

Technology Tools to Tackle Tax Evasion and Tax Fraud



This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Photo credits: all images courtesy of Shutterstock.com

Table of contents

Executive summary	3
Chapter 1. Introduction: A compelling case	5
Chapter 2. Electronic sales suppression and counter-technology	9
What is the problem?	10
What solutions can address electronic sales suppression?	11
What are the results and benefits?	11
What features do these solutions have?	13
What are the costs?	14
What other actions are needed to implement the solution?	14
Chapter 3. False invoicing	17
What is the problem?	18
What solutions can address false invoicing?	18
What are the results and benefits?	19
What features do these solutions have?	19
What other actions are needed to implement the solution?	20
Chapter 4. The cash economy and the sharing economy:	
Complementary work to address the risks	21
What are the challenges posed by the cash economy?	22
What work is being undertaken to address the cash economy?	22
What are the challenges posed by the sharing economy?	23
What work is being undertaken the sharing economy?	23
Chapter 5. Introducing technology tools: Best practice approaches	27
Chapter 6. Conclusion	31
Annex A. Catalogue of country solutions for electronic sales suppression	33
Annex B. Catalogue of country solutions for electronic invoicing	47
Bibliography	54

Executive summary

While most taxpayers comply with their tax obligations, some are determined not to. Tax evasion and tax fraud continues to occur and can be substantial, amounting to many billions per year. Not only is this against the law and defrauds the government of revenue, but it also creates an un-level playing field for compliant taxpayers.

Many tax authorities around the world are seeing particular types of tax evasion: under-reporting of income through electronic sales suppression and over-reporting of deductions through false invoicing. Tax evasion and fraud can be further facilitated by the cash economy and the sharing (or online) economy.

However, cost effective technology solutions are already available for tax authorities to implement, and which prevent and detect these types of tax evasion and tax fraud.

This report draws on the experience of 21 countries in this area, including several developing countries, and highlights their key successes in using these technology tools. Not only has substantial tax revenue been raised due to the reduction in tax evasion and tax fraud, but where these solutions have been implemented; a deterrent effect is shown, with overall increasing compliance by taxpayers.

This report has been prepared with a view to encouraging other tax authorities to consider whether the same approach may be effective in their jurisdiction. It is the second in a series of reports focusing on the use of technology and digital solutions to address tax evasion, the first being the report *Electronic Sales Suppression: A threat to tax revenue* (OECD, 2013).

This report is divided into four key parts:

- **Electronic sales suppression and counter-technology:** the problem, the key features of available technology solutions, the proven benefits as well as the costs, and the complementary actions needed to implement such solutions;
- **False invoicing:** the problem, the key features of available technology solutions, the results and benefits, and the complementary actions needed to implement such solutions;

- **The cash economy and the sharing economy:** the challenges posed by these segments of the economy and the work tax authorities are doing to address the cash and sharing economy; and
- **Best practices:** the lessons from other tax authorities as to how these technology solutions can be effectively implemented.

The annexes to the report contain a more detailed technical catalogue of the technology solutions being used by tax authorities to address electronic sales suppression and false invoicing. To increase the potential for sharing of experience between tax authorities on the solutions they are using, the OECD Secretariat can also provide contact details for tax authorities to follow up on particular solutions contained in the report.

Chapter 1

Chapter 1

Introduction: A compelling case



Chapter 1

Introduction: A compelling case

Tax evasion and fraud is illegal and intentional misrepresentation of tax obligations. It can involve deliberate omission or falsification of income or revenue, as well as efforts to be invisible to tax authorities altogether. This results in the reduction of income that lawfully belongs to the government, and to the people. The loss of income can be substantial; for example, a study by European Commission reported that the total VAT Gap for 26 EU countries amounted to approximately EUR 193 billion in the year 2011 alone.

Tax evasion and tax fraud not only cheats the public of revenue that is to be used for public goods, but also puts compliant taxpayers that obey the law at a disadvantage. It makes it harder for those compliant businesses to be profitable when they are competing with businesses that do not bear the expense of paying their fair share of taxes.

Two particular types of tax evasion and tax fraud appear to be widespread in their use: underreporting of income through sales suppression and over-reporting of deductions through false invoicing. These are simple for criminals to achieve and can affect countries of all sizes. These types of tax evasion and fraud can be further facilitated by the cash economy and sharing economy. The impact of this tax crime is huge, with anecdotal evidence alone indicating that it amounts to many billions of dollars in lost tax revenue.

In the past, underreporting of income and over-reporting of deductions were difficult and time consuming for tax authorities to detect. This is changing. Many tax authorities are now using technology solutions to detect these tax crimes. These solutions have been effective, and these tax authorities are making progress in bringing previously undetected and lost income into the revenue base, in a way that is also resource efficient for the tax authority. As more solutions become available in the market and the costs reduce, tax authorities have an opportunity to prevent and detect crime, significantly improve their revenue collection and increase the efficiency of their operations.

For this reason, the Task Force on Tax Crime and Other Crimes (TFTC) called for a report to publicise the importance and effectiveness of technology solutions that are being used to detect tax fraud and evasion. This report was based on survey responses and discussions with 21 tax authorities¹ on the solutions they are using or putting in place, as well as publicly available information and consultation with the private sector providers of the relevant technology solutions.

1. Information received from Argentina, Australia, Austria, Belgium, Canada, Finland, France, Germany, Ghana, Greece, Hungary, Italy, Kenya, Mexico, the Netherlands, the People's Republic of China, Rwanda, Singapore, Slovak Republic, Sweden, and the United Kingdom.

This report is not intended to be a comprehensive picture of all technology solutions being used by tax authorities around the world. Rather, it gives a clear picture of the direction that a number of tax authorities are taking, and should lead to further work on sharing information on other technology solutions as they emerge.

The report is divided into two sections. The first provides a brief overview of the types of technology tools that tax administrations have implemented to address tax evasion and tax fraud problems. Looking first at electronic sales suppression and then at false invoicing, it describes the problem, the key features of the technology solutions being used to address the problem, the results, and the complementary tools used to implement the solutions. The report then considers complementary work that is being undertaken to address the cash economy and sharing economy, which, although not types of tax evasion and fraud themselves, can facilitate it.

Table.1.1 Chart of solutions contained in this report

Problem	Sector	Solution	Report Reference
Under-reporting of income	Business – to – consumer <i>e.g.</i> restaurant, bars, taxi, convenience store	Data recording technology in electronic cash registers / sales machines	Chapter 2 and Annex A
Over-reporting of deductions	Business – to – business <i>e.g.</i> construction	Electronic invoicing and automated reporting	Chapter 3 and Annex B
Lack of visibility of business activity	Cash and sharing economy	Legal, policy and analytics	Chapter 4

The second section in Annexes A and B is a more detailed catalogue of the technology solutions being used to address electronic sales suppression and false invoicing, with a view to allowing other tax administrations that are facing the same types of challenges to draw on that experience.

The report concludes that the case for the use of technology to assist in countering tax fraud and evasion is compelling. To make the best use of these available tools, tax authorities must continue to be proactive in sharing experience in order to stay abreast of the tax evasion and fraud techniques as they continue to evolve.

Chapter 2

Chapter 2

Electronic sales suppression and counter-technology



Chapter 2

Electronic sales suppression and counter-technology

At a basic level, sales suppression can be as simple as not recording some cash sales with the intention of under-reporting the amount of sales and thereby under-reporting the corresponding tax liability. However, more sophisticated methods have become very prevalent. With the increased use of technology in businesses, and the increased use of electronic payment forms such as debit cards, sales suppression is also being undertaken through electronic tools that can alter evidence of transactions whether paid in cash or card, without leaving a trace of the alteration. These transactions can also be underreported by using the cash register in training mode, or cancelling transactions after they have occurred. Without the correct data, tax authorities cannot assess the correct tax.

In the past, sales suppression could be achieved simply through putting cash straight into your pocket or editing the accounting books. Now, sales suppression has become more sophisticated through the use of technology which makes it much harder for administrations to detect. The two main electronic sales suppression tools that are used are phantomware and zappers.

Phantomware involves the installation of software as part of the sales register. It allows a program to operate on the sales register which can alter the data that has been recorded. The program is only accessible through a hidden menu which allows the business owner to covertly manipulate the sales records after the transaction has occurred.

A zapper is an external device or external program accessed online that can be connected to the cash register. When connected to a cash register, it allows the manipulation of transaction records, performing a similar function to phantomware.

Both phantomware and zappers allow the user to delete individual sales records altogether and also to substitute the sales amounts to a lower figure and thereby reducing the overall sales. Because of their concealed nature, the cash register appears to users to operate normally and poses a challenge to tax auditors to detect.

New sales suppression techniques have emerged. Referred to as “sales suppression as a service”, this tool allows a taxpayer to achieve sales suppression through a foreign zapper which operates over the internet. The service provides deletion, alteration and replacement of sales data or remote crashing of the hard drive. This can be very difficult for the tax authority to detect as it otherwise appears authentic, or appears not to be attributable to any actions of the taxpayer. Often the service provider is in a foreign jurisdiction, making it difficult for domestic authorities to take enforcement action.

► What solutions can address electronic sales suppression?

Where tax crime is facilitated by technology, a technology response is needed. The most common counter-suppression tool used to address electronic sales suppression is data recording technology. This tool records and secures the sales data immediately as the transaction occurs and stores it in a manner that means it is tamper proof. This means it cannot be manipulated by phantomware or zappers, or if tampering has occurred, it is traceable and detectable. The data should be stored securely and preserved even if there is loss of power.

There are different types of tools that are being used to perform this function, which are referred to in different countries and by different service providers as a fiscal control unit, electronic fiscal device, fiscal memory device, sales data controller or sales recording module. This type of technology should be able to be used in any type of cash register, such as traditional electronic cash registers (ECRs), computer-based point of sales systems, or those that are tablet or smartphone-based. Different solutions are available which can either be included as an integrated part of a cash register, or as an add-on installed with an existing cash register.

As an additional feature, these types of tools are also being used to send data automatically to the tax authority, connecting cash registers online to their data server systems. This can occur either in real time or in bulk scheduled transfers, such as at the end of the day or each month. The tax authority then has the opportunity to access the data remotely for compliance and audit purposes.

► What are the results and benefits?

Results from these devices have been impressive their ability to bring previously untaxed amounts into the revenue base.



Box 1. Highlights of results from electronic data recording technology

In Austria, results from the electronic sales suppression tools are expected to be an additional EUR 900 million in tax revenues.

In Belgium, initial comparisons shows an 8% increase in restaurant sales reported after installation of their solution as with sales reported before.

In Quebec in Canada, At 31 March 2016, CAD 1.2 billion (EUR 822 million) in taxes was recovered following the introduction of sales recording modules into the restaurant industry. Projections are that, by 2018-2019, this will cumulatively amount to CAD 2.1 billion (EUR 1.44 billion). In addition to tax losses, in 2008 the Canadian Revenue Agency criminally charged the owners of four restaurants with tax evasion involving the “zapping” of nearly 200 000 cash transactions, totaling EUR 3.1 million.

In Hungary, electronic cash registers were installed with a fiscal control unit. After the first year of operation, VAT revenue increased by 15% in the concerned sectors. The increase in VAT revenues has exceeded the overall costs of the project of introducing the new systems.

In Rwanda, electronic cash registers were introduced in March 2013. In 2015, VAT collected on sales had increased by 20%.

In Sweden, since 2010, 135 000 cash registers are connected to a fiscal control unit. This includes all companies selling goods and services paid in cash. Increased VAT and income tax revenues has been estimated to around SEK 3 billion (EUR 300 million) per annum since the legislation was implemented. The legislation has also led to better control measures for the Swedish Tax Agency.

There are also benefits for businesses. For instance, tools that prevent the manipulation of sales data and ensure secure accurate reporting will also protect from theft by employees. In addition, tools that accurately record and store data and share it with the tax authority can reduce the burdens of an audit for both the tax authority and the taxpayer.

For example, in the province of Quebec the time required to audit a restaurant used to take 70 hours, but after the introduction of their sales recording module, it now takes three hours. This allowed the tax authority to significantly increase the number of inspections from 120 to 8000 per year. This can be beneficial for business, as the audit can occur electronically and remotely rather than at the business and requiring the production of volumes of hard copy documents, meaning reduced time and interruption to the business.

► What features do these solutions have?

Common regulatory and design features of these solutions include:

Table 2.1 Key features of data recording technology solutions

Feature	Benefits
Regulation and certification of cash registers	Ensures that the cash registers that are authorised for use are only those that have the requisite functions (and do not have prohibited functions that allow sales suppression). One mechanism for doing this is to license only certain market vendors of cash registers. Another mechanism is to introduce regulations that detail the specifications that must be present in cash registers, and allowing the market to provide solutions that meet these requirements.
Data content requirements	Prescribing the details of what data must be recorded and printed on the purchase receipt ensures that the information is useful to the tax administration for verification and for compliance action. This data can be defined as fiscal data and can include the amount of the sale, amount of VAT / sales tax due, time, date, invoice number, the mode of operation that the register was in (such as training mode), and the type of receipt (such as refund or a non-final bill in a restaurant).
Data security: Digital signature of receipt	A digital signature or a control code provides a unique identifier with the details of the transaction such as date, time and amount of the transaction. The digital signature or control code is stored with the transaction data and also printed on the customer's receipt. The signature can be encrypted or a certificate e-signature, for which the tax authority has the corresponding key to identify the creator of the data. Digital signatures allow each transaction to be traced and verified, because the unique identifier guarantees that the data has been generated by the particular taxpayer and has not been altered since the signature was created. If the transaction is subsequently altered, a different digital signature identifier will be generated, leaving a trace of the change.
Data storage	Data must be stored separately and securely from the cash register in a tamper proof environment to prevent manipulation or hacking. The data should be stored at the point the transaction occurs. The data can be stored on an external device that is connected to the cash register (a "black box"), fully integrated inside the cash register or the receipt printer (such as a microchip or sim card), or connected to and stored in cloud-based solutions.
Online data accessibility: Remote access by the tax administration	Where the tax authority has remote access to the information at any time, it deters taxpayers from subsequently altering records. It also allows the tax authority to use the data for audit case selection and in compliance activities, and may make such activities more efficient as the data is already available without having to send a specific request or attend an on-site audit examination. This also assists tax authorities where data may otherwise be stored offshore which can pose challenges for audit.
Data transmission: Reporting to tax administration	Regular data transmission of the records to the tax authority deters taxpayers from altering records as they know the tax authority will have direct data. Information exchange with the tax office can be in real time or at periodic intervals. As online automatic transmission relies on Ethernet or GSM net connectivity, periodic uploading through mobile online devices with secure data buffering capabilities may be suitable in places where reliable connectivity is not in place, and may in some cases be more manageable for the tax authority. It also allows the tax authority to use the data for audit case selection and in compliance activities, and may make such activities more efficient as the data is already available without having to send a specific request or attend an on-site audit examination. This also assists tax authorities where data may otherwise be stored offshore which can pose challenges for audit.

The above described features can be combined in a counter-suppression technical solution in different ways. Important aspects to consider when choosing a solution is the degree of data security (encryption or e-signing) and tamper proof storage; whether to store the secured fiscal data in an external add-on device (a fiscal box) or fully integrated as a module inside the cash register. Requiring certification of solutions and cash registers will simplify and enforce compliance.

A more detailed summary of solutions implemented by some countries is included in Annex A.

► What are the costs?

A key factor in making a technology choice that will be as affordable, effective and easy to implement as possible is to assess the structure of a jurisdiction's cash register market, in particular the range of cash registers in use in different market sectors, from traditional simple cash registers to more sophisticated point of sales equipment. This can make it easier to determine how many cash registers could be upgraded or replaced and the technology price range accordingly.

Costs of these types of solutions have been decreasing over time. Many solutions being used are off-the-shelf solutions that can be installed by the taxpayer, or are already installed in certified cash registers. Factors that can affect the costs of the solution include the degree of modification required to existing machines (as modification of existing systems can be more expensive than adding on a separate component), the size of the market that is implementing the solution, and whether the solution is procured through the open market. Although it is difficult to generalise, costs can be as low as under EUR 30 and up to around EUR 1 000.

The costs to the tax authority should also be considered. This should include giving consideration to the most effective means of enforcing the implementation of the technology solution, including the extent to which the tax administration is itself responsible for technical aspects such as certifying individual cash registers, or inspecting bespoke modifications to existing machines. In addition, the costs for the tax authority of either remotely accessing or receiving and storing bulk transaction data should be considered. In either case, automated data analytics tools could be considered to detect patterns, anomalies or gaps, which would reduce the costs of detecting any unusual results.

► What other actions are needed to implement the solution?

The degree and type of other tools needed to implement data recording technology solutions may depend on the domestic legal framework, such as the regulatory power of the tax authority and the extent to which there is evidence of electronic sales suppression in the country that justifies the introduction of mandatory technology tools. In most cases,

the legal framework will be at the heart of any solution. Additional tasks that should be considered when introducing a technology tool include consultation with taxpayers and the private sector, incentives to taxpayers, legislation and regulatory, as well as monitoring and enforcement. These tools can be used in conjunction and are not mutually exclusive. Further examples on each are included below.

Figure 2.1 Key building blocks to implement the solution



- Legislation** to require the production of invoices for every transaction, together with legislation requiring the use of data recording technology or cash register that are compliant with specified standards. The technical requirements should be very clear and its implementation easily able to be verified. Legislation can also specify how cash registers should be used, such as prohibitions on using cash registers in training mode which prevents transactions being recorded or providing restrictions on how refunds should be recorded to ensure transactions are not falsely reversed as a refund where the taxpayer keeps the payment. Examples: Austria's Fiscal Procedure Code, Sweden's Cash Registers Act.
- Consultation and collaboration** with taxpayers and the providers of cash registers is beneficial when defining the appropriate standards. Examples: the Netherlands worked with the industry to develop a set of "quality marks" which are indicators of reliable cash registers. The state of Ontario in Canada is undertaking a public consultation with businesses and others to obtain input on technology solutions can address electronic sales suppression, in ways that minimise the burden for industry.

- **Incentives** for business to voluntarily install data recording technology, such as an enhanced tax deduction, subsidised costs or linking the use of compliant cash registers to a reduced likelihood of audit.
Examples: Austria provides a special tax deduction upon the taxpayer reporting to the tax authority that they have installed the required device. Experience has shown that even where the government pays for the systems to be used, this is paid for very quickly in the revenue results.
- **Compliance awareness among customers** such as a receipt lottery. This encourages awareness amongst the public of the risk of tax evasion and tax fraud through the misuse of invoices, and enables them to act as an enforcement mechanism, giving taxpayers a business incentive to comply. An extra incentive can apply where customers can enter their receipt into a lottery or accumulate points for each receipt submitted, giving them a chance to win a prize.
Examples: Colombia and Portugal.
- **Monitoring** the introduction of the new technology. This can include requiring suppliers of the cash registers to report to the tax authority to certify that their products meet the specifications, and / or requiring taxpayers to report when they have installed a compliant data recording technology device. The tax authority could then maintain a register or database to assist in follow up audits.
Example: In Sweden a person possessing a cash register must report this to the tax authority, and each cash register has a unique identification number.
- **Enforcement**, such as legislation and penalties for using or distributing electronic sales suppression devices to deter and penalise both the use and the supply of sales suppression technology.
Examples: almost 20 states in the United States have enacted such legislation. This must be supported by effective audit strategies to detect non-compliance with the requirements and ability to enforce penalties.

Chapter 3

Chapter 3

False invoicing



Chapter 3

False invoicing

► What is the problem?

Whereas sales suppression techniques seek to under-report revenue, false invoicing seeks to over-report deductions, and to falsify invoices to mask non-deductible personal expenses as legitimate deductions. False invoicing occurs where a business fabricates or inflates invoices which name the business as the debtor. This allows it to fraudulently claim expenses for tax purposes that have not been incurred. Although in theory a tax authority can verify the validity of each invoice by comparing it to the records of the counterparty to the transaction, it is time consuming and resource intensive to do so.



Box 2. Estimated impact of false invoicing

Between 2007 and 2009 Mexico lost just under EUR 3 billion in tax revenue due to forged invoices.

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.

► What solutions can address false invoicing?

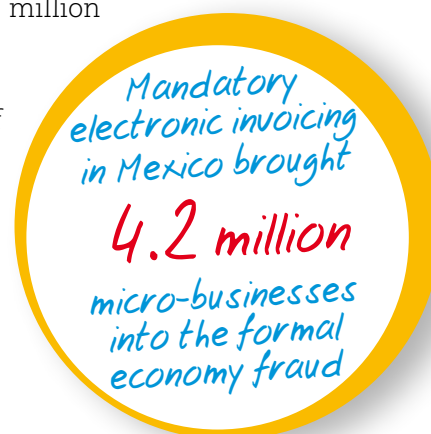
A solution to address the problem of false invoicing is requiring electronic invoicing. Generally businesses must retain records of transactions with customers and provide an invoice to a customer, either in electronic or paper form. An electronic invoice documents the transaction in electronic format. The electronic invoicing system should have additional features to ensure the integrity of the data and the identity of the creator. This can be done by using a digital signature to ensure authenticity of the invoice and that it has not been altered after its creation.

Electronic invoicing will be most effective where the invoices must be registered or otherwise provided to the tax authority. The detection of false over-reporting of deductible expenses can be achieved by automatic matching of the data for the purchaser and seller. Where this is undertaken through periodic or real time data transfers, the tax authority has substantially enhanced visibility of its taxpayers, and can perform audits, analytics and tax return functions in an efficient way.

► What are the results and benefits?

Electronic invoicing has been implemented in a number of countries, with evidence beginning to be collected on its impact. For example, Argentina, Bolivia, Brazil, Colombia, Costa Rica, Ecuador, Guatemala, Italy, the People's Republic of China, Peru, Rwanda and Uruguay have implemented electronic invoicing. The impact in Mexico alone was that mandatory electronic invoicing in Mexico brought 4.2 million micro-businesses into the formal economy.

Electronic invoicing can have the additional benefit of replacing paper invoices, eliminating the need to print, send and store invoices. Recognising the substantial cost savings that arise, the European Union introduced standardised electronic invoicing (Directive 2014/55/EU) for use in public procurement.



► What features do these solutions have?

Common features of electronic invoicing are shown in Table 3.1.:

Table 3.1 Key features of electronic invoicing solutions

Feature	Benefits
Standardising the requirements of electronic invoices	Specifying the requirements such as the content or format, or certifying the providers of electronic invoicing solutions gives quality assurance and ease of audit. It also makes the widespread introduction of electronic invoicing clear and consistent for businesses. Where one standardised format is required, this can make the automatic processing and analysis of bulk data easier for the tax authority.
Digital signature of receipt	Signature provides a unique identifier with the details of the transaction such as date, time and amount of the transaction. The tax authority has the matching key to decrypt the signature and can determine if the receipt is complete and authentic. If the transaction is subsequently altered, a different digital signature identifier will be generated, leaving a trace of the change. Using a digital signature is therefore an important aspect of also being able to verify invoices.
Connection of electronic invoicing to sales recording device	This gives assurance that the invoices are correct when created, and that the data is correctly stored and tamper-proof.
Provision of invoice information to the tax authority	The information generated through electronic invoicing can be provided to the tax authority. This can be by requiring the transmission of all invoices, or specifying the summary information to be transmitted. This could be in real time through online connection to the tax authority, or at scheduled intervals.

► What other actions are needed to implement the solution?

As with electronic sales suppression, technology is not a standalone solution, but features as part of a package. To make the introduction of electronic invoicing effective, the following complementary features have been used:

- **Legislation** requiring electronic invoices, supported by penalties for failure to do so. This could be supported by legislation allowing the tax authority to access third party data to match payment flows to taxpayers.
- **Online verification tools**. Example: in Argentina, after the transaction is approved the taxpayer has to apply to the tax authority for authorisation. If the invoice contains the required information, it is authorised as valid and has fiscal effects against third parties. The information is kept in the database of the tax authority which can be used to subsequently cross-check other tax reporting and collection. In addition, third parties can access a verification tool online, in which they can enter the details of the invoice they have received and instantly verify that it matches the information already registered with the tax authority and therefore know whether it can be relied upon for tax and other purposes.
- Aligning the requirements for the format and content of the electronic invoices to other **tax record keeping and reporting obligations**, or using it to pre-fill returns, can streamline the compliance burden for businesses. Another approach that has been used is to provide relief from tax penalties in the event of an audit provided that the business has implemented the required invoicing tool.
- **Incentives** for taxpayers, such as providing software to assist. Examples: in Italy the Revenue Agency is making software available to businesses for free from July 2016 to conduct electronic invoicing in business to business transactions enabling the operators (especially the micro-small enterprises) to create, transmit and store the electronic invoices. In Chile, the government provides online accounting software which allows small businesses to record transactions and generate pre-filled tax returns. Negative incentives can also be used, such as making the use of electronic invoicing a requirement for the business and the customer to be entitled to claim a deduction in respect of certain transactions or claim input credits for value added taxes. Example: in Italy, the option to electronically transmit invoices would relieve the taxpayer from existing reporting obligations, which is expected to significantly reduce the compliance burden for taxpayers.

Since taxpayers are generally required to maintain business records, the introduction of electronic invoicing may not be a significant departure from existing obligations. Where businesses are currently using paper based record keeping, the introduction of electronic invoicing can bring benefits of greater accuracy and efficiency, particularly where the electronic invoicing system can be used to easily fulfil other tax compliance obligations.

A more detailed summary of solutions implemented by some countries is included in Annex B.

Chapter 4

Chapter 4

The cash economy and the sharing economy: Complementary work to address the risks



Chapter 4

The cash economy and the sharing economy:

Complementary work to address the risks

► What are the challenges posed by the cash economy?

The cash economy and the sharing economy, while not forms of tax evasion or fraud *per se*, have features that can facilitate tax crime. As such, the work that is being undertaken in this area can have a complementary impact on the effectiveness of the technology solutions described above.

The features of the cash economy that can facilitate tax crime are that cash is fungible and untraceable. This makes it easier for under-reporting and falsification to occur as there is not necessarily a record trail as there might be when credit and debit cards and electronic funds transfers are used. The solutions identified above - using tamper proof data recording technology and requiring electronic invoicing - will work together to reduce the risks posed by the cash economy.

► What work is being undertaken to address the cash economy?

Tax authorities are working on a range of solutions, including legislation, analytical tools and encouraging the use of cashless payments such as mobile phone payment methods.

Box 3. Examples of other approaches to address the cash economy

In Argentina, a partial reimbursement of VAT is offered for purchases of personal property or hiring of services when the final consumers perform the transaction using authorised credit card or bank transfers.

In Austria, legislation provides that cash payments for services in the construction industry (including labour) exceeding EUR 500 are no longer tax deductible. The payments must be performed via bank transfer in order to claim the deduction, and this is auditable. Payments for wages for work in the construction sector must not be afforded or accepted in cash if the employee has a bank account or legitimate claim for one.

In Finland, ATM withdrawals are monitored. Withdrawals are summarised by credit / debit card number and cardholders are identified by card number (domestic issued cards) or other means (cards issued abroad). A photograph is taken at the ATM to identify the person withdrawing the cash, and this is available to the tax authority through online connection. If necessary, the photograph will be used for identification purposes at a later stage and this can be used as a risk indicator and / or in conjunction with other information during an investigation.

Box 3. Examples of other approaches to address the cash economy *(continued)*

In France, limits are imposed prohibiting cash payments over EUR 1 000.

In Greece, limits are imposed prohibiting cash payments over EUR 1 500.

In Italy, restrictions on cash were put in place in the real estate sector. In order to obtain allowances for refurbishment expenses and for energy efficiency improvements to buildings, the payment must be performed through a bank or postal transfer. A withholding tax of 8% is also applied. This system reduces the risk of untraceable transactions but also has an immediate revenue impact.

In Sweden, companies can refuse to accept cash payments. This approach is already being used by some restaurants, public transportation and hotels. In Sweden the use of cash is decreasing, and approximately 80 % of all transactions are made electronically, including through new techniques such as smartphones and contactless payment methods. An app developed by banks in Sweden facilitates money transfers between private persons and make payments to companies, which has increased in use from 76 000 transactions in 2012 to 76 million transactions in 2015.

► What are the challenges posed by the sharing economy?

While the cash economy has long been considered by tax authorities, the sharing economy is a relatively new issue. A number of tax administrations have started to investigate the risks of tax evasion and fraud posed by the sharing economy. This includes businesses that operate online through community marketplaces, such as private renting of residential premises through sharing platforms such as Airbnb, driving services through online platforms such as Uber and professional selling through online platforms such as eBay. PriceWaterhouseCoopers estimates that the sharing economy generates USD 15 billion in revenue around the world, and this this could grow to USD 335 billion by 2025.

The challenge of the sharing economy that means it can facilitate tax fraud and evasion is that it can be more difficult to identify the existence of business activity. This is particularly true where the person is not registered as conducting a business or is in a foreign jurisdiction. However, the online nature of these platforms also presents an opportunity to deploy technology to tackle this.

► What work is being undertaken the sharing economy?

Tax authorities are starting work in this area, including analytics, regulatory and policy considerations. In addition, legislative solutions and international co-operation amongst tax authorities is likely to be of assistance in this area, particularly where online platforms are located in jurisdictions other than the location of the customer. For example, the country in which an online platform is situated could introduce requirements that online platforms keep records of its users, which could be reported to the tax authority and exchanged internationally pursuant to information sharing agreements.

Box 4. Examples of approaches to address the sharing economy

Argentina has introduced a special registration system for VAT purposes. This applies to the operator of online portals used for sales operations of new personal property, and online portals where the hiring of services is agreed or performed electronically. The operator of the online portal is obliged to act as VAT collection agents in respect of the transactions performed through the online portal.

Australia makes extensive use of third party data. The tax authority has access to information held in the Australian Transaction Reports and Analysis Centre (AUSTRAC) which is Australia's financial intelligence unit with regulatory responsibility for anti-money laundering and counter-terrorism financing. Through this information, it has traced funds flowing to drivers and renters from overseas to local banks from where they are distributed. The tax authority is using its powers to obtain data from these banks to identify unregistered business activity such as Uber drivers. So far it has been able to identify a large portion of drivers. In addition, the tax authority is working with the platform facilitators, Uber and Airbnb in particular, to have taxation information provided to their partners (i.e. drivers and letters of properties).

Austria uses internet monitoring using different internet scraping tools (web harvesting or web data extraction), some of which are open source and others are custom-made tools. The results of this work feeds into compliance measures such as letters to presumptive taxpayers and information campaigns. Compliance efforts targeting foreign companies offering goods or services in Austria led to VAT collection of EUR 10 million, as well as 44 voluntary declarations resulting in collection of VAT of EUR 5.5 million.

Belgium is using internet scraping and requesting all digital data to enable data mining with existing taxpayer files. This is used in conjunction with other analytics tools such as a 'Forensic Toolkit' to collect and cull data in a forensic inspired way; using Accounting Command Language to analyse semi-structured data which allows importing data from different accounting packages to create a 'standard audit file' and to perform some standard checks; and using an e-discovery solution Zylab to analyse unstructured data like e-mail and PDF documents to search and review this data.

The province of Ontario in Canada is recognising the economic potential of the sharing economy by partnering with Airbnb to launch a new pilot project. Airbnb will educate its hosts through an email notification during tax season to remind them of their tax obligations. The province of Ontario and Airbnb have collaborated to create a webpage with content specific to Ontario regulations.

Finland has legislation to enable the collection of third party information. In addition to audits to collect data to identify shared economy actors, legislation is now used to monitor online credit / debit card payments to detect unregistered remote sellers and VAT EU distance sellers. Data is filtered and clustered by using scripts. Where a significant volume of payments are identified as being made to an unknown person, this can be investigated to determine if the person is an unregistered business. To date, the tax authority has identified 188 unregistered distance sellers, amounting to sales of EUR 50 million. Based on sales, the estimated VAT loss is EUR 12 million yearly.

Box 4. Examples of approaches to address the sharing economy *(continued)*

Japan gathers and analyses information on information-providing services on the internet such as fee-charging websites to identify suspected online businesses, using a general search engine. After picking up a specific suspicious company, comprehensive information is collected using internet crawlers which enable an exhaustive search on the internet. Thus, a variety of materials and information is collated in a database and matched against taxpayers in the system of the tax authority. This matching system enables the tax authority to visualise the risks for each taxpayer.

The United Kingdom is using a product called COSAIN which automates the collation and filtering of social media and websites. The tool collates profiles, which can be used to monitor the trends within a geographic area or specific business sector. In future the e-commerce sector will be able to be analysed, such as collating data from sites such as Craigslist, eBay and Gumtree.

Chapter 5

Chapter 5

Introducing technology tools: Best practice approaches



Chapter 5

Introducing technology tools: Best practice approaches

The experience of tax administrations in introducing a technology solution shows that there are best practices that can assist in making the implementation swift and effective.

First, as there are a variety of solutions available for any given problem, it is critical that the **tax administration has clearly defined its objective**. This includes careful identification of the problem that is being addressed, comparing the options available to it, investigating the technology solutions and preparing an implementation plan that is transparent to the taxpayers. It may also be helpful to seek the input of a range of government stakeholders, including policy, budgetary, tax, technical and legislative functions.

Engagement and **consultation with the taxpayers** that will be affected is an important aspect of implementing a new solution. This can equip the tax administration with insights into the most cost effective solutions, the solutions that would be suitable for different types, maturity and sizes of businesses, provide an opportunity to resolve questions, provide guidance and identify if other supporting measures (such as incentives or enforcement measures) may be needed to bring about swift change. Framing this dialogue in a positive manner can be particularly effective, as although there may be costs for taxpayers there is an opportunity to present the benefits for taxpayers. This includes the importance of ensuring a level playing field between competitors, the ability to streamline other tax reporting obligations, and the ability to guard against reputational damage that arises from tax crimes.

Collaboration with the private sector providers of the solutions from an early stage can be helpful if the market will be supplying the relevant technology solution, and market competition in this field can reduce the costs for taxpayers. Early engagement with the private sector can also assist the tax administration in learning the technical terminology and equipping it to accurately describe the required specifications. This can in turn ensure that the private sector understands how to meet the requirements. Engagement with the private sector can also assist in designing a solution that will be future proofed; for example, to ensure that any updates in software or improvements in the design are able to be implemented in a cost effective manner over time rather than requiring substantial and repeated investments. Testing prototypes of technology test or practical proof of concept evaluations can further support the development of relevant technology requirements and specifications, which ultimately facilitates efficient implementation.

In some cases, tax administrations have adopted a **pilot project approach**. This approach can introduce the solution for an initial test period, such as in a particular region or a particular business sector which is at high risk of tax fraud and evasion, or introducing

it as a voluntary solution coupled with an incentive for businesses that participate in the pilot project. This can be helpful in identifying any implementation problems or unforeseen practical questions. Once any implementation problems have been resolved, the solution can be implemented more widely in industry sectors or locations which are the next priority in terms of risk.

Harnessing the deterrent effect is also an important aspect. This can be done by efforts to raise the public awareness of the extent of the problem, which can mean that the public is an important advocate of change. This can be particularly helpful if legislative changes will be used to introduce a technology solution. Campaigns can be continued over time to publicise the results of technology solutions in recovering public revenue, as these boost taxpayer morale, reinforce the deterrent effect of these solutions and lend support to further expansion of the use of technology tools in preventing and detecting tax fraud.

Enforcement efforts are also necessary to ensure the effective use of technology solutions. These act as a deterrent for businesses in avoiding or misusing the required technology solution as well as penalising any offenders. In addition to pecuniary penalties, other examples of penalties that are used include the suspension of a business licence, imposing a period of enhanced supervision by the tax authority, and public “naming and shaming” of non-compliant taxpayers. The public can also be encouraged to act as an enforcement mechanism where there is a whistleblowing mechanism, allowing employees or customers to inform the tax authority of suspected violations of tax obligations, and possibly offering a reward for doing so. In order to enforce the requirements, the tax authority will need a mechanism to detect and measure non-compliance, including an ability to measure the correct functioning of a technology solution such as through certification.

Finally, tax administrations should continue to engage with taxpayers, the private sector and with each other in order to stay abreast of new risks and share the gains made in implementing new solutions. Technology is a fast changing area, and criminals will continue to find new approaches that demand new response from tax authorities. Tax authorities should continue to share their experiences and insight in utilising technology to combat and deter tax evasion and tax fraud, as well as provide feedback into the broader reform efforts across the tax administration to improve tax compliance.

Chapter 6

Chapter 6

Conclusion



Chapter 6

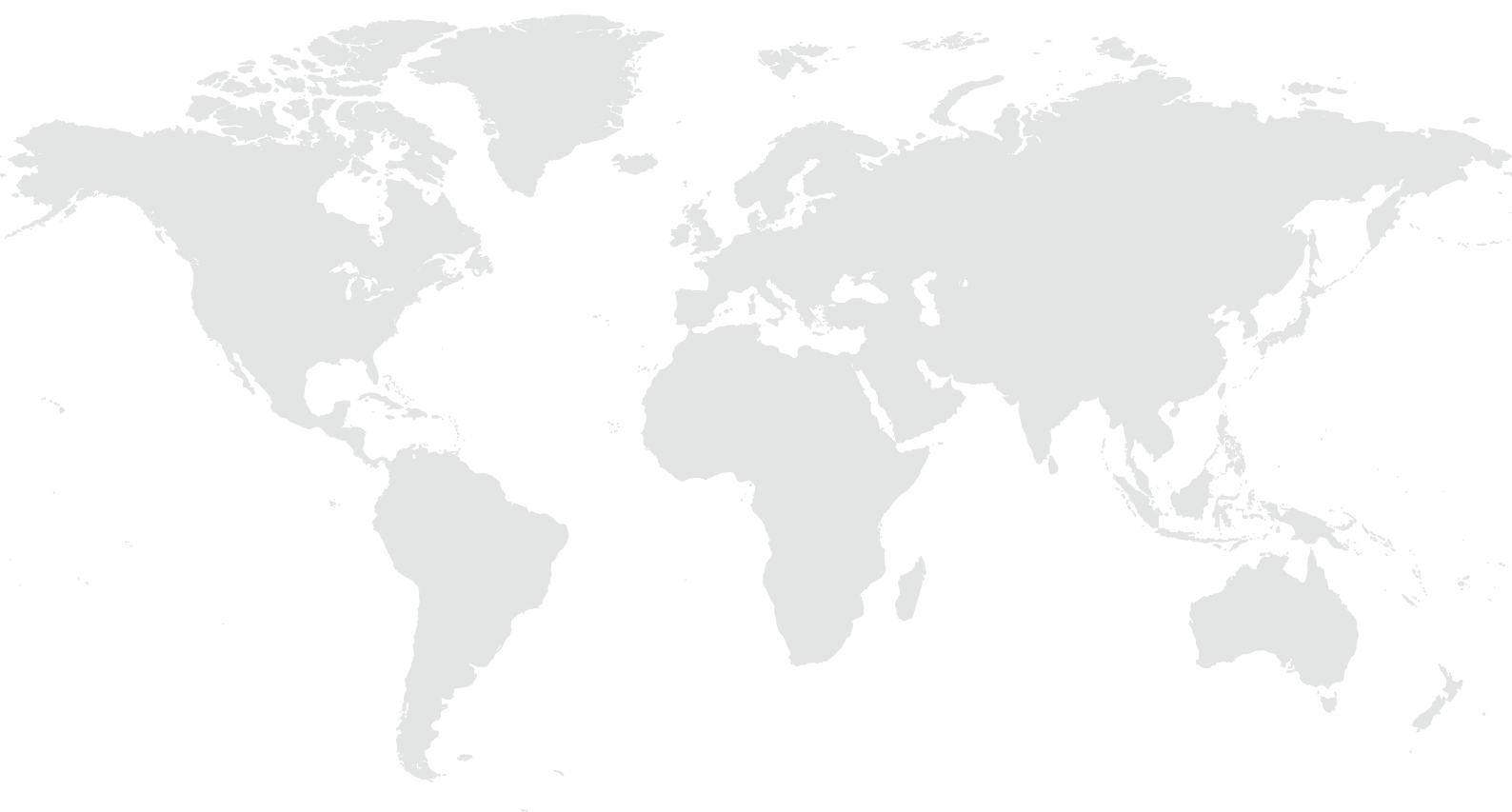
Conclusion

The results that can be achieved by utilising technology to detect and prevent tax fraud and tax evasion speak for themselves. These solutions can offer a win-win: better detection of crime, higher revenue recovery, and synergies that can make tax compliance easier for business and tax administrations. This short report shows that in many cases working solutions are already in place, and that a number of countries are already able to share their experience in the implementation process. It is hoped that this brief report serves as an encouragement for all countries to consider the risks in their taxpayer segments, and to take advantage of the experience of others included in this report to leverage the lessons already learned.

Technology tools are not a single fix to the problem of tax fraud and tax evasion, but if implemented effectively, substantial progress can be made in high risk areas. These solutions should always be accompanied by the other necessary tools available to tax authorities, including legislative measures, effective enforcement, taxpayer consultation and international co-operation.

This report has focused on just a few areas where technology solutions are having a significant impact. As technology and taxpayer behaviour continues to evolve, further areas of work will become relevant. This could include further work on the sharing economy; carousel fraud; customs fraud. Any further work in this area could also build on the ongoing work in the field of data analytics undertaken by both the Task Force on Tax Crimes and Other Crimes and the Forum on Tax Administration.



Catalogue of country solutions for electronic sales suppression



Argentina • Austria • Belgium • Canada (Quebec) • Finland • France • Germany • Ghana • Greece
• Hungary • Italy • Kenya • Netherlands • Rwanda • Slovak Republic • Sweden

Annex A

Catalogue of country solutions for electronic sales suppression

 <p>Argentina</p>	<p>Electronic cash registers / fiscal printers have been implemented in Argentina since the late 1990s. In December 2013, the requirements were strengthened to incorporate new technology with improved intelligence and security in response to evasion techniques that emerged. The new equipment will generate electronic files of the transactions performed, including a digital signature. The files will be regularly transmitted to the tax authority in a similar mechanism as is used for the filing of tax returns.</p> <p>For reference, see General Resolution N° 3561/13 AFIP, at www.infoleg.gov.ar.</p> <p>The challenges that need to be considered in introducing the technology tools include:</p> <ul style="list-style-type: none"> • Limitation of the implementation by the taxpayers who are located in areas of the country with low or no internet connectivity; • Preference for paper procedures in some sectors (mainly small taxpayers or areas within the country); • Costs that have to be paid by the taxpayers for the adaptation of their invoice systems and/or the acquisition of the equipment; • Need to detect possible mistakes in the development of taxpayers invoicing systems early.
 <p>Austria</p>	<p>Technical features: Changes to the Austrian Federal Fiscal Code were introduced in two tranches.</p> <p>From 1 January 2016:</p> <ul style="list-style-type: none"> • For every transaction a receipt has to be issued. • Compulsory introduction of electronic cash registers or other electronic recording systems for digital recording business cases and for printing receipts for all businesses with annual turnover of more than EUR 15 000 provided that annual cash turnover exceeds EUR 7 500. • Each cash register must draw up a data collection log (DCL) to record and store each individual cash transaction. The DCL has to be exportable without delay in case of a request from the tax authorities. <p>From 1 April 2017:</p> <ul style="list-style-type: none"> • A secure signature creation device has to be implemented in the cash register. • All receipts have to be signed. • The cash register has to have a cumulative memory, meaning that the transactions recorded in the cash register are added up continuously. The cumulative memory is part of the signature and constitutes another measure for the prevention of manipulation. • The cash register has to print a monthly final zero-receipt with the level of the cumulative memory and to store it in the DCL. <p>Companies must acquire the required number of signature creation devices from a certified service provider offering qualified signature certificates that is established in the EU, EEA or in Switzerland. The recording-software of the cash register does not have to be certified because the security mechanism consists of linking cash transactions using the electronic signature of the signature creation device. The linking is formed in the signature to be generated by including elements from the last assigned signature saved in the data collection log. When recording the first cash sale, the cash register identification number replaces the last assigned signature.</p>

	<p>Enforcement: At the request of the tax authorities, the company must record a cash transaction set to zero and hand over the receipt issued by the cash register for inspection purpose. For cash registers with a device to transmit payment receipts electronically, the receipt must be made available electronically. At the request of the tax authorities, the company must export and hand over the DCL for a period specified by the tax authorities to an external data carrier. The data carrier must be provided by the company.</p> <p>There are penalties for manipulating cash registers, which apply both to the taxpayers as well as the producers / software engineers of the electronic recording systems.</p> <p>This solution has been beneficial as it offers technical accuracy, is low cost, and allows efficient and effective management of controls and audits.</p>
 <p>Belgium</p>	<p>In 2014, Belgium introduced legislation for certified cash registers, designed to address VAT fraud.</p> <p>The solution consists of four important pillars: technical solution that secures data (making tempering detectable); certification of the devices; registration of all devices by the different stakeholders with the Ministry of Finance; and auditing on the field.</p> <p>Technical features: The 'Registered Cash Register System' (RCRS) applies for the hospitality sector. This RCRS always includes three 'devices':</p> <ol style="list-style-type: none"> 1. the Electronic Cash Register / Point of Sale (ECR/POS) with regulation specifying the forbidden and mandatory functions; 2. the Fiscal Data Module (FDM) that stores the relevant data; 3. the VAT Signing Card (VSC) that contains two certificates to digitally sign the receipt. <p>When a transaction is registered in the ECR/POS, the relevant content is transmitted to the FDM, where it is time stamped and stored and receives the digital signature. The data includes updated counters from the VSC. Some of the control data is also printed on the receipt, making signature verification possible. The digital encryption and signature is very strong, since the Public Key Infrastructure pair of keys is individually created by Belgium's certification authorities in a safe Hardware Security Module environment which is unknown to all other involved stakeholders (such as manufacturers of ECR/POS and FDM and taxpayers).</p> <p>Implementation: Both the ECR/POS and FDM are available on the market, but each model must be certified by the Belgian Ministry of Finance's fiscal department.</p> <p>In addition to the certification, Belgium introduced a registration system. This allows the Belgian Ministry of Finance to know exactly which taxpayers have what equipment, where it is installed and from what time. Furthermore, each certified software has to be hashed, which enables the Ministry of Finance to determine whether the installed system is a correct clone of the certified model or not. The fiscal auditors will have an audit tool to both analyse the FDM data and check the integrity of the data through automatic verification of signatures.</p> <p>The solution has been introduced in the hospitality sector. Originally this applied to establishments with sales turnover of which at least 10 % consisted of meals to be consumed in the premises. In future, the target group will be limited to the establishments with a sales turnover of meals to be consumed in the premises that exceeds EUR 25 000. Full implementation is ongoing and expected to be finished by the end of 2016.</p> <p>Results: The initial results from comparing the declared sales turnover on meals in the restaurants that installed the solution during 2015 with the sales turnover in 2014 shows an increase in 8%. This is notwithstanding that 80% of the restaurants taken into account in the 2015 sales results had only been using the solution for two months. There is also some evidence to suggest a longer trend of increased sales turnover since 2010 of over 20% each year, possibly indicating a 'whitening process' even before the RCRS became mandatory.</p>



Canada (Quebec)

In the province of Quebec, the tax authority developed a Sales Recording Module (SRM).

There are four aspects to this solution: (1) an obligation on the business to provide receipt; (2) the receipt has to be generated using the SRM; (3) inspection activities by the tax authority; and (4) a public awareness campaign.

The legislative basis for the implementation was a modification of the Act respecting the Québec sales tax (CQLR, chapter T-0.1) and the Regulation respecting the Québec sales tax (CQLR, chapter T-0.1, r.2) as well as an amendment to the Tax Administration Act (CQLR, chapter A-6.002) to provide, among other things, for the imposition of penalties.

Technical features: The SRM has three main functions. The SRM receives, registers and sends the transaction data from the point of sale / cash register to the receipt printer. The receipt produced by the SRM must notably contain the total amount of tax due from the transaction, the date and time of the invoice, information on the establishment providing restaurant services, a barcode and a unique digital signature which guarantees the authenticity of the document. The data generated by the SRM also results in the standardised creation of accounting records for all bars and restaurants, which is a significant administrative benefit for taxpayers. The SRM also produces sales summaries which can be sent to the tax authority on request.

The tax authority identifies the specifications required in the point of sale / cash register in order to be compatible with the SRM, lists a number of compatible systems that meet them and can also issue certificates of compliance where an existing system has been adapted.

Enforcement: Inspections are conducted through the use of hand held computers. Inspectors may attend a restaurant posing as an ordinary customer or in uniform identifying themselves and verify if a receipt is issued to them for the meal. The device can then read the barcode on the invoice. This validates the signature on the invoice and identifies whether the invoice was produced using the SRM. The inspector can retrieve information stored in the SRM by downloading it onto a USB key and compare the data from the SRM to the information otherwise reported by the taxpayer.

The public awareness campaign consisted of launching a multimedia ad campaign in order to promote the new measures, thus informing the general public that the operator of a restaurant or bar is required to provide them with an SRM-generated bill, among other things.

Implementation: The SRM was first implemented in the restaurant sector, as there was evidence of sales suppression in this industry. When implementation was launched, 33 000 SRMs were installed in 20 000 establishments. The provincial government subsidised the purchase and installation of SRMs for a temporary period.

Results: At 31 March 2016, CAD 1.2 billion (EUR 822 million) in taxes was recovered following the introduction of the SRM into the restaurant industry. Projections are that, by 2018-2019, this will cumulatively amount to CAD 2.1 billion (EUR 1.44 billion).

The SRM was then implemented in the bar sector as of 1 February 2016. At the time, tax losses were estimated at CAD 76 million (EUR 52 million) per year.

The future plans include upgrading the solution and implementing it in taxi driving businesses.

 <p>Finland</p>	<p>Based on the Finnish Government's Resolution on a National Strategy for Tackling the Shadow Economy and Economic Crime for 2016–2020, an Action Plan against the Shadow Economy and Economic Crime has been drawn up. The Action Plan is dated 7 June 2016 and comprises 20 projects, one of which is a study on the applicability of type-approved point-of-sale systems in Finland.</p> <p>According to the project, the tax administration will prepare a study on the applicability of type approved point of sale systems in Finland. The study will take into account technical implementation, costs to the authorities and businesses as well as impact assessments. Views on the study will be requested from business representatives as well as from other stakeholders involved.</p> <p>The purpose of type-approved point-of-sale systems is to ensure the recording of cash transactions, prevent the manipulation of data by encryption methods and other technical strategies, and ensure that the authorities performing supervision have access to data in standardised form.</p> <p>Because of the global trend, the study will focus on 'online' point-of-sale systems. The study will be implemented by the end of 2018.</p>
 <p>France</p>	<p>In order to fight against VAT fraud related to the use of fraudulent software, the Finance Bill for 2016 establishes the obligation for merchants and other professionals subject to VAT to use a secure and certified cash register system or accounting software.</p> <p>As of 1 January 2018, the use of a secure system will have to be attested by a certificate issued by an accredited organisation or an attested by a certificate issued by the publisher.</p> <p>In cases where there is no certification meeting the requirements, a penalty of EUR 7 500 per item of software will apply, and the offender will have to rectify the situation within 60 days.</p> <p>It is anticipated that some merchants will be able to comply by updating their existing software, as part of a maintenance contract purchased when buying the software.</p>
 <p>Germany</p>	<p>Ensuring that digital records cannot be changed requires the introduction of legal provisions as well as technical measures. For this reason, the new Act on the Protection of Digital Records from Manipulation was implemented (Federal Law Gazette 2016 I page 3152). The intention is that all taxpayers who use an electronic cash register (both cash registers and computer-based tills) will be required to protect the system by means of technical security features.</p> <p>The measures consist of the following elements:</p> <ol style="list-style-type: none"> 1. Mandatory use of technical security features in an electronic recording system. 2. Introduction of cash register inspections. 3. Sanctions against violations. <p>Technical security features: The technical features of electronic recording systems include that it must consist of a security module, a storage medium and a digital interface. The Federal Office for Information Security will specify and certify the technical requirements for each of these components. The electronic basic records must be recorded individually, completely, accurately, promptly, in consecutive order and in a way that they are unchangeable. They must be saved on a storage medium and kept available. These requirements will make it possible in the future for the direct subsequent verification of individual transactions to take place.</p>

**Germany
(continued)**

A Technical Ordinance on the Implementation of the Act on the Protection of Digital Records from Manipulation will describe the requirements for the logging of the individual electronic records. Pursuant to the ordinance, a new transaction must be recorded simultaneously as it occurs by the electronic recording system for every transaction or other operation. This means the data is recorded and stored in a uniform process by means of which the logged individual digital records cannot be manipulated after it has occurred. For this reason, each transaction must be assigned the time of the start of the operation, an unambiguous consecutive transaction number, the type of operation, the date of the operation, the operation's end time or the time when the operation was cancelled, and a check value. If a manipulation should nevertheless occur, this can be detected at any time by means of the transaction chain.

Inspections: Furthermore, unannounced cash register inspections will take place, in order to ensure a significantly increased risk of detection for the taxpayer. Cash register inspections will be used to verify conformity with the law, in particular the correct use of the technical security features. An inspection can take place without advance notice and will take the form of a special process aimed at promptly reviewing the correctness of the cash register records and whether the cash register records have been correctly entered into the accounts. In this context it is worth mentioning the digital interface, which will enable the auditors from the revenue authorities to carry out the inspection more quickly, as well as the option of more easily recognising whether the registration of the basic records is complete by means of the issued receipts.

Sanctions: If violations of the new obligations regarding the proper use of the technical security features are detected, then this can be punished as a tax-related administrative offence with a fine of up to EUR 25 000, irrespective of whether any loss of tax revenue has occurred. This is intended to achieve a general preventive deterrent effect.

Costs: It is anticipated that this solution would mean one-off compliance costs for industry totalling approximately EUR 470 million for the procurement of new equipment and the conversion of existing equipment, plus annual ongoing compliance costs of approximately EUR 106 million, which comprises certification costs, personnel costs relating to helping with inspections and ongoing costs for maintenance and support. These estimates are based on the following calculations:

- Estimated 2.1 million devices affected.
- One-off procurement and installation costs of approximately EUR 224 per device (EUR 470 million in total for industry). This includes the procurement of new equipment (around EUR 193 per device, or EUR 405 million in total for industry) and the retrofitting of existing equipment (around EUR 11 per device, or EUR 22.5 million in total for industry). According to estimates, around 411 000 devices could be replaced and 1.7 million devices could be converted. The total cost also includes an additional amount of around EUR 8 per device (or EUR 17 million in total for industry) for the acquisition of the security module for the conversion plus around EUR 12 per device (or EUR 26 million for industry in total) in personnel costs for the conversion.
- A time burden of an average of 30 minutes per company and cash register inspection would be placed on industry. This estimate takes into account that inspection per company can be of different intensity and length. Based on the expected audit rate of all companies, this results in annual personnel costs of around EUR 343 000.

An amount of EUR 50 per device per year was estimated for the purposes of maintenance and support (e.g. updating the cash register software). This would result in total costs for industry of EUR 105 million per annum.



Ghana

Draft legislation is being considered which would make it mandatory for specifically listed categories of taxpayers to use a fiscal electronic device, including offences and sanctions for failure to do so. This was borne out of the work of a cross-agency committee, including the ministry of finance, tax authority, attorney-general's department and others to study the problem, the technical options, the feasibility of a solution and cost / benefit analysis, which then made a proposal to Cabinet for consideration.

Technical features: the device will be linked to a central point in the tax authority, meaning transactions will be transmitted to the tax authority in encrypted form in real time. The device is also expected to verify / detect input tax claims by taxpayers and possible rejection of fraudulent ones. It is further expected to generate several management reports.

Enforcement: The data provided to the tax authority will be used to generate risk analysis reports, which would identify unusual data to be used for compliance activities. Field audit staff will perform a benchmark study at the start of implementation, which would be used in future for compliance. This has been based on experience from some compliance work performed in the past where field auditors were stationed in businesses such as shops or offices over a period of time to record sales, and thereafter the taxpayers did not subsequently report lower sales to the tax authority.

Benefits and costs: The committee established to study the feasibility of introducing the device estimate conservatively that the introduction of the fiscal electronic device would increase revenue mobilisation by 20%. It is also expected significantly improve taxpayer's record keeping and bring a substantial amount of the informal sector into the tax net. It is also expected to reduce the cost of tax collection. For taxpayers, implementation of the fiscal electronic device is expected to reduce record keeping costs for taxpayers, reduce transaction errors, and assist with stock management and recording employee activity and performance. It is estimated that the fiscal electronic device will cost USD 800 – USD 1 500 (EUR 726 – USD 1 362). The government is considering ways to support taxpayers in bearing this cost.



Greece

New legislation is planned, which regulates the product evaluation and authorisation of point of sale machines, as well as the requirements for businesses to use approved point of sale machines.

Product evaluation and authorisation: In order to be an approved point of sales machine, it must meet the required technical specifications. This device must contain a port for sending its identification data online to the server of the tax authority. If approved, it is authorised for sale in the Greek market, known as a Fiscal Electronic Device.

The process for approving a point of sales product is as follows. Every manufacturer or importer of such machines must seek approval from a committee in the Department of Fiscal Electronic Cash Registers and Systems which is part of the Ministry of Finance. The application includes submission of a working sample of the fiscal model for evaluation and test.

The committee is responsible for checking whether the machine meets the technical specifications, in conjunction with expert evaluators in the National Technical University of Athens.

Once a model has successfully passed all tests, the committee issues the applicant with a unique license number for the specific model. This license number is included on each receipt and affixed on the approved model. This enables any person to check the lawfulness of a specific model by looking at the license number on the issued receipt.

**Greece
(continued)**

Requirement for businesses: A business selling goods and services in return for cash payments must have a Fiscal Electronic Device. Whichever device is used, the taxpayer is obliged to print a receipt for each retail transaction and give it to the customer. Only receipts issued by an approved model of Fiscal Electronic Device are considered as official, legal receipts (see also information on electronic invoicing below). Exemptions may apply in the Decision of the General Secretary of Public Revenue (1002/31.12.2014). The taxpayer must keep a copy of each receipt in either a hard copy or electronic journal. If kept in an electronic journal, this must also be signed at the end of each day.

At the end of each day, a report must be printed with the daily totals. These must be kept for at least five years and must be presented to auditing authorities on request.

The daily report is verified as authentic through the use of a signature. The signature is created upon final issue of the daily report and is registered as a special record in the device memory, accompanied by the date and time and printed on a special daily record signature slip. This slip is issued automatically without requiring the intervention of the operator of the device. It is then stored electronically.

The device memory is protected in a special box, which is an integral part of the fiscal electronic device and is sealed with a special material such that the removal of the memory is impossible without destroying the cover of the device. The preservation of this data is independent of any integrated or external power source. The memory is either built-in and sealed inside of the device or installed as an external add-on.

All receipts issued by the Fiscal Electronic Device during the day from the issue of the previous daily total report until the issue of the next daily total report are registered in an electronic journal. Consideration is being given to constructing a mechanism for the data with the digital signature for the transactions to be automatically transmitted to the tax authority server. The transmission of this data is encrypted and after the decryption is only accessible by relevant personnel in the tax authority and by the owner of Fiscal Electronic Device.

Enforcement: These solutions are monitored and enforces as follows:

- Legislation and regulations state that businesses providing goods or services to retail customers are obliged to inform customers of their obligation to issue receipts. Taxpayers may only claim a tax deduction with respect to the purchase if it can be verified with a legal receipt, giving them an incentive to ensure they obtain a receipt when they purchase goods.
- Random audits will be undertaken by tax authorities to check that customers exiting the business have a legally issued receipt.
- Strict penalties are imposed for a breach of the legal obligations, including for failure to maintain these records, distortion of fiscal devices, alteration of the data or destruction or corruption of these records.

In 2014, Hungary introduced an online cash register.

Hungary

Technical specifications: Regulation includes technical specifications for the cash registers, the security requirements, the user identification process and rules on licensing cash registers. The data is recorded in a Fiscal Control Unit (FCU) equipped with a mechanical seal, which is embedded in the machine at the point of sales.

Data transmission: The data is then transmitted in high frequency to the tax authority. Having regard to the need to ensure reliability, it was considered best to use mobile phone network operators as they are identifiable and reliable service providers, and the mobile network covers almost all of the country. To ensure confidentiality, bank-level cryptographic solutions have been introduced, the infrastructure of which is provided by the tax authority.

<p>Hungary (continued)</p>	<p>Implementation: The IT-solution was developed by market players based on published criteria and a competitive tender from the market was launched. The system was first introduced in the retail and hospitality sectors which had previously been obliged to use (not on-line) cash registers as well, and in 2016 it was expanded to the service sector and to car dealerships and car parts dealers. More than 225 000 cash registers are connected to the system. In order to obtain the solution, small businesses receive subsidies for up to five changes of cash machines.</p> <p>Inspection: The tax authority has mobile inspection devices, from which display operating cash registers on a map. Using these devices an inspector can directly access the data of a particular taxpayer. The incoming data are stored in a data warehouse which allows continuous risk assessment, analysis, and setting up a list of shops selected for spot checks. The auditor can also verify whether the number and type of electronic cash registers in a particular shop match the number and type registered in the central database, as well as check whether the amount of money or money equivalent in the cash register matches the amount recorded on the fiscal control unit.</p> <p>Results: In the first year of introduction (2014), VAT revenue increased by 15% in the concerned sectors, and as a result, the increase in VAT revenues has exceeded the overall costs of the whole project already during the introduction. Since then, there has been a continuous clearing of the economy in the concerned sectors. In addition, there was an increase in the number of employees registered for tax.</p>
 <p>Italy</p>	<p>To address the risk of data alteration using illegal sales suppression software, Italy introduced Legislative Decree no. 127 dated 05.08.2015. The Decree is designed to encourage the electronic transmission of payment data as well as the use of e-invoicing (electronic documents undersigned with electronic signature). See below for more detail on electronic invoicing.</p> <p>It applies to retailers, and introduces a cash register system directly transmitting data to the tax authority at the end of each day, securely and without altering any information. In this way, some accounting obligations are not due.</p> <p>This measure is designed to:</p> <ul style="list-style-type: none"> • Boost the risk analysis. • Simplify the system. • Promote and support the digitalisation.
 <p>Kenya</p>	<p>Kenya is currently testing a new solution, Accounting Command Language, I Tax Management and electronic cash registers to address the problem of manipulation of sales data, and non-reporting of sales transactions. These are focussed on the risks posed in the construction sector, supermarkets and shopping malls and medium – large taxpayers.</p> <p>Additional tax has been reported since tax transactions have been required to be performed online such as tax return filling and payments. Audit and investigation modules are at an advanced stage of being implemented.</p>
 <p>Netherlands</p>	<p>In the Netherlands a “voluntary” quality-mark is developed.</p> <p>Features: A cash register with a quality mark fulfils the requirements to store and process data reliably, and whereby alternations to transactions can be detected. The set of quality mark indicators were developed with inputs from many developers and distributors of cash registers.</p> <p>Implementation: The Netherlands Tax and Customs Administration encourages the implementation of these “quality-mark” point of sale-systems in the whole market. In particular, it focussed on franchisors, which have an interest in preventing any harm to the name and reputation of their business. The tax administration made an agreement with the franchisees on checking doubtful returns based on EDP scripts. Any improbabilities were shared with the franchisor and they were given the opportunity to explain the findings.</p>

**Netherlands
(continued)**

Results: The results of this were positive. Of 45% of the fraudulent franchisees, 85% came to a voluntary agreement with the tax administration in order to restore the misconduct. The profit from investigated supermarkets alone was around EUR 15 million, including fraud cases and voluntary statements of franchisees. The publicity may have also had an impact on these results.

Another aim was to establish a change in behaviour among franchises by creating an atmosphere in which committing fraud was unacceptable. This has led to more governance in the sector, more control mechanisms like new software tools, more transparency between retail organisations and more discussion between supermarkets about audit mechanisms and experiences.

**Rwanda**

Rwanda has introduced legislation and regulations requiring Value Added Tax (VAT) registered taxpayers to buy and use electronic billing machines (EBM).

Context of introduction of EBM:

- Manual invoicing systems were paper based which are easily destroyable by fire, water or any other disaster.
- Forgery of invoices resulting into unreported sales and undue VAT refund claims.
- Double sales invoice books (especially large, medium or small family owned businesses).
- Cost and time taken during tax audits.
- Lack of transparency in the course of tax audits.

Legal framework: Law No 37/2012 Establishing Value Added Tax as modified and complemented to date and Ministerial Order N° 002/13/10/TC of 31/07/2013 on Modalities of Use of Certified Electronic Billing Machine. For reference, the Ministerial Order is available here: www.rra.gov.rw/typo3conf/ext/complete/Resources/Public/download/pdf/ogazette.pdf

Technical features: There are two aspects of the system: a Certified Invoicing System (CIS) and a Sales Data Controller (SDC), also available as a certified All in One device incorporating CIS and SDC features in one device and certified software meeting CIS requirements.

The CIS is the point of sale machine, which must send the transaction data to the SDC. Each CIS has a unique registration number. The CIS must generate a receipt containing at least the following data: taxpayer's name; identification number; address where the sale took place; receipt type and transaction type; serial number of the receipt in uninterrupted ascending number series; description of the sale / service items with quantity, price and other actions such as cancellation or corrections; total sale amount; tax rate; tax on the sale; means of payment; SDC information including date and time stamp, sequential receipt number, receipt signature and SDC identification number; data and time stamp by CIS; machine registration code.

The SDC is connected to the CIS and processes and stores the receipts. The SDC is secure and tamper-proof, and each certified SDC has a unique serial number. The SDC assigns an electronic signature to the transaction which is printed on the receipt. The signature is verifiable by the tax authority using a special decryption tool which is unique for every installed SDC device, meaning that falsification of the signature can be immediately detected.

The electronic billing machine must be clearly visible to customers, with a statement including the name of the user, the unique identification numbers for the CIS and SDC, and that customers should not pay if a receipt is not issued. The electronic billing machine must be connected to the tax authority's server accessible to both the customs and domestic tax officials. Data is transmitted in encrypted form. The tax authority can then perform local audit or remote audit.

**Rwanda
(continued)**

Implementation: Implementation of the electronic billing machine requirements is occurring in a progressive manner, with the tax authority specifying particular categories of taxpayers required to use electronic billing machines. Once fully implemented, every business registered for VAT will have to provide a customer with a special receipt issued through the electronic billing machine for every sold good or service.

The suppliers of electronic billing machines must obtain authorisation from the tax authority in order to obtain certification of their systems. This includes a test of the software through a live demonstration or machine inspection. Once certified, the supplier is added to the list of certified products which is published on the tax authority's website. Taxpayers will either procure the electronic billing machine from the list of certified suppliers, or if they choose to modify their existing system, this must be specifically inspected and authorised by the tax authority as meeting the requirements.

Benefits of EBM for taxpayers:

- EBM constitutes an internal control tool.
- EBM helps in stock taking.
- EBM data serve for accounting purposes.
- Information safely kept.
- A means for business transparency.
- A means of information for business stakeholders and partners.
- Less time and financial audit costing.

Benefits of EBM for the tax authority

- Real time sharing of information between tax administration and taxpayers.
- Information safely kept.
- Less time and financial audit costing.
- Improve transparency in tax audit process.
- Improve the VAT refund process.
- Improve the level of VAT collections.
- EBM constitutes a management tool and an efficiency control mechanism.

Results: In March 2013, implementation started with 800 machines. At July 2016, there are now 13 520 machines which are used by 85% of the VAT registered taxpayers. VAT collections have increased since the introduction of EBM:

- In March 2013 to June 2014, EBM contributed to the increase of 6.5% of VAT collections.
- VAT collected on sales increased in 2015 by 20% when compared to 2014.
- VAT payable registered an increase of 22% for 2015/2016 fiscal year compared to 2014/2015 fiscal year.
- Cases of undue refund claims identified and prosecuted.

Rwanda (continued)

Implementation challenges:

- Low culture of invoice requesting whenever a sale is made.
- EBM users not issuing EBM invoices (they issue manual invoices, delivery notes or simply nothing) especially in service industry such as in Restaurants, Bars but also in Supermarkets.
- EBM users issue an invoice with the price lower than the actual money received.
- Misuse of tax rates (taxable goods considered as exempted ones).

Enforcement: Each taxpayer that is required to use an electronic billing machine must register with the tax authority. The tax authority has the power to conduct inspections of electronic billing machines to verify compliance with the technical specifications and other taxpayer obligations with respect to the electronic billing machine. Substantial fines will apply to businesses that do not install and use the electronic billing machine as required, and to suppliers of CIS or SDC machines.

The tax authority has also used enforcement and deterrence strategies including the following:

- Education and sensitisation of consumers.
- Sensitisation of university, secondary schools students, religious leaders, private and public institutions.
- Consumer motivation “EBM lottery scheme”.
- Introduction of Supply Chain Management software.
- Mystery shopping.
- Understanding of price structure for some commodities.

More information is available here: www.rra.gov.rw/index.php?id=33.



Slovak Republic

Electronic cash registers were introduced in the Slovak Republic in 2008. The legislation with effect from 1 January 2015 extended the list of service providers who must use electronic cash registers (“ECR”) when selling goods and services and also created a virtual electronic cash register (“VECR”).

Technical features: The VECR is a platform set up on the Financial Directorate’s website and communicates with devices such as PC, tablet or smartphone and a printer. The Financial Directorate developed the VECR application and made it available free of charge for all the entrepreneurs that are obliged to use cash registers.

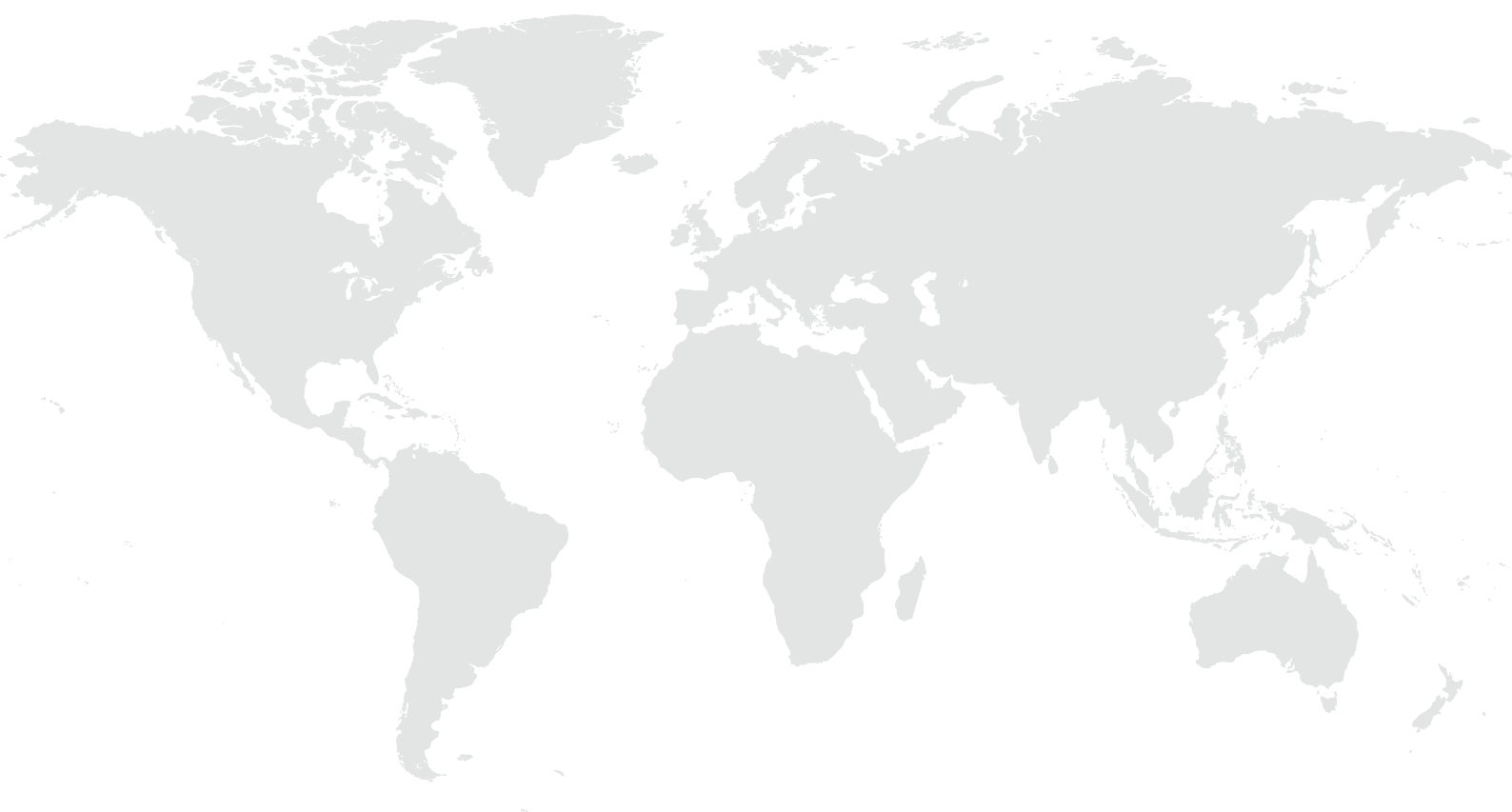
Compared to a receipt issued by the ECR, the receipt issued by the VECR contains a unique identification code and QR code with all the data of issued receipt but also identification data about the entrepreneur: business name of entrepreneur, billing address, address of the sales point, tax identification number, and VAT identification number.

Access for the tax administration: All the financial transactions made by the seller are saved on the Financial Directorate’s servers and are accessible to the tax administration. Tax auditors can immediately access information about all the users such as the location of the sales points, the issued receipts (fiscal receipts), the other receipts (non-fiscal receipts), the amount of money in the VECR’s cash drawer and they can generate financial closing accounts or reports including financial data regarding to a specific VECR user and a specific time interval.

All the reports generated by the tax auditors are easily processable with analytical software like IDEA from their desk. Tax auditors can run analytical tests over the reports and can gain exact knowledge about the entrepreneur’s fiscal behaviour and detect risky fiscal transactions (e.g. issuing lots of non-fiscal receipts, issuing receipts with returned items which are reducing the tax duty). Using the data from VECR and analytical tools such as IDEA can contribute to a more effective selection of sellers for later auditing.

<p>Slovak Republic (continued)</p>	<p>Third party verification: The QR code can be easily checked by another application developed by the Financial Directorate named “Check the receipt”, an application designed for the customers or clients so they can verify themselves the data contained in the receipt issued with the VECR. If customers or clients find that the data on the issued receipt does not match the data on the VECR server, they can contact the Financial administration.</p> <p>Next steps: The Financial Directorate is working on another application which will be used by the tax auditors on the premises where the tax audit takes place. This new application will be connected to the VECR server and will provide tax auditors with on-line and on site information about the fiscal behaviour of the entrepreneurs, the issued receipts and allow them to generate financial closing reports.</p> <p>This new application should help the tax auditors to audit and control service providers even more efficiently.</p>
<p> Sweden</p>	<p>Sweden requires that sales must be registered in a cash register connected to a fiscal control unit.</p> <p>Technical features: The cash register must meet a certain standard, which the manufacturers of the cash register are responsible for meeting. The fiscal control unit must be certified by a specific body in the Swedish tax authority. Taxpayers must register with the tax authority to confirm that they are using a cash register connected to a fiscal control unit.</p> <p>The requirements for the content of the data that must be recorded in the fiscal control unit are included in regulations. This includes:</p> <ul style="list-style-type: none"> • One log for counters: The total number of receipts issued, missing receipts, the number of regular receipts, the number of training receipts, the number of copies of receipts, the total sales and the grand total. • Another log for specific information about each receipt: receipt number, date, time, sales amount, VAT amount, and a unique control code generated by the control unit. <p>The information in the control unit is encrypted and can only be read and decrypted by the Swedish tax authority.</p> <p>Implementation: Sweden targeted all sectors that are selling goods and services which are often paid in cash. Some general exemptions apply, including for taxis, e-commerce, vending machines, amusements games, slot machines, and governmental or municipal organisations. It is also possible for taxpayers to apply for an exemption, where the bookkeeping is reliable and that the fiscal control can be guaranteed in other ways than using a control unit; or if it is unreasonable for any reasons to have a certified cash register. The cost for implementation was in average about EUR 2 500 per cash register, including hardware and installations costs.</p> <p>Enforcement: The tax authority analyses information from the electronic journal and from the control unit using traditional e-audit methods. In addition, the tax authority conducts a lot of unannounced on sight inspections to verify whether receipts are given and that sales are registered, as well as doing undercover purchases posing as customers and counting customers. Penalties can be issued if a sale is not registered. The information from the inspections is then used as feedback to determine risk levels for follow up action. The visibility of enforcement actions has been crucial for acceptance of the legislation and compliance, as well as ensuring a level playing field between businesses.</p> <p>Results: Compliance has increased both among users of cash registers and the manufacturers of cash registers. Manufacturers are more compliant and the tax authority has not found any zappers or phantomware since the legislation was implemented.</p> <p>The immediate revenue effect once the requirements were introduced was a 5% increase in the reported revenues. The estimation of the ongoing effect will be at least a 1% increase in reported revenue. This means that the reform has resulted in increased tax revenues of at least SEK 3 billion (EUR 320 million) per annum as a result of reduced tax evasion. In addition, the introduction of the fiscal control unit has had a significant preventative effect which has also contributed to increased revenue collection.</p>

Catalogue of country solutions for electronic invoicing



Argentina • Greece • Italy • Kenya • Mexico • The People's Republic of China
• Singapore • Slovak Republic

Annex B

Catalogue of country solutions for electronic invoicing



Argentina

Argentina has used mandatory electronic invoicing for certain sectors since 2007 (and optional electronic invoicing since 2006). Since then, the use of the electronic invoices has been expanded in a gradual and phased manner according to the business activity and type of taxpayer. During 2016, the implementation will be completed so that it will be mandatory for all taxpayers registered for Value Added Tax (VAT).

Technical features: The model is based on the “online” authorisation of the documents. This means that the taxpayer, after the approval of the operation, has to apply to the tax authority for authorisation so that the document is considered an invoice and has fiscal effects against third parties. The information is validated online and if the invoice is authorised it is given an authorisation code and all the information entered is kept in the database of the tax authority. In this way, the revenue body has the information of the issuer and receiver of the invoice, of the applicable tax debit and the possible tax credit to compute before the submission of the VAT return.


For more details see General Resolution N° 2485/08 AFIP www.infoleg.gov.ar and www.afip.gob.ar/fe/#que.




Benefits: The implementation of digital documents has had the following advantages and strengths (also relevant for electronic sales suppression above):

- There is a formal control at the moment of authorising the printing of receipts.
- The tax authority has timely access to the tax debit and possible calculation of tax credit of the transactions.
- The digitalisation of the information, together with technological developments, allow for the exploitation of large volumes of data more dynamically.
- They place the obligation on the taxpayer to comply with the procedures and include the data in the making of the receipts in accordance with the existing rules, reducing the administrative cost for the tax authority.
- Once the transaction is registered, the possibility of it being subsequently falsified is significantly reduced as the invalidation of a receipt may only take place with a new document adjusting the previous one, leaving a record of the change, or through a fraudulent manoeuvre that violates security standards in the electronic cash register.
- There is an increased risk perception on the part of business and customers because the information in electronic format and there are tools for third parties to verify receipts.

Enforcement: Electronic invoicing is monitored and enforced as follows.

- There is a tool designed to verify receipts, whereby the receiver of the electronic invoice, or entities dealing with tax/social security procedures, are able to verify if the information contained in the receipt matches the information timely entered and authorised by the tax authority. The online authorisation model provides an almost immediate response to taxpayers has proved to be very productive from its early stages in 2006 and has assisted progress with the generalised implementation of the electronic invoice system to more sectors and taxpayers.
- The information on invoices received through the authorisation process provides valuable information to perform cross-checking with other data recorded by the tax authority.

	<ul style="list-style-type: none"> • Publication on the web site of a list of non-reliable taxpayers, based on the controls performed. The consequence of publication is limitation on the use of the individual Taxpayer Identification Number and temporary suspension of the authorisations to issue invoices. • The solutions implemented strengthen the controls performed by the tax office and in turn generate risk perception by the taxpayers. • In addition, although many of the measures are preventive, ongoing control is required to maintain the risk perception levels. It is also necessary to periodically define new prevention tools to respond to emerging risks and technologies. <p>Results: The results and impacts of the incorporation of the electronic invoice in Argentina have generated positive effects in a gradual, phased manner, together with the progress of its implementation during the last 10 years. To date, there are more than 750 000 users already incorporated in the system and more than 4 billion electronic receipts have been issued.</p>
 <p>Greece</p>	<p>Greece is in the process of introducing electronic invoicing requirements.</p> <p>Technical features: All invoices, credit notes and consignment notes issued by computers will be required to be signed electronically using a special licensed fiscal electronic signature device (FESD). Each relevant business will be required to buy an approved FESD or adapt the existing computer equipment to meet the technical specifications. This is one of the methods of authentication under the L.4308/2014.</p> <p>When the invoice is printed, the unique e-signature generated by the FESD is printed at the end of the document. This works as follows. After entering and formatting the data to be printed in the computer, and after initialisation of the record issuing – printing, the computer's software saves, communicates and transmits to the FESD the set of the required data of the slip being issued. The FESD receives this data, processes it with a special security algorithm (SHA-1) that creates a hash value (sign) and sends the result of this processing back to the connected computer. The hash value, which represents a sequence of characters and digits, is the unique electronic digital “fingerprint” of the data of the slip being issued. The FESD saves this hash value into his own working daily memory and issues a relevant slip – receipt with the date, the time, the daily ascending sequential number and the general ascending sequential number of slip issue.</p> <p>All the produced signatures are stored securely the inside FESD's memory at the end of each day and collated in a day-end report. The day-end summary report is also assigned a unique e-signature and saved permanently in the secure fiscal memory of the FESD. These must be preserved for at least five years and provided to tax auditors in an audit. These files are considered as primary transactional data and must be reflected to the totals in accounting books.</p> <p>Each day the business owner automatically sends the summary file to the tax authority server, in encrypted form to be decrypted automatically only by the server. The fiscal data are accessible by the owner of FESD and by the authorised personnel of the tax authority.</p> <p>Benefits: The validity and integrity of those files are checked using an algorithm. It takes approximately two minutes to check 150 000 invoices stored on a CD, running an application on a typical laptop.</p>

	<p>Italy first introduced an obligation from early 2014 for electronic invoicing for the supplies to the public sector. Electronic invoices are the only type of invoice that will be accepted by the public sector bodies procuring supplies.</p>
 <p>Italy</p>	<p>Technical features: The supplier must use the transmission channel identified by the tax authority (the Exchange System) for transmitting the invoices to the tax authority. The electronic invoicing has the following characteristics:</p> <ul style="list-style-type: none"> • The content is structured in an XML (eXtensible Markup Language) file. This format is the only one accepted by the Exchange System. • The authenticity of origin and the integrity of the content are guaranteed by the person who issues the invoice by affixing a certified electronic signature or a digital signature. • The transmission is conditional on the presence of the unique identification code of the office to which the invoice is addressed, and which can be found in the Index of Public Administrations. <p>Expanded implementation: Electronic invoicing is now being expanded for use in transactions between private businesses. Legislative Decree no. 127 of 5 August 2015 introduced measures for the electronic transmission of data on VAT transactions to the Revenue Agency. For transactions carried out as from 1 January 2017, taxpayers that supply goods and retail services (pursuant to Article 22 of Presidential Decree no. 633 dated 26.10.1972) may choose between:</p> <ul style="list-style-type: none"> • Supplying information to the Revenue Agency in a more manual fashion, including customers and suppliers lists, black list transactions, summary statements for intra-EU acquisitions of goods and services; or • Transmitting electronically to the Revenue Agency all the invoices issued and received without any other communication obligations. <p>The tax authority is making software available to businesses for free from July 2016 to conduct electronic invoicing in business to business transactions enable the operators (especially the micro-small enterprises) to issue, transmit and store the electronic invoices.</p> <p>Results: In the first implementation period of June 2014 – February 2015, 2 672 780 invoices were received. The tax authority is enhancing the processes to cross-check data, such as domestic supplier and customer listings which allow crosschecking of data submitted by domestic suppliers and customers so that potential tax gaps and losses can be intercepted. The electronic storage and linked transmission of the payment data will replace the obligation of fiscal certifications of the payments through the issuance of fiscal or cash register receipts.</p> <p>The widespread adoption of the electronic invoicing and data transmission tools, besides resulting in substantial reductions of the compliance procedures for taxpayers, will greatly enhance the detection and prevention of tax evasion, since the information available to the tax authority will allow it to carry out more precise risk analyses, through the execution of verifications and data cross-checks in an automatic and timely manner.</p>
	<p>Kenya is using Accounting Command Language to manipulate data and to check repeated invoices and skipped invoices. The focus is on all taxpayers, but medium – large taxpayers in particular. Although there have been some initial challenges in using the tool, the results have shown that where it is used regularly, the result has been very positive.</p>
 <p>Mexico</p>	<p>Mexico introduced electronic invoicing in several stages.</p> <p>Prior to its introduction, taxpayers used only printed invoices, which were freely prepared and printed without tax administration controls. The disadvantages were that there was a high volume of false transactions using fake invoices to claim tax deductions and reduce tax; a high volume of hidden income in cases where no invoice was issued; and compliance action by the tax authority required manual checking.</p>

**Mexico
(continued)*****The first stage: Establishing controls***

A requirement was introduced such that only authorised printers could produce invoices. All invoices were required to have a unique number which was controlled by the tax authorities and the authorised invoice number had to be linked to an updated taxpayer register. The printer produced reports of the invoice numbers that were issued.

The results of this stage indicated that the authorised printers increased taxpayers' perceptions of risk. However, a black market of "cloned" invoices emerged which were produced by the authorised printers. A cloned invoice had a real folio number, but contained false amounts and false clients. Because of this, the tax authority could not check the operations of all authorised printers.

The second stage: from 1990s

The tax authority focussed on making intensive use of new technologies. This included the use of digital advanced signatures; internet services; standardised electronic documents; and enhanced data analysis.

The result: this led to the creation of the first electronic invoice (e-invoice), referred to as "CFD".

Third stage: from 2005

The standardised e-invoice contained the folio number which was controlled by the tax authority as well as the taxpayer's digital seal. The tax authority received monthly folio reports. The e-invoices used XML (eXtensible Markup Language) tags, as it ensured easier electronic data exchange and thus allowed compliance with the technological standard to be an automated process.

At first, the use of e-invoices was optional for taxpayers. The use of e-invoices was then made mandatory for larger corporations. The taxpayer either devised their own systems to create the e-invoice or used the services of a provider.

The result: the number of false invoices was reduced. Larger taxpayers took advantage of the standardised electronic XML documents in their broader record keeping and administrative process and pushed their providers to use e-invoices. Technology companies started developing software to use and manage data from e-invoices.

Some problems remained. Some issuers did not comply with the obligation to submit monthly folio reports to the tax authority. The implementation cost was an obstacle for adopting the e-invoice for some taxpayers and some taxpayers preferred to continue using printer invoices.

Fourth stage: enhancing the e-invoices from 2011

Enhancements were made in order to ensure the best data use of e-invoices and make their issuance by taxpayers easier. E-invoicing would work as follows. This resulted in a 134% increase in the number of e-invoices issued from 2010 to 2011.

Step 1: The customer requests a fiscal receipt from the vendor, who generates the e-invoice and digitally stamps it according to the standards.

Step 2: The vendor sends the e-invoice to an Authorized Certification Service Provider (PAC). The PAC is a trusted third party authorised by the tax authority.

Step 3: The PAC validates the structure, syntax and tax attributes of the e-invoice. If it is valid, the PAC digitally stamps it with the folio number on behalf of the tax authority. The folio numbers were assigned online by the tax authority to the authorised certification service providers. The PAC also sends a copy of all invoices to the tax authority in real time in XML format.

Step 4: The PAC returns the validated e-invoice to the vendor, who then sends it to its customer by converting it from XML to PDF format.

Step 5: Both the customer and vendor can verify the authenticity of e-invoices.

<p>Mexico (continued)</p>	<p>Results: The only kind of invoice in Mexico is now e-invoice by internet. The use of e-invoicing has been expanded for use in payroll. A similar format and standardisation is also being used to document withholding tax and payments for dividends, trust operations, derivatives, payments abroad and electronic accounting reports.</p> <p>As at September 2014, there were 3 837 876 issuers of electronic invoices, and since introduction almost 13.5 billion e-invoices had been issued. Mandatory electronic invoicing in Mexico brought 4.2 million micro businesses into the formal economy.</p>
 <p>The People's Republic of China</p>	<p>In 2003, the VAT anti-counterfeit tax control system was introduced throughout China, covering all the general taxpayers. In 2014, the VAT invoice processing system was upgraded, and was rolled out step by step by the State Administration of Taxation of China (SAT) from 1 Jan 2015, applicable to both general taxpayers and small scaled taxpayers above a de minimus threshold.</p> <p>Technical features: The new VAT invoice processing system boasts of collecting comprehensive VAT invoice data, including name of taxpayers, name and code of goods (services), price, quantity, tax base, tax rate and amount of tax payable, etc. Taxpayers upload the encrypted VAT invoice data into the database of tax administrations via internet, each invoice with a digitally signed certificate. The invoice data is transmitted in a real-time fashion fully monitored by tax administrations, and then classified and sent to receiver taxpayers as the basis of tax filing, verification of the invoice authenticity, revenue source management as well as data analysis and utilisation.</p> <p>Benefits: When a taxpayer files a tax return, the new VAT invoice processing system will automatically cross-check the data of both input tax and output tax against those in the invoice database of tax administrations to prevent against under-reporting of the tax payable or over claim of the input tax. Moreover, combining the VAT invoice data with the tax return information, tax administrations across the country can also conduct tax risk analysis and economy-taxation correlation analysis, with a view to detecting potential tax risks and providing inputs for economic decision-making.</p> <p>To sum up, with a broad prospect of application, the electronic data of VAT invoices will play a positive role in standardising tax administration, preventing and controlling tax risks, and conducting economic performance analysis.</p>
 <p>Singapore</p>	<p>Singapore has implemented a cross referencing system to detect incorrect Goods and Services Tax (GST) information.</p> <p>Technical features: This system captures sales and purchase transaction listings which are requested from GST taxpayers through routine audits. The listing of information provided is determined by the scope of the audit and would be complete in relation to the scope of the audit. A standard data format is prescribed by the tax authority for taxpayers under audit to submit sales and purchase listings. The standard format is in Microsoft Excel.</p> <p>Benefits: These transactions are then cross referenced with transactions submitted in the past to uncover discrepancies. There are three main purposes for the cross-referencing system:</p> <ul style="list-style-type: none"> • For the tax authority to match transactions in the sales / purchase listings obtained from the audited taxpayer against any existing transactions listings in the database (using the same supplier/customer ID and invoice number); • For the tax authority to carry out third party confirmation for selected transactions that are “unmatched” in the database to verify if the claims are in order; • For the tax authority to identify the network of entities that have substantial transactions with each other and the flow of such transactions - particularly in suspected fraud cases - to all GST taxpayers across all industries.

<p>Singapore (continued)</p>	<p>The data is uploaded into a database system. The system will then enable auditors to cross reference transactions which have been submitted previously to uncover discrepancies. Periodically, certain transactions will also be selected to be sent to the businesses' suppliers and customers for third party confirmation.</p> <p>Results: The main strength is to maximise the benefits of existing audit processes by making available collected data for use in future audit cases. In addition, the tax authority's compliance strategy subjects high risk industries and taxpayers to more frequent audits – hence, the system will have more transaction data for high risks taxpayers.</p> <p>Challenges: The main weakness of the system is that it does not have full coverage of transactions, as data submission is triggered only when an audit is carried out. The tax authority may, in the future, consider exploring e invoicing with 100% coverage of GST taxpayers.</p>
<div data-bbox="229 734 416 831" data-label="Image"> </div> <p>Slovak Republic</p>	<p>In the Slovak Republic, the VAT control statement (domestic recapitulative statement) came into effect on 1 January 2014. It was implemented by Amendment § 78a Act No. 222/2004 Coll. on value added tax.</p> <p>Technical features: The VAT control statement is provided by both the supplier and the purchaser, and is provided to the Financial Administration electronically in XML format. Data is provided monthly or quarterly (according to the taxable period, with the latest due date being the same date as submission of the VAT return. The VAT control statement contains all types of transactions (input supplies, output supplies, and electronic cash register receipts). Each transaction in the VAT control statement is identified by VAT number of the supplier and the VAT number of purchaser, with the number of the invoice, date and value.</p> <p>Benefits: Automatic cross-checking of data provided by the supplier and the purchaser in the VAT control statements (and combined with information from other sources on risk factors) allows us to detect:</p> <ul style="list-style-type: none"> • carousel fraud and chain fraud; • issued invoices that later on are not recorded in the accounting; • varying of accounting; • replacement of invoices in the accounting; • not-issued invoices; • not using electronic cash registers; • non-taxable persons issuing the invoice with tax included; • taxable persons that applied twice for tax deduction from the same invoice in two different taxable periods. <p>Results: During the years 2014 and 2015, amount of risky VAT detected in domestic chain frauds was more than EUR 500 million.</p> <ul style="list-style-type: none"> • Effective planning of tax audit and performance – elimination of a human factor failure in auditing taxpayers, exactly specified set of questions derived from the retrieved data and its evaluation, when dealing with tax audit. • Encouragement of voluntary compliance. • Early awareness on tax fraud, its new trends and the territorial determination.

Bibliography

OECD (2013), *Electronic Sales Suppression: A threat to tax revenues*, OECD Publishing, Paris, www.oecd.org/ctp/crime/electronicssalessuppressionathreattotaxrevenues.htm

PriceWaterhouseCoopers (2015), *The Sharing Economy*, www.pwc.com/us/en/technology/publications/assets/pwc-consumer-intelligence-series-the-sharing-economy.pdf (accessed on 1 March 2017)

European Commission (2012), *Study to quantify and analyse the VAT Gap in the EU 27 Member States, Final Report*, TAXUD/2012/DE/316

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

For more information:

ctp.contact@oecd.org

www.oecd.org/tax/crime
[@OECDtax](https://twitter.com/OECDtax)

