taxnotes®

state

Volume 94, Number 9 ■ December 2, 2019

Washington's 'Cutting-Edge' Solution To Combat Sales Tax Fraud

by Richard T. Ainsworth, Robert Chicoine, Andrew Leahey, and Sunder Gee

Reprinted from *Tax Notes State*, December 2, 2019, p. 717

Washington's 'Cutting-Edge' Solution To Combat Sales Tax Fraud

by Richard T. Ainsworth, Robert Chicoine, Andrew Leahey, and Sunder Gee


Richard T. Ainsworth


Robert Chicoine


Andrew Leahey


Sunder Gee

Richard T. Ainsworth is an adjunct professor at the Boston University graduate tax program and the New York University graduate tax program. Robert Chicoine focuses his practice on criminal and civil tax controversy matters at Robert Chicoine Law in Seattle. Andrew Leahey is a tax and technology attorney pursuing an LLM in taxation at New York University. And Sunder Gee is a data analytic specialist and former electronic commerce audit adviser with the Canada Revenue Agency.

In this article, the authors discuss Washington's solution to address sophisticated tax fraud in the digital age.

Globally, consumption tax compliance for value added tax and retail sales tax (RST) 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 nearly real time.[4] This is the trajectory for the modern RST imposed by most U.S. states. While this may appear to be revolutionary to the average American tax practitioner, it is a well-worn path among global nations using the VAT. The RST will eventually follow. Washington state 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

[1] *See, e.g.*, the Council Implementing Decision (EU) 2018/593 of Apr. 16, 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). This would "introduce mandatory electronic invoicing for all taxable persons established in the territory of Italy, . . . [it would] apply from 1 July 2018 until 31 December 2021."

[2] *See, e.g.*, Trustweaver, "Tax-Compliant Global Electronic Invoice Lifecycle Management," 3 (White Paper 9th edition, Feb. 2018), 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); and OECD, "Technology Tools to Tackle Tax Evasion and Tax Fraud," 13, 16 (2017).

[3] *See, e.g.*, Smart Cloud Inc., "Tax Intelligence System," Microsoft Appsource & Press Release (Mar. 21, 2019) (discussing the XAI Tax Intelligence System in operation in the State of Ceará, Brazil — soon to expand to four other states); and Patricia Araújo Vieira et al., "Effects of the Electronic Invoice Program on the Increase of State Collection," *Revista de Administração Pública* (Apr. 25, 2019).

[4] *See, e.g.*, PwC — Poland, "Mandatory Split Payments From November 1, 2019" (July 22, 2019).

operating a highly regarded Asian restaurant in Seattle.

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

There were four scenarios that were numbered, characterized with a single word, differentiated by their primary focus, and then made more concrete by identifying what Gartner Inc. — the consulting firm that conducted the study — considered to be a representative country for each scenario.

- Alternative 1: Foundational — Internal Focus ("Like U.K."), but more likely Japan;[7]
- Alternative 2: Targeted — External Focus ("Like Netherlands");
- Alternative 3: Broad — External Focus ("Like Belgium"); and
- Alternative 4: Cutting Edge — External Focus ("Like Fiji").[8]

Unfortunately, the report lacks reference to an ongoing pilot project conducted by the DOR as a result of a plea agreement in *Washington v. Wong*.[9] The plea 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 used first on May 30, 2017. It was replaced on April 2, 2019, with a fully digital solution installed by a European firm, Data Tech International, which pioneered the cutting-edge solution with its work in several jurisdictions, 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 Gartner report, but they do not appear in the redacted version.

Alternative 2 ("Like Netherlands") requires establishing a productive working relationship among three parties: the DOR, the POS firm, and the business. The idea behind Alternative 2, which is unlikely to work in a marketplace 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 on what is commercially reasonable is necessary. In this case any synergies between the DOR and the POS firm were negated by problems created for operation of the business,[12] which wanted change and was willing to participate in and fund installation of cutting-edge technology.

[5] Gartner Inc., "A Report for WA Department of Revenue, Deliverable 7: Final Report" (Apr. 22, 2019), Engagement 3300052217.

[6] *Id.* at 126.

[7] Placing the U.K. as the representative country for Alternative 1 is emblematic of the deficiencies in the Gartner report. If Gartner needed an example of an internally focused, foundational country, the classic example would have been like Japan, not the U.K., but Gartner does not consider Japan. Instead, it supports its U.K. selection with references to analysis in a paper on Quebec's Sales Recording Module (Richard T. Ainsworth and Urs Hengartner, "Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud With Technology," 57 *Canadian Tax Journal* 715 (2009).) A more appropriate source would have been: Ainsworth, Musdaad Alwohaibi, and Mike Cheetham, "A High-Tech Proposal for the U.K. and Saudi VATs: Fighting Fraud With Mini-Blockchains and VATCoins," *Tax Notes Int'l*, Nov. 11, 2019, p. 511). This paper compares developments in the U.K.'s Making Tax Digital (MTD) program, with similar efforts in the Kingdom of Saudi Arabia's Esal program. Gartner's redacted report contains no reference to either.

Since 2014 the U.K. has been working on the MTD program. It took effect April 1 — 21 days before the Gartner report was submitted. The omission is glaring. The U.K. is not "focused on incremental improvements in key supporting technologies for improving auditing processes." It is a back-end digitization and universal mandate to help taxpayers comply and to prevent fraud. *See* U.K. Office of Tax Simplification, "Technology Review: A Vision for Tax Simplification," at paras. 1.100, 1.20 (Jan. 2019).

[8] Gartner, *supra* note 5, at 120-133.

[9] No. 16-1-00179-0 (Wash. Super. Ct. 2017).

[10] Portugal illustrates the problem. The Portuguese have made mandatory the OECD's Standard Audit Files for Tax (SAF-T) reporting regime. ESS delete sales from the POS, leaving little or no artifacts. Reports are then generated from the POS and 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, *supra* note 5, at 126.

[12] For example, in *Wong* the chefs wanted orders sent to the kitchen in Chinese. The original POS lacked that functionality, which significantly affected business flow. The speed of the kitchen should not be constrained by tax authority impositions. Monitoring must be seamless.

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.

Even though the redacted report is weakened considerably by not referring to the ongoing pilot project, there is a lot to learn from the choices made by the DOR and Yu-Ling Wong. One gets the impression that Washington — like Fiji and several other foreign jurisdictions — is operating at the cutting edge in applying technology solutions to consumption tax problems.

This paper intends to explain the inner workings of Washington's cutting-edge pilot. What is happening in Washington is happening nowhere else in the United States. Wong, the owner of the pilot participants, Facing East and QQ Taiwanese Bite restaurants, 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 would not be at the forefront of solving tax fraud through technology.

Wong's Washington Pilot Project: An Anti-Sales-Suppression Program Modeled on Fiji

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 *Wong*.[14] This is the state's first judicially resolved case involving an automated sales suppression device.[15] Months of negotiations led to the agreement, which was finalized on August 30, 2017.[16] The negotiations focused on a practical technology solution to monitoring sales data and on protections for taxpayers who, for whatever reason, are being monitored by taxing authorities. The initial monitoring agreement followed Gartner's Alternative 2 model (although it was selected before Gartner began its research) and was rejected and replaced on April 2, 2019, with the current Alternative 4 model.[17]

The taxpayer admitted during a civil audit that she had violated Wash. Rev. Code section 82.32.290 (4)(a) by knowingly possessing and using a "zapper" to suppress sales.[18] Potential statutory penalties were severe. Not only were all taxes, penalties, and interest lawfully due,[19] but incarceration of up to five years, a $10,000 fine, or both were possible.[20] An even more severe penalty for the taxpayer prohibited her from participating in any business unless she "enter[ed] 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]

[13] Gartner, *supra* note 5, at 126.

[14] No. 16-1-00179-0.

[15] For a discussion of Washington's thought process as it worked through its electronic sales suppression problems before the Gartner report, see Richard T. Ainsworth and Robert Chicoine, "Fighting Technology With Technology: Taking Aim at Electronic Sales Suppression," *State Tax Notes*, Mar. 12, 2018, p. 995.

[16] For an analysis of Washington's first electronic monitoring agreement, see Ainsworth and Chicoine, "Zapped! An Analysis of Washington's Electronic Monitoring Agreement," *State Tax Notes*, Mar. 5, 2018, p. 885.

[17] An analysis of the technology requirements in Washington's electronic monitoring agreement which were met by both the Alternative 2 and Alternative 4 models is discussed in Ainsworth and Chicoine, "The Technology Requirements of the First Electronic Monitoring Agreement in U.S. for Zappers," *State Tax Notes*, Oct. 16, 2017, p. 239.

[18] A zapper places sales suppression programming on a removable CD or memory stick. Phantomware is similar suppression programming that 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.

[19] "Lawfully due" is statutory language that is undefined in statute or regulation. This is problematic for audit and in settlement because the amount of tax should not be left to the DOR's discretion.

[20] Wash. Rev. Code section 9a.20.021.

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

A major problem was that the DOR did not have a specific acceptable method in mind, although it did have criteria. The taxpayer was required, at her expense, to find a solution that met the DOR criteria. She elected to do so to remain in business, negotiated a favorable plea agreement, and reached a stipulated civil restitution 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 spared no expense in her efforts to "make this monitoring work" for the state. There were dropped orders and system shutdowns, and when it became apparent after more than a year 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.

The Fiji model comprises two elements: (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 in real time by the DOR through proprietary software called Tax Core.[24] The TaxCore validation includes a digital signature on the receipt and a verifying hyperlink in the QR code.[25] The process is called "the fiscalization" of the receipt or 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 tax authority software issues the response. The fiscalizing system operates both online and offline.[26]

It is important to realize how quickly this process moves and how the speed (coupled with the technology's security features) provides additional protection against zappers and "phantomware." The process described below is fully encrypted, saved in multiple locations that can be cross-referenced, 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 it takes to swipe 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 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 purchase's digital loop. Both the sales amount and tax paid would be identified. All tax attributes would be confirmed.

The figures illustrate the two-step request and response procedure at the heart of the Fiji anti-sales-suppression system.

[22]Wong was able to negotiate a civil tax assessment that was significantly less than the DOR's original proposal. No small part of this success was because of her willingness to cooperate and assist the DOR as it tried to find workable monitoring solutions.

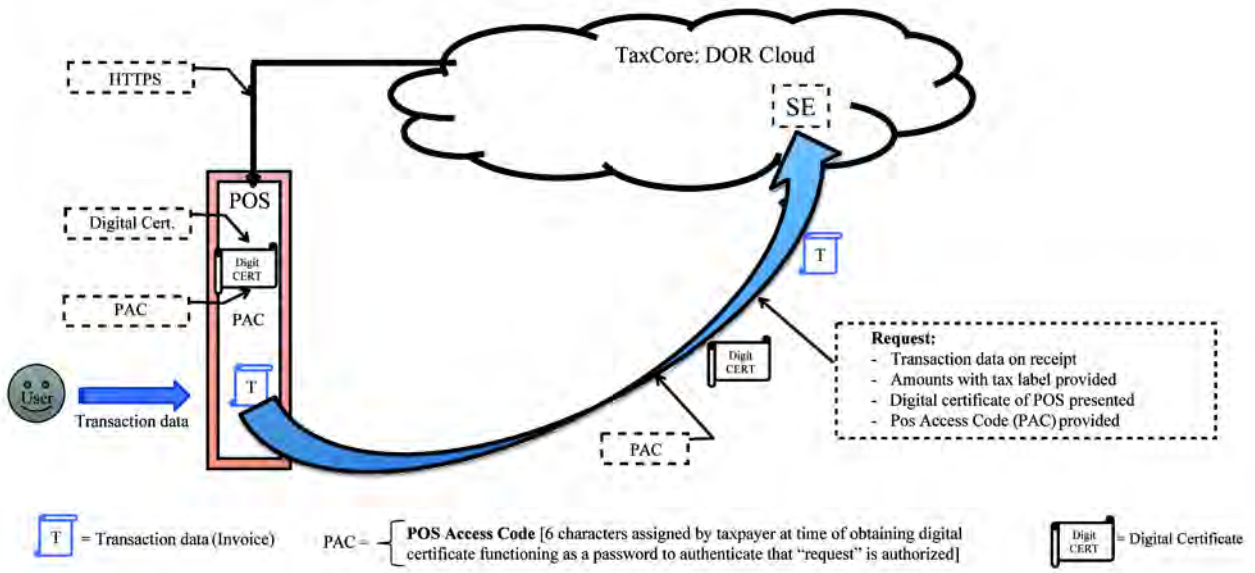
[23]There is no monetary penalty in Washington for not issuing a valid digital receipt other than breach of the monitoring agreement. It is expected that if the pilot is considered a success and is adopted more widely, then Washington would follow other jurisdictions and impose monetary penalties. Penalties 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 offense within five years, and $5,000 to $50,000 for multiple offenses within five years. Sanctions related specifically to the Sales Recording Module are $300 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. In Brazil, commercial law requires invoices to be digital to be enforced. Tax compliance follows commercial practice. See Decree 6022 of 2007, which 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 up to $50,000 (Fiji dollars) depending on the gross annual turnover of the business. Government of Fiji Gazette, "Tax Administration Act 2009 (Electronic Fiscal Device) Regulations 2017," article 23 (June 1, 2017).

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

[25]The QR code is not unique. Many countries use QR codes on the receipt — even Quebec uses a 2D bar code — but none except Fiji's has an embedded hyperlink that will lead the person scanning it to the tax authority's web service, where a confirmation of the validity of the receipt can be obtained firsthand.

[26]There are minor hardware differences between an online system (using a virtual sales data controller — V-SDC) and an off-line system (using an external sales data controller — E-SDC). Cost is not a factor. Most locations in Fiji use both online and off-line. The technical differences are discussed in Ainsworth and Goran Todorov, "Fiji: A Digital Invoice System Fights Fraud and Enforces Real-Time VAT Compliance," *Tax Notes Int'l*, Nov. 12, 2018, p. 697.

Figure 1.
Request for Fiscal Invoice [accredited POS]



Source: Reprinted from Richard T. Ainsworth and Goran Todorov, "Fiji: A Digital Invoice System Fights Fraud and Enforces Real-Time VAT Compliance," *Tax Notes Int'l*, Nov. 12, 2018, p. 697.

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) either on the taxpayer's premises or in TaxCore at the DOR.[28] The transaction data elements[29] will be combined with the POS's digital certificate and POS access code[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).

The Response — Figure 2

After confirming the validity of the request, the SE associates the previously specified transactional data with additional elements as required by the system,[31] including a digital signature and the verification URL through which the POS can generate a QR code. The result is the fiscal invoice. The customer or any other party can scan the QR code printed on the receipt or 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 and get an immediate assurance that the receipt provided by the cashier is properly reported in Washington's TaxCore.[32]

[27] There is no requirement that a POS system be used. The reference to POS could be replaced by several other platforms: a mobile POS app; a cashier working off a desktop computer with an app; an online shopping forum; an invoice-generating enterprise resource planning system. This paper will use POS generically to mean all of these.

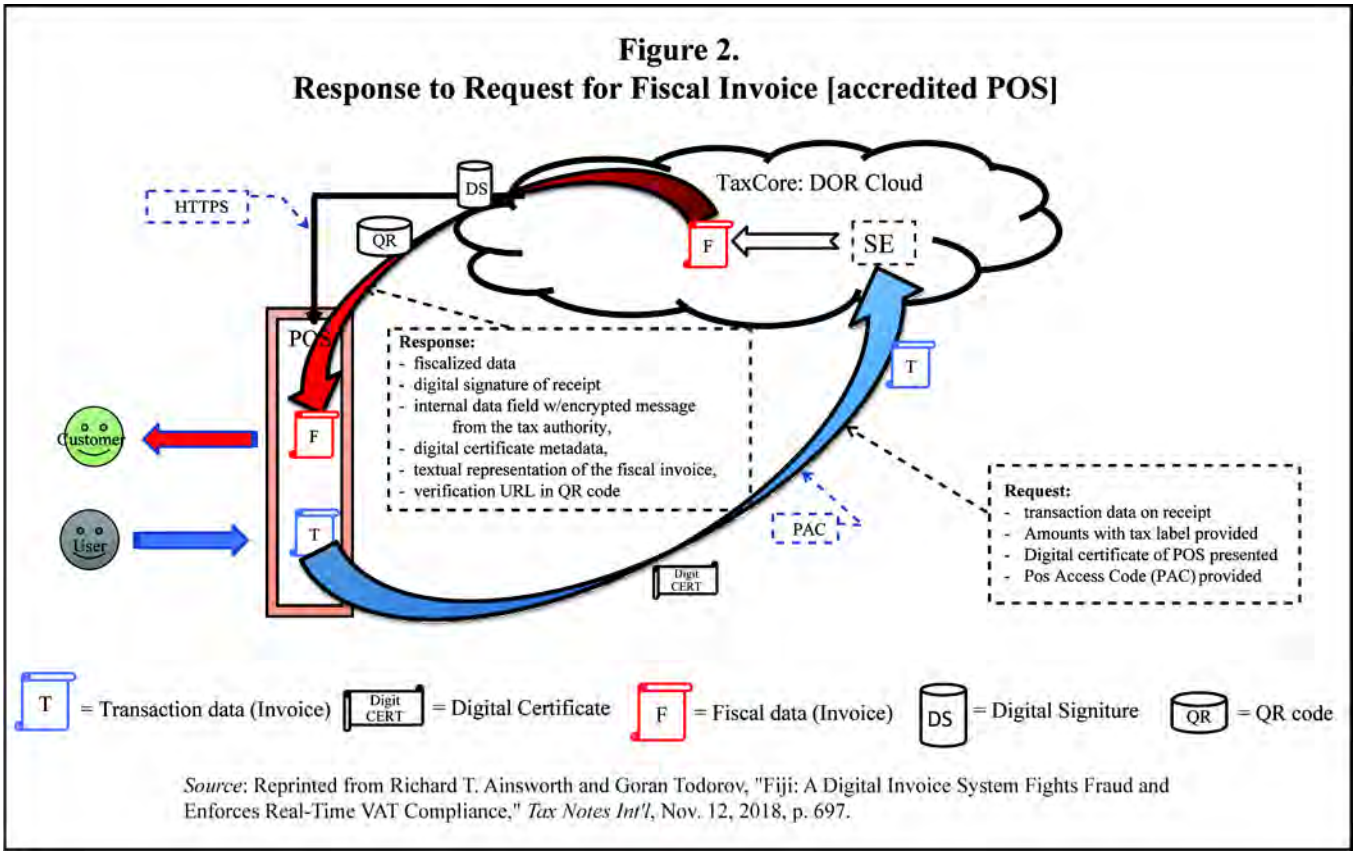
[28] Figure 1 illustrates the V-SDC.

[29] In Fiji these elements are specified in EFD reg. section 20(2)(a)-(j).

[30] The POS access code comprises six characters assigned by the taxpayer when it obtains the digital certificate, and it functions as a password to authenticate that the fiscalization request has been authorized.

[31] In Fiji these elements are specified in EFD reg. section 20(2)(k)-(o). In *Wong*'s installation these elements are added to facilitate the workability and security of the system without mandatory or statutory demands.

[32] The traditional method of finding electronic sales suppression is the expensive multi-step process of dispatching undercover auditors to a restaurant who purchase a meal with cash and save the printed receipt, collecting several receipts from that location at different times of the day and providing them to the official audit team, which searches for the receipts in POS records. For many reasons, this traditional method has been largely inefficient and ineffective.



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

Artificial intelligence engines are applied in Fiji and can be, but not yet, used in Washington. In Fiji's larger tax ecosystem, risk analysis and audit selection are streamlined. Audits are not chosen blindly or based on hunches — they are data-driven. The same will be true in Washington as the pilot project grows. But even at this level of engagement, there is much more in Washington's solution than what has been discussed. 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 Review

Fiji's fiscalized digital invoices and Washington's fiscalized receipts do more than confirm the accuracy of an invoice or receipt and construct a centralized database of transactions in TaxCore. They organize invoice data so that technology can be applied to tax problems. Three organizational structures dominate: (1) a mini-blockchain of invoices, (2) a counting system that sequences tax attributes, and (3) an automated proof of audit 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. Alternative 2 is premised on a DOR/POS provider partnership. Its goal is to produce a standard data output file. This neither assures data accuracy, nor does it elevate compliance. Standardized data output may facilitate traditional audit, but it goes no further.

There are real, substantive reasons why Alternative 4 is a cutting-edge solution. We consider them in the following sections.

Mini-Blockchain

With the Fiji solution, a mini-blockchain of transactions is preserved in the SE assigned to the POS, in the tax authority's TaxCore, and in the embedded QR code on each customer's receipt or invoice.

As with all blockchains, the data is permanent and immutable. It is currently 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 her transaction, but the mini-blockchain in which the transaction is preserved.

Counters

In the Fiji system, there is a mechanism for automated counting of tax attributes, receipt-by-receipt. This "count" is recorded and embedded in the QR code. This is non-discretionary. Counting cannot be turned off or adjusted, although a "cap" or limit can be set. The cap on each counter is preconfigured by the DOR. It is reset only by the Department.

Proof of Audit

Counters in the Fiji/Seattle solution start with customized caps (limits). When the 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 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 Counters Are the Key

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 pro forma sales (PS). Additional counters reside in the SE, which records line-item cumulative totals: cumulative turnover, tax totals, refund totals, per-tax refund totals, and others.

Figure 3 illustrates a single accredited POS which fiscalizes six receipts in a sequence. The diagram suggests that there can be 10 or more POS (or accredited invoice[34]) systems, but only one is represented.[35] In fact, the Washington pilot project has five accredited POS systems engaged. Three are at the Facing East restaurant, and two at the QQ restaurant. Three illustrated types of receipt are normal sales (NS), normal refund (NR), and pro forma sales (PS).

There are 12 tax attributes associated with these receipts. They are counted throughout this six-receipt sequence. Three counters relate to attributes of the receipt being considered (PS, NR, and NS), and three more relate to the associated RST (RST on NS, RST on NR, and RST on PS). Six additional counters sequentially aggregate these amounts throughout the sequence (Ttl. PS, Ttl. NR, Ttl. NS, Ttl. RST on NS, Ttl. RST on NR, and Ttl. RST on PS).

[33] Sales transactions 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 and collects and remits RST, in cases of missing receipts the buyer can declare the purchase and report his tax payment to the seller. This occurs in the Fiji 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* Ainsworth and Chang Che, "Data First, Tax Next: How Fiji's Technology Can Improve New Zealand's Netflix Tax (Electronic Marketplaces) (Part 3)," *Tax Notes Int'l*, Sept. 23, 2019, p. 1249.

[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 POS system is one specific application on an AIS.

[35] The simplicity of the diagram in Figure 3 should not be underestimated. If POS-1 were Amazon, these six transactions would occur in less than 100th of a second. Jay Yarow, "Amazon Was Selling 306 Items Every Second At Its Peak This Year," *Business Insider* (Dec. 27, 2012) (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 business-to-customer transactions. This application has been explored in Ainsworth and Che, *supra* note 33.

Table 1 – Data Applied in Figures 3 and 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

A summary of the data used in Figures 3 and 4 is provided in Table 1.

Figure 3 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.

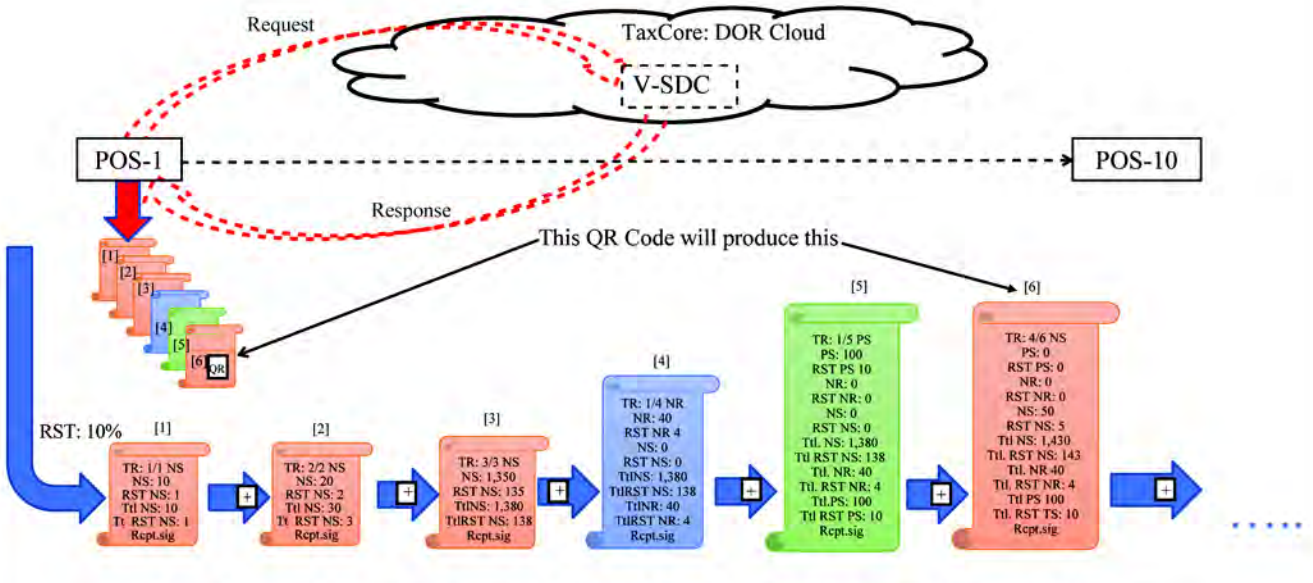
Figure 3 assumes that these are the first six transactions in a business cycle. The first three transactions (receipts) are normal sales (NS), followed by a normal return (NR), and then a pro forma sale (PS), before returning to make another normal sale (NS) at the sixth receipt.

Each receipt's QR code can be scanned by the purchaser or a tax auditor. The purchaser will see in an unequivocal format the complete data set of all information on the invoice. A scan by the tax authority would disclose more data. Some QR data is encrypted, but 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 percent 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 increases the third receipt's aggregates to total normal sales of $1,380 and total RST collected from normal sales of $138.

Figure 3.
Fiscal Counters Supporting the Proof of Audit Structure



Source: Reprinted from Richard T. Ainsworth and Goran Todorov, "Fiji: A Digital Invoice System Fights Fraud and Enforces Real-Time VAT Compliance," *Tax Notes Int'l*, Nov. 12, 2018, p. 607.

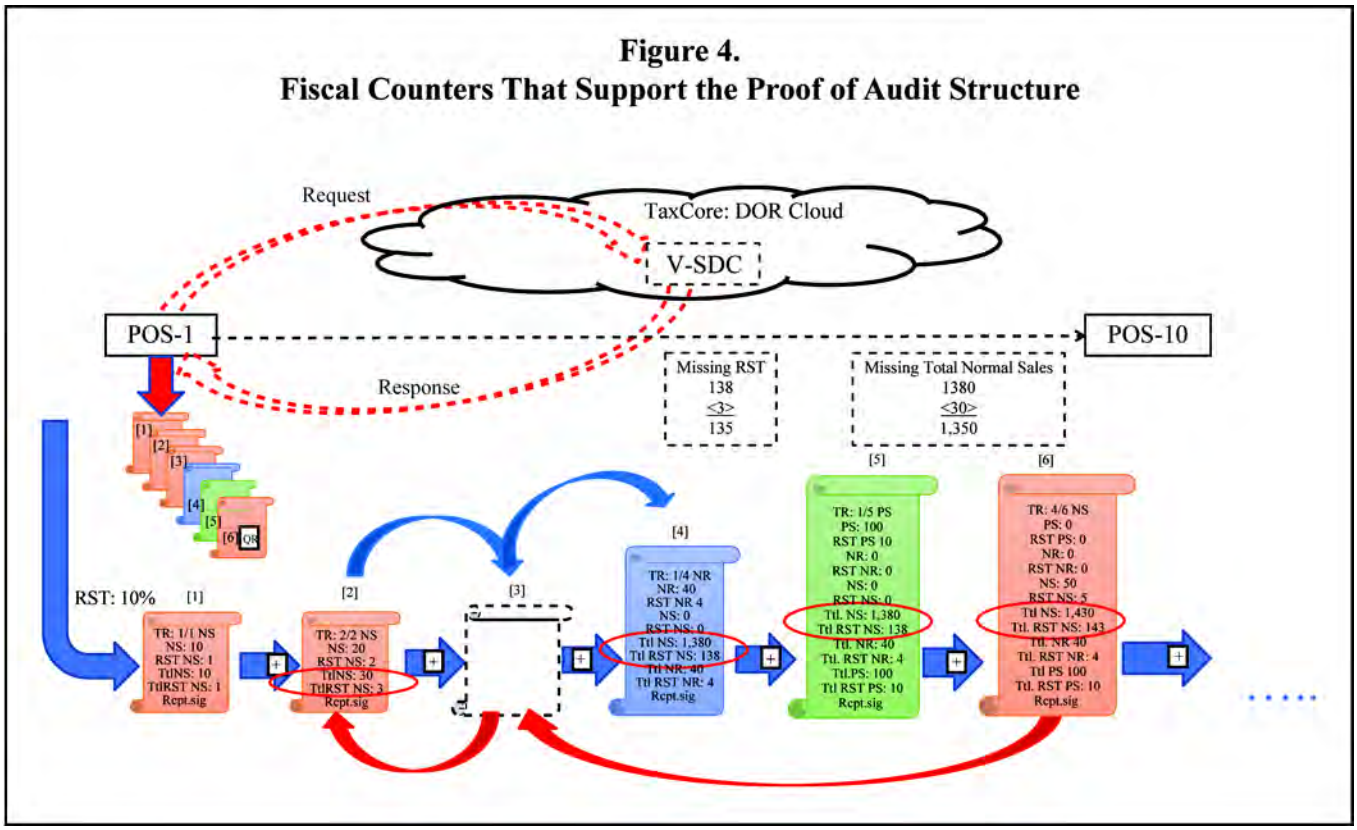
The fourth and fifth receipts record different functions. Receipt four is a normal refund, and receipt five is a pro forma sale.[36] Each receipt has a base number and a related RST amount. The diagram at Figure 3 shows receipts 4 and 5 to be larger than the first three receipts. This reflects the larger data content from the use of new counters, and that counters do not aggregate data across categories. For example, normal refunds and their related RST are not netted against normal sales and their related RST. NS and NR are separate counters. Counters initially record and report 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 (pro forma) receipts. However, as a NS, receipt 6 can 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.

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 connected 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 SE is embedded in TaxCore, or (b) associated with an external sales data controller (E-SDC), where the SE is loaded on a smart card inserted in the SDC.

[36] A pro forma sale occurs in a restaurant when a waiter drafts a trial receipt to show customers what an order will cost before a decision is made to place the order.

[37] This function is like the Portuguese solution when 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 in the tax administration and the customer-based links related to the scanned QR codes.



The Facing East and QQ restaurants in Seattle are associated with both V-SDCs and E-SDCs and work easily online or off — the system technology doing the work does not change. Regardless of the setup, the tax problem the counters solve is the identification of (and if possible, the recovery of) missing receipts.

Example

The following hypothetical is designed to highlight two of the most common audit problems with missing receipts: (1) If a receipt is missing, how can an auditor determine the tax able amount and the tax properly due? (2) How is an auditor to determine that a receipt is missing in the first place?

Assume that certified POS-1 is located at a small hamburger shop where normal sales are $10-$15 and occasionally as much as $50, but rarely $100. However, on special occasions (holidays, public gatherings in the neighborhood) single-ticket charges can increase considerably. There are two kinds of exceptionally large sales made by the hamburger shop: bulk sales to corporations in the area that provide free meals for their employees who are asked to work long hours on occasion, and street sales by roller skating servers.

This hamburger shop is popular because its servers 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 for skaters to enter their sales late in the day, having sold burgers, collected funds, and made change for individual purchases with cash on hand.

Suspicion of Fraud

The DOR has long suspected that the owner of the hamburger shop suppresses sales with a zapper or phantomware, and that the preferred target for manipulation is one or more of the larger sales tickets. Figure 4 replicates the facts of Figure 3. However, in Figure 4, receipt number 3

is missing. This was the exceptionally high sale of $1,350.

The first thing the counters do in this situation is show how to derive the missing sales amount ($1,350) and missing RST of $135. The sixth receipt confirms that the missing receipt must be a NS. The sixth receipt is marked as the fourth NS receipt and the sixth receipt overall (TR: 4/6 NS). The receipt issued immediately before 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 that the (NS) sale was for $1,350, and there was $135 in RST collected because the NS immediately before the missing receipt reported total NS of $30, and the receipt immediately after it reported total NS of $1,380. Similarly, with total RST from NS at $3 (on the prior receipt) and $138 on the receipt following, the RST in this case was $135. It does not matter that the receipt coming after the missing receipt was not a NS. Aggregating counters preserve sales data continuously.

Mini-Blockchain

What makes the counters so effective is that they are built into the receipts in a way that builds a mini-blockchain. Each receipt preserves the data embedded in the receipts before and after. The receipts are linked. The entire chain is lodged in TaxCore, replicated in the SE of the taxpayer's certified POS, confirmed by every consumer or taxpayer who scans the QR code on their receipt to verify authenticity. Consumers build consensus by "pinging" TaxCore and by any auditor (or AI program) that assembles the data embedded in the invoices and recalculates each receipt, confirming the blockchain's validity.

Solving the First Missing Receipt Problem

This solution is ingenious, simple, and effective.[38] Auditors that manage to identify a receipt is missing from an audit file find it almost impossible to determine how much was removed in sales and how much in tax 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 $10-$15. How would a traditional auditor determine that the amount suppressed was actually $1,350 in gross sales and $135 in RST, and not $15 for one burger and fries with RST of $1.50? The counters solve this problem.

Solving the Second Missing Receipt Problem

The second missing receipt 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 to purchase meals for cash over several days and save the receipts. The auditor searches the taxpayer's records to see if any receipts have been removed. Aside from being time consuming, this method is inherently hit or miss.

Once again, the Fiji/Washington system turns to the counters. The context is the automated proof of audit review. V-SDCs and E-SDCs 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 — all the metadata related to a transaction.

V-SDCs and E-SDCs are programmed to regularly and continuously upload audit packages to TaxCore. The upload is authenticated with the 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 the prior data, including the data from the new audit packages, in the POS and the associated SE are recorded in TaxCore and that 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 because the third receipt is missing. Similarly, the

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

proof of audit requested after the fifth (TR: 1/5 PS) and sixth (TR: 4/6 NS) receipts should fail for the same reason: receipt 3 is missing.

The V-SDC 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 sent to the owner. Everyone is aware of the problem.

There is one more step. Each counter has a preset 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 at $1,430. There is only $70 in cap room left. If receipts over $70 are issued, the system will shut down and the POS will no longer issue fiscal receipts.

This is when the monetary fines for issuing invalid receipts become important in most jurisdictions.[39] However, in the Washington pilot, if a business subject to Wash. Rev. Code section 82.32.290(4)(a) is issuing receipts without a monitoring device, it would be violating the basic agreement with the DOR mandating closure per the statue and the agreement. This would likely result in closure of the business.

There are three solutions for a business that has been shut down after reaching the cap limit:

(1) If the owner of the hamburger shop can find the missing receipt, he should enter it in the accounting system. A proof of audit request will immediately be sent and returned successfully. All the counters will be reset to zero.

(2) A second remedy would be for the customer to scan the QR code on the receipt originally issued by the hamburger shop. This would register the sale in the accounting system and initiate a proof of audit request.

(3) The third solution is to undergo a DOR audit, pay the tax, penalties, and interest and secure a DOR counter reset.

The Fiji 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 allows precise calculations of the amount of the suppression so that the eventual audit can be accurate if there is no earlier resolution of the apparent suppression.

Conclusion

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

There is no POS manufacturer, standardized file format, or third-party security system provider recommended — or even suggested — by the DOR. The desired outcome is clear, but the means each taxpayer will use to achieve that outcome is not dictated. It is up to the taxpayer to find an acceptable solution, pay for it, present it to the DOR, and then convince the authority that this solution solves sales suppression as the DOR sees it.[41] Without reaching an agreement with the DOR, the taxpayer may not continue to operate a business in the state. The Washington statute is very clear that such a business must

[39] *See supra* note 18.

[40] One would not know much about the design and implementation of the pilot project on electronic sales suppression from the Gartner report. 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. Regarding that issue, the report states:

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.

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

"enter[] into a written agreement with the department for the electronic monitoring of the business's sales, by a method acceptable to the department, for five years at the business's expense."[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 it.[43]

In a very real sense, Washington's electronic monitoring pilot project has been designed, developed, and paid for by Yu-Ling Wong. Without her efforts to try multiple solutions, Washington would not have an electronic monitoring pilot and it certainly would not be on the cutting edge. Washington's pilot project is important for several reasons:

- It is the first of its kind in an area of tax administration that is close to nonexistent. Technology is being used to combat technology-based tax fraud.
- Its potential to ensure accurate compliance with tax statutes and raise revenue is enormous.
- It allows taxing authorities, such as the Washington DOR, to confidently oversee business activities remotely — while they actually occur — in a manner that potentially has minimal commercial impact on the business involved but is vastly more efficient than traditional antiquated audit methods.
- Real-time capture of tax data and secure transmission to tax authorities is the international standard and is a proven way to combat the underreporting of income that should be legitimately subject to tax for the common good.
- It may be the beginning of an eventual change in state legislation, which will require its use in situations other than criminal law enforcement. The day may come when federal or state governments mandate that all businesses in a specific economic sector join a real-time electronic monitoring program. ■

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

[43]As the pilot grows, 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.