance (value added tax and retail sales tax) has gone digital – digital invoices are becoming mandatory,[1] centralized monitoring of transactions and tax payments are increasingly common,[2] and artificial intelligence is assessing fraud risks in real-time.[3] When tax is collected, it is increasingly being remitted in near-real-time.[4] This is the trajectory for the modern retail sales tax (RST) imposed by most states in the US. While this may appear to be revolutionary to the average American tax practitioner, like the first "moon shot," it is a well-worn path among global nations using the value added tax (VAT). The RST will eventually be following suit. Washington has taken the first step on this journey with the help and cooperation of a small business owner who admitted to using an Electronic Sales Suppression (ESS) device when operating a highly regarded Asian restaurant in Seattle.

To address sophisticated tax fraud in the digital age, the Washington State Legislature commissioned a world-wide study, which was delivered April 22, 2019, the Washington Department of Revenue (DOR) which "... completed a review of relevant research into technology trends; Point of Sales (POS) solutions, the ecosystem of integrated retail software

[1] See for example the COUNCIL IMPLIMENTING DECISION (EU) 2018/593 of 16 April 2018 authorizing the Italian Republic to introduce a special measure derogating from Articles 218 and 232 of Directive 2006/112/EC on the common system of value added tax. The Decision recites that: "By letter registered with the Commission on 27 September 2017, Italy requested authorization for a special measure to derogate from Articles 218 and 232 of Directive 2006/112/EC and to introduce mandatory electronic invoicing for all taxable persons established in the territory of Italy, ... [and that] This Decision shall apply from 1 July 2018 until 31 December 2021.")

[2] See for example see: Trustweaver, *Tax-Compliant Global Electronic Invoice Lifecycle Management* (White Paper 9th edition, February 2018) at 3, which discusses "centralized clearance of invoices" as follows:

> The trend towards tax "clearance" of invoices impacts businesses far beyond the obvious need to comply with varying hard-and-fast, real-time technical controls in many countries. Indeed, this revolution in tax collection and compliance can be expected to turn some facets of the enterprise software and services market on their head ...

Listing and discussing (at 54 through 77) variances among clearance systems in Belarus, Russia, Turkey, Argentina, Costa Rica, Mexico, Uruguay, Azerbaijan, Indonesia, Kazakhstan, South Korea, Taiwan, Vietnam, and Tunisia. OECD, *Technology Tools to Tackle Tax Evasion and Tax Fraud* (2017) at 13 & 16.

[3] See for example Smart Cloud, Inc. *Tax Intelligence System* MICROSOFT APPSOURCE & Press Release (Brasilia, Brazil, March 21, 2019) (discussing the XAI Tax Intelligence System in operation in the State of Cearå, Brazil – soon to expand to four other states) *available at*: https://appsource.microsoft.com/en-us/product/web-apps/smartcloud.smartcloud-tax-intelligence-trial-app?src=web_industry_govenhance&tab=Overview; Patricia Araújo Vieira, Daiana Paula Pimenta, Alethéia Ferreira da Cruz & Eliane Moreira Sá de Souza, Effects of the Electronic Invoice Program on the Increase of State Collection, Revista de Administração Pública (April 25, 2019) available at: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-76122019000200481&lng=en&nrm=iso&tlng=en

[4] See for example, the move to split payments: PwC - Poland, *Mandatory split payments [in Poland] from November 1, 2019* (July 22, 2019) *available at*: https://www.pwc.pl/en/articles/tax-news/2019/2019-01-28-mandatory-split-payment.html

solutions, cloud technologies, [and] other underpinning technologies ..."[5] The research effort was practical, market-driven, and encapsulated in a set of "... scenarios represent[ing] the full set of reasonable solutions for DOR's consideration, ..."[6]

The scenarios were distilled to four. In each instance the scenarios were numbered, characterized with a single word, differentiated by their primary focus, and then made more concrete by identifying (what Gartner considered to be) a representative country for each scenario.

- Alternative #1: Foundational – Internal Focus ("Like UK") (but more likely Japan)[7]
- Alternative #2: Targeted – External Focus ("Like Netherlands")

[5] Gartner, Inc., *A Report for WA Department of Revenue, Deliverable 7: Final Report*, - Updated Version, Redacted, (April 22, 2019) Engagement 3300052217.

[6] Gartner, *Report* at 126.

[7] Placing the UK as the representative country for Alternative #1 is emblematic of the deficiencies in the Garner report. An internally focused, foundational country would be a country "like Japan,' not "like UK," but Gartner does not consider Japan. Consider:

> The primary components for this alternative [#1] are focused on incremental improvements in key supporting technologies for improving DOR auditing processes. These foundational investments in centralized data storage, analytics solution and configuration of the existing audit tracking system will also set the stage for potential future investments in advanced sales suppression technologies. Gartner, *Report* at 125.

And

> Thus far the UK has taken a cautious approach to rolling out a broader technology-based solution to sales suppression, especially given their culture is not a good fit for broad government mandates, similar to the Netherlands. Gartner, *Report* at 29.

At its page 29 (above), and to make this point, Gartner cites generally to my paper (no page reference) with Urs Hengartner on Quebec's Sales Recording Module, which has no analysis of the UK system. A current work in progress *Mini-Blockchain, VATCoin and VAT Fraud* (forthcoming in TAX NOTES INTERNATIONAL) would have been more appropriate. The forthcoming paper compares developments in the UK's MTD, with similar efforts in the Kingdom of Saudi Arabia's Esal program. Gartner's redacted report contains no reference to either program.

What is important for the Washington study is to recognize that the UK does not fit Alternative #1, but Japan does. The UK has, since it was announced in 2015, been working on its Making Tax Digital (MTD) program. It went into effect on April 1, 2019 (21 days before the Gartner Report was submitted). The omission is glaringly obvious.

MTD is applied to VAT (first), and will eventually include the corporate and personal income taxes. The essence of MTD-VAT is that VAT-registered businesses above the threshold (currently £85,000) are required to (a) keep records digitally and (b) file returns using MTD compatible software. There is no requirement to issue or receive digital invoices. The UK effort can be seen as a back-end digitization universal mandate to help taxpayers comply and to prevent fraud. See: UK Office of Tax Simplification, *Technology Review: a vision for tax simplification*, (January 2019) at ¶¶ 1.100 & 1.20.

> The push by the financial services sector for people to move towards cashless transactions (and therefore away from cash) is a contentious issue. In theory, it should lead to more efficient processes for business, with electronic transactions leaving an auditable trail allowing for more accurate calculation of tax, and a reduction in fraudulent activity. ....

And also:

> HMRC's vision for their digital transformation (MTD) work is to provide digital services for their customers that:
>
> - are easy-to-use, convenient and personalized for individuals, businesses and agents
> - promote digital take-up and voluntary compliance by designing for customer needs
> - use data to help customers avoid errors through pre-population
> - provide assistance in using or accessing our services for those who need it.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771123/OTS_Technology_paper_Jan_19.pdf

- Alternative #3: Broad – External Focus ("Like Belgium")
- Alternative #4: Cutting Edge – External Focus ("Like Fiji")[8]

Unfortunately. the report makes no reference to an ongoing pilot project conducted by the DOR as a result of a plea agreement in the *State of Washington v. Wong*,[9] that initially followed an Alternative #2 approach, and then shifted to Alternative #4 to improve data monitoring scope and accuracy. Allagma Technologies, a security and POS provider from Montreal, which had considerable experience as an installer and service provider for Revenue Quebec's Sales Recording Modules, was deployed first, May 30, 2017. It was replaced on April 2, 2019 with a fully digital solution installed by a European firm, Data Tech International (DTI). DTI pioneered the "cutting edge" solution with its work in a number of jurisdictions, but most notably Fiji.

The reason for replacing the Montreal solution 22 months after the pilot began, sheds considerable light on the differences between Alternative #2 and Alternative #4. These insights would have been an important contribution to the Report, but they do not appear in any part of the redacted version.

Alternative #2 which is "like Netherlands" is dependent on establishing a productive working relationship among three parties: the DOR, the POS firm, and the business. The idea behind Alternative #2 (which is very unlikely to work in a marketplace already rife with ESS devices)[10] is that "... the DOR would partner with [the] Point of Sale provider[s] to establish standards that [would] produce a standard data output file, ..."[11] Business input would be necessary to show what was commercially reasonable. In this case whatever synergies there were between the DOR and the POS firm, were negated by the problems created for operation of the business,[12] which wanted change and was willing to participate in and fund installation of cutting-edge technology.

Changing to the technology-intensive approach of Alternative #4 was the right move. The tech solution molded itself around the pilot businesses (multiple POS terminals, online ordering, with pickup or delivery options) and also "... provided transformative benefits for auditing processes with real-time access to data [for the DOR], effectively shifting the focus to proactive deterrence."[13] A lot has already been learned through Washington's pilot which is clearly poised for expansion.

[8] Gartner, *Report* at 120-133.
[9] Wash. Super. Ct., No. 16-1-00179-0.
[10] One only has to look to Portugal to see the problem. The Portuguese have adopted (and made mandatory) the OECD's Standard Audit Files for Tax (SAF-T) reporting regime. ESS (Zappers and Phantonware) act to delete sales from the POS, leaving little or no artifacts. Reports are then generated from the POS, and then presented to the accountant for SAF-T reporting. As the Portuguese have found out, this process "bakes in" the suppression. It does not come close to tackling sales tax fraud.
[11] Gartner, *Report* at 126.
[12] For example, in the Wong case, the chefs in the kitchen wanted orders sent to the kitchen in Chinese. Not originally having that functionality in the initial POS had a significant impact on business flow. The speed of the kitchen at busy times should not be constrained by impositions of the tax authority. Monitoring must be seamless.
[13] Gartner, *Report* at 126.

Even though the redacted report is weakened considerably by not making any reference to the ongoing pilot project, there is a lot to learn from the choices made by the DOR and Ms. Wong. One gets the distinct impression that Washington is very aware that it is operating at the "cutting edge," along with Fiji and a number of other select foreign jurisdictions, in applying technology solutions to consumption tax problems.

The intent of this paper is to explain the inner workings of the State of Washington's cutting-edge pilot. What is happening in Washington is happening nowhere else in the US. This pilot is (for the moment) America's cutting-edge pilot project in retail sales tax compliance. Ms. Wong, the owner of the Facing East and QQ Taiwanese Bite restaurants who are participating in the pilot project, was initially vilified in DOR press releases as a tax cheat who harmed Washington citizens. The reality is that but for her acceptance of responsibility and efforts to make things right, Washington state would not be in the forefront of solving tax fraud by state-of-the-art technology.

## *Wong's Washington Pilot Project: An anti-sales suppression program modeled on Fiji*

The State of Washington's pilot project in anti-sales suppression technology solutions is the result of the monitoring agreement entered into between the taxpayer and the DOR in the *State of Washington v. Wong*.[14] This is Washington State's first judicially resolved case involving an automated sales suppression device.[15] Months of negotiations led to a plea agreement and Washington State's first-in-the-nation electronic sales monitoring agreement (August 30, 2017).[16] The negotiations were focused on a practical state of the art technology solution to monitoring sales data, and on protections for taxpayers who are being monitored by taxing authorities, for whatever reason. This initial monitoring agreement followed Gartner's *Alternative #2* model (although it was selected before Gartner began research), and was rejected and replaced on April 2, 2019 with the current *Alternative #4* model.[17]

The unrepresented taxpayer admitted during a civil audit that she had violated RCW 82.32.290 (4)(a) by knowingly possessing, and using a Zapper to suppress sales.[18] Potential penalties were severe under the statute. Not only were all taxes, penalties, and interest lawfully

[14] Wash. Super. Ct., No. 16-1-00179-0.

[15] For a discussion of Washington State's thought process as it worked through its electronic sales suppression problems (before the Gartner Report see: Richard T. Ainsworth & Robert Chicoine, *Fighting Technology with Technology: Taking Aim at Electronic Sales Suppression*, 89 STATE TAX NOTES 1037 (March 12, 2018)

[16] For an analysis of Washington's first electronic monitoring agreement see: Richard T. Ainsworth & Robert Chicoine, *Zapped! An Analysis of Washington's Electronic Monitoring Agreement,* 87 STATE TAX NOTES 885 (March 5, 2018)

[17] An analysis of the technology requirements in Washington State's electronic monitoring agreement which were met by both the *Alternative #2* and *Alternative #4* models is discussed in Richard T. Ainsworth & Robert Chicoine, *The Technology Requirements of the First Electronic Monitoring Agreement in U.S. for Zappers,* 86 STATE TAX NOTES 239 (October 16, 2017)

[18] A Zapper places sales suppression programming on a removable CD or memory stick. Phantomware is similar suppression programming which is also prohibited by the Washington statute, but it is installed within the ECR/POS system, and is not readily removable from them. Zappers and Phantomware perform the same sales suppression functions in much the same manner.

due[19] required to be paid, but as a Class C felony incarceration of up to 5 years, a $10,000 fine, or both were possible.[20] An even a more severe penalty for the taxpayer involved prohibited her from participating in any business unless she:

> … entere[d] 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.[21]

A major problem was that the DOR did not have a specific method in mind that was acceptable to it, although it did have certain criteria. The taxpayer was burdened, at her expense, with finding an acceptable solution that met the DOR criteria. She elected to do so in an effort to remain in business, negotiate a favorable plea agreement and reach a stipulated civil restitution (tax loss) amount to satisfy the statutory requirements.[22] Even though the penalties were substantial, the taxpayer realized the importance of her participation in the pilot and saved no expense in her efforts to "make this monitoring work" for the State. There were dropped orders and system shut-downs that had to be recovered from on the busiest days, and when it became apparent after more than a year of effort that a better security system was needed she proposed and funded the transition to the monitoring system being used in Fiji. Twenty days before the Gartner report was issued, the switch was made.

Two elements combine in the Fiji model (or *Alternative #4*): (a) there must be a valid receipt issued for each sale, and this receipt must be digital (although a paper copy can be provided in addition),[23] and (b) each receipt must be validated by the DOR through proprietary software call Tax Core[24] in real-time. The validation received from TaxCore will include a

[19] "Lawfully due" is statutory language that is undefined in statute or regulation. It becomes problematical on audit and in settlement, because the amount of tax should not be left to the discretion and proposed assessments of the DOR.

[20] RCW 9a.20.021.

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

[22] It should be noted that Ms. Wong was able to negotiate a civil tax assessment that was significantly less than what was originally proposed by the DOR. No small part of this success was due to her willingness to cooperate and assist the DOR as it endeavored to find workable monitoring solutions.

[23] There is currently no monetary penalty in Washington State for not issuing a valid digital receipt other than breach of the monitoring agreement. It is expected that of the pilot is considered a success and is adopted more widely, then Washington would follow other jurisdictions and impose monetary penalties. Penalties related to missing or incomplete digital invoices in Quebec are $100, or $300 to $5,000 depending on severity, with $1,000 to $5,000 for a second offence within five years, and $5,000 to $50,000 for multiple offenses within five years. Sanctions related specifically to the Sales Recording Module are a $300 penalty (per invoice) and a $2,000 to $100,000 fine with a maximum of six months in prison with suspension or revocation of the registration certificate. https://www.revenuquebec.ca/en/fair-for-all/ensuring-tax-compliance/penalties-and-interest/penalties/penalties-specific-situations/penalties-and-fines-in-the-restaurant-sector/. In Brazil commercial law requires invoices to be digital to be enforced. Tax compliance follows commercial practice. See: Decree 6022 of 2007 established the *Public System of Digital Accounting* (*Institui o Sistema Público de Escrituração Digital*) (SPED). In Fiji the penalties for violating the invoicing rules range from up to $10,000, or up to $25,000, or $50,000 depending on the gross annual turnover of the business (less than $500,000, or less than $1,5000, or over 41,500,000). All figures are in Fiji dollars. Government of Fiji Gazette, Tax Administration Act 2009, Electronic Fiscal Device Regulations 2017, Article 23, *available at*: https://www.frcs.org.fj/wp-content/uploads/2018/04/LN-37-Tax-Administration-Electronic-Fiscal-Device-Regulations-2017.pdf

[24] The TaxCore is the back-end software tool where all data from accredited POSes and their associated secure elements is merged unpacked and decrypted for viewing. This software manages life-cycle (start to end) of each taxpayer's system, offers analysis and reporting.

digital signature on the receipt and a verifying hyperlink within the QR code.[25] The process is called "the fiscalization" of the receipt/invoice.

Fiscalizing an invoice is a simple two-step procedure accommodated by secure software at the business issuing the invoice. The *request* is made first, and companion software within the tax authority issues the *response*. The fiscalizing system operates both online and offline.[26]

It is important to realize the speed with which this process moves, and how the speed (coupled with the technology's security features) provides additional protection against Zappers and Phantomware. The "round-trip" process described below is fully encrypted, saved in multiple (cross-referenceable) locations, and takes less than three milliseconds to complete. The data entered by the cashier, is returned to the customer immediately in the receipt (taking less time than swiping a credit card). The receipt has an embedded QR code that when scanned with a smart phone will confirm the accuracy of the receipt and the recording of the transaction on site and with the DOR.

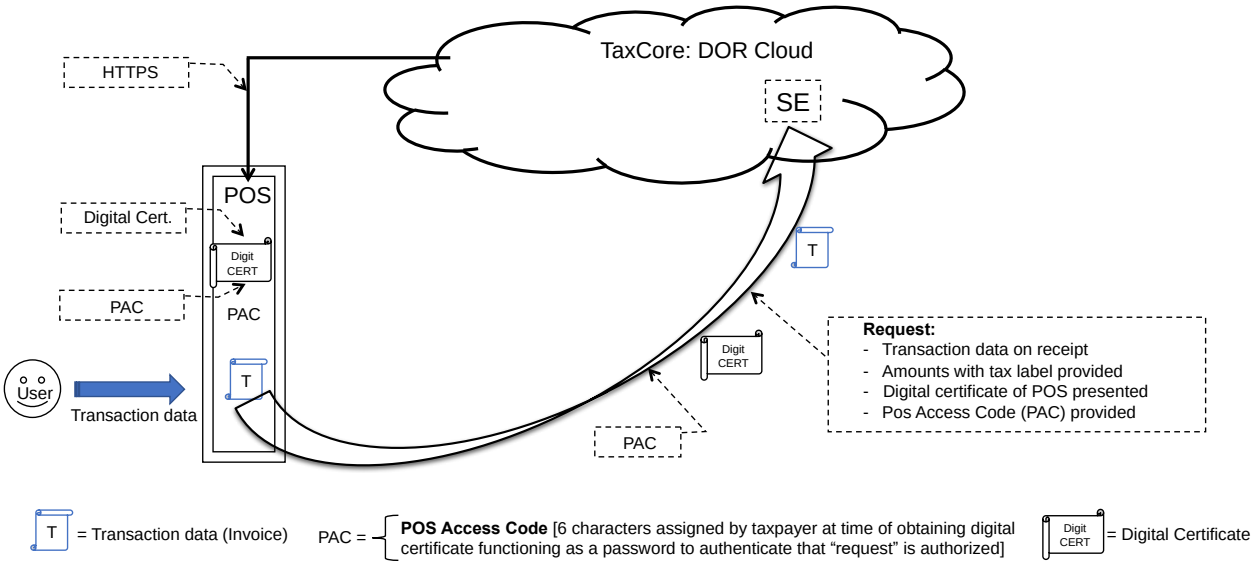
If a business owner were to delete the receipt from the POS a mere two seconds after passing the receipt to the customer, the record of the transaction would already be in the TaxCore. If the customer immediately took the receipt and scanned the QR code, the receipt would be visible in the DOR's system. But more importantly, scanning would make this record permanent. The customer would be closing the digital loop of the purchase. Both the sales amount, and tax paid would be identified. All tax attributes would be confirmed.

The following figures sketch the two-step request and response procedure at the heart of the Fiji/Washington anti-sales suppression system.

*The Request – Figure 1*. The *request* is a fully automated process. Immediately after the POS, or other platform has assembled the transaction data the *accredited* (POS) system[27] will make a direct internet-based request for fiscalization through an associated Sales Data Controller (SDC) residing either on the taxpayer's premises, or within TaxCore at the DOR.[28] The transaction data elements[29] will be combined with the POS's Digital Certificate and PAC[30] to be sent forward to the *secure element* (SE). The SE verifies the request, and identifies the caller (the authorized taxpayer using the POS).

[25] The QR code itself is not a unique attribute. Many countries use QR codes on the receipt, even Quebec uses 2d bar code, but none (other than Fiji) has a hyperlink embedded within it that will lead the person scanning it to the Tax Authority's web service from where a confirmation of the validity of the receipt is obtained first hand.
[26] There are some minor hardware differences between an online system (utilizing a virtual sales data controller – V-SDC) and an off-line system (utilizing an external sales data controller – E-SDC). Cost is not a factor. Most locations in Fiji utilize both online and off-line. The technical differences are discussed in Richard T. Ainsworth & Goran Todorov, *Fiji: A Digital Invoice System Fights Fraud and Enforces Real-Time VAT Compliance*, 92 TAX NOTES INTERNATIONAL 697 (November 12, 2018).
[27] There is no requirement that POS system be used. The reference to "POS" could be replaced by a number of other platforms: a mobile POS app; a cashier working off a desktop computer with an app; an online shopping forum; an invoice generating ERP system. This paper will use POS generically to mean all of these.
[28] As indicated above, there are virtual and physical (external) SDCs. Figure 1 illustrates the V-SDC
[29] In Fiji these elements are specified in EFD Reg. §20(2)(a) – (j).
[30] PAC is the POS Access Code. It is comprised of 6 characters assigned by taxpayer at time the taxpayer obtains the digital certificate, and it functions as a password to authenticate that "request" for fiscalization is authorized.

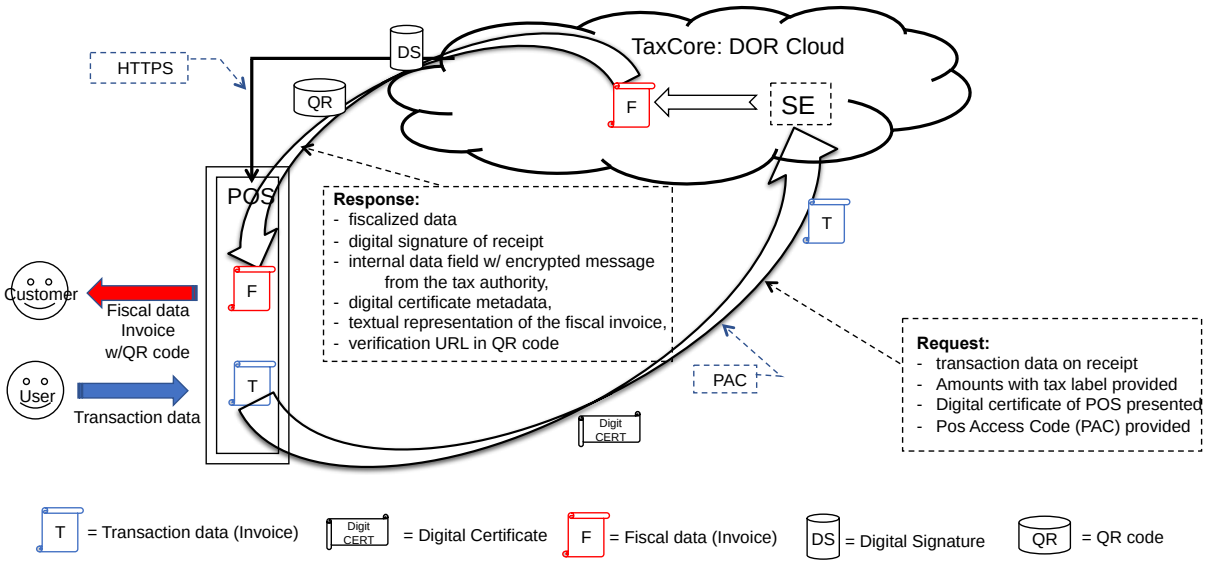
Figure 1
Request for Fiscal Invoice [accredited POS]
Reprinted from: Richard T. Ainsworth & Goran Todorov, *Fiji: A Digital Invoice System Fights Fraud and Enforces Real-Time VAT Compliance*, 92 TAX NOTES INTERNATIONAL 697, 703, figure 1 (November 12, 2018).




*The Response – Figure 2*. After confirming the validity of the request, the secure element associates the transactional data (specified previously) with additional elements as required by the system,[31] including a digital signature and the verification URL through which a QR code can be generated by the POS. The result is the fiscal invoice. The customer (or any other party) can scan the QR code that will be printed on the receipt/ invoice to confirm that the invoice data has been recorded in TaxCore. As a result, in both the Facing East and QQ restaurants today a Washington DOR auditor can anonymously scan a receipt at any time of a day and get an immediate assurance that the receipt provided by the cashier is properly reported in Washington's TaxCore.[32]

[31] In Fiji these elements are specified in EFD Reg. §20(2)(k) – (o). In Ms. Wong's installation these elements are added to facilitate the workability and security of the system without mandatory or statutory demands.
[32] It's important to note here that the most effective (traditional) method of finding electronic sales suppression, is an expensive multi-step process of (a) dispatching undercover auditors to a restaurant who purchase a meal with cash and save the printed receipt, (b) collecting a number of receipts from that location at different times of the day, and providing them to the official audit team, who (c) undertakes a search for these receipts in the POS records.

Figure 2
Response to request for Fiscal Invoice [accredited POS]
Reprinted from: Richard T. Ainsworth & Goran Todorov, *Fiji: A Digital Invoice System Fights Fraud and Enforces Real-Time VAT Compliance*, 92 TAX NOTES INTERNATIONAL 697, 703, figure 1 (November 12, 2018).




Fiji's fiscalized digital invoices not only allows customers to confirm that all indirect taxes were remitted, but it also develops (within TaxCore) a comprehensive data-base of all transactions within the domestic ecosystem. The same is true of the Wong pilot project being used in Washington State, with the difference being just a matter of size. Fiji's system is larger, for the moment.

Artificial intelligence (AI) engines are applied in Fiji and can be, but are not yet being used in Washington. In Fiji's larger tax ecosystem, risk analysis and audit selection are is streamlined. Audits are not chosen blindly, or based on "hunches." They are data-driven. The same will be true in Washington State as the pilot project grows.

But even at this level of engagement, there is much more here in Washington than what has been discussed above. Counters embedded in the data streams fine-tune the remote assessment. Data is preserved in a mini-blockchain for highly efficient domestic audits.

*Mini-blockchains, Counters, and Proof of Audit*

Fiji's fiscalized digital invoices, and Washington State's fiscalized receipts do more than just confirm the accuracy of a particular invoice/ receipt, and construct a centralized data-base of transactions within TaxCore. They also build a POS-specific blockchain of transactions with "counters" that are aligned to provide an automated "proof of audit," if all data conforms, as expected, after a full review. These three attributes set the Fiji/Seattle solution apart from other solutions, and place it head-and-shoulders above an Alternative #2 approach to data security where the DOR is expected to partner with POS providers to establish standards that would produce a standard data output file. There are real, substantive reasons why Alternative #4 is

considered a "cutting-edge" solution – notably, mini-blockchains, counters, and proof of audit functionality. Just as there is clear and verifiable revenue authority analysis from jurisdictions, like Portugal, that have endeavored to control sales suppression fraud through SAF-T.

*Mini-blockchain*. With the Fiji solution a mini-blockchain of transactions is preserved (a) within the specific secure element assigned to the POS, (b) within the Tax Authority's TaxCore, and is also (c) embedded in the QR code on each receipt/invoice held by a customer. As with all blockchains, the data is permanent and immutable. It is impossible to obscure a transaction once it has been input and fiscalized. Each customer becomes an extension of a government audit team when they scan the QR code on a receipt to verify its contents.[33] By doing so, the customer reports and confirms not only his/her specific transaction, but the mini-blockchain within which the transaction is preserved.

*Counters*. In the Fiji solution counters record the tax attributes of each receipt *as those attributes are sequentially placed on receipts*. The record is embedded in the QR code of all valid receipts. Counting is non-discretionary [that is, counters cannot be turned off.] Counters cannot be adjusted but their limits can be specified. The cap on each counter is pre-configured by the DOR, and can only be reset by the DOR.

*Proof of audit*. Counters in the Fiji/Seattle solution start with customized caps (limits). When the secure element (SE) observes that a particular counter is getting close to its cap the SE will notify the operator that it will shut down, if it does not receive a *proof of audit* notification from TaxCore. If it does receive this notification the TaxCore automatically resets to zero.

The notification indicates that all data from the POS and the associated Secure Element (SE) has been recorded in Tax Core, nothing is missing, and all counters are working properly. Said another way, the proof of audit means the mini-blockchain is complete and intact. There have been no manipulations, omissions, or removals of data.

The process is seamless, fully automated, and a nearly continuous process. Most of the time, a *proof of audit* is completely invisible to the taxpayer.

*Why the counters are the key (examples)*

The standard counters are the tax-attributes found on a signed receipt issued by an accredited POS. Counters are related to the type of receipt. There are seven basic types of receipt: Normal Sales [NS], Normal Refund [NR], Copy Sales [CS], Copy Refund [CR], Training Sales [TS], Training Refund [TR] and Proforma Sales [PS]. Additional counters reside

[33] Sales transaction can be reported to the DOR either by the seller or the buyer. Although the norm is that the seller reports sales to the DOR, collects and remits RST, in cases of missing receipts the buyer can declare the purchase and report his payment of the tax to the seller. This occurs in the Fiji/Seattle system when the buyer scans the QR to verify the transaction and report the data to the DOR. In a cross-border or international context buyer-scanning of a mandated QR code on receipts has an additional value (not considered in this paper). Cross-border/ international scanning can help detect fraudulent sales, and assist the DOR in identifying remote sellers who may be collecting RST, not filing returns and disappearing. See: Richard T. Ainsworth & Chang Che, *Data First, Tax Next: How Fiji's Technology Can Improve New Zealand's NetFlix Tax (Electronic Marketplaces) (Part 3)* 95 TAX NOTES INTERNATIONAL 1249 (September 23, 2019).

in the SE which records line item cumulative totals: cumulative turnover, tax totals, refund totals, per tax refund totals, and others.

Figure 3 (below) illustrates a single accredited POS which fiscalizes six receipts in a sequence. The diagram suggests that there can be ten or more POS (or Accredited Invoice[34]) systems in this diagram, but only one is represented.[35] In fact, the Washington pilot project has five accredited POS engaged. Three are at the Facing East restaurant, and two at the QQ restaurant. Three types of receipts are illustrated:

- Normal Sales [NS],
- Normal Refund [NR], and
- Proforma Sales [PS].

There are twelve tax attributes (associated with these receipts) that are "counted" throughout this six-receipt sequence. Six "counters" relate to specific attributes of the receipt being considered, and the RST associated with that attribute (NS; NR; PS; RST on NS; RST on NR; RST on PS). Six additional counters sequentially aggregate these amounts across these specific categories throughout the six-receipt sequence.

A summary of the data used in Figures 3 and 4 is provided in Chart 1 (below):

34 An Accredited Invoice System (AIS) is an umbrella term covering devices and systems capable of producing receipts (normally issued in B2C transactions) and invoices (normally issued in B2B transactions. A point-of-sale (POS) system is one specific application on an AIS. POS and AIS will be used interchangeably in this text.

35 The simplicity of the diagram in Figure 7 should not be underestimated. If POS-1 was Amazon these six transactions would occur in less than a hundredth of a second. Jay Yarow, *Amazon was Selling 306 Items Every Second At Its Peak This Year*, BUSINESS INSIDER (December 27, 2012) available at: https://www.businessinsider.com/amazon-holiday-facts-2012-12 (this amount is 26.5 million transactions per day, and comparable statistics have never been released again by Amazon). In fact, the application of the Fiji monitoring system to online marketplaces yields revenue benefits far exceeding those in standard B2C transactions. This, application has been explored in Richard T. Ainsworth & Chang Che, Data First – Tax Next: How Fiji's Technology can Improve New Zealand's "NetFlix Tax," (Part 3) – Electronic Marketplaces, TAX NOTES INTERNATIONAL (forthcoming.)

Chart 1 – Data applied in Figures 3 & 4

Invoice Sequence (1-6) →

| COUNTERS APPLIED | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| PS (pro forma sales) | | | | | 100 | 0 |
| RST on PS | | | | | 10 | 0 |
| NR (normal refunds) | | | | 40 | 0 | 0 |
| RST on NR | | | | 4 | 0 | 0 |
| NS (normal sales) | 10 | 20 | 1,350 | 0 | 0 | 50 |
| RST on NS | 1 | 2 | 135 | 0 | 0 | 5 |
| Ttl NS | 10 | 30 | 1,380 | 1,380 | 1,380 | 1,430 |
| Ttl RST NS | 1 | 3 | 138 | 138 | 138 | 143 |
| Ttl NR | | | | 40 | 40 | 40 |
| Ttl RST NR | | | | 4 | 4 | 4 |
| Ttl PS | | | | | 100 | 100 |
| Ttl RST PS | | | | | 10 | 10 |
| | | | | | | |
| | | | | | | |

Figure 3 (further below) shows POS-1 making six requests for fiscalization, and TaxCore responding six times, signing each response after verifying the sender and the data. The signature is noted as [Rcpt. Sig.] at the bottom of each receipt.

Figure 3 assumes that these are the first six transactions in a business cycle. The first three transactions (receipts) are normal sales [NS], followed by a normal return [NR], and then a proforma sale [PS], before returning to make another normal sale [NS] at the sixth receipt.

A QR code appearing on each receipt can be scanned by the purchaser (or any tax official). The purchaser will see in an unequivocal format the complete data set of all information on the invoice issued. A scan by the Tax Authority would disclose more data. Some QR data is encrypted. An auditor would be able to see not only the basic invoice, but also the separate and aggregate tax-values captured by the counters. Thus, assuming a 10% RST, a scan of the first two receipts shows, in the first receipt, normal sales of 10, and RST collected of 1.

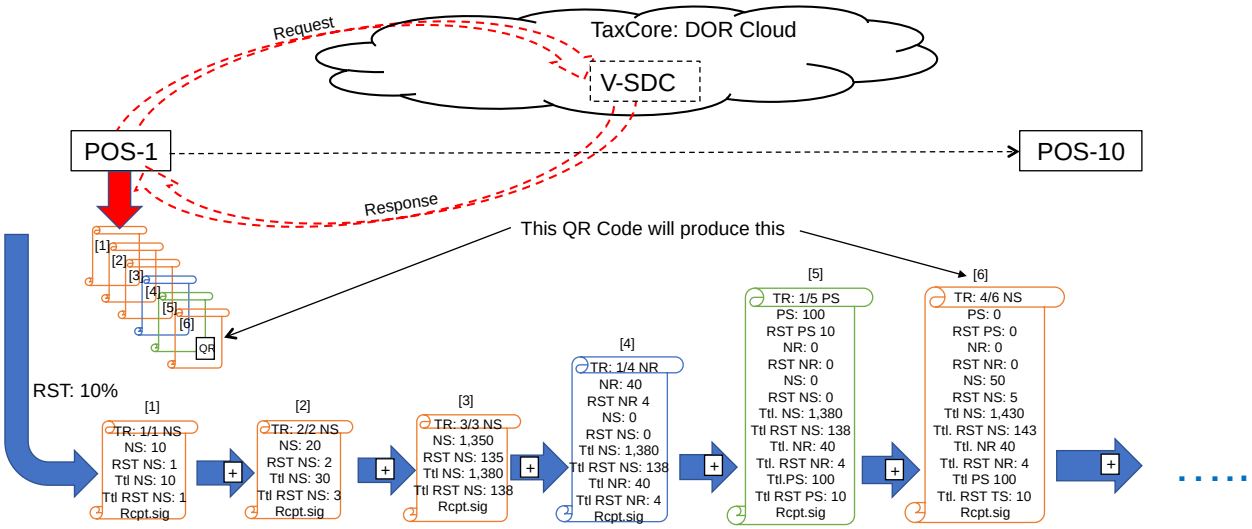
The second receipt shows aggregate tax-values in addition to the second set of normal sales (20), and RST from normal sales (2). The aggregate counters on the second receipt show total normal sales of 30 (10 + 20), and total RST collected on normal sales of 3 (1 + 2). These results would be visible to any auditor scanning the QR code on the second receipt.

The third receipt is similar, but the numbers are larger. There are normal sales of 1,350 and RST from normal sales of 135. This transaction lifts the aggregate counters on the third receipt to total normal sales of 1,380 and total RST collected from normal sales to 138.

The fourth and fifth receipts record different functions. Receipt four is a normal refund, and receipt five is a proforma sale.[36] Each receipt has a base number and a related RST amount. The diagram at Figure 3 shows receipts number four and five to be visibly larger than the first three receipts. This reflects the larger data content from the use of new counters, and the fact that counters do not aggregate data across categories. For example, *normal refunds* (and the RST related to it) are not netted against *normal sales* (and the RST from normal sales). NS and NR are separate counters. Counters initially record data separately, report that data separately, and continue to reproduce that data separately on later receipts.

Thus, the sixth receipt, which is a return to a normal sales transaction of 50 with an additional RST from normal sales of 5, reproduces all the data from the fourth (refund) and fifth (proforma) receipts. However, as a NS, receipt six is able to aggregate its normal sales data into the previously recorded total normal sales to get the new figure of 1,430 total normal sales, and a total RST from normal sales amount of 143.

Figure 3
Fiscal Counters supporting the Proof of Audit structure
Reprinted and modified from: Richard T. Ainsworth & Goran Todorov, *Fiji: A Digital Invoice System Fights Fraud and Enforces Real-Time VAT Compliance*, 92 TAX NOTES INTERNATIONAL 697, 711, figure 7 (November 12, 2018).




It's important to remember that counters serve several purposes. They show immediate transaction values, but they also reach back to the prior invoice and connect these two invoices in a chain, while waiting (for a millisecond or two) to be further bonded to the next invoice in the sequence.[37] This is the mini-blockchain. Counters provide continuous audit capabilities regardless of whether the certified POS is (a) associated with a Virtual Sales Data Controller (V-SDC), where the Secure Element (SE) is embedded in Tax Core, or (b) associated with an

[36] A proforma sale will occur in a restaurant situation where a waiter drafts a trial receipt to show customers what an order will cost before a decision (commitment) is made to place the order with the kitchen.
[37] This function is similar to the Portuguese solution where a security code is designed to link to the previous invoice thereby initiating a (limited) internal *mini-blockchain* of invoices but without the consensus mechanisms of corresponding blockchains within the tax administration, and the customer-based links related to the scanned QR codes.

External Sales Data Controller (E-SDC), where the Secure Element is loaded on a smart card inserted in the SDC.

The Facing East and QQ restaurants in Seattle are associated with both V-SDC's and E-SDC's. The Seattle restaurants work easily online or off. The technology of how the systems do their job does not change. Regardless of the set-up, the tax problem the counters solve is the identification of (and if possible the recovery of) missing receipts.

A business-story based example may help further. Assume that certified POS-1 is located at a small hamburger shop, where normal sales are in the $10 to $15 range, occasionally a $50 sale is made, but rarely is a sale made for $100. However, on special occasions (holidays, public gatherings in the neighborhood) the amounts charged on a single ticket can jump-up considerably. There are two kinds of exceptionally large sales made by the hamburger shop: (a) bulk sales to corporations in the area that provide free meals for their employees who are asked to work long hours on occasion, and (b) street sales by roller skating waiters and waitresses.

This hamburger shop is popular because its waiters and waitresses sell and deliver meals on roller skates. The skaters tend to aggregate sales (on the fly) and record all sales as one batch in the certified POS. When a large sale shows up in the shop's POS it is invariably the result of either a corporate bulk purchase or a skater's aggregation of sales for an entire evening shift.

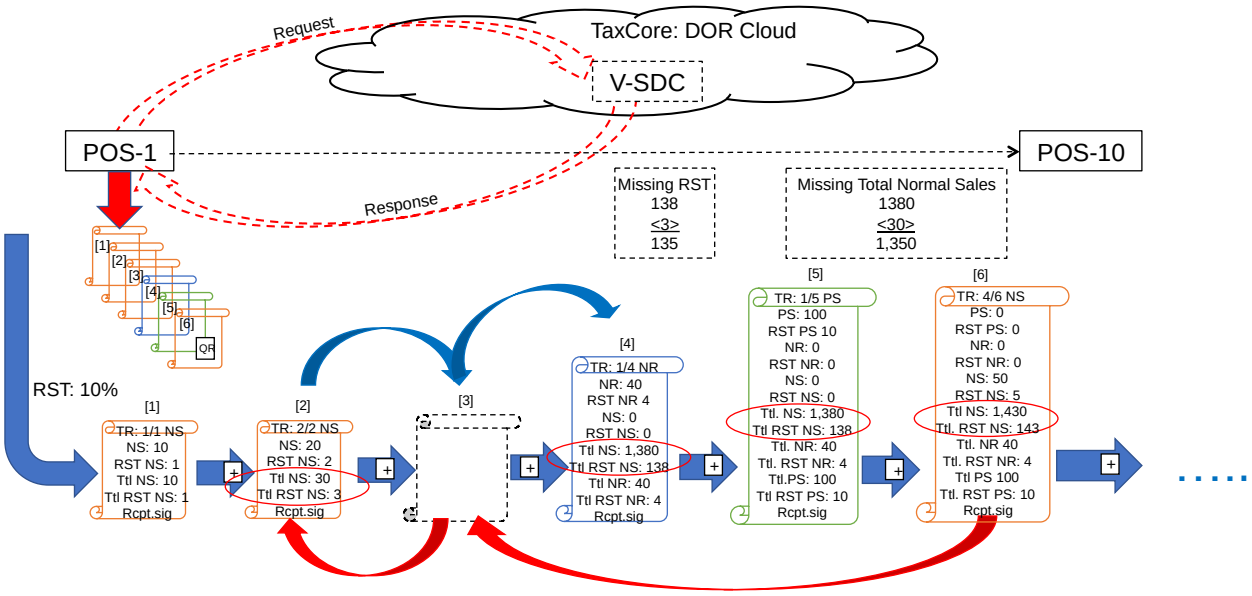
On high traffic days in the summer it is common to find one or more skaters entering their sales late in the day having sold burgers, collected funds, and made change for individual purchases with cash-on-hand. The DOR has long suspected that the owner suppresses sales with a Zapper or Phantomware. The preferred target for manipulation (the DOR suspects) is one or more of the largest sales tickets.

Figure 4 (below) replicates the facts of Figure 3 (above). In figure 4 receipt number 3 is missing. This was the exceptionally high sale of 1,350.

The first thing the counters do is they show how to derive the missing sales amount (1,350) and missing RST amount (135). The sixth receipt confirms that the missing receipt must be a NS. The sixth receipt is marked as the 4th NS receipt and the 6th receipt overall [TR:4/6 NS]. The receipt issued immediately prior to the missing receipt is [TR: 2/2 NS]. There is no other NS receipt in the chain, so the missing receipt must be the third NS.

We can calculate the tax attributes of the missing NS receipt. We know they are 1,350 in NS and 135 in RST, because the NS immediately prior to the missing receipt reported total NS of 30, and the receipt immediately after it reported total NS of 1,380 with total RST from NS at 3 and 138 respectively. It does not matter that the receipt coming after the missing receipt was not a NS. Aggregating counters preserve sales data continuously.

Figure 4
Fiscal Counters that support the Proof of Audit structure




What makes the counters so effective is that they are built into the receipts in a manner that builds a mini-blockchain. Each link (receipt) preserves the data embedded in the receipts before and after. The entire chain is lodged in Tax Core, replicated in the secure element of the taxpayer's certified POS, confirmed by every consumer or taxpayer who scans a receipt to verify its authenticity (by "pinging" Tax Core), and by any auditor (or AI program) that assembles the data embedded in the invoices and re-calculates each receipt.

There are two long-standing audit problems with missing receipts.[38] First, if an auditor identifies that receipts are missing from an audit file, it is almost impossible to determine how much was skimmed. As a result, the audit turns into an uncomfortable game of estimates and guesswork.

For example, in the hamburger shop setting described above, where sales are normally made in the $10 to $15 range. How would a traditional auditor determine that the amount suppressed was actually $1,350 in gross sales, $135 in RST, and not $15 for one burger and fries with RST of $1.50? The counters solve this problem directly.

The second problem is just as difficult to resolve. How does an auditor know that there is a missing receipt in the first place, and how quickly can the auditor find this out? The traditional approach is to suspect fraud, then send undercover consumers into the restaurant who (over a number of days) purchase meals for cash, and save the receipts. The auditor then begins a search

[38] The diagram presents the most common fact pattern where "missing receipt numbers" or "gaps" in receipt sequences are the result of actual receipts that are missing. Depending on the specific POS configuration technology-based errors could arise from the way the POS handles voids, or perhaps with the internal numbering system employed by the POS. Permutations following these error patterns are not considered here, but are equally well resolved with the Fiji/Seattle system.

in the taxpayer's records to see if any receipts have been removed. Aside from being time consuming, this method is inherently hit or miss.

This is where the Fiji/Seattle system turns again to the counters. The context is the automated *proof of audit.* V-SDC's and E-SDC's are programmed to continuously assemble "audit packages," essentially complete receipts (or a collection of several complete receipts). The "audit package' is the full journal record. In other words, it is all the meta data related to a transaction.

V-SDC's and E-SDC's are programmed to upload audit packages to TaxCore on a regular and continuous basis. The upload is authenticated with the Secure Element (SE). If TaxCore allows a successful upload, the V-SDC or E-SDC then requests a *proof of audit.*

The proof of audit function takes the new data and moves backwards (link-by-link) through the mini-blockchain, confirming that all of the data (including the data from the new audit packages) contained in the POS and the associated Secure Element (SE) have been accurately recorded in Tax Core. Nothing is missing, nothing is manipulated, and all the counters are working properly.

In the example above, when an audit package is assembled and submitted for the fourth receipt [TR: 1/4 NR], the *proof of audit* should fail. It will fail because the third receipt is missing. Similarly, the *proof of audit* requested after the fifth [TR: 1/5 PS] and sixth [TR: 4/6 NS] receipts should also fail, and fail for the same reason. Receipt three is missing.

The V-SDC and/or E-SDC will continue to upload receipts. They will continue to request a proof of audit, and continue to fail the *proof of audit*. TaxCore will notify the DOR that something is amiss at the hamburger shop, and an auditor should be assigned to visit the business. Similar notices are regularly being sent to the owner. Everyone is aware of the problem.

There is one more step.

Each counter has a pre-set cap. The DOR determines each cap, per counter, and per certified POS. If we assume that the cap set by the DOR on the NS counter at the hamburger shop is $1,500, then after the sixth receipt we are $1,430. There is only $70 in "cap room" left to work with. If receipts are issued in excess of $70, the system will shut down. The POS will no longer issue fiscal receipts.

This is the place where the monetary fines for issuing invalid receipts become important in most jurisdictions.[39] However in the Washington State pilot, if a business subject to RCW 82.32.290 (4)(a) is issuing receipts without a monitoring device they would be in violation of the basic agreement with the DOR. This would likely result in closure of the business.

There are three solutions to a business reaching the cap limit. If the owner of the hamburger shop can find the missing receipt, he should enter it in the accounting system. A

[39] See *supra* note 23.

*proof of audit* request will immediately be sent and returned successfully. All the counters will be re-set to zero. A second option would be for the customer to scan the QR code on the receipt originally issued by the hamburger shop. This would also register the sale in the accounting system, and initiate a *proof of audit* request. The third solution is to undergo a DOR audit, pay the tax, penalties and interest and secure a DOR reset of the counters.

The Fiji/Seattle system clearly answers the most difficult sales suppression questions. It alerts tax authorities (and the taxpayer) early on that sales suppression has been detected, and needs to be resolved. It also allows precise calculations of the amount of the suppression so that the eventual audit can be accurate, that is, if is there is no earlier resolution of the apparent suppression is found.

## CONCLUSION

The State of Washington's pilot program on preventive technology for monitor electronic sale suppression is extraordinary, both in its design and in its implementation.[40] As pilot programs go, this is a uniquely marketplace-driven effort controlled by self-interest and achievement not by fiat. This is not a top-down pilot. It is a DOR hands-off, but outcome-controlled effort that forces the parties (POS providers, third-party security firms, and businesses/taxpayers) to explore the data security options that promise to counter suppression, and select the best.

For example, there is no POS manufacturer or standardized file format, no third-party provider of security systems recommended or even suggested by the DOR (not in person, in regulation, nor on a DOR web site). The desired outcome is very clear, but the means each taxpayer will employ to achieve that outcome is not dictated. It is entirely up to the taxpayer to find an acceptable solution, pay for it, present it to the DOR and then convince the authority that

[40] One would not know much about the extraordinary design and implementation of Wong's Washington Pilot Project on electronic sales suppression from the Gartner Report. Gartner's assessment is "missing in action." This is most apparent in Gartner's closing pages (p. 66) where it lists "Key Opportunities for Improvement," in the section devoted to *Potential Policy, Business/Procedure, and Staffing Changes*, and more specifically where it targets *Formalization of Peer Agency Info Sharing: Formalize the process for interactions with government agencies*.

> PURPOSE: To enable better sharing of information relating to sales suppression and best practices around detection techniques, POS system/vendors, experiences with sales suppression etc.
> POTENTIAL CHALLENGES: Experiences in other states or countries may not be applicable due to different political climates. WA is further ahead than most states and might be mostly providing information with limited learning opportunities.

As this assessment of the redacted Gartner Report has shown, Gartner was really not aware of what Washington was doing in this area as it drafted its report for the legislature. Washington is indeed "further ahead than most states," but Gartner does not know why. Gartner seems to have had no knowledge of the pilot project in Seattle. The "experiences of other states or countries" are very applicable to Washington. In fact, the Seattle pilot project has borrowed heavily from Canada, Europe, and Fiji, although as a first-in-the-nation effort it has not borrowed from other US states. But more importantly, Washington is 'further ahead" precisely because it has borrowed from the "experiences of others." Washington should be willing and anxious to share what it has learned from others. Sales suppression is a near universal fraud, not a fraud that varies by political climates. We are sincerely, "all in this together."

this solution solves sales suppression, as the DOR sees it.[41] Without reaching an agreement with the DOR, the taxpayer may not continue to engage in business in the state. The Washington statute is very clear.

> The person, if the person is engaging in business subject to tax under this title, or the business in which the person participates, [must]*enter[s] 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.[42]

There is no rule, regulation or other guidance provided by the DOR on what constitutes "a method acceptable to the department." It is up to the taxpayer to find an acceptable method.[43]

In a very real sense, the State of Washington's electronic monitoring pilot project has been designed, developed, and paid for by Ms. Yu-Ling Wong. Without her sincere efforts to try one solution after another, the State of Washington would not have an electronic monitoring pilot. Washington would not be on the "cutting edge" without her.

The Gartner Report is another story. Gartner conducted a worldwide search for monitoring systems for the Washington State Legislature. It found the "cutting-edge" solution in Fiji. It found Fiji's answer, not because they went to Fiji to investigate, but because they read about it in our earlier papers. Although Gartner quoted from our earlier papers, anointed the Fiji solution as the "cutting-edge" in sales suppression technology, they apparently did not know that there were already five installations of the Fiji solution in Seattle Washington.

Is Washington's application of the Fiji solution analyzed in the unredacted portion if the Gartner Report? Very unlikely. Gartner indicated that to the best of its knowledge, the Fiji alternative "... has not been deployed in the United States to date."[44] The Washington State Legislature would probably have found it useful if Garner had noted the five Seattle installations, and considered the reasons for switching from Gartner's recommended Alternative #2 to the Fiji-like Alternative #4 in the pilot. If it had been so aware, and if it had applied its analytical tools to the ongoing pilot project, Gartner could then have either revised its analysis, or further justified their belief that the rejected Alternative #2 was indeed "the highest rated option among the four Alternatives."[45] As it stands, the Gartner Report seems uninformed.

[41] This facet of the Washington pilot program is also deserving of commentary by Gartner, but appears to be missing in the redacted report. For this kind of highly flexible, open-concept pilot to work requires a reasonable DOR that is system-knowledgeable, and open to new technology, and ideas. The taxpayer will always face uncertainty under this model, making workability a function of DOR adaptation.

[42] RCW 82.32.290(4)(b)(iii) (emphasis added)

[43] As the pilot matures, it is inevitable that the DOR will end up with numerous and possibly disparate solutions that it will eventually want to integrate, if not select a single source as a preferred monitoring solution.

[44] Gartner, *Report* at 129.

[45] Gartner, *Report* at 132.