Securing the Fisc via Digitization

The views expressed herein are those of the authors and do not necessarily represent the views of Vertex or their employees, officers, or partners. All legal and other issues must be independently researched and no specific tax or legal advice is being provided.

David Deputy, Vertex, Inc.

Goran Todorov, Data Tech International

Tax evasion, the unlawful nonpayment or underpayment of taxes, is a worldwide phenomenon. Revenue authorities are fighting back through the use of digital technologies and process control frameworks. In this paper, we survey state of the art implementations that have shown real world success and extend forth a vision for a comprehensive secured digital chain of custody capable of ensuring the right tax is paid at the right time by taxpayers within the US.

Successful efforts to reduce tax evasion are starting to emerge in numerous regions of the world. These efforts primarily focus on digitizing the various elements of transaction tax revenue collection. In addition to digital technologies, many regions also combine processes that build trust, such as tax control frameworks and attestation requirements. These efforts have yielded significant results in following countries[1]:

The vision is a comprehensive secured digital chain of custody capable of ensuring the right tax is paid at the right time by taxpayers within the US.

- Sweden has experienced increased tax revenue by EUR 300 million per annum.
- Mexico brought 4.2 million micro businesses into the formal economy as a result of e-invoicing.
- Rwanda saw a VAT revenue increase of 8% in the first 6 months and 20% in two years with its solution.
- Hungary saw VAT revenue increase by 15% in the first year of operation, which more than covered the implementation costs.
- In Quebec, Canada, not only was substantial revenue recovered, but the solution also increased the efficiency for the tax authority to conduct audits, with the number of inspections increasing from 120 to 8000 per year.
- In the Slovak Republic during the years 2014 and 2015, the amount of risky VAT detected in domestic invoicing fraud was more than EUR 500 million.

Lost sales tax revenue from underreporting totals over $16 billion per year.

Appendix A presents a rough estimate of over $16 billion per year in lost US sales tax revenue due to underreporting. The restaurant sector alone is estimated to generate $6.3 billion in losses per year due to underreporting of sales. A survey of the literature illustrates specific examples of successful revenue authority actions to reduce these losses through employing digital technologies. Many of these can be described as attempts to "secure the chain" from transaction to taxation to tax payment. The 2014 OECD document *Tax Compliance by Design*[2] recommends adopting a systems perspective as a key approach to improving SME tax compliance. As elaborated more fully in the document, the systemic thinking approach focuses on designing compliance such that tax in as an integral and inseparable part of business transaction processing.

Elements of this approach have been put into practice in enough jurisdictions to allow identification of key success criteria and propose a comprehensive approach to digitally securing the tax base. In the rest

[1] OECD, (2017), *Technology Tools to Tackle Tax Evasion and Tax Fraud*, http://www.oecd.org/tax/crime/technology-tools-to-tackle-tax-evasion-and-tax-fraud.htm

[2] OECD (2014), *Tax Compliance by Design: Achieving Improved SME Tax Compliance by Adopting a System Perspective*, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264223219-en

of this paper we describe the challenges and categorize them into those for which solutions are available today; those for which we believe solutions will emerge in the near term; and visionary longer term projections. Finally, for solutions available today, we discuss the successes, failures and lessons learned from real world experience around the globe as well as how a revenue authority might approach moving to a digital secured chain based methodology.

The overall intent is to inform and educate the reader as to what a best practice digital solution might encompass and how an individual revenue authority might take advantage thereof. We describe the possibilities around a set of modular components, individually deployable to benefit, and comprehensively complete to secure the entire chain of taxation, and therefore the state's tax base, when deployed together.

> The potential solution involves modular components, individually deployable to benefit, and comprehensively complete to secure the entire chain of taxation.

BACKGROUND AND SCOPE OF THE CHALLENGE

Registered taxpayers have an obligation to collect tax on behalf of the state government for every taxable good and service exchanged for cash, cashless payment or any other form of compensation. Furthermore, the total sum of all sales, including the totals for non-taxable items or services, is levied by way of an income tax (minus all permitted deductions and credits) at the end of the fiscal period prescribed by the government. The following subsections outline the major categories of tax collection risks that are identified across the US. The next section explains how movement to a digitally secured chain approach might be able to mitigate these risks.

CATEGORIES OF TAX COLLECTION RISK

The following four risk categories represent the major of tax collection risk for revenue authorities:

RISK 1: UNDERREPORTING

A taxpayer discloses only part of their sales data to the department of revenue, usually by falsifying books or deleting sales records. The three most common types are:

Risk 1.1: Not issuing receipts

It is very common for consumers not to ask for their receipts; or, if they do ask for it, not to review it. They don't usually have motivation to justify their purchases, unless they require an invoice for possible deductions on personal income tax and similar activities. As a result, taxpayers simply neglect to issue invoices and avoid creating sales records. This applies to participants from all sectors, from retailers who take payments and give change without ringing them, to service providers such as lawyers who render services and simply pocket the payment without recording it.

Risk 1.2: Double set of books

The illegal "two sets of books" practice consists of hiding or disguising certain financial transactions from auditors by having a set of fraudulent accounting records for official use and another set for personal records. This malpractice is usually found in family-owned businesses where the accounting is not outsourced.

Risk 1.3: Use of revenue suppression techniques (Zappers and Phantomware)

A more sophisticated way to underreport sales in an attempt to deceive auditors is to use software, which is orchestrated by series of parameters to alter original sales records and reduce the total tax liability by the desired rate. This mechanism appears to be widespread in the US and Canada as more cases and evidence come to light.

RISK 2: APPLYING THE WRONG TAX RATE

Every jurisdiction mandates application of a certain tax rate to a product or service. However, business people may not be up to date in regard to the rates, or may intentionally apply a lower rate in an attempt to reduce tax liability.

RISK 3: COLLECTED BUT UNREMITTED TAX

In practice, taxpayers often initiate a cessation of business before being properly audited and thus neglect to pay their taxes, which remain unreported.

RISK 4: FALSE EXPENSES/CREDITS/REFUNDS

Taxpayers can claim more business expenses than are true. A very common way is going through the trouble of presenting false receipts for equipment or furniture not actually purchased.

DIGITAL REMEDIES

As illustrated below, existing and emerging digital technologies provide current and plausible future remedies to many of these challenges.

Challenge Category	Digital Remedy	Timing
Underreporting	Secure the Business Transaction	Today
Applying the Wrong Tax Rate	Secure the Tax Computation	1-3 Years
Collected but Unremitted Funds	Secure the Tax Payment	3-5 Years
False Expenses/Credits/Refunds	Secure the Reconciliation	Long Term

We will discuss each challenge individually, focusing the majority of the discussion on the underreporting area where digital remedies are available today. We will also propose for consideration plausible digital designs to remedy the other three areas. Where global examples exist of success in each of these areas, we will provide them.

SECURE THE BUSINESS TRANSACTION TO REMEDY UNDERREPORTING

A recent criminal case in the US sheds some light on the extent of diversion of taxable business transactions from taxation. Most of these issues revolve around small and medium sized businesses, including many in the food service and hospitality industries that employ revenue suppression software, or “zappers,” designed to eliminate a portion of sales from taxation. In this case, a Washington state salesman for a Canadian point of sale (POS) software company pleaded guilty to charges stemming from his sale and distribution of zapper software to restaurants, resulting in a loss of $3.4 million. One Seattle-area restaurant that used the zapper software underpaid taxes by over $900,000 between 2010 and 2013.[3]

According to prosecutors involved in the case, “through the defendant, a hundred restaurants created a hundred sets of false books.”[4] Given this background, projections of the revenue losses among the US may be quite large (see Appendix A). These losses stem from the inability of revenue authorities to secure the chain of business transaction custody in order to ensure that all appropriate business transactions are taxed. The Washington state Department of Revenue is thought to be currently reviewing options to address these issues, as their prevalence is recently becoming much more widely known.

In a related Canadian case involving the same POS vendor, the audited sales losses from the 23 restaurants that were sold the zapper software amounted to $14 million[5].

> “[A] hundred restaurants created a hundred sets of false books.”

The Quebec government, which has been successfully cracking down on cash register fraud since the implementation of black boxes (the SRM project), has estimated that it lost $425 million in 2007-2008 to tax evasion. Prior to launching the SRM project, the government banned the manufacture and use of Zapper programs. InfoSpec Systems Inc. of Richmond, British Columbia, and two employees were charged with nine counts of criminal tax fraud for allegedly supplying area restaurants with zapper software.

Digitally securing the business transaction is the first foundational pillar of a digital secured chain approach. Given the prevalence and impact to state revenue, and the availability today of a digital remedy, it is likely to be the first area a revenue authority would explore. The approach to securing the business transaction relies on three principal components:

1. Implementation of an ordinance, in the form of a set of open standards to which POS and billing/commerce systems vendors must adhere in order to sell their devices within the state;
2. Transmission of verifiable invoices issued through systems using these standards to a central revenue authority database; and
3. Creation of incentive whereby all transactions issued through this system are eligible to participate in programs that randomly award consumers who attempt to verify their transactions,

[3] United States v. John Yin, No. CR16-314 RAJ (W.D. Wash.).

[4] United States Department of Justice, April 14, 2017. *Everett Software Salesman Sentenced to Prison for Selling ‘Tax Zapper’ Software to Enable Cheating on State and Federal Taxes.* https://www.justice.gov/usao-wdwa/pr/everett-software-salesman-sentenced-prison-selling-tax-zapper-software-enable-cheating

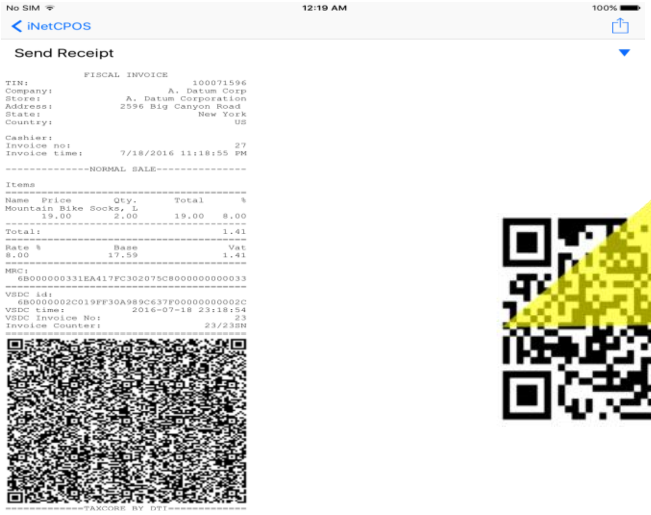
[5] Regina v. InfoSpec Systems, Inc. 2013 BCCA 333, Docket: CA040174, Date: 2013-07-17

commonly known as Consumer Compliance Award programs (CCAs), and often instituted through lotteries.

The creation of a system that adheres to the open standards[6] results in a "secured element" within each device. Every activated secure element is personalized for each individual taxpayer (a similar process to issuing a credit card to an individual). A transaction signed by the secure element remains in the system in encrypted form, which eliminates any risk of tampering. The counters on the records originate from the secured source and thus cannot be changed. Therefore, every receipt issued in this manner is publicly and online verifiable (even by anyone in another jurisdiction), thus preserving true records of every transaction in its original form, forever. Current best practice is to issue a unique QR code for each invoice so that consumers can use their cell phones to enter the lottery, and therefore validate the invoice. In this way consumers are effectively turned into auditors.

Fraud detection by public eye

DEMO



```
              FISCAL INVOICE
TIN:                           100071596
Company:                    A. Datum Corp
Store:               A. Datum Corporation
Address:             2596 Big Canyon Road
State:                           New York
Country:                               US

Cashier:
Invoice no:                            27
Invoice time:       7/18/2016 11:18:55 PM

--------------NORMAL SALE---------------

Items
========================================
Name  Price      Qty.       Total      %
Mountain Bike Socks, L
      19.00      2.00       19.00   8.00
----------------------------------------
Total:                              1.41
========================================
Rate %           Base                Vat
8.00            17.59               1.41
========================================
MRC:
  6B000000331EA417FC302075C8000000000033
========================================
VSDC id:
  6B0000002C019FF30A989C637F000000000002C
VSDC time:           2016-07-18 23:18:54
VSDC Invoice No:                      23
Invoice Counter:                 23/23SN
========================================
==================TAXCORE BY DTI===========
```

SECURE THE TAX COMPUTATION TO REMEDY APPLYING THE WRONG TAX RATE

Just because all appropriate transactions are made available for taxation, it does not mean the correct tax is applied. Taxation errors, both intentional and inadvertent, can occur across the common taxation factors of product, geography/nexus, as well as application of specific rules. Use of third-party-supplied tax rate files or tax engines are also not guaranteed, as these systems provide override capabilities. However, use of third party solutions does set the expectation that the right tax rates are available to be applied, and for tax software engines, rules as well.

Care should be taken to not overly rely on these systems, as individual companies can control the application of taxation through a variety of means, including:

- Required maintenance of the content which drives taxation, generally on a monthly basis;
- Standard configuration via mapping of invoicing/billing/POS systems feeds;

[6] For an example of Open Standards see Appendix B

- Standard configuration via mapping of products to taxation categories;
- Custom configurations whereby the third party vendor's rates and rules can be overridden.

In a secured chain approach, the initial system for taxation of transactions would be set-up and then monitored moving forward. So, rather than testing each transaction for appropriate taxation, as occurs in audits today, the focus shifts to ensuring the tax determination configuration which is driving the taxation is correct and stays that way. One approach would be to integrate an upfront configuration audit to establish an initial correct baseline. Any changes to the configuration from the initial baseline point forward, other than standard monthly rate file updates, would automatically be transmitted to the tax authority for their inspection. Taxpayers might also be able to provide comments contemporaneously with changes that could serve as an explanation.

In this manner, taxpayer-initiated changes, such as remapping an existing product to a new taxability category, might trigger questions from the tax authority if not satisfied by the initial explanation. For example, questions could be about whether the change should have been made in prior periods, and, if so, the impact on prior taxation might be appropriate. This notify-and-question approach might be thought of as a contemporaneous continuous audit, albeit one that is highly automated. In the most automated approach data mining techniques could be used to sift through notifications and perform initial risk assessment screening for targeted audit investigation.

Digital technologies exist today to ensure that all changes to systems of tax determination are tracked and shared with tax authorities.

Digital technologies exist today to ensure that all changes to systems of tax determination are tracked and shared with tax authorities. Through these technologies, and the initial configuration audits, a secured chain of (correct) tax calculation can be created. Since technologies exist, we give this a one to three year timeframe for becoming available for use.

SECURE THE PAYMENT TO REMEDY COLLECTED BUT UNREMITTED FUNDS

Aside from audits, tax payments are the final step in the compliance process. Current processes focus on monthly payments made in conjunction with filing of a return containing summary level transaction and tax information. The funds collected by a business from taxation are accumulated and are generally available for use by the business for any purposes during the month and up until the payment is made. Given the often tight cash flow conditions of many small businesses, and the lack of forced segregation of funds, it can be tempting to use the funds accrued for tax to cover shortfalls during the month. This can give rise to tax liabilities which may never be collected due to business bankruptcies or movements out of state. These challenges are also prevalent in the intentional carousel fraud targeted against input/output VAT regimes.

In a secured chain approach, funds are segregated and transmitted to revenue authorities at the time of the transaction. This approach embeds tax payment processing and funds transmission as part of the tax computation. By design, funds are transmitted immediately. and there is no access to the funds available to the business during the month. This is possible through leveraging emerging digital technologies and standards that enable cost effective and high volume payments down to the fraction of a cent. These capabilities, once matured, would need to be integrated with tax engine/POS/e-commerce vendor systems. As with the other two key technical components of the secure chain approach, this might best be accomplished by a specific regulatory mandate written in a technology agnostic manner; that is, written at the level of standard that must be adhered to by vendors seeking to certify their solutions for use within the state. As the underlying technologies are still experimental, we provide a three to five year projection for availability.

SECURE THE RECONCILIATION TO REMEDY FALSE EXPENSES/CREDITS/REFUNDS

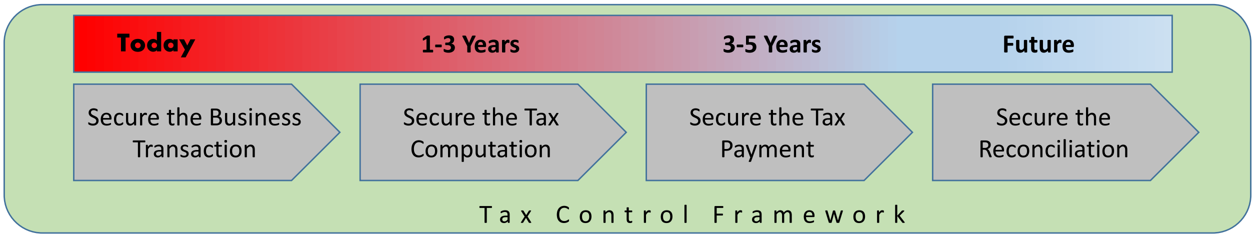
India's new Goods and Services Tax (GST) regime, implemented July 1, 2017, takes a unique approach to reconciliation. The regime is implemented through a central database into which all corporate taxpayers must submit returns which provide identifying details and aggregate transaction amounts segregate for all buyers and sellers with whom they transacted nationwide. The submissions are staggered: one week a taxpayer will submit sales, and the next week they reconcile to their purchases and submit discrepancies. The Goods and Services Tax Network which runs the system intends to tie out the information reported across all buyers and sellers, and flag discrepancies. This is particularly important as the GST has characteristics of an input/output VAT system and is therefore susceptible to over-reported input VAT. Aspects of this approach might be useful in a US income tax context. For example, such an approach might help spot fraud where invoices for expenses/credits/refunds are simply fraudulent rather than misreported.

Finally, we note that India is not the first country to automate reconciliations. China's Golden Tax system operates similarly within each of 31 provinces; current Phase III changes are targeting nationwide reconciliations. Each of these approaches is predicated upon:

- Global identifiers being provided by each entity for every transaction;
- Detailed data being provided to the tax authority central systems; and
- Matching algorithms and digital communication protocols for discrepancy handling.

With the adoption of the secured chain approach and the establishment of databases of validated consumer and B2B transaction data, a similar approach might be possible either within or across states in the US. As there are significant prerequisites, we provide no estimate for when this type of approach may be available for use.

Enable a Tax Control Framework


Today
1-3 Years
3-5 Years
Future
Secure the Business Transaction
Secure the Tax Computation
Secure the Tax Payment
Secure the Reconciliation
Tax Control Framework

Changes in application of a TCF are needed to ensure an appropriate fit to the SMB and indirect tax space.

In order to ensure the effectiveness of the overall secured chain approach, or of any independent component, a control framework must be established. The concept of a Tax Control Framework (TCF) is not new. A good body of materials exist from the Big 4, OECD and elsewhere which document the key elements. However, the majority of the discussions center around TCF as part of a cooperative compliance initiative targeted a large corporations and the income tax domain. As such, they all note that the importance of the TCF lies in its ability to provide a verifiable assurance that the information and returns submitted by a taxpayer are both accurate and complete. The integrity and robust function of a well-designed and effective TCF, one that has been tested by the revenue body, is that it represents empirical evidence that underpins the justified trust in a taxpayer, and in return, the revenue body can provide certainty on the disclosed positions.

While these overall concepts are in line with the secured chain approach to SMB transaction tax compliance, changes in application of a TCF are needed to ensure an appropriate fit to the SMB and indirect tax space. The majority of the changes are focused on moving from a governance and control mentality to a digitized system, with little or no manual intervention. Six principles of an effective TCF can be noted.[7] We summarize them in the left column and contrast them with the types of controls applicable in a similar framework designed for SMB's/Indirect Tax as follows:

Enterprise Income Tax Focused TCF	**SMB Indirect Tax Focused TCF**
Tax Strategy Established	Secured Chain System Established
Applied Comprehensively	All Transactions Processed
Responsibility Assigned	Digital Communications Established
Governance Documented	Notifications of Changes Communicated
Testing Performed	Baseline Established, Changes Tracked
Assurance Provided	Third Party Signoff & Standards Adopted

The Enterprise Income Tax Focused TCF discussed in the literature are process controls that are consistent with internal control frameworks like COSO, which are clearly the domain of large enterprises and unlikely to be relevant to the SMB space. For example, the first element, Tax Strategy Established, proposes that the strategy be "owned" by the company's Board of Directors. While conceptually this is still correct, in the SMB space, a Board may not exist, or may not be capable of this level of diligence.

The focus shifts to creating an automated secured digital flow.

Therefore, in the SMB transaction tax space, the focus shifts from strategy, governance and controls to focus upon creating an automated secured digital flow; from business transaction to tax computation to tax payment and even into cross-company reconciliation. The initial integrity of the flow and the subsequent inability to tamper with it without detection must be established. Both the integrity of the initial process and the ongoing ability of it to capture changes that provide visibility to the tax authority are paramount. To ensure the integrity of this flow, third parties might be used as part of the testing and assurance elements. For example, in securing the tax computation, the initial audit of the taxation settings and configurations could be outsourced to audit firms or the software vendor rather than being done by tax administration personnel. Another example might be where a third party POS, ecommerce or tax engine configuration might need to certify its compliance with open digital standards around securing the business transaction before being allowed to be sold or used in the state.

[7] OECD (2016), *Co-operative Tax Compliance: Building Better Tax Control Frameworks.* Page 17. OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264253384-en.

There are numerous other examples: in Australia, use of third parties and mandated digital standards have reduced the compliance burden on taxpayers and raised the revenue of tax authorities.[8] With respect to standards, our experience has found that legislating specific standards that must be complied with by vendors that supply solutions to taxpayers offers a much more effective approach than mandating taxpayer behavior or systems.

Conclusion

There are real world solutions in use today that can have significant impact upon the fiscal base of many US states, and many more are on the horizon as technology rapidly matures. Accordingly, the issue is no longer whether securing the fiscal revenue flows can be done; the question becomes, should it be done? For revenue authorities with an interest in learning what is possible, now is a good time to become engaged as the non-US entities are laying the groundwork and proving the concepts.

[8] For a relatively complete and recent list see the OECD document Technology and Tools to Tackle Tax Evasion and Tax Fraud where Appendix A lists Sale Suppression Country Examples and B lists electronic invoicing examples

About DTI

With the use of innovative and cutting-edge technologies, we commenced our business operation in the year 2011, to provide a wide spectrum of reliable hardware and software solutions and applications used by tax collecting organs. DTI's mission is to increase tax collection by establishing fraud prevention mechanisms, and thus increase the inflow of funds into the budget. With experienced industry experts on board, DTI is superior in consultancy, provides various certification methods for invoicing products/solutions and offers hardware and software development. We also offer ECR/POS forensic analysis to uncover evidence of unlawful use of zapper and phantom-ware.

For addition information on DTI solutions in use at revenue authorities worldwide see Appendix D. For more information about DTI, visit www.dti.rs or email goran.todorov@dti.rs

About Vertex

Founded in 1978, Vertex Inc. is the leading provider of corporate tax software and services for companies of all sizes, from small to medium-sized businesses to global multinationals. Our solutions enable companies to realize the full strategic potential of the corporate tax function. We offer a variety of products and services that allow businesses to automate, integrate, and streamline their corporate tax processes. Vertex provides solutions in every major line of tax including income, sales and consumer use, value added and payroll. We also offer tailored solutions for specific industries including retail, communications, hospitality and leasing. Vertex Managed Services allows companies to outsource sales and use tax returns and exemption certificate management. Known for our innovative culture, Vertex is a privately held company that employs 900 professionals across the globe, at its headquarters in the U.S. (Berwyn, Pa.) and offices in Europe (London), Brazil (São Paulo), Dallas, Fort Collins, Naperville, Phoenix, San Francisco, Sarasota and Seattle.

For more information about Vertex, visit www.vertexinc.com or email david.deputy@vertexinc.com

APPENDIX A – TAX LOSS ESTIMATES

Sales tax losses are thought to be quite significant, but unfortunately there is a lack of comprehensive US studies to confirm accurate numbers. We present below relevant information that may provide guidance on total tax losses.

Infection Rate: The infection rate has been variously confirmed 30% in Canada, 50% in Germany, 70% in Sweden. Anecdotal evidence indicates US infection rates may be in this range or higher. In 2009, the New York state Department of Revenue ran a sting operation targeting zapper sellers; 26 different cash register and POS makers came to offer solutions to the two state investigators who pretended to be setting up four restaurants in Buffalo, Albany, Dutchess County and New York City. "Of the 26 targets, 25 offered that they could help us evade taxes and showed us in detail how to do it," said the lead agent. "Then the last one called us back and said, 'By the way, there's something else I can do for you.'[9] 90% of the POS vendors offered zappers out of the box. "It's a competitive market and the big thing they could do for you was tax evasion," concluded the lead agent in his report. Some of the companies involved in the scam were part of big publicly held companies. This and many other prosecuted cases prove that this kind of fraud is widespread and infects all types of businesses.

Restaurant Sector: Existing estimates available focus only on the restaurant sector, which is a primary offender but is in good company with hotels, convenience stores, dry cleaners, and other hospitality and service industry participants. With respect to the restaurant sector, estimates of lost tax revenue ranges from $2.3 billion[10] to $21 billion[11] on an annual basis. In Fall 2016, there were 620,807 restaurants in the US. In 2015, food and drinks sales in restaurants in the US exceeded $740 billion[12], which at an average sales tax rate of 8.45%,[13] yields about $62 billion in sales taxes. If 10% of all sales are not reported in this sector, then $6.2 billion of revenue is being lost each year – squarely within the range of the low and high estimates of $2 billion and $21 billion.

All Sectors: Extrapolating our $6.2 billion estimate for the restaurant sector to all sectors of the economy, we come up with a very rough estimate of $16.4 billion per year of lost sales tax revenue. Studies to help refine this estimate would be beneficial.

[9] Professor Richard T. Ainsworth personal communication on file with author.

[10] FTA Technology Conference August 2014 – Research presented by CGI.

[11] Professor Richard T. Ainsworth personal communication on file with author.

[12] https://www.statista.com/statistics/203358/food-and-drinks-sales-of-us-restaurants-since-1970/

[13] https://www.usatoday.com/story/money/personalfinance/2017/03/10/whats-the-average-americans-tax-rate/98734396/

Estimated US Sales Tax Losses ($ Billions 2015)				
	# Establishments	Revenue	Tax	Tax Losses
Restaurants	620,807	$ 740	$ 62	$ 6.2
Bars/nightclubs	68,039	$ 24	$ 2	$ 0.2
Dry cleaners/laundromats	59,521	$ 14	$ 1	$ 0.1
Hotels	92,331	$ 182	$ 15	$ 1.5
Convenience stores	42,032	$ 27	$ 2	$ 0.2
Other	n/a	$ 987	$ 83	$ 8.2
Total US:		$ 1,974	$ 166	**$ 16.4**

Assumptions:

Revenue & # Establishments Source: https://www.ibisworld.com/
All tax & losses at 8.45% and 10%. Other Sector = 2X listed sectors.

APPENDIX B – OPEN STANDARDS APPROACH TO SECURING THE BUSINESS TRANSACTION

The following are 15 high level principles for anti-revenue suppression system design. Applying these principles as legislative requirements by any jurisdiction will provoke vendors and service providers to deliver technology to prevent tax evasion at the point of origin:

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 are 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.

7. An inspection conducted in simplest form must immediately provide information about the integrity of the payment document.

8. Simple on the 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 a 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.

12. Requirements for compliance must be transparent to allow a level playing field for all suppliers to offer their products.

13. A variety of models of invoicing systems must be made available to accommodate different business needs.

14. Information on payment documents, in both printed and electronic form, has to be unequivocally presented to the client.

15. In B2B transactions, the unique identity of a purchasing party must be safeguarded from any modifications by electronic signature.

A standard invoice format should support mandatory data elements of the receipt; also a selection of additional data elements and support for the compliance needs of users in relation to tax and other regulatory requirements. Nowadays there is no universal standard for invoice content. This is due to the differing needs of industries, geographies and jurisdictions, as well as the existence of legacy systems. These differing needs and historical circumstances have resulted in a huge variety of content standards, and datasets tailored to specific requirements.

Taxpayers are often concerned with compliance due the associated costs, complexity of the system working on the taxpayer's side and integration of existing ERP systems in the case of large taxpayers. Making it easy to comply is an important objective when designing and building certification, registration, and audit processes, but it also relates to building taxpayer services and educating taxpayers about the Certified Invoicing System and their rights and obligations.

Making it easy to comply implies focus on the following areas:

- Guidance for suppliers in the form of instructions on how to comply with technical specification and process of accreditation
- Publication of accredited models and vendors for taxpayer's awareness;
- Instruction on how to install and use secure element associated with the invoicing process

There is no need to contemplate a worldwide invoice content standard or data set and indeed this absence of a universal standard is not a barrier to the introduction of a simple set of rules each jurisdiction can make on their own. However, these rules have to flexible enough to enable technology development.

APPENDIX C –SECURE BUSINESS TRANSACTION PROCESSING STEPS

The primary component added to the Certified Invoicing System (CIS) for any POS/ECR device is the Secure Element. This can be the preferred software version (V-SDC)[14] or optionally a hardware version (SDC).[15] These secure elements connect the POS devices to DOR server. The main purpose of either is to transfer a digitally signed invoice to from the POS to the DOR.

There are four primary steps in the solution that define the process of transmitting invoice/receipt data from the taxpayer to the Department of Revenue or appointed service provider in a safe and secure environment:

1. Prior to use, the Secure Element, which is issued to taxpayer for digitally signing receipt and the invoicing system, is tested to ensure compliance with the accreditation requirement requirements. This process is simple and can be performed by even by the cashier.

2. In Online Scenario (real-time audit):
    a. Invoice is sent to the web service, encrypted, after each transaction. Secure Element (in the cloud) performs basic validation and signs invoice if data is valid. Invoice and journal are encrypted and stored as audit data.
    b. The Secure Element transmits audit data to the DOR server. Because the transaction is encrypted, the contents are secure.

3. In Offline Scenario (optional, near real-time audit):
    a. Invoice is sent to secure element, which resides at the taxpayer's premise. Secure element performs basic validation and signs invoice if data is valid. Invoice and journal are encrypted and stored as audit data in local memory.
    b. As soon as Internet connection is available, audit data is immediately dispatched to the DOR server. Otherwise, audit data will be sent as soon as a connection is available or copying audit data to a removable medium could perform a local audit.

4. DOR server receives audit data, extracts, and verifies the payload information.

An advance feature, highly recommendable, is called Proof of Audit and represents a message generated by the software at the DOR once audit data has been received and securely stored on the DOR server. Minimum information contained in the Proof of Audit message must ensure that is used only by the Secure Element, the one that signed invoices in the first place.

[14] http://www.salesdatacontroller.com/sales-data-controller/sdc-implementation/
Virtual Sales Data Controller (V-SDC) is a software solution designed to apply approved encryption algorithm to stamp and safeguard details of receipt/invoice and justify tax liability for the remote issuer.

[15] http://www.salesdatacontroller.com/sales-data-controller/sdc-implementation/
SDC is device that is connected to **ECR/POS** system. **ECR/POS** system communicates with **SDC**, exchanging relevant data.

APPENDIX D – SECURING THE BUSINESS TRANSACTION CUSTOMER REFERENCE IMPLEMENTATIONS

Belgium Ministry of Finance, Cash Register Workgroup

Under the new legislation, the operators of an establishment that regularly serve meals (hospitality sector), from 01/01/2010 must use registered cash register system. This POS system shall be equipped with a Control Module (black box). Since both the technical specifications of the control module is not yet known a workgroup is created within Ministry of Finance to establish all procedures.

Project Resume:

System designed to apply secure electronic signature on customer receipts (certified receipt). Fiscal Data Module device with smart card is added to cash register system to provide source of electronic signature based on PKI.

Carefully specified technical requirements and communication protocol for easy and reliable implementation. Performing cash register inspection made easy by simply plugging a media to a trusted source for detailed transaction report.

Product:

- Drafting Rules and set of instructions for proper implementation of the system
- Drafting communication protocols

Critical factors:

• Separation of signature security distribution (VAT smart card - VSC) and product vendor (Fiscal Data Module -FDM)

• Local audit principles using high speed SD memory cards

Ethiopian Revenue and Customs Authority - ERCA

System was installed in 2008 with 800 sales recording machines equipped with remote audit capabilities. As of 2016 it has more than 100,000 registered devices. Tasks provided by DTI include:

- Design Technical Specification;
- Assist the project office in the planning, managing and controlling of implementation of Sales Register Systems based on the facts provided by the tax collecting organs;
- Advising the project office on how to enforce technical parameters and set standards in the regulations and the guidelines;
- Design and implement work systems, procedures and manuals supporting the project implementation unit;
- Training the project members on how to investigate applications, issuing accreditation compliance and follow test cases before certification;
- Describe business cases for mobile operator;
- Inspection and documentation of reports; and
- Preparing implementation reports with detailed analysis of progress and problems

Rwanda Revenue Authority - RRA

DTI supported creation of the Design Technical Specification, including secure crypto algorithms, and assisted the project office in the planning, managing and controlling of implementation of a Certified Invoicing System based on the facts provided by the tax collecting organizations. Tasks provided include:

- Advising the project office on how to enforce technical parameters and set standards in the regulations and the guidelines;
- Design and implement work systems, procedures and manuals supporting the project implementation unit;
- Training the project members on how to investigate applications, issuing accreditations compliance and follow test cases before certification;
- Provide Business process reengineering required for the development of the software development and to manage the Certified Systems Invoicing software;
- Conduct testing software;
- Describe business cases for mobile operators;
- Inspection and documentation of reports;
- Preparing implementation reports with detailed analysis of progress and problems.
- Delivered software:
    - Security key management module;
    - Certification module;
    - Audit module;
    - Receipt verification module.

System is successful according to the Rwanda Government reports, IGC research and IMF report.