FIJI - MANDATORY DIGITAL INVOICES

REAL-TIME VAT COMPLIANCE

notes:

FIJI – MANDATORY DIGITAL INVOICES REAL-TIME VAT COMPLIANCE

Richard T. Ainsworth, NYU
Goran Todorov, DTI

Fiji, the largest of the Pacific Island Countries (PICs), is implementing a comprehensive digital invoice regime with the goal of the automatic, real-time and encrypted reporting of *all taxable transactions*, business-to-business (B2B), and business-to-consumer (B2C). A pilot was launched and deemed successful.[1] The first phase (involving the supermarket and pharmacy sectors) has been completed.[2] Hardware companies, accounting firms, medical centers, travel agencies, and law firms are involved in the second phase. This is set for completion June 30, 2018.[3]

Fiji's technology reform is intended to increase VAT compliance. It has attracted global attention because the technology reform has been undertaken along with a 40% reduction in the VAT rate, an expansion of the VAT base, and a prediction that VAT revenues would increase. Fiji's single rate was reduced from 15% to 9% on January 1, 2016. At the same time, the VAT base was expanded by removing exemptions on rice, cooking oil, fish, flour, tea, powdered milk and kerosene.[4]

The 2016 Budget estimated that the net impact of these changes would be a *short-term reduction* in VAT revenues of FJ$87.4 million.[5] In the November 6, 2015 budget speech the Minister of Finance, Auyaz Sayed-Khaiyum, assured Parliament of a *long-term* revenue gain of FJ$38.5 million.[6] These are extremely difficult predictions to make, and it appears that both estimates missed the mark. *Short term reductions* were deeper, *long-term gains* are most likely greater.

The *short-term reduction* in VAT revenues came in at FJ$225,461,857. To meet 2016-2017 revenue projections 32% more VAT needed to be collected. VAT revenues were expected to be FJ$928,242,012. Actual collections were FJ$702,780,155.[7] This was a 22.6% improvement over 2015 when FJ$572.8 was collected, but it was far short of the revenue target, which was set well in advance of the rate reduction and the base expansion. Where is the missing revenue?

With FJ$928,242,012 as the *expected revenue* figure, and an anticipated *short-term loss* of FJ$87.4 million, we have an unexplained revenue loss of FJ$138,061,857.[8] What accounts for this projection-measured shortfall? The projection of short-term revenue losses is clearly due to the fact that the rate reduction was universal and immediate, and the adoption of digital security measures were gradual. This tension could have been mitigated if the rate reduction was tied to the business groups adopting the technology. For example, groceries would be taxed at 9%, when grocery stores adopted the digital security measures, others would remain at 15%.

Revenue sources not accounted for in the current measures are substantial. There is revenue yet to be realized between FJ$214,500,000 and FJ$217,350,000. These amounts are from:

- full roll-out of the technology reform, which can be roughly estimated at FJ$185 million (at a minimum), and
- revenues from closing structural flaws in the Fiji VAT – notably the inherent flaws that a *residence-based* VAT has when dealing with cross-border trade in services, and low-value goods, which can be roughly estimated for Fiji to be between FJ$29.5 and FJ$32.35 million.

---

[1] *VMS/EFD pilot successful: FRCS*, FIJI NEWS (December 19, 2017) *available at*: http://www.fbc.com.fj/fiji/57836/vmsefd-pilot-test-successful-frcs

[2] GOVERNMENT OF FIJI GAZETTE Vol. 18, No. 62 (July 3, 2017) publishing regulation 28 of the TAX ADMINISTRATION (ELECTRONIC FISCAL DEVICE) REGULATIONS 2017 indicated that completion of the first phase was set for December 31, 2017. However, it became necessary to extend the time for completion of the first phase to February 28, 2018. *Notice of Extension and Phase 2 Group* (December 27, 2017) available at: https://www.frcs.org.fj/news/2017-2/notice-extension-phase-2-group/ Even as of June 2018 phase 1 remains "open" in the sense that enforcement actions to clean up the registry have not commenced. The invitation to fiscalize is encouraging absentee owners to deregister inactive companies and revise declarations of business activity.

[3] GOVERNMENT OF FIJI GAZETTE Vol. 18, No. 122 (December 22, 2017) publishing regulation 28 of the TAX ADMINISTRATION (ELECTRONIC FISCAL DEVICE) REGULATIONS 2017 at (a) & (b); *No extension of time limits for VMS implementation: FRCS*, FIJI NEWS (December 19, 2017) *available at*: http://www.fbc.com.fj/fiji/59982/no-extension-of-timelines-for-vms-implementationfrcs

[4] It should be noted that these are supermarket inventory items, and the supermarket market segment was the in the first technology phase (completed in February).

[5] FJ$120 million from increased compliance, and FJ$108.6 million from base expansion, would be netted against losses of FJ$316 million attributable to the rate reduction.

[6] Jason Roberts, *Fiji's Proposal to Increase VAT Collection: Lower VAT Rate,* THOMSON REUTERS – TAX AND ACCOUNTING BLOG (November 13, 2015) *available at*: https://tax.thomsonreuters.com/blog/onesource/FijiVatProposal/ ; Amelia Schwanke, Fiji Budget 2016: VAT Cut and Administrative Streamlining, INRTERNARTIONAL TAX REVIEW, (November 11, 2015) *available at*: http://www.internationaltaxreview.com/Article/3505668/Fiji-Budget-2016-VAT-cut-and-administrative-streamlining.html

[7] Fiji Revenue and Customs Service, 2016/17 ANNUAL REPORT (August 1st to July 31st) *available at*: https://www.frcs.org.fj/wp-content/uploads/2017/12/annual-report-2015.pdf

[8] FJ$225,461,857 less FJ$87.4 million equals FJ$138,061,857.

If we combine the unexplained shortfall (FJ$138,061,857) with the promised long-term gain (FJ$38,500,000) then the funds needed to meet projected *long-term revenue gains* are FJ$176,561,857. This is roughly FJ$37,938,143 to FJ$40,788,143 less than what is *yet to be realized*.

This paper considers the mechanisms for the first of these (projected) increased revenue flows. The second revenue stream, derived from applying the lessons learned in the technology reform to cross-border trade in services and low-value goods, will be considered in a second paper. The application there will follow reforms in New Zealand and Australia (the so-called NetFlix and Amazon Taxes) and suggest that these efforts would be more successful if they were to be implemented in the same manner that Fiji has approached its current technology reform.

Taken together these papers suggest that Australia and New Zealand should look to Fiji for a technology methodology for tax reform, in much the same manner as Fiji should look to Australia and New Zealand on where a re-shaping of their residence-based VAT is needed in light of the changing mix and dynamics of world trade.

FULL-ROLL-OUT OF THE ELECTRONIC FISCAL DEVICE (EFD) REGULATION FJ$185 million

Jurisdictions imposing transaction taxes (VATs or RSTs) that have adopted a real-time security system that encrypts and automatically reports all transactions to the tax authority have realized significant revenue recovery. When fully operational the revenue boost for the VAT alone is rarely less than 20%.[9] At this standard rate of return a fully successful roll-out in Fiji will recover VAT revenues of approximately FJ$185 million.

In February 2015 Fiji published a technology tender based on a thoroughly researched study of global compliance systems in Asia and Europe and settled on the Belgian approach which blends German (smart card) and Swedish (control unit) methodologies.[10] Fiji officials visited Belgium to observe the system in operation.[11] After these consultations Fiji determined to move forward with its Electronic Fiscal Device (EFD) regulation, implementing it in measured phases of roughly three-month intervals.[12]

The pace of the program has understandably muted revenue improvements. Increases are expected to be gradual, not immediate. There is no published overall time table for roll-out, although it appears that each "group of businesses" [13] will be treated in a similar manner with the same amount of time and government resources devoted to making a smooth transition. There is a built-in flexibility,[14] and a clear "learning path" for the Fiji Revenue and Customs Service (FRCS).

---

[9] Take for example the reform in Ethiopia which began in February 2008 (first in Addis Ababa). It mandated the use of certified Electronic Tax Registers (ETRs) more widely known as a Sales Recording Modules (SRMs). This is an earlier version of the technology used in the Fiji reform. SRM technology is considered outdated, too costly for taxpayers, and providing limited results for tax authorities. However, by January 2013 ETRs were widely in use (53,241 taxpayers). A comparison of pre-ETR (2005/06) revenues with post-ETR (2011/12) revenues show a total revenue increase of 42.3% with 20.4% coming from corporate tax, and 21.9% from VAT. A 2014 study noted a sharp rise in VAT revenues in 2008 that coincided with the introduction of the ETR:

> … the trend of indirect domestic tax revenue indicates clearly how VAT and turnover tax revenue collection has improved after the introduction of ETRs in 2008/09.

Hamdu Kedir Mohammed & Zinash Degife Gela, *Challenges of Electronics Tax Register Machine (ETRS) to Businesses and its Impact in Improving Tax Revenue,* INTERNATIONAL JOURNAL OF SCIENTIFIC KNOWLEDGE - COMPUTING AND INFORMATION TECHNOLOGY, July 2014 (Vol. 5, No. 3) at 20. Similar stories of dramatically significant revenue improvement after the introduction of secure, real-time compliance systems can be found in Slovenia 16%; Rwanda 20%; Croatia 42%.

[10] For a discussion of the Belgian precursor system as currently in use (in French only) *see*: LE SYSTÈME DE CAISSE ENREGISTREUSE *available at*: https://www.systemedecaisseenregistreuse.be/fr

[11] The February 2015 tender (due by December 2015) is *available at*: http://www.webmediassp.com/wp-content/uploads/2015/02/Specifications-ElectronicDataCollection.pdf.

[12] Initially called a VAT Monitoring System (VMS) the name was changed to Electronic Fiscal Device (EFD) system because it was recognized that the electronic system could be used to monitor more that the tax on value added, but it could monitor compliance with other taxes also. See for example: FRCS, *Step by Step Instructions on the Road to Fiscalization* (VMS/EFD) *available at*: https://www.frcs.org.fj/wp-content/uploads/2018/05/VMS-Fiscalization-Guide_v1.0.pdf

[13] "Group of businesses" is a defined term in the regulations. The parameters of a group is defined *ad hoc* by the Minister and is set out from time to time in the Gazette along with the "period of time … within which a taxpayer, who has a business that is a member of the group, must be operating an EFD for the business." GOVERNMENT OF FIJI GAZETTE SUPPLEMENT, No. 19 (June 1, 2017) *Tax Administration (Electronic Fiscal Device) Regulations 2017* Art. 28(1).

[14] For example, during the roll-out of the EFDs for the first group FRCS announced:

> For the first phase, the supermarket and pharmacy sectors will be required to implement an EFD. We estimate that it will take between 1 to 3 months for sectors to comply. However, phase 1 is given 6 months because this is the first round of implementation process and it will take some time for nominated stakeholders to adjust.

From a high level, Fiji envisions a business-government digital partnership producing "… an electronic system [designed to] transmit[s], receive[s], record[s], analyze[s], format[s], store[s], and monitor[s] fiscal data."[15] The partnership is comprised of (a) the "*Authority's system*," the TaxCore, and (b) the mandatory *electronic fiscal device* (EFD), that is, the system "… used by taxpayers in operating their business,"[16]

From the taxpayer's perspective, the central element of this program is clearly, the electronic fiscal device (EFD). This expression needs elaboration, and definition. Although an *electronic fiscal device* appears to describe a specific physical product (a tangible *device* – possibly some kind of computer hardware), it is in fact, a *system*[17] (not a unitary device). It has two parts either of which or both may be entirely software-based.

Electronic fiscal device. An electronic fiscal device is comprised of: (a) a Point of Sale (POS) system, or more generally an Accredited Invoice System (AIS)[18] and (b) a Sales Data Controller (SDC) with a Secure Element (SE).

The AIS or POS part of the EFD

The POS/AIS[19] in the EFD must be *accredited*.[20] The *Electronic Fiscal Device* regulation provides POS accreditation guidelines in Schedule 1.[21] The base requirements to be an *accredited* POS are simply stated.

An *accredited POS* needs to be able to connect with an *accredited SDC* and be able to issue a *fiscal invoice*. Essentially the regulation takes a wide (market) view of accreditation.[22] The regulation is aware that the POS market is both diverse and dynamic, that the government needs to work *with* the market as a regulator of the outcomes, not as an advocate of one-size-fits all POS systems. It states:

> Accredited POSes are developed for different platforms, designed to use a variety of communication standards to connect to other software or hardware components. As wide acceptance and low cost of integration are crucial for successful fiscalization, the Authority is dedicated to providing detailed integration instructions for all manufacturers and software developers (suppliers).

FRCS, *VAT Monitoring System (VMS) | Electronic Fiscal Device (EFD) available at*: http://www.webmediassp.com/wp-content/uploads/2017/08/VMS-flyer1.pdf

[15] EFD REGULATION, *supra* note 2 at §4(1) at 77.

[16] *Id*., at 78.

[17] In the initial phases of this project FRCS described it as a VAT Monitoring System (VMS). However, it soon became apparent that the system that was being developed would/ could monitor much more than VAT, given that there are other taxes imposed, and which would be digitally recorded on the same transactions. Those taxes include the Service Turnover Tax (STT), the Environmental Levy (EL), and occasionally the Stamp Duty. A similar confluence of taxes, recordkeeping and enforcement was noted in the VATs adopted in the Gulf Community Council where the cigarette tax crossed paths with the automation of the VAT (digital invoices, central storage of encrypted transaction data in the local tax administration, and blockchained cross-border exchangers within the GCC community). Richard T. Ainsworth & Musaad Alwohaibi, *The First Real-Time Blockchain VAT: GCC Solves MTICV Fraud*, 86 TAX NOTES INTERNATIONAL 695 (May 22, 2017).

[18] 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.

[19] The EFD REGULATION, *supra* note 2 at §2(1) at 76 define a POS as follows:

> "POS" means a point of sale invoicing device or software which is an electronic device or software application that is—
>
> (a) used by a business for management control in the areas of sales analysis and stock control; and
>
> (b) a component of the business's EFD—
>
> (i) into which a cashier enters the transaction data for each transaction made by the business; and
>
> (ii) from which a fiscal invoice for the transaction is issued;

[20] While all POS systems perform the same basic functions of a traditional cash register (issuing receipts) modern POS systems are much more complicated than a basic electronic cash register (ECR). It will include a computer, monitor, cash drawer, receipt printer, customer display and a bar code scanner along with a debit/credit card reader.

[21] EFD REGULATION, *supra* note 2 referenced at §20(a) & provided in *Schedule 1* at 90-96.

[22] Take for example the legalized marijuana market in the US. The POS systems used in the marijuana dispensaries are unique, with the first marijuana-specific POS constructed by Mark Goldfogel. See Mark's discussion in *The Ugly Truth About POS in the Cannabis Industry*, CANNABIS BUSINESS EXECUTIVE – CANNABIS AND MARIJUANA INDUSTRY NEWS (April 7, 2015) *available at*: https://www.cannabisbusinessexecutive.com/2015/04/the-ugly-truth-about-pos-in-the-cannabis-industry/. See also: Richard T. Ainsworth & Brendan Magauran, Taxing and Zapping Marijuana: Blockchain Compliance and Trump, (Five Part Series from April 16, 2018 through July 9, 2018) 88 STATE TAX NOTES 241 & 419; 89 STATE TAX NOTES 4 & 21; and forthcoming.

The regulation identifies the two avenues for producing a *fiscal receipt* with an *accredited POS*, one [a hardware or software solution] uses an *external SDC* (E-SDC). This is a non-internet-*semi-connected scenario*.[23] The other [a software solution] uses a *virtual SDC* (V-SDC). This is an internet-*connected scenario*.[24] Base entirely on how the taxpayer's business is set up, and how it achieves connectivity with the outside world, a choice must be made between a POS plus E-SDC, or a POS plus V-SDC. But regardless of this choice, the EFD must produce the specified compliance outcomes.

To help the market achieve these goals the regulation tasks the FRCS with setting up a *development environment* accessible to all software developers seeking to produce an *accredited POS* or *accredited E-SDC* components. By registering on the FRCS web page, a developer will be able to receive test certificates, technical documentation and a user manual.[25]

System is built on the top of the Public Key Infrastructure using a certificate authority which is significant improvement comparing to the similar systems relying on hardware vendor manufacturers to provide security. Application of PKI addresses Taxpayer and Tax Authority mutual authentication, non-repudiation of digital signatures and data transport security and invoice integrity. Fiji Revenue and Customs Services acts as a registration authority, verifying identity information before digital certificates are issued to Taxpayers.

The goal in each case is to demonstrate the creation of a fully compliant *fiscal invoice*. There are two data-intensive parts of a fiscal invoice: (1) some data is included in the *invoice request* sent by an accredited POS to an E-SDC or V-SDC, and (2) other data is included in the *invoice response* which is generated by the E-SDC or V-SDC in reply. Both the request, and the response must include specific data points.[26]

The i*nvoice request* (by the POS) must include:

(a) the type of receipt;
(b) the type of transaction;
(c) the method of payment;
(d) the name or unique identification of the cashier;
(e) the name or unit code of each good or service supplied;
(f) the unit price and quantity of each good or service supplied;
(g) the total price of the goods or services supplied;
(h) the taxes that are a part of the invoice and the tax rates applied;
(i) the total amount payable by the customer;
(j) if the customer is a taxpayer, the customer's TIN;

The *invoice response* (by the SDC) must include:

(k) the name and TIN of the business, and the identification of the business premises where the transaction occurred;
(l) the date and time the receipt is issued;
(m) the sequential serial number of the receipt;
(n) the serial number of the digital certificate of the business's EFD;
(o) the digital signature and internal data[27] of the EFD.

The regulation also specifies five types of receipts that an accredited POS must be able to issue when connected to an accredited SDC. Each test case is set out (Normal receipts, Refund receipts, Copy receipts, Training or Pro-forma receipts, and Normal or Refund receipts for B2B transactions). Expected results are specified.[28]

The SDC part of the EFD

[23] *Id.,* EFD REGULATION, *Schedule 1(3.1)* at 92.
[24] *Id.,* EFD REGULATION, *Schedule 1(3.2)* at 92-3.
[25] *Id.,* EFD REGULATION, *Schedule 1(4 & 5)* at 93.
[26] *Id.,* EFD REGULATION, §12(2) at 81-82.
[27] Internal data contains fiscal data (total of all counters) in encrypted form. Content of internal data is readable by the Authority only.
[28] *Id.,* EFD REGULATION, at §21(1) and *Schedule 1(7)* at 93-96.

The SDC (sales data controller) is the second part of the EFD (electronic fiscal device). As indicated above, there are both hardware (E-SDC) and software (V-SDC) versions. Accreditation is not an issue for the V-SDCs, because this device resides under the *Authority's* control. However, accreditation is important for E-SDCs. In this context, *accreditation* means that the E-SDC has proven to integrate fully with the *Authority's system.* Only accredited suppliers may provide taxpayers with an E-SDC. An E-SDC must be accredited (by the manufacturer) prior to being sold (at retail) in Fiji.[29]

The reason for having an E-SDC in addition to a V-SDC is that the V- SDC has a down-side in its dependency on the internet. V-SDCs are simpler for the taxpayer to handle, but if the internet is unreliable (or fully unavailable) then an alternate way to connect the taxpayer's POS with the Authority's system is necessary. The E-SDC is this alternative. The difficulty with E-SDCs is moving a secure function out from under the Authority's firewall, and thus the Tax Authority must be sure these operations remain fully secure. The data can neither be compromised nor manipulated. The expression used to describe these protected functions is the *secure element* (SE). Safeguarding the SE is a major concern for the E-SDC, and as a result the E-SDC option is more complicated than the V-SDC option.

The E-SDC's Secure Element

The *secure element* (SE) is provided by the *Authority* to an accredited E-SDC on a smart card. The card is designed to prevent tampering and unauthorized use of the fiscal data that will be transmitted to the *Authority* through it.[30] The smart card that implements the SE contains a digital certificate and a special applet.[31]

Procedurally, the first step is for the accredited POS is to generate the contents of a receipt with the *transaction data* that has been entered into the POS by an operator. Secondly, the *transaction data* is sent to the E-SDC, where the E-SDC verifies format, tax labels, current date, time, and PIN code/password for the digital certificate.[32] Thirdly, the data is then sent to the SE for fiscalization (*at this moment the transactional data becomes fiscal data*).[33]

The fourth step is for the SE to verify that all numbers are positive, it re-calculates the internal data, encrypts the data with the *Authority's* public key, and signs the receipt. The fifth and final step is for the SDC to transmit a *fiscal invoice* back to the POS, while permanently preserving the transactional and fiscal data, and simultaneously transmitting the *fiscal data* to the *Authority*. This transmission may be delayed until there is a communication opportunity (possibly through an internet connection that is revived, or through another communication medium, or even manually through the delivery of a memory stick to the FRCS). The customer standing at the POS terminal where the initial data entry occurred will not see much of a difference (time wise) from a normal transaction at a stand-alone POS. The visible difference will be that the receipt (invoice) will be printed with a scannable QR code which will allow the customer to verify the data on the receipt (invoice) with records of the transaction to be retained on the *Authority's system*.

A sense of the complexities and differences between using an E-SDC or a V-SDC can be gleaned from the diagrams below.

Figures 1 and 2 set out an EFD comprised of an accredited POS and V-SDC. They show the entire process of *transaction data* being entered into an accredited POS, passing to the secure element

---

[29] Un-accredited SDCs (like un-accredited POSs) may not be sold in Fiji, and no business can operate without an accredited POS and SDC. EFD REGULATION, §15 at 84.

[30] *Id.*, EFD REGULATION, §2(1) at 76.

[31] *Id.,* EFD REGULATION, at *Schedule 1(3.2\)* at 92.

[32] EFD REGULATION, §11 at 81. The digital certificate does the following:

(a) reproduces the taxpayer's digital signature for recording on each fiscal invoice issued by the taxpayer to a customer;

(b) reproduces the protected password or PIN code of the taxpayer and securely delivers the password or PIN Code to the Authority's system to enable the EFD to link to the Authority's system and securely transmit the fiscal data to the Authority's system; and

(c) records the date on which the data is transmitted to the Authority's system.

[33] EFD REGULATION, §5(d) at 78 (emphasis added):

SDCs that receive *transaction data* from POSes, **instantly** format that data into *fiscal data* and *fiscal invoices*, transmit the fiscal data to the Authority's system and transmit the fiscal invoices to POSes.

Indicating that the transformation of transaction data to fiscal data, and fiscal invoices is **instantly** performed.

(within the *Authority's* system), being fiscalized, and then returning to the customer in a *fiscal invoice* complete with a QR code that will allow verification of the transaction – instant verification.

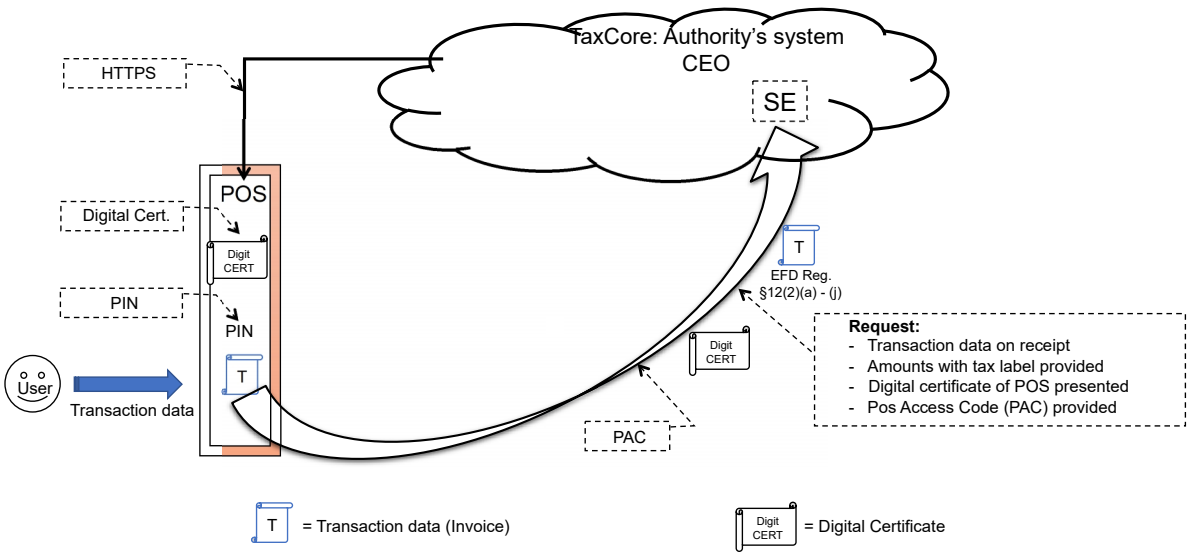
It is important to note that instantaneous verification is not dependent on the type of SDC employed. The QR code on the customer's receipt (invoice) can always and immediately be scanned by the customer and confirmed by the TaxCore. It may be that the customer may scan a receipt (and thereby get data to the TaxCore) before an E-SDC transmits it (due to unreliable internet connectivity, for example), but verification is assured with a valid QR code.

Figure 1 starts with an accredited POS. The manufacturer will have followed the *Technical Instructions for POS and Cash Register Developers* and received accreditation. The POS will receive a digital certificate and associated POS Access Code (PAC)[34] after the registration process.[35] To enroll the taxpayer will activate an administrative card that will allow access to the Taxpayer Access Point (TAP). At TAP the taxpayer may delegate certificates to himself.[36] An Enrollment Officer at the FRCS will oversee the granting of digital certificates and smart cards. PINs and PACs are provided and known only by the taxpayer who files the electronic request.

The initial data entry process (which occurs when an authorized user engages with the POS terminal to make a sale) will produce a *transaction data invoice.* The data on this (pro-forma) invoice will comprise the substantive elements that will be communicated in the *immediate request* for a *fiscal invoice*.

The Request – Figure 1. The *request* is an automatic process. Immediately after the POS has assembled the transaction data the *accredited* POS[37] will make a direct internet-based request for fiscalization through an associated V-SDC residing within the *Authority*. The transaction data elements (specified under EFD Reg. §20(2)(a) – (j)) will be combined with the POS's Digital Certificate and PAC to be sent forward to the *secure element.* The SE verifies and identifies the caller (taxpayer using the POS). The V-SDC has an accompanying Digital Certificate which verifies its identity.

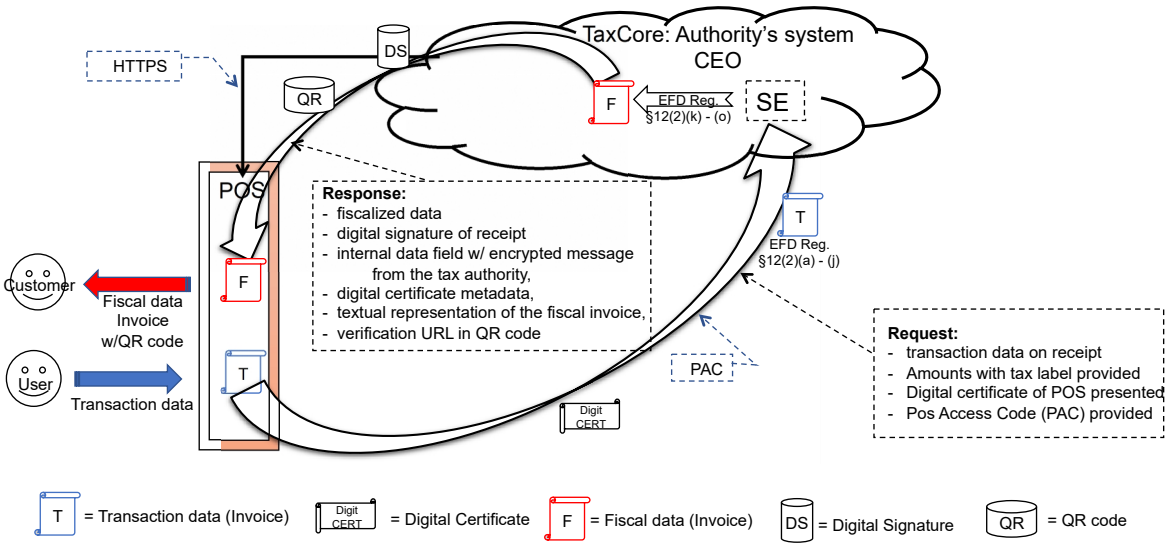
Figure 1
Request for Fiscal Invoice [accredited POS w/ V-SDC]



[34] The POS Access Code (PAC) is assigned to the POS and used along with the digital certificate (which is distributed as a PFX file) to authenticate the POS to the V-SDC.
[35] The following YouTube video sets out this process: https://youtu.be/1tYKeXkLGzE
[36] The six administrative steps to enrollment, securing smart cards, and digital certificates are set out in FRCS, *Step by Step Instructions on the Road to Fiscalization (VMS/EFD)*, available at: https://www.frcs.org.fj/wp-content/uploads/2018/05/VMS-Fiscalization-Guide_v1.0.pdf
[37] There is no requirement that the first element be a POS. It 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.

The Response – Figure 2. After confirming the validity of the request, the secure element associates the transactional data with the elements required under EFD Reg. §20(2)(k) – (o), 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 can scan the QR code to confirm that the invoice data has been recorded by the Authority.

Figure 2
Response to request for Fiscal Invoice [accredited POS w/ V-SDC]



Performing the same invoice fiscalization process through an external SDC (E-SDC) is more complicated.[38] Taxpayers are encouraged to use the V-SDC service whenever possible. An accredited POS is able to use both E-SDC and V-SDC.[39]

Figures 3, 4 and 5 (below) chart the fiscalization pathway with an E-SDC. Figure 3 sets out the first two steps: (a) integrating an *accredited* POS with an *accredited* E-SDC, and (b) securing and installing the secure element in the E-SDC. Technical guidelines for accrediting POSes, and E-SDCs are set out in the regulation,[40] aided by specifications in the *Technical Instructions for POS and Cash Register Developers.*[41] It is highly likely that taxpayers purchasing a POS and E-SDC in Fiji will find that the manufacturer has already gone through the necessary accreditation steps. The taxpayer simply needs to assemble the parts and select a password for the POS and for the E-SDC so they will recognize each other during data-transfers and communications.

In the next step, the taxpayer receives the *secure element* (stored on a smart card) from the *Authority* and installs it in the E-SDC.[42] The regulations define a secure element as, "… the software and hardware used by an EFD and the Authority to prevent tampering and unauthorized use of fiscal data transmitted to the Authority's system and to maintain the integrity of the fiscal data …"[43]

---

[38] FRCA, *Technical Instructions for POS and Cash Register Developers version 2.3* at 24 *available at*: https://www.frcs.org.fj/wp-content/uploads/2018/04/TaxCore-Technical-Instructions-for-POS-and-cash-Register-Developers-v.2.3.pdf

[39] Commonly a POS will be set to work with either an E-SDC or V-SDC by the supplier who has followed the technical instructions to make the device accredited. It is entirely possible that a supplier may set up the POS to toggle back and forth between E-SDC and V-SDC preferring the V-SDC except in cases where the internet is unavailable. As the simplest system, the V-SDC is preferred. EFD REGULATION, *Schedule 1*, at §3.1 at 92.

[40] EFD REGULATION, at *Schedule 1 & Schedule 2.*

[41] FRCS, *Technical Instructions for POS and Cash Register Developers* v. 2.3, *available at*: https://www.frcs.org.fj/wp-content/uploads/2018/01/TaxCore-Technical-Instructions-for-POS-and-cash-Register-Developers-v.2.2.pdf

[42] EFD REGULATION, at *Schedule 2(3.1)* at 101..

[43] EFD REGULATION, §2(1) at 76.

The purpose of the *secure element* is to allow the *Authority* to own and control the security on each E-SDC (much as they do with respect to the V-SDCs that reside within the Authority's firewalls), and to exercise this control entirely independent of the POS or E-SDC vendor. The *secure element* is placed on a smart card.[44] The taxpayer slots the card into a reader (connected to the POS), then goes to the browser and calls-up the URL of the tax administration.[45] There will be a prompt for the PIN, and then credentials will be read from the smart card.

Figure 3:
Setting up an E-SDC for an *Electronic Fiscal Device*

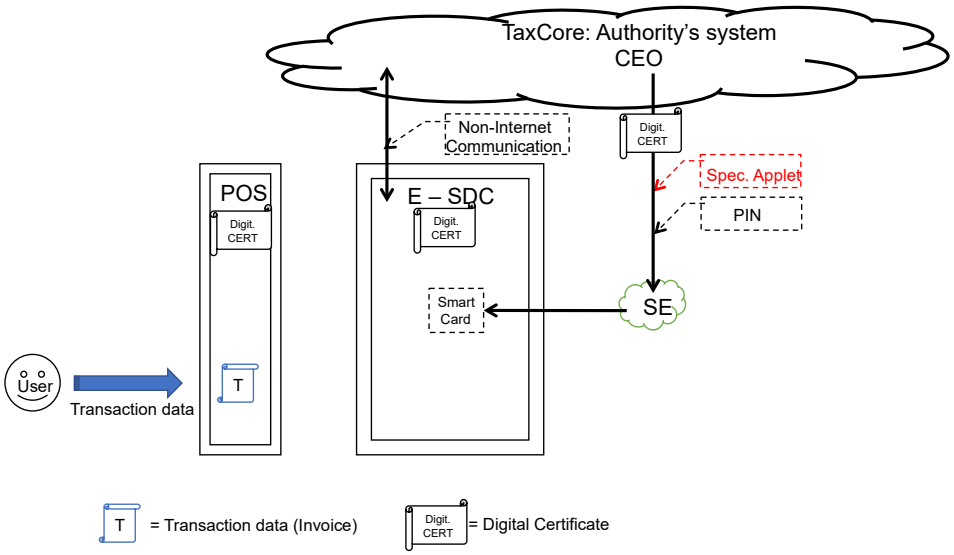


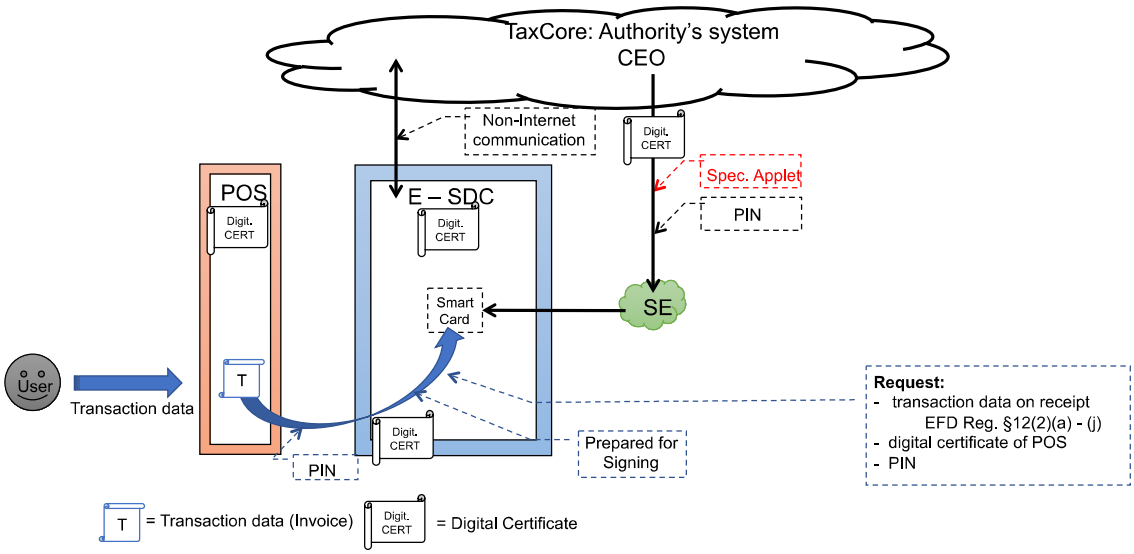
Figure 4 presents the same request for fiscalization of transaction data set out in Figure 1, except in this instance the *request* is presented to the *secure element* within the external SDC (E-SDC) not the virtual SDC (V-SDC) within the *Authority's system*.[46] E-SDC is needed because the internet is not always available. The *secure element* is designed to replicate the functions of the *Authority's system* after the E-SDC prepares the transactional data for signing.

[44] The Authority does this after it has received a *request for fiscalization* on the Authority's web site from the taxpayer who has recently purchased an accredited POS and E-SDC. After the Authority validates the information received from the taxpayer, an invitation to enroll is sent, and the taxpayer selects a PIN which is recorded in the system. The Authority then produces a secure element placed on a smart card, and sends a notification to the taxpayer that the application has been approved and the smart card (secure element) is available to be picked up at an FRCS location. FRCS, *Step By Step Instructions on the Road to Fiscalization (VMS/EFD)*, available at: https://www.frcs.org.fj/wp-content/uploads/2018/05/VMS-Fiscalization-Guide_v1.0.pdf

[45] In Fiji this URL is https://tap.vms.frcs.org.fj. At log-in the system will prompt entry of the PIN, and will then read the credentials of the user from the smart card.

[46] EFD REGULATION, at *Schedule 2(3.1)* at 101.

Figure 4:
Request for Fiscal Invoice [accredited POS w/ E-SDC]

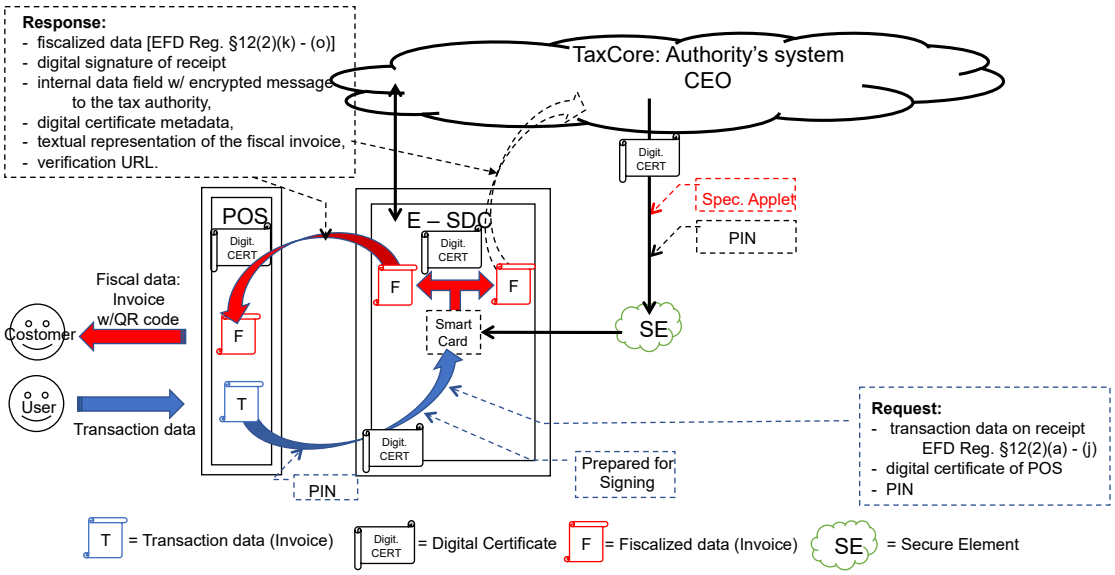


With the exception of the *proof of audit* function,[47] Figure 5 completes the diagrams presenting the E-SDC. Figure 5 is more complex than Figure 2 even though they both chart the *response* to the *request* for a fiscal invoice.

When the *secure element* in an E-SDC fiscalizes the transaction data that it receives from the POS it verifies amounts, calculations, signs and encrypts the file for two purposes[48] (a) it prepares it for transmission back to the POS where a fiscal receipt will be issued with a QR code for the customer, and it (b) prepares it for later transmission to the *Authority's system* when the internet connection is restored, or an alternate transmission mechanism is available (to include manual delivery of the data to an office of the FRCS).[49] The secure element will retain fiscal data on location until the fiscal data is transferred and a notification is received from the Authority's system that the transfer is complete.[50]

[47] Proof of audit is directly related to the operation of the secure element, but it is considered separately further below because of its importance to a full understanding of the Fiji system, and the importance of the contributions made by DTI ltd. in the development of the system. EFD REGULATION, *Schedule 2 at §2(2.5)* at 100.
[48] EFD REGULATION, *Schedule 2 at §2(2.2)* at 99
[49] EFD REGULATION, *Schedule 1 at §2(3.2)(6)* at 92.
[50] EFD REGULATION, *Schedule 2 at §2(2.2)* at 99; & *§2(2.6.1 & 2)* at 101.

Figure 5:
Response to request for Fiscal Invoice [accredited POS w/ E-SDC]



Proof of Audit

Proof of audit (POA)[51] is the most unique aspect of Fiji's VAT Monitoring System (VMS). It is certainly the most creative and important. POA was designed and developed by Data Tech International (DTI) for the FRCS. POA is a risk analysis template that is simpler to use than artificial intelligence (AI), achieves more granular results, and provides real-time solutions to fraud attempts within the VMS. *Proof of audit* uses automatic *counters* that are built into the production of each fiscal invoice, by secure processes in the TaxCore, and the *secure element*. The operation of the *counters* identify frauds attempts before they are established, and automatically stops standard frauds as they begin. It is a unique attribute of the Fiji VAT that is sure to be emulated.

To fully grasp what *proof of audit* means in the context of Fiji's technology-intensive VMS at least one term needs defining (re-defining), and the *proof of audit* processes need to be set out. The term is audit – what is an *audit* (note: this is not an accountant's definition)?

> An audit is a process of *sequentially* transferring *audit packages* from an E-SDC (or an SDC) to the Tax Authority's system [the TaxCore] and handling the *response* generated … for the specific device.[52]

This definition is cast in technology terms – there is a *request* made by the SDC (accomplished through the sequential transfer of audit packages) and a *response generated* by the TaxCore. The vehicle for the *proof of audit* is the *audit package* generated by the SDC. An audit then, is the process by which the data in the technology devices at the business location are fully replicated (proven to be in sync with) the data recorded in the TaxCore. This is the technological equivalent of sending a human auditor from the tax administration offices to the taxpayer's place of business and confirming every line item on a receipt (invoice), then repeating this for every receipt (invoice) produced by the taxpayer, and then finally recording the result in a sequential record that replicate how the original transactions occurred.

The *audit package* is composed of the receipt(s) or invoice(s) that are assembled for a single *proof of audit* as they pass through the taxpayer's POS/AIS. So, *when* is an EFD ready to engage in a *proof of audit*? The answer is surprisingly simple:

---

[51] FRCS, Technical Instructions for E-SDC Developers (version 2.3) available at: https://www.frcs.org.fj/wp-content/uploads/2018/04/TaxCore-Technical-Instructions-for-E-SDC-Developers-v.2.3-.pdf

[52] *Id.*, at 37 (emphasis added).

Once an invoice is created (Invoice Fiscalization Request and Invoice Fiscalization Result) the E-SDC is ready to create an audit package and store it in the non-volatile memory.[53] This means that proof of audit can go forward with just one invoice.

More technical detail is provided by the FRCS. In fact, the FRCS sets out an eleven-step process on how to create an audit package. These steps (expressed in technological terms) are essentially the same steps recorded above (see Figure 5) for creating a fiscal invoice.[54] In its essence, an *audit* is a secure digital *conversation* among three machines – the SDC, the TaxCore, and the secure element. The *full audit* involves the sequential confirmation (through this conversation) that all the data that was entered in the AIS/POS is precisely the same data that resides in the TaxCore – no changes, no omissions, and no manipulations.[55]

In short, *proof of audit* is a real-time confirmation of transactional data accuracy, preserved and validated in the sequence it was created.

What triggers an audit? Because we are dealing with machines, not people, and because we are conducting a complete (line-by-line) audit of all transactions, not a partial (sampling) audit of suspect transactions this audit can be (needs to be) pre-programmed so that it is conducted nearly simultaneous with the execution of the underlying transactions. If a *proof of audit* cannot be completed, no subsequent proof of audit can be undertaken without correcting the errors in the prior effort. The *proof of audit* triggers are:

(1) every five minutes;
(2) whenever a fiscal invoice is completed;
(3) on demand by the Tax Authority;
(4) on demand by the Taxpayer.

The fourth item on this list need to be explained. The incentive for a taxpayer to request an audit from the tax authority is not apparent on its face. The incentive (or taxpayer stimulus) is provided by another special feature of the Fiji VAT – the *counters*.

Counters

---

[53] *Id.*, at 37.

[54] The eleven steps are:

1. Convert all Date and Time data to UTC;
2. Generate a random one-time symmetric key for AES256;
3. Encrypt string JSON representation of the invoice using the one-time key;
4. Convert the encrypted invoice to base64 string and store it in the Payload field of JSON representation of the Invoice;
5. Get the TaxCore Public key using Export TaxCore Public Key APDU command.
6. Encrypt the one-time key using TaxCore public key, convert it to base64 string and store it in the Key field;
7. Encrypt Initialization Vector (IV) using the TaxCore public key, convert it to base64 string and store it in the IV field;
8. Save the Audits as an Audit Package file, named as {UID}-{Ordinal_Number}.json;
9. (Optionally) Generate an QR code, and attach it to InvoiceFiscalizationResult (make sure that the QR code is not stored in the Audit Package);
10. Return InvoiceFiscalizationResult to the POS;
11. If the internet connection is available try to send the AuditData to Backend.Api as explained in the section Remote Audit;

Id., at 37.

[55] The seven steps in the *conversation*:

1. E-SDC signals the beginning of the audit to the Secure Element (Invokes Start Audit APDU command);
2. The Secure Element returns ARP (256 bytes) to the E-SDC;
3. E-SDC starts the audit by sending audit data (over HTTPS) or dumping them on external memory (e.g. SD card, USB flash drive), starting with the oldest unaudited package, in piecemeal fashion. ARP is sent to the Tax Service's system using the same communication channel;
4. If verification is successful, the Tax Service's system shall generate a proof of audit (PoA) and return it as a Proof of Audit Command;
5. E-SDC receives the proof of audit command and passes the payload to the End Audit APDU command;
6. The Secure Element verifies if proof of audit is valid, meaning the audit data has been successfully received by the Tax Service's system;
7. If proof of audit is valid, the Secure Element will conclude the audit process;

Id., at 37.

Counters count the tax attributes on each invoice *as those attributes are sequentially placed on invoices*. The results of the *counting* function are embedded in the QR code of all Fiji invoices. *Counting* is non-discretionary [that is, the *counters* cannot be turned off]. *Counters* can be adjusted [in the sense that the cap on each counter can be changed], but that can be done only by the Tax Authority.

Each *counter* has a customized cap set by the tax authority at any point of time (per sales location). When the *secure element* in an E-SDC or V-SDC 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 the TaxCore. This may happen when a business has been offline for a time, and normal remote audits (with proof of audit notifications) have not been conducted. To prevent shut-down the taxpayer may need to use a secure phone line, or manually take records (on a SD card or memory stick) to the tax authority. *Proof of audit* is the only way to re-set the counters to zero and prevent the *secure element* from going to sleep (without which the taxpayer cannot issue a fiscal invoice).

Because the Fiji VMS employs both V-SDC and E-SDC devices *proof of audit* and the *counter* structure can appear complex. There is an EFD counter (unique for each secure element) assigned to each E-SDC and V-SDC. This counter will record (count in a sequence) the signed receipts issued by the POS (subdivided by type of receipt). The types of receipts include Normal Sales [NS], Normal Refund [NR], Copy Sales [CS], Copy Refund [CR], Training Sales [TS], Training Refund [TR] and Proforma Sales [PS].[56] There are also *secure element* counters that record line item cumulative totals: cumulative turnover, tax totals, refund totals, per tax refund totals, and others.

Figure 6 (below) contrasts EFD structures when using an E-SDC with an EFD using a V-SDC. For simplicity, the example assumes an environment where there are only four taxpayers, (a), (b), (c), and (d). They are using POS(a), POS(b), POS(c), and POS(d). Businesses (a) and (b) use E-SDCs (also labeled (a) and (b)), whereas businesses (c) and (d) use a V-SDC housed within the Authority's system. In addition, business (b) switches SDCs during the year. It starts by associating POS(b) with E-SDC(b) but moves to a V-SDC after issuing the first six invoices.

The Authority's system has direct (immediate) control over the invoice data for businesses (c) and (d), but indirect control when businesses (a) and (b) are using E-SDCs. In the figure below there is a simple one-to-one transmission from POS(c) and POS(d) to the V-SDC housed within the Authority's system. When transaction data is forwarded to the V-SDC the TaxCore checks, encrypts and retains the data in sequential form. Counters are immediately applied. Fiji currently has three V-SDC's operating 24/7 to assure that any *request* for a fiscal receipt can be *responded* to within less than a second. *Proof of audit* can be immediate (near real-time) with a V-SDC.

It is a different story with POS(a) and POS(b). These systems are corresponding with E-SDCs which are not controlled in real-time by the Authority's system. In this instance, for the taxpayer to be able to issue a valid fiscal receipt, with a QR code to customers within less than a second the data needs to be checked, encrypted and securely stored on location (by the *secure element*) and transmitted at a later time to the Authority's system. This delay is an inherent security risk, but that risk is mitigated by the technology. In Fiji the very next transaction scanned by a customer, or audited in any other way will show the gap between the last successful transaction and the current one.

The timing difference in receiving Audit data between E-SDCs and V-SDCs will likely result in the fiscal invoices 1, 2, 3, and 4 issued by POS(b) arriving at the TaxCore *before* some of the earlier issued fiscal invoices by POS(b) numbers 1, 2, 3, 4, 5, or 6. The TaxCore will nevertheless, align and save the invoices in sequence by issue date.[57]

One of the main reasons for the extensive use of counters by the Fiji system is to close the risk gap caused by the inherent delay in the TaxCore's receipt of invoices from various E-SDCs and V-SDCs. The caps on the counters will be adjusted on a case-by-case basis determined on individual risk analysis estimates.

---

[56] See the prescribed notations for each type of receipt within the counters structure in the "expected outcomes" sections of EFD REGULATION, *Schedule 1 at §§7.1.2; 7.2.2; 7.3.2; 7.4.2; & 7.5.2.*

[57] There is a unique number containing the ordinal position assigned by the *secure element*. Thus, even if the date and time are recorded wrong for some reason the VMS is able to reproduce the correct invoice order.

Figure 6
Comparison EFD counters with E-SDC & V-SDC

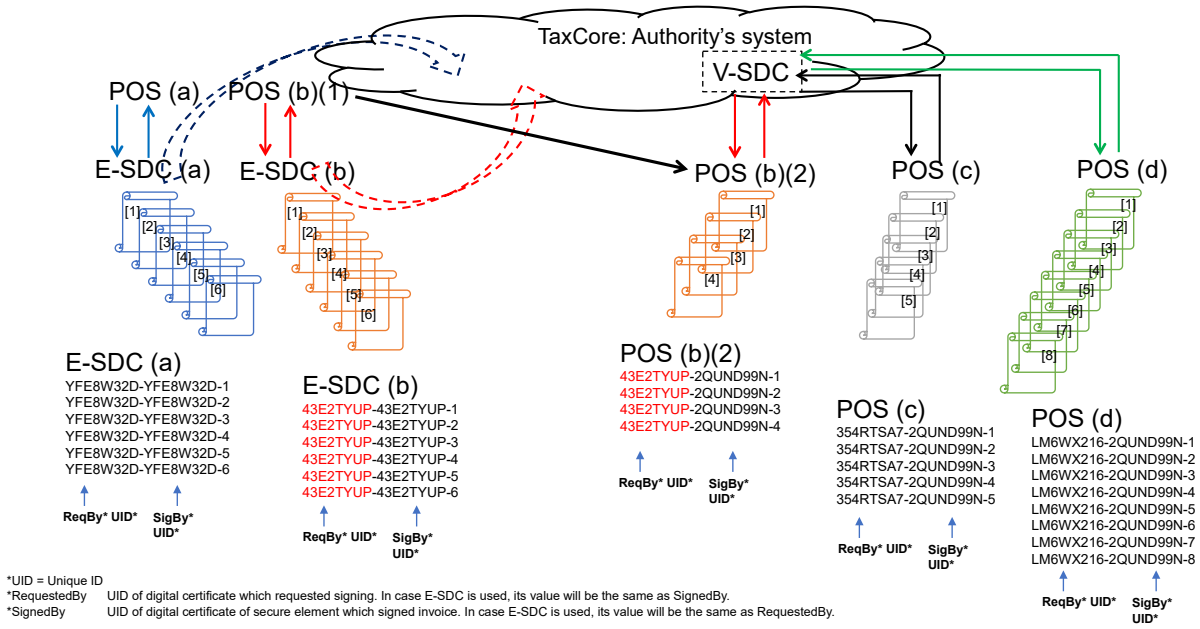


Figure 6 (above) also replicates the unique ID of the digital certificate that requests the digital signature on the fiscal invoice, and the unique ID of the *secure element* that signed the invoice. Set off in sequential pairs the invoices themselves now have a unique identifier. Of particular note is what happens when POS(b) switches from E-SDC(b) to the V-SDC. When using the E-SDC the "request by UID" and the "signed by UID" segments of the identifier have the same root, because the same element is performing both tasks. However, when the V-SDC is engaged the "signed by UID" changes. The portion of these strings set out in red are highlighted to show consistency in the "request by" element, and the differential in the "signed by" segments.

Audit

To clearly see the audit function, the diagram above at Figure 6 needs to be a little more granular. Figure 7 (below) provides a breakdown of some of the tax data collected on each invoice for business (a). The first thing to notice is that there is a digital signature verifying the accuracy of the data that appears on each document. Each invoice can be called up on command and checked as need-be. These are fiscal invoices containing QR codes.

The first invoice is a normal sale invoice (designated in the system as: TR: 1/1 NS for the first transaction from E-SDC(a) and the first Normal Sale of the sequence). It is followed by a second normal sale (TR: 2/2 NS) and a third normal sale (TR: 3/3 NS). Internal data indicates that the invoice amounts for these sales were for 100, 20, and 230. The total sales counter shows running totals of 100, 120 and 350. The same is true of the VAT counter (assuming a 10% VAT). The VAT collected on each invoice is 10, 2 and 23. Running totals show 10, 12 and 35.

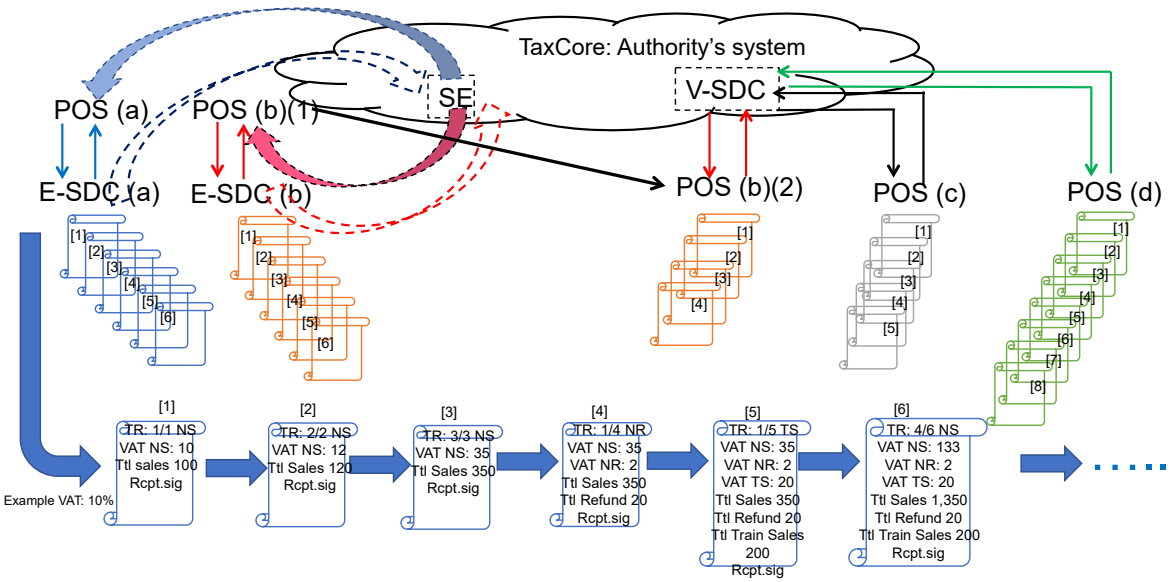
The fourth and fifth invoices are different. The fourth is a normal refund (NR) of 20, including a return of VAT of 2. This is the first normal refund and the fourth invoice in this sequence (TR: 1/4 NR). The counters show aggregate VAT collected of 35 (no change), VAT refunded VAT of 2 (new data) and total normal sales of 350 (no change), and total normal returns of 20 (new data).[58] The fifth invoice (TR: 1/5 TS) is a sales training invoice. Once again there is no impact to the aggregate VAT (35), or total sales (350). However, there are new records of total training sale (200), and total training VAT (20) recorded.

[58] NOTE: the counters are only positive and do not net total VAT collected of 35 with total VAT refunded of 2 to get 33. Each amount is kept separate.

Finally, the sixth invoice records the fourth normal sale transaction (TR: 4/6 NS). The sale is for 1,000 with VAT of 100 which increases both the aggregate sales counters to 1,350 and the aggregate VAT to 135 respectively.

This process goes on for each invoice sent for fiscalization throughout the entire Fiji VMS (every business, and every transaction in Fiji, currently limited by the present extent of the roll-out at phase two). The process takes less than a second for each invoice. It is comprehensive and thorough.

Figure 7
Fiscal Counters that support the Proof of Audit structure



Examples

To make this discussion more concrete, consider the following standard VAT frauds and how Fiji's VMS interacts with them. The importance of *proof of audit* and the central role of the *counters* in defeating frauds will be notable. Each of the following schemes are common in VAT jurisdictions globally as indicated in the notes (they are no longer preset in Fiji):

(1) Zappers - a retail business issues accurate (paper) receipts with a POS, but the owner (at a later time) inserts a transaction-deleting program on a memory stick into the POS and deletes either the entire record or line items on a record for some specific transactions;[59]

(2) Phantomware - a retail business issues accurate (paper) receipts with a POS, but the owner (at a later time) accesses a (hidden) program in the POS and deletes either the entire record or line items on a record for some specific transactions;[60]

(3) a business issues one valid receipt early in the business day for a commonly purchased item (large cheese pizza – B2C, or commercial building supplies – B2B) and then photocopies the receipt (invoice) and use these copies throughout the day (not a new receipt or invoice) whenever

[59] *State of Washington v. Wong*, Wash. Super. Ct., No. 16-1-00179-0 (August 30, 2017 plea to the possession and use of a Zapper purchased from John Yin, a salesman from Profitek, the maker of the POS system used in the restaurant.) John Yin also pled guilty in a companion federal case, agreeing to restitution of $3,445,589. *United States v. John Yin*, Case 2:16-cr-00314-RAJ (April 14, 2017).

[60] See: *The Grande Café Dudok* case from the District Court of Rotterdam, LJN: AX6802 (Jun 2, 2006) *available at*: http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AX6802 (in Dutch) (translation on file with author); appealed to the District Court of The Hague where the judgment is upheld LJN: BC5500 (Feb. 29, 2008) *available at*: http://zoeken.rechtspraak.nl (in Dutch) (translation on file with author).

this item is sold. Customers assume that they have received a valid receipt (invoice), but the business does not report the transaction;[61]

(4) a fraudster manufactures false invoices with an accredited POS and E-SDC stolen from a legitimate business, or a fraudster steels valid invoices. In either case these "extra invoices" are sold in the black market to businesses seeking additional VAT deductions;[62]

(5) a business switches an accredited POS in and out of "training mode" even though all transactions are normal business exchanges. The taxpayer keeps the tax collected on these training sales for himself.[63]

The traditional response to VAT avoidance is *audit*. In Fiji it is no different. However, the Fiji audit response is fully automated and very close to real-time.[64] This is possible because of the *proof of audit* function.[65]

[61] The "large cheese pizza" example comes from *Personal Communication*, Dave Bergeron, Directeur Général Adjoint, Ministry of Revenue Quebec, at a joint presentation with the author at the New York Prosecutor's Training Institute, July 31, 2008. Joint Presentation, *Zappers (Automated Sales Suppression)* (available from the author on request).

[62] See cases from China where the Golden Tax Project implemented a rudimentary digital security system. There are cases involving stolen systems, and cases where just the invoices appear to be stolen (or at least misused by a party different from the one they were issued to). For a stolen POS and security system see: *Nanjing Shuangchao Trade Co. Ltd. v. Xuanwu District State Tax Bureau, Nanjing Municipality* (Judgment of the First Instance, Xuanwu District People's Court, Nanjing Municipality, Jiangsu Province (2005) Xuan Xing Chu Zi No. 70) (concerning theft of tax control cards [smart cards] aka Golden Tax Cards, for the purpose of manufacturing false invoices for sale to businesses seeking greater input deductions). For a case involving the misuse of invoices (possible stolen) from a certified POS with Golden Tax Project security systems in place see: *Inspection Bureau of Zhanjiang Municipal State Tax Bureau v Shengjie Trading Co. Ltd., Zhanjiang Development Zone* (2012) in the Intermediate People's Court of Zhanjiang Municipality, Guangdong Province, (2012) Zhan Zhong Fa Xing Zhong Zi No. 112 (September 13, 2012) case discussed with summary in Alan Schenk, Victor Thuronyi & Wei Cui, VALUE ADDED TAX – A COMPARATIVE APPROACH, Cambridge University Press (2015), *Denial of Input Credit for "Sham" Invoices*, at 493-489 & 496-503.

[63] See: OECD, *Electronic Sales Suppression: A Threat to Tax Revenues* (2013) (discussing the misuse of functions within the ECR/POS software, specifically the training mode, for either the entire till, or an individual clerk so that items are not recorded in the normal reports).

[64] The regulations define an audit.

> An audit is a process of *sequential transfer of audit data* from an E-SDC to the Authority's system and handling the response generated by the Authority's system for the specific device.

EFD REGULATION, *Schedule 2 at §6.3* (emphasis added).

[65] EFD REGULATION, *Schedule 2 at §6.2*

Fraud Prevention
Fraud schemes #1 and #2

Zappers and Phantomware are similar electronic sales suppression (ESS) devises. They differ only in respect of the storage of their fraud programming. A Zapper is stored external to the POS; Phantomware is stored internally (embedded in the POS). Both use specially designed programming to alter the internal records of the POS after sales transactions are completed.

Traditionally, retail records were made and stored locally in POS machines. Zappers and Phantomware operate by altering this record within the taxpayer's POS. They can manipulate selective items on a receipt or delete the entire receipt. The deletions and related removal of cash normally occur after business hours. There is a strong preference for targeting cash transactions.

In frauds schemes #1 and #2 Fiji's VMS severely limits the taxpayer's ability to *manipulate* records with Zappers and Phantomware. Fiji prevents this technology from eliminating line items from a receipt or substituting less expensive items for the more expensive items actually purchased. In the Fiji VMS data passes too quickly for line-item manipulation frauds. It takes less than a second to go from:

- keystroke entry by the operator into the AIS/POS,
- passing on into the SE, and then
- coming back again (encrypted, signed, and with an accompanying QR code).

If line-item manipulation is foreclosed, there still remains a slight possibility that a Zapper or Phantomware sales suppression device could act to *delete* an entire audit package (the whole invoice) before an audit is completed. This deletion will need to be performed within a short five-minute window as the next *proof of audit* is likely to be scheduled soon. For an owner to wait until closing-time to use an electronic sales suppression device will no longer work. If this were to occur, and if the customer scanned the receipt (QR scan), then the difference between the amount paid by the customer, and the amount recorded by the MVS would be visible. A message would notify the customer to compare the amounts and report differences to the FRCS.

But if the deletion is successful the ultimate fraud will not be. With a deleted audit package in the commercial trail it will not be possible to complete the next *proof of audit.* Sequential data will be missing from the chain of transactions.

Recall in Figure 7, TR: 1/1 NS is followed by TR: 2/2 NS, then TR: 3/3 NS, and TR: 1/4 NR, and TR: 1/5 TS, and finally TR: 4/6 NS. If the large 230 sales represented by the third invoice (TR: 3/3 NS) is deleted by a sales suppression program then the *secure element* will notify the TaxCore of a missing invoice when an audit is attempted. In other words, TR: 2/2 cannot be followed by TR: 1/4. No *proof of audit* can be issued. No subsequent *proof of audit* can be issued. The *secure element* will shut down.

The secure element will also shut down whenever a *counter* reaches a cap. No re-sets are possible. The taxpayer will soon be off line without the possibility of generating a fiscal invoice.[66]

The Tax Authority will be immediately aware of the SE shutdown. The enforcement responses are to either (a) scan the last receipt and obtain the internal data from the QR code, or (b) perform an audit of the SE. Effectively, if a Zapper or Phantomware application used in a Fiji system, it will be defeated (quickly) by the technology.

Fraud Schemes #3 and #4

Where fraud schemes #1 and #2 are concerned *missing* fiscal invoices, fraud schemes #3 and #4 involve *false* fiscal invoices. Scheme #3 is either a B2C or B2B scenario; scheme #4 is B2B.

[66] EFD REGULATION, *Schedule 2 §2.5 at 100.*
Proof of audit is transmitted to the secure element to unlock signing or to update maximum allowed sum of fiscal invoice amounts counter. … Updates maximum sum of fiscal invoice amounts allowed for the particular secure element – used to limit total number of fiscal invoices issued between two audits

In fraud scheme #3 a single invoice is photocopied and re-issued throughout the day to customers purchasing the same product. In fraud scheme #4 fraudsters secure apparently valid invoices for re-sale on the black market either by (a) manufacturing them on stolen equipment or by (b) stealing them outright. Fiji's VMS applies two devices to stop these frauds:

- A lottery (customer compliance award)
- VMS's verification function

B2C compliance is very difficult to automate, largely because the non-taxpayer customer is half of the transaction, and incentives are weak in trying to get him/her to report potential fraud transactions to the Tax Authority. Fiji is preparing a *customer compliance award*, or lottery system as a stimulus.[67] The system will provide a web page where individuals or businesses will be able to scan the QR code on their receipts to enter a lottery.

What the FRCS wants from the customer is a verifiable record of the sale, and all the associated data on the QR code. Getting consumers to demand a valid receipt is the best way to assure that businesses provide them. A lottery provides an incentive for consumers to tell the Tax Authority about the transaction. Allowing businesses to participate in the lottery (for a different range or type of prizes) helps make scanning the QR a cultural habit. A chance to win is always the incentive.[68]

Selecting the right lottery prize has an impact on participation.[69] A particularly fitting award would be of free prepaid mobile minutes, awarded more frequently in the industry which demonstrates low compliance rates. In other instances, an award of a tax-free purchase at the same establishment the next time the customer comes in – a limited "tax holiday." The customer would simply scan the older ("winning") receipt into the POS system and the VAT would be removed on the next purchase. This incentive encourages both customer and business owner to embrace the technology.

Encouraging customers to ask for receipts and then scan them has two effects: (1) it discourages collusion frauds, and (2) it allows the Authority to develop an enforcement database of individuals claiming to own the same receipt (the large cheese pizza example). The lottery is one of the things Fiji has not put in place yet, although its outlines are in the regulations.[70]

When the lottery is operational the VMS will then be able to flag duplicate claims of invoice ownership. Enforcement should be swift. The FRCS can immediately terminate the fiscal invoice issuing capacity of the business.

In fraud scheme #4, it is a reasonable assumption that the individual whose POS and E-SDC are stolen will notify the Authority. The thief will need to know the PIN number of the POS to make it work, but if he does and invoices are processed, then the owner's call to the FRCS customer service desk will effectively be a request that the certificate in the stolen POS be revoked. No more fiscal invoices will be able to be issued.

---

[67] OECD, *Technology Tools to Tackle Tax Evasion and Tax Fraud*, April 1, 2017 at 16 (discussing the effectiveness of programs of "… compliance awareness among customers …" and noting the successful lottery programs in Colombia Portugal, Portugal, Poland, Malta and Rwanda) *available at*: https://www.oecd.org/tax/crime/technology-tools-to-tackle-tax-evasion-and-tax-fraud.pdf

[68] There are other incentives that can be used. For example, in Brazil contracts or enforceable only if the party has a digital original document. A similar rule would be that a transaction would only be enforceable if the party seeking to enforce it had a fiscal invoice with valid QR code.

[69] Some jurisdictions, like Malta, prefer lotteries where relatively modest amounts are distributed monthly. *See*: Michael Graham, Mellieħa, *VAT lottery results: four wins in nine months!* TIMES OF MALTA (April 27, 2016) (reporting that a single individual won the monthly VAT lottery in July 2015 - €233; November 2015 - €233; December 2015- €550; March 2016 - €1,569) *available at*: https://www.timesofmalta.com/articles/view/20160427/opinion/VAT-lottery-results.610168. Other jurisdictions prefer large expensive prizes, like new Audi automobiles in Portugal where 40 were awarded in a year. *See*: Patricia Kowsmann, *Get Receipts, Win a Car: How Greece's VAT Lottery Plan Worked in Portugal,* WALL STREET JOURNAL (March 10, 2015) available at: https://blogs.wsj.com/brussels/2015/03/10/get-receipts-win-a-car-how-greeces-vat-lottery-plan-worked-in-portugal/

[70] EFD REGULATION, §26(1) & (2) & *Schedule 2 §6.1* at §26 indicates:

> (1) The CEO may conduct a customer compliance award program involving a fiscal invoice lottery.
> (2) The procedure and criteria for participation in the customer compliance award program are those specified in writing by the CEO and publicly displayed on the premises of the businesses that are part of the program.

If the POS is using a V-SDC that is within the TaxCore this revocation will be instantaneous. The same result would happen with an E-SDC, as the TaxCore can revoke an E-SDC certificate remotely. Any invoice issued after the revocation order will be automatically marked "INVALID."

Fraud scheme #5

The fifth of the common VAT fraud schemes has a long history.[71] Ever since the electronic cash register arrived in the mid 1960's businesses have been manipulating the programming to allow the ECR to function perfectly, but have the records kept in "training mode." These records could be excluded from the electronic memory or deleted all together.

Training mode data manipulation efforts remain popular today.[72] Some fraudsters re-program ECRs to delete training mode data from internal records (Z-Report or the Electronic Journal).[73] In other instances the data is recorded separately but blended in with the general sales files without any indication that the included training amounts are not part of the sales totals (in other words, the training tickets data is hiding in plain sight).[74] Stopping training mode frauds is all about preserving training mode data in detail, and making the operation transparent.

In 2005 the UK explained to the EU Fiscalis how a single restaurant in London had used the training mode to remove over £500,000 of VAT from the records and stole additional taxes exceeding £1 million.[75] Belgium presented similar examples in the Fiscalis meetings. This kind of fraud is nearly impossible in Fiji. If it started it would be identified and stopped fast.

In Figure 7 (above) invoice 5 was a *sales training invoice*. The EFD counters operate just the same for *training sales* as they do for *normal sales*. They aggregate and align the training mode invoices, they place them in a time-sequence and account for each invoice. For example, if we extended the Figure 7 fact pattern we might have TR: 1/5 TS followed by TR: 2/10 TS; TR: 3/11 TS; and TR: 4/15 TS. This would mean that the 5th, 10th, 11th, and 15th invoices are all part of a training program. The *secure element's* counters would preserve the total training mode sales amounts and the total training mode VAT amounts. The data would be kept clear, separate, and not aggregated.

For each training mode invoice a QR code is produced by the VMS. It would indicate that the receipt was issued for training purposes and could not be used to claim an input credit or to apply for a *customer compliance award* (the lottery). The *counters* in the Fiji VMS in conjunction with *proof of audit* would eliminate this variation on fraud schemes #1 and #2, both of which deleted legitimate transactions allowing profits to be skimmed).

In Fiji basic data cannot be manipulated. The VMS captures transaction data and fiscalizes it before any other functions in the POS touch it. But the VMS captures much more than basic data through the *secure element* counters.

All critical data elements are preserved: total sales, total VAT, other taxes like the 10% Services Turnover Tax (STT) and the 6% Environmental and Health Levy (EL) are recorded.[76] The ID of the person undergoing training, the time and duration of the training session is retained. Caps that would force the owner to perform a self-audit [transmitting E-SDC data to the TaxCore and receiving back a *proof of audit*] will come into play. The FRCS is able to set caps on the number of hours per day the training mode

[71] European Commission (DGTCU) Fiscalis FP12 *Cash Register Project Group, Cash Register Good Practice Guide*, v. 1.00 (December 28, 2005 - January 2, 2006) (Restricted – for administrative use only) (one of the first multinational studies of Electronic Sale Suppression [ESS] and the leading document describing the enforcement efforts to date and projections moving forward at the time). Draft copy on file with authors.
[72] See: OECD, *Electronic Sales Suppression: A Threat to Tax Revenues* (2013) (discussing the misuse of functions within the ECR/POS software, specifically the training mode, for either the entire till, or an individual clerk so that items are not recorded in the normal reports).
[73] *Supra* note 71, Fiscalis FP12, *Cash Register Good Practice Guide*, Appendix B, at 2 & 20-24.
[74] *Supra* note 71, Fiscalis FP12, *Cash Register Good Practice Guide*, Appendix B, at 22
[75] *Supra* note 71, Fiscalis FP12, *Cash Register Good Practice Guide*, Appendix B, at 16.
[76] Aside from the VAT, the current system in Fiji tracks: the Services Turnover Tax, the Environment Climate Adaptation Levy, the Plastic Bag Levy, as well as a non-tax classification. One of the distinct advantages of this regime in Fiji is that a tax rate increase (or decrease) can be implemented uniformly throughout the country at a moment's notice. New taxes can be accommodated easily. See: FRCS, *Taxpayer's User Guides*, https://www.frcs.org.fj/our-services/vat-monitoring-system-vms/taxpayer-user-guides/

is used, the number of hours of training each employee undertakes, the sales volumes during training as compared with sales volumes in the normal business at the same time.

CONCLUSION

The strength (and the uniqueness) of the Fiji VAT is in its real-time data collection, its data protection,[77] and its data retention capabilities. When fully implemented these technological reforms promise to capture lost revenues in Fiji of at least FJ$185 million. The amount could be much higher, but it is unlikely to be lower.

There are exceptional efficiencies in this comprehensive digital invoice regime. Fiji will be the first VAT jurisdiction in the South Pacific, and one of the few globally to secure real-time, encrypted reporting of *all taxable transactions*, business-to-business (B2B), and business-to-consumer (B2C). Many of the traditional VAT frauds are simply unworkable in this system. Enforcement flows directly from the technology.

A considerable amount of the auditing function in Fiji will be automated. The *proof of audit* concept, and the *counters* are unique, as well as the use of E-SDC and V-SDCs around the TaxCore.

Fiji is the classic example (in the tax world) of where the Code (meaning the computer code) is the law.[78] The code, or the data structures, and data collection mechanisms of the Fiji VAT compel compliance. For example, an invoice (receipt) without a QR code is visually invalid, while one with a QR code is not necessarily valid, but can be immediately validated at any time, in any place by scanning the QR code. The coding makes this a *truth* of the tax system.

[77] Although not considered here in detail, the Fiji VMS is built upon Public Key Infrastructure. It benefits from services provided like non-repudiation, time stamping, encryption and safe encryption key exchange. One recent example is striking. When the west side of Fiji was hit hard by a cyclone on March 31, 2018 four people were killed. An IT manager of supermarkets in the area called FRCS and reported that two of their three stores were completely flooded, and all POS equipment destroyed. They needed new secure element smart cards for their stores (20 cards for 20 POSs). The old cards were immediately revoked, and new cards were issued (it takes about 60 seconds to produce one card). All the data on the old cards was successfully stored on FRCS servers before revocation. If any of the old cards remained viable the FRCS would know as soon as any receipt from the old secure elements were used. The verification attempt would show the invoice to be "invalid." Staff Reporter, *Tropical Cyclone Josie claims four lives in Fiji*, RNZ [Radio New Zealand] (April 2, 2018) *available at*: https://www.radionz.co.nz/international/pacific-news/353882/tropical-cyclone-josie-claims-four-lives-in-fiji

[78] Lawrence Lessig, *Code Is Law – On Liberty and Cyberspace*, HARVARD MAGAZINE (January-February 2000)

> Our choice is not between "regulation" and "no regulation." The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things. People write the code. Thus, the choice is not whether people will decide how cyberspace regulates. People – coders – will. The only choice is whether we collectively will have a role in their choice – and thus in determining how these values regulate – or whether collectively we will allow the coders to select our values for us.

MANIFESTO

PRINCIPLES BEHIND SALES SUPPRESSION PREVENTION

ANTI-SALES SUPPRESSION SYSTEM DESIGN:

1. A document acknowledging that a payment has been made must contain sufficient transactional data to confirm proper tax calculations.
2. A document must be safeguarded by electronic signature produced by associated secure element, which uses encryption to confirm that issued document is authentic and manipulation free.
3. A secure element used for signing payment documents must be independent from the creator of the automated tax calculation system designed to serve business needs of the user (invoice system).
4. A secure element and invoice system can be used as separate products or integrated into one product and be available in any place at any given time.
5. Work between secure element and invoice system must be optimized in a way to avoid any delay in producing the document.
6. System must be personalized in such way that either document that it produces clearly identifies the issuer.

VERIFICATION OF DOCUMENT INTEGRITY, INSPECTION AND AUDIT:

7. An inspection conducted in simplest form must immediately provide information about the integrity of the payment document.
8. Simple on spot-inspection does not require authorized personnel or sophisticated technical knowledge to perform verification of encrypted data.
9. Authorized personnel follow a unified method to inspect the secure element from which information about each transaction can be extracted, preferably in encrypted form.
10. Electronic journal records in human readable form, must be provided for the user through the invoice system or made available through secure element data collector.
11. Verification services to authenticate documents for both authorized personnel and the public must be available at any time, preferably online, and in various media types.

LEVELING THE PLAYING FIELD FOR ALL SUPPLIERS:

12. Requirements for compliance must be transparent to allow a level playing field for all suppliers to offer their products.
13. Variety models of invoicing systems must be made available to accommodate different business needs.

USER ACCEPTANCE:

14. Information on payment documents, in both printed and electronic form, has to be unequivocally presented to the client.
15. In business-to-business transactions, unique identity of purchasing party must be safeguarded from any modifications by electronic signature.

TAXCORE

DATA TECH INTERNATIONAL