ELECTRONIC SALES SUPPRESSION: A THREAT TO TAX REVENUES

OECD

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.

Photo credits: cover photo © Patryk Kosmider - Fotolia.com

Table of contents

Executive Summary

"Electronic sales suppression" techniques facilitate tax evasion and result in massive tax loss globally. Point of sales systems (POS) in the retail sector are a key component in comprehensive sales and accounting systems and are relied on as effective business accounting tools for managing the enterprise. Consequently, they are expected to contain the original data which tax auditors can inspect. In reality such systems not only permit "skimming" of cash receipts just as much as manual systems like a cash box, but once equipped with electronic sales suppression software, they facilitate far more elaborate frauds because of their ability to reconstitute records to match the skimming activity.

Tax administrations are losing billions of dollars/ euros through unreported sales and income hidden by the use of these techniques. Since the OECD's Task Force on Tax Crimes and Other Crimes (TFTC) began to work on and to spread awareness of this phenomenon a number of countries (including France, Ireland, Norway and the United Kingdom) have tested their retail sector and found significant problems. Among these countries, Ireland has moved quickly to put in place legislation to help tackle such abuse. Tackling this issue aggressively is seen by a number of countries as an important ingredient of a strategy to reduce their overall tax gap.

This report describes the functions of POS systems and the specific risk areas. It sets out in detail the electronic sales suppression techniques that have been uncovered by experts, in particular "Phantomware" and "Zappers", and shows how such methods can be detected by tax auditors and investigators. It notes the constant development of electronic suppression techniques and the need to be alert to changes.

The report compiles and analyses the range of government responses that are being used to tackle the abuse created by electronic sales suppression and identifies some best practices. These include strengthening compliance with a focus on voluntary compliance through industry bodies, raising awareness with all stakeholders including the public, improving audit and investigation skills, developing and sharing intelligence and the use of technical solutions such as certified POS systems.

The report makes the following recommendations.

- Tax administrations should develop a strategy for tackling electronic sales suppression within their overall approach to tax compliance to ensure that it deals with the risks posed by electronic sales suppression systems and promotes voluntary compliance as well as improving detection and counter measures.
- A communications programme should be developed aimed at raising awareness among all the stakeholders of the criminal nature of the use of such techniques and the serious consequences of investigation and prosecution.

- Tax administrations should review whether their legal powers are adequate for the audit and forensic examination of POS systems.
- Tax administrations should invest in acquiring the skills and tools to audit and investigate POS systems including developing the role of specialist e-auditors and recruiting digital forensic specialists where appropriate.
- Tax administrations should consider recommending legislation criminalising the supply, possession and use of electronic sales suppression software.

Introduction

Background

The use of electronic sales suppression techniques in point of sales systems is a disquieting development in tax evasion. It has been growing for more than a decade. During that time, attempts to confront it have been localised most notably in Canada, Germany, the Netherlands and Sweden. Since the OECD's Task Force on Tax Crimes and Other Crimes (TFTC) began to work on the topic and to spread awareness of the phenomenon, a number of other countries (including France, Ireland, Norway and the United Kingdom) have taken determined counter action. This report aims to bring the issues to a wider audience, to show that tackling the issue requires a variety of solutions, technical and operational, policy as well as strategic ones, and to make recommendations for action by tax administrations and governments.

Modern cash registers in the retail sector operate as comprehensive sales and accounting systems, often using standard business software, and are relied on as effective business accounting tools for managing the enterprise. Consequently, they are expected to contain the original data which tax auditors need to inspect, including those auditing Value Added Tax (VAT) or sales tax compliance. It is now apparent that such systems can be manipulated to permit "skimming" of cash receipts just as much as manual systems (like a cash box or having two tills), but once equipped with sales suppression software they facilitate far more elaborate frauds through the ability to reconstitute records matching the skimming activity.

The terms electronic cash registers (ECR) or electronic point of sales systems (EPoS) are often used to describe modern cash registers, but when both types and hybrids of either are intended they are referred to in this report using the generic name "POS systems".

Forensic experts, e-auditors and criminal tax investigators as well as policy makers have been brought together to gather the information to produce this report.[1] They have also worked on developing a set of tools (including training packages, guidance and a library of technical information) for tax auditors and investigators. They have used the experience to make advances in their own work and the tools they have produced will be of great help to other tax administrations.

The report looks at the functions of modern cash registers and considers the roles of the manufacturers, suppliers, and other parties involved in their use. It looks at the varieties of sales suppression tools and techniques that have been found and at the forensic traces that can lead to their discovery. The report also examines the available estimates of the extent of use and the consequent tax losses. It describes the range of compliance and investigative strategies that countries can adopt and it makes recommendations on actions to take.

Other related work

This report has a focus on the criminal behaviour involved in the use of electronic sales suppression, as well as the work of criminal investigators to detect, disrupt and prosecute such behaviours. Other work focusing more on compliance and the issues faced by auditors has been carried out by the OECD Forum on Tax Administration and the EU Fiscalis Project.

A **European Union "Project Group on Cash Registers"**[2] within the Fiscalis programme delivered a "Cash Register Good Practice Guide",[3] in 2006 which includes a comprehensive overview of the legislation in all EU Member States, the available hardware and software systems for cash registers, a specific risk catalogue, and recommendations on good practices for the audit of cash registers and POS systems.

The **Forum on Tax Administration** produced a guidance note in April 2010, which includes recommendations on procedures to ensure the reliability of electronic records.[4]

In the second half of 2010, an Activity Team on Zappers and Phantomware (ZAPAT) was set up under the existing **EU Project Group on E-Audit**. Based on new audit solutions and developments adopted by the tax administrations of the EU Member States, ZAPAT will pool best practices and thereby further help to improve the e-audit of POS systems. Based on its findings, the Activity Team will produce a guidance note on the e-audit of POS systems, which will be available to auditors in EU member countries and complement the work included in this report.

Estimates of tax loss and other fraud

Quebec tax losses estimated at **CAD 417 million** for 2007-2008

Sweden recovered **EUR 150 million** in 2,000 audits over 4 years

In South Africa **EUR 22 million** was expatriated in a single case

In Norway, a single case involved **EUR 7 million** under-reported

Estimates of losses due to the use of electronic sales suppression have been made in respect of certain sectors and in specific geographical regions. These can be indicative of possible losses in other regions. There are valuable statistics from Canada which are based on strong evidence of found cases. Revenu Québec, the agency responsible for the administration and collection of income taxes and consumption taxes within the Canadian Province of Québec has estimated their tax losses from such techniques to be CAD 417 million for 2007-2008.

In 2008, the Canada Revenue Agency charged the owners of just 4 restaurants with evasion involving the "zapping" of nearly 200,000 cash transactions totalling CAD 4.6 million.

The German Bundesrechnungshof (the federal audit office) raised concerns in its "Annual Report 2003 on Federal Financial Management" about losses from the use of electronic sales suppression and concluded that "with cash transactions running into tens of billions of Euros, the risk of tax evasion should not to be underestimated."[5]

Other indicators include the following.

- In one case investigated in Norway there was a sum equivalent to EUR 7 million under-reported.
- In a South African case the wholesalers had expatriated a sum equivalent to EUR 22 million out of South Africa.
- In an investigation by Slovenia inspections carried out in retail stores at the end of the trading day had found that sales in the systems at that time were three times the volume on other days.

The Swedish Tax Agency has addressed the issue in the context of the national tax gap. Their estimate of the total turnover in all cash businesses in Sweden is EUR 100 billion. The estimated annual tax gap in the cash business is EUR 2 billion, which is about one sixth of the entire tax gap in Sweden.

From 2006 to 2010 Sweden has carried out about 2,000 audits including restaurants, hairdressers, clothing stores, food stores etc. The underpayment of taxes in the companies audited was about EUR 150 million including income taxes, VAT and employment taxes. The audits showed that between 20-40% of the turnover was under-reported. The under-reported turnover is feeding the grey or underground economy and in some cases supporting organized crime.

There is evidence that the use of Zappers and Phantomware has been spreading around the globe – and so there is continued growth in the size of the threat to tax revenues. Some of the suppliers of, for example, restaurant POS software market their systems with electronic sales suppression features internationally. As for the prognosis for the future, auditors and investigators working in the area report continued development and increasing sophistication of the techniques in order to avoid detection.

No evidence has been found of businesses using similar techniques to inflate sales figures, for example to launder the proceeds of crime. However, this is something that may be possible and tax administrations should be aware of this risk.

Notes

1. The expert group was co-ordinated by Norway with participants from Belgium, Canada, France, Germany, Greece, Ireland, the Netherlands, Norway, Portugal, Sweden, Turkey, the United Kingdom and the United States.

2. The Project Group's objective was to identify risks in cash registers and POS systems and to develop ideas on how to counter such risks. The detailed objectives of this project group were:
   - to collect the different rules and demands given by tax authorities of the EU Member States on cash registers and POS systems as well as the way they are used in practice, including an inventory of the rules and conditions for the hardware and software industry;
   - to collect, share and improve knowledge and experience of the technical features of cash registers and POS systems;
   - to identify different concepts and exchange experiences to improve the use of data on business transactions in a fiscal audit; and
   - to collect information on how the different systems are subject to possible abuse.

3. *Cash Register Good Practice Guide*, EU Fiscalis Project Group 12, 2006. (Not publically available).

4. *Guidance and Specifications for Tax Compliance of Business and Accounting Software*, Forum on Tax Administration, OECD, April 2010.

5. Federal Parliament circular 15/2020 at 197-198 (Nov. 24, 2003).

Point of Sales Systems

POS systems

When James Ritty invented the first cash register in 1879, his aim was to create a system for recording cash transactions to prevent employees in his saloon from pilfering profits. An early model was advertised as the "Incorruptible Cashier". It soon became a key tool in managing the finances of a business. The accurate recording of sales transactions and the preservation of the transaction records remains a key business requirement of cash registers. Cash registers issue receipts which function as sales documents between the business and its customers. The cash register receipt is the first document or statement that shows the content of the transaction. The function of a cash register evolved over time covering not only the documentation of the sales transaction but also bookkeeping and audit requirements.

This evolution has continued and businesses now use modern POS systems for a variety of reasons. They provide security and control of cash, are speedy in use, reduce transaction errors, provide ease of record keeping and reporting, provide stock control, monitor the work of staff, issue receipts and generally provide a professional image for a business.

In the retail sales and hospitality sectors, cash registers play an important role in the business management process. Inputting the customer's order or transaction is the trigger for subsequent actions e.g. the food order in a restaurant can be communicated automatically to the kitchen while responsibility for the customer service is allocated to a specific waiter. In fully integrated business systems the POS system is one of many sub-systems, but it is the system that initiates the business transaction and passes information to other processes and there will be interfaces between cash registers, logistic systems, accounting systems and other business systems.

The functionality of POS systems varies in sophistication from the fairly simple to the extremely comprehensive. It is possible that not all of the functions that are available from the supplier will be activated in the system that is delivered and installed for the particular business user. Mid-range to high range systems often include either touch pads or touch screens and can be optionally networked to computers and linked to scanning systems. The sophistication and variety in such systems can present a challenge to the tax auditor who needs to understand how to effectively audit them.

Auditing POS systems – the legal framework

It is essential that the legal framework for audit takes into account the audit needs of digital business systems including POS. Most countries have legislation requiring businesses to establish adequate business information and accounting systems. Entrepreneurs are free to independently establish the systems that conform to these principles. The following are some common features of such legislation or regulations.

- The data generated by business information and accounting systems that affect fiscal obligations is required to be preserved for a certain period.
- The business owner has the responsibility to ensure that the accounting records are in such form that they can be audited within a reasonable time.
- The conversion of data that has been processed electronically to paper is permissible if the conversion does not hinder the ability to perform an audit.

In a number of countries there are specific regulations applying to the accounting requirements for cash businesses and these take into account the use of POS systems. These regulations may specify the reports that should be made, the format, language and the length of time they should be retained. This is the approach taken in Norway.

There is a further set of countries where the use of specific certified POS systems is mandated either generally or for certain retail or service sectors. These are known as "fiscal tills" and are described further under the 'Government Responses' section.

Tax audit requirements

Requirements from a tax audit point of view fully align with the normal needs of an enterprise in terms of business information management. In addition to the features above, the specific requirements for tax audit include:

- electronic preservation of the detailed data of transactions;
- detailed records that are available for the tax auditor if and when required;
- preservation of a complete audit trail; and
- taking adequate measures to guard against subsequent alterations in a manner that will ensure that data integrity is maintained.

Detailed business process information is needed in order to carry out an audit on the completeness of reported sales. From a tax audit point of view, the demands on business information are relatively simple - the sales record must give a complete and correct presentation of the sales. These records must allow tax officers to verify within a reasonable period of time that the figures presented are a complete and accurate representation of the sales. The data must present a provable, complete, and correct picture of the sales.

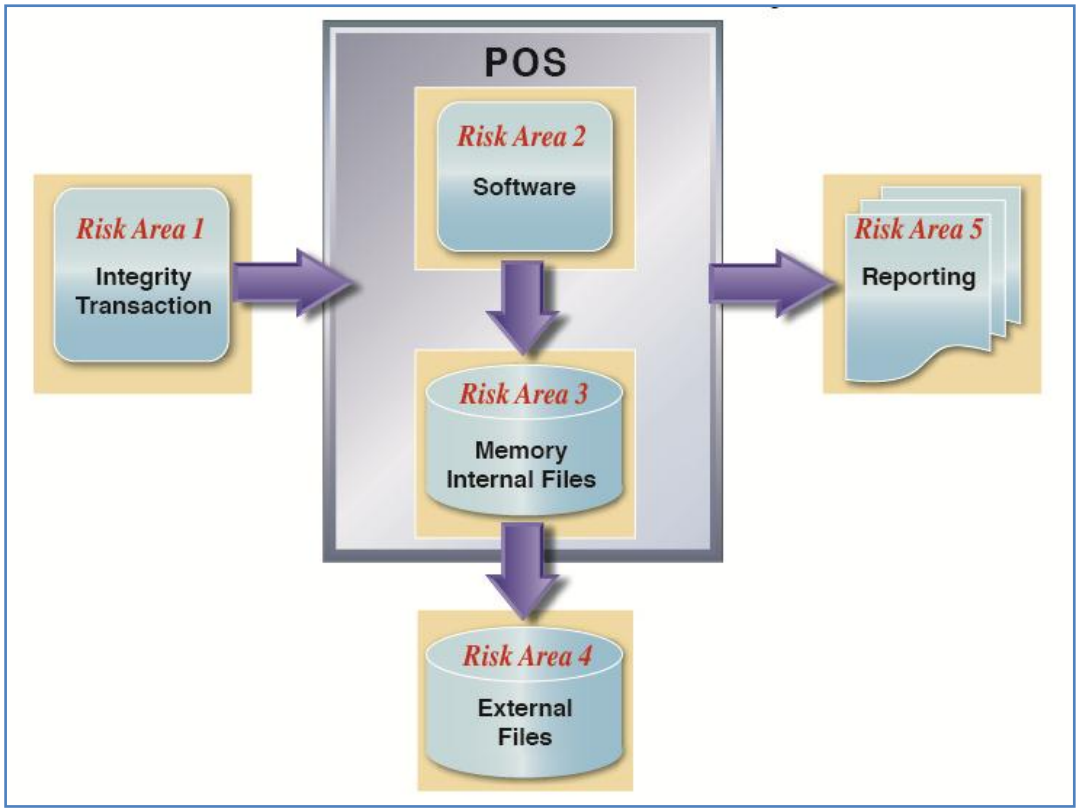
These demands correspond to the general requirements of any business in relation to the technology used to support its business systems: from the moment a transaction is recorded, a business expects that the transaction information is stored accurately. Furthermore, it is expected that these transactions are completely and accurately represented in reports made at any moment and at least until the moment of reconciliation.

Larger companies take adequate measures to securely store data that are vital for business processes. The responsible managers of larger firms need to have a firm grip on the business. They need this data to get business information that supports long-term profitability decisions, and it is also needed to provide proper financial statements and accounting reports for shareholders and regulatory authorities.

POS system risks

The vulnerabilities in terms of electronic sales suppression can be considered as present in specific risk areas of the POS system configuration. Each of these risk areas presents opportunities for sales data to be deleted, changed – or, in the case of the actual transaction, not being recorded at all. The following diagram[1] illustrates the five risk areas.

Figure 1. Risk Model for Point of Sale System



Source: Information provided by The Netherlands

Integrity of the transaction. To safeguard the integrity of the transactions the cash register must contain measures to ensure that input of the transaction is complete, correct and on time. If input of the transaction is not complete, correct and on time, the system produces unreliable business information with risks in terms of the ability to make the right management decisions and to file accurate tax returns.

Software. The software needs to be designed to ensure integrity, confidentiality and availability of the process performed by the cash register system. If the system cannot ensure integrity, confidentiality and availability, the system would again produce unreliable information with the risks to management decisions and accounting for tax. It is important to ensure that the software operates so as to store all information of all actions carried out on the cash register system and creates a clear audit trail. This is necessary for effective management and control of the complete business process.

Internal memory. The transaction data, stored in memory and internal files, is the basis for all reporting and is also within the scope of data to be examined for audits and investigations. It is in this area that the greatest risks arise of electronic sales suppression software (or other file tampering methods) being used to manipulate this information contained in transaction data.

External files. The risk is in the transfer to and storage of transaction data in offline files needed for example, when the electronic journal in an ECR is full. Generally, countries have laws that require businesses to keep for a certain period appropriate books and accounts and this includes the data carriers on which these books and accounts are recorded. In some laws, the books and accounts should be organized in such a manner that it allows the tax auditor to audit them within a reasonable period of time. The external files could also be the files that are transferred on a daily basis from the POS system to the back office system on a separate computer. The external files could also include the backup files for the POS system. The backup files may be stored either on an external media or on the hard drive within the system itself but in a different folder. The backup files may contain vital information for revealing the use of electronic sales suppression in a cash register system.

Reporting. This risk area is strongly connected to the second risk area, the software, which controls the reporting and therefore opens possibilities for manipulation in the design and creation of reports. The reports are important for the management of the business and are used to transfer information into the accounting system, to create tax returns etc. In case of loss of the transaction data, it is very important that the business owner can rely on hard copies of reports that will show all the transaction input and stored in the cash register.

Notes

1. The POS system suppliers in the Netherlands in conjunction with the tax authorities have developed a model of risks for POS systems in order to stimulate compliance with tax obligations. This is part of the Dutch project "Quality Mark for Reliable POS systems" which is described in the Chapter on Government Responses. The OECD's electronic sales suppression expert group has adapted the Dutch model to provide a general model for considering risks within POS systems.

Electronic Sales Suppression Techniques

The problem posed by the use of electronic sales suppression techniques is the scale of tax evasion it enables by under-reporting of sales and profits. This Chapter describes how simple techniques of skimming, which are still in use, have been automated and integrated into the POS system.

Sales suppression, also known as "skimming", has always existed in one form or another in order to *inter alia* evade taxes. Skimming could be achieved through various simple acts, such as:

- failing to ring cash sales into the cash register with the cash being kept by the owner of the business; or
- diverting sales to a second cash register which was kept "off the books".

This is most common in small and medium sized businesses since they usually have fewer internal controls and are often closely held businesses. In some cases, the business involved in "skimming" will keep two sets of books and records, one for the tax authorities and the other for the owner of the business since they may want to show the real sales to a potential buyer when the business is being sold. Skimming by closing the cash registers at a certain point in the evening resulted in a large scale fraud in an Australian restaurant where the amended assessments issued on the business owners amounted to AUD 8.4 million in tax and penalties.

Modern business technology has automated these frauds with the use of electronic sales suppression software known as Phantomware (where the software is installed in the POS system) and Zappers (which are external programs often carried on USB keys). This software now provides the opportunity to perform the skimming in a fully computerised environment which allows the business owner to operate in what appears to be a perfectly normal manner (all sales are rung into a cash register by staff where they are recorded as sales transactions). The new technology allows the business owner to perform the electronic sales suppression at a convenient time, usually at the end of the business day. The suppression can be in the form of a pre-set monetary value each day or simply a percentage of the cash sales. There is no longer any need to keep the "second till"; everything is fully computerised and available to the business owner using relatively simple methods to access the suppression software, for example with a swipe-card or a hidden button on the screen to activate a special menu. Investigators have also seen instances where pressing a combination of keys is used to activate the special menu.

In the past, a critical feature for any type of "skimming" was the existence of a substantial amount of cash sales. Credit and debit sales were rarely the target of "skimming" because of the audit trail left by these types of transactions. However, recently evidence of the suppression of credit and debit sales has also been found. This is currently being investigated by a number of countries to see whether it may indicate a new trend and how it can be countered. This work is not yet advanced enough to be reported here.

In terms of the cost for Phantomware or Zappers, evidence in Canada and the United States has shown that it can range from being included in the cost of the POS system, particularly with Phantomware, to around CAD 1,500 for a Zapper in addition to the cost of the POS system.

Misuse of functions within the ECR/POS software

A modern POS has numerous programming options and some of these can be used to carry out sales suppression. For example, a POS terminal can be set to:

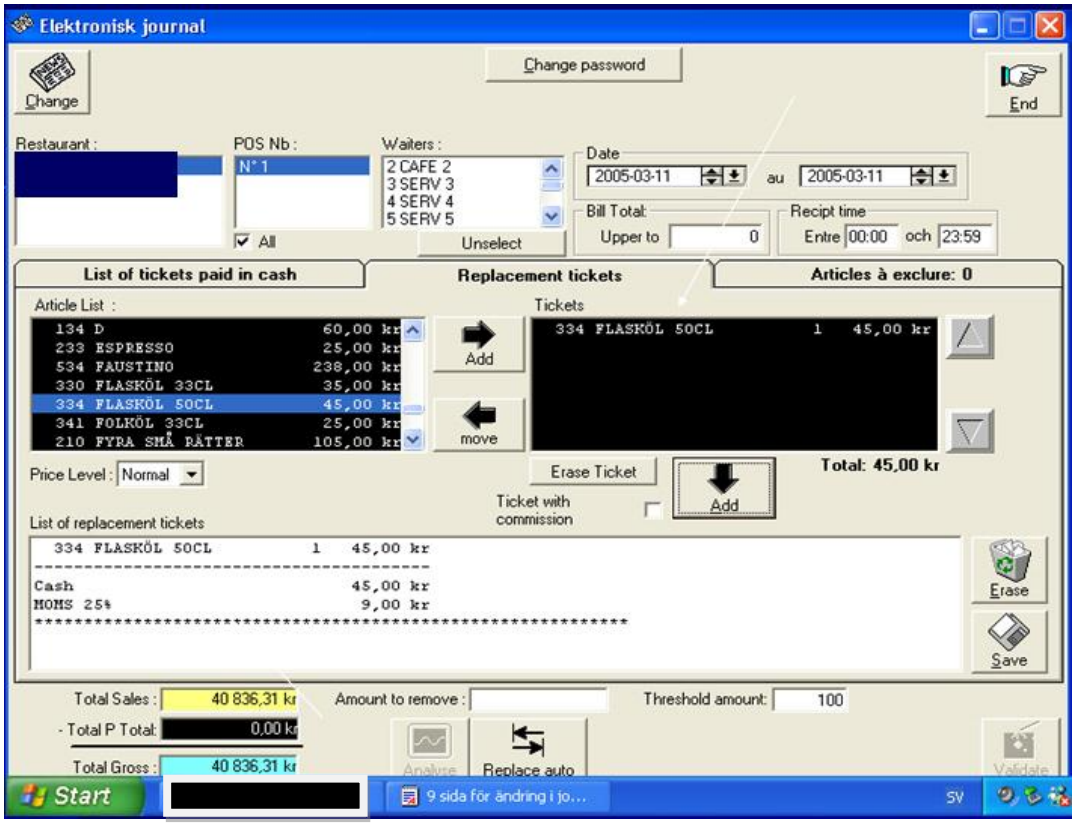
- stop certain items, such as refunds, voids and other negative transactions, from appearing on the report or journal;
- stop certain items, such as refunds, voids and other negative transactions, from being added to the grand totals;
- use the training mode, for either the entire till, or an individual clerk, meaning that the items are not recorded in the normal reports;
- reset grand totals and other counters to zero, or in some cases any specified number; and
- specify that certain line items are programmed so that they do not appear in the report or journal.

The program choices to select these items are not hidden within the programming menu (unlike Phantomware) and are documented in the programming or suppliers' manual; however, this manual is not usually supplied to the end customer and is generally only made available to official dealers. In the majority of cash registers, the programming is done by entering codes, necessitating some technical knowledge by the programmer. Most computer-based POS systems also contain similar options, but there is less of a need for the business owner to have any technical knowledge to use them.

Phantomware

Phantomware is a software program already installed or embedded in the accounting application software of the ECR or computerised POS system. It is concealed from the unsuspecting user and may be accessed by clicking on an invisible button on the screen or a specific command sequence or key combination. This brings up a menu of options for selectively deleting sales transactions and/or for printing sales reports with missing lines. When sales are deleted, the tool can automatically adjust inventory details to avoid an apparent mismatch; in the option for omitting lines the sales report alone may be affected. Where accounting changes have been made it may also print out a log of the transactions deleted so the business owner can manage (and track) what has changed. A clear example of this comes from the experience of Sweden and a program used in the restaurant sector, which collects the data from the computerized POS system and saves it to an electronic journal. The following screen from the system highlights its ability to easily switch items, namely the "List of tickets paid in cash" and "Replacement tickets".

Figure 2. Phantomware Example



Source: Information provided by Sweden

In this Phantomware example, the sales are not actually deleted, but are adjusted by the substitution of higher priced menu items for lower priced items. This type of electronic sales suppression is more sophisticated than just deleting sales because it avoids gaps in the sequential sales transaction numbers which deletions cause. The auditor needs to be aware that other versions of Phantomware are in use, which delete sales and renumber the remaining transactions to provide sequential transaction numbers. So the presence of sequential transaction numbering does not rule out the use of suppression techniques.

Zappers

Zappers are external software programs for carrying out sales suppression. They are carried on some form of electronic media such as USB keys, removable CDs, or they can be accessed on line through an internet link. Zappers are designed, sold, and maintained by the same people who develop industry-specific POS systems, but some independent contractors have also developed these techniques. Their operation is similar to the Phantomware products but they are more difficult to detect because of their sophisticated design and because the offending software is not present on the machine during normal use. Examples of Zappers have been revealed in the Canadian experience where Zappers have been found in many restaurants. In each case, a USB device is utilised to activate the Zapper. This brings up a special screen on the POS system which allows the business owner to commence deleting and/or modifying sales.

Summary of techniques

Regardless of the type of program that is used, evidence suggests that in most cases the retailer supplying the POS system has programmed it to allow fraudulent use. They may also arrange for training or provide written instructions in its use. This is sometimes done at no additional expense to the customer.

In the case of Phantomware and Zappers, the user interface is generally professional and easy to use. It is usually developed by someone involved in the creation of the POS operating software and the format is often similar, so the look and feel of the suppression software is the same as that of the professional legitimate business software. Selecting items to change is usually simple, often by merely clicking on the items you want to delete or replace with an item of a lower value, or by entering a monetary amount or percentage of sales to be zapped (deleted). Filters may also be available, allowing the user to zap certain categories of sales, for example if the business owner is employing someone illegally, the owner can delete all of the sales by that clerk, or if the owner is selling contraband goods (e.g. illegal tobacco) the owner can zap all of these sales in order to remove evidence of involvement in smuggling.

The functions of electronic sales suppression systems can be summarised as:

- access the hidden software;
- present details of cash transactions (though there is also now evidence of suppression of credit and debit transactions);
- delete selected sale items and delete the corresponding stock records;
- substitute selected items with lower cost items;
- automatically select items to delete to a specified value (e.g. where the business owner wants to cover unreported withdrawals from the business of say EUR 1,000 per day and is content for the software to decide which items to zap);
- remove log and other traces of transactions; and
- store original data in another location.

No evidence has been found of businesses using similar techniques to inflate sales figures, for example to launder the proceeds of crime. However, this is something that may be possible and tax administrations should be aware of this risk.

Detection Strategies

Financial audit

General best practices in auditing will provide useful methods to determine whether there are reasons to believe that a business is engaged in electronic sales suppression.

Box 1. Audit Methods

- **Private consumption** calculation establishes how much money the taxpayer has available for private use based on income, cash expenditures and changes in assets. If the private consumption is found to be extremely low or negative, it means that the suspect has used more money than he or she had reported for disposal. This means that there may be undeclared income that may have originated from withheld revenues. Other relevant methods are the Net Worth method and the Cash Deposit method.
- **Negative cash holdings** mean that the suspected taxpayer has used more cash from the cash register than it is actually reported to contain. This is not possible and means that there is a cash in-flow that is unexplained or hidden.
- **Gross profits** analysis is used to analyse the sales. The sales are first analysed by calculating the theoretical gross profit based on the official stated sales prices and purchases by the taxpayer. The gross profit is then calculated on the recorded figures (purchases and sales) in the bookkeeping records. A recorded gross profit lower than theoretical GP indicates that not all sales have been recorded.
- **Volume control** is used to analyse the flow of goods. This may indicate whether the business is selling more goods than it has purchased and has in stock and thus there are unrecorded sales. It is usually used along with gross profits analysis.
- **Operating Cash Flow / Net Sales**; this ratio is expressed as a percentage of a company's net operating cash flow to its net sales, or revenue (from the income statement). The higher the percentage the better for the cash intensive business and a ratio lower than that expected for a particular business sector might indicate under-recording. It should also be noted that industry and company ratios can vary widely. In one particular case in the restaurant sector, the cash ratio reported was a figure that did not deviate from national statistical norms, but in reality, when the suppressed cash flow has been found, the real ratio was calculated to a much higher figure even above the upper median in the public statistics.
- **Covert operations** may be used by tax administrations to observe a business in operation. This may give auditors important information on how a POS system is being used in practice. The tax administration may also pose as a potential user and acquire copies of the relevant software for analysis.
- **Other finance and management systems operated by a business**, such as stock control and billing, are often closely linked to its cash register system. In an audit, information obtained from these systems can be important in testing the reliability of that contained in the cash register.

An auditor can be taught how to obtain useful information from a POS system. An auditor can learn to reprogramme an ECR in order to reveal suppressed sales and transactions and print reports detailing these. This approach has been adopted in the UK where auditors attend a three day course. In a local project this resulted in assessments in 68% of cases audited.

E-Audit

Electronic commerce auditors or e-auditors are also known as Electronic Commerce Audit Specialists (ECAS). The POS systems often contain thousands of transactions making it impossible to audit without using Computer Assisted Audit Tools and Techniques (CAATTs) such as IDEA. This type of tool enables the auditor to import data from almost any format or file and carry out a wide range of analyses on it as well as produce reports and charts (some of these are shown later). It can support normal internal audits and financial analysis as well as identifying unusual transactions that might suggest fraud or money laundering. ECAS are auditors that receive specialised training in using CAATTs. Given the emergence of EPOS systems in many cash businesses, the ECAS are relied upon to analyse and understand complex systems and obtain key relevant information to be tested using audit software such as IDEA, ACL or SESAM. The selection of data files is not a straight-forward procedure, particularly where a business uses an ECR or Hybrid system, as opposed to a PC-based POS system. Furthermore, the ECAS has the necessary training to thoroughly analyse the large and complex EPOS datasets for indicators of electronic sales suppression and other non-compliance issues. The ECAS can also share their findings with other members of the audit team and compare them with other information obtained by the tax auditor.

Computer forensic investigation

The computer forensic investigator will use many of the same forensic tools available to e-auditors. It is critical to the validity of the forensic analysis that the actual POS system has been secured for analysis in the forensic laboratory; in other words, as with any other criminal investigation, it is critical to secure the evidence of the crime, including the tools used. Once these systems have been seized, usually pursuant to a search warrant, they can be imaged (this is often described as creating a clone of the original hard drive) and forensic testing can then commence.

Detecting traces

A detailed list of traces that can be identified by the auditor, the e-auditor and the forensic investigator has been compiled and is held by the OECD on a confidential basis.

Criminal investigation techniques

The role of the criminal investigator in terms of electronic sales suppression, as with any other form of tax evasion, is to conduct a criminal investigation of the financial affairs of the corporations and/or individuals who are suspected of tax evasion for purposes of a criminal prosecution.

In the case of electronic sales suppression, the criminal investigator will continue to use traditional investigative techniques to gather evidence through the use of judicially authorised search warrants (to seize POS systems, POS backup data, emails, and other

forms of electronic data), production orders or other forms of administrative warrants to obtain financial information, as well as interviewing potential witnesses from both the place of business under investigation as well as third parties such as POS system manufacturers, etc.

The criminal investigator may also use undercover operations or a joint forces operation with other law enforcement bodies to target POS manufacturers. Undercover operations require the highest degree of skill and planning. They can allow the investigator to obtain direct evidence of the crime and develop reasonable grounds for search warrants. There is also a greater probability of obtaining guilty pleas when undercover evidence has been obtained and presented to the accused. Canada has used an undercover operation targeting a software developer where the officers posed as wealthy restaurant owners from abroad seeking to open restaurants in Vancouver. In the operation the undercover officers negotiated with a software developer for the purchase of a Zapper and the evidence gained provided sufficient grounds for search warrants of the developers' premises.

When sufficient evidence has been obtained to indicate guilt beyond a reasonable doubt, a referral is made to the prosecutor for tax and/or other criminal charges. The goal of any criminal prosecution, in addition to punishing the offender, is to deter others from committing a similar offence and to enhance compliance by communicating the message that tax evasion is a criminal offence, which will be prosecuted and publicised.

Investigating traces

In cases where electronic sales suppression software is used, it can be assumed that the measures that reduce the cash flow will also make it difficult or impossible to uncover the real revenue through a standard audit of books and records. This is clear from recent investigations of Phantomware and the conclusion is that investigators are largely dependent on digital forensics to uncover what has happened. However, even though digital forensic tools will often not be available to auditors, their e-audit skills may still allow the auditor to locate and copy valuable back-up and other files.

Cases, reported from Sweden and Norway, illustrate how changes have been made to the way the electronic sales suppression software works in order to make detection more difficult. In early versions of a Phantomware program in a back office system, a large number of traces were left, related to the changes that were made, and files remained in the system that contained the original sales data. The tax administrations uncovered the use of the electronic sales suppression software and the manufacturer obtained information about their findings. Upon a subsequent investigation it was found that the program had been modified to not leave such traces. Newer versions of the program remove most traces of the original sale and have functionality that appears intended to prevent discovery by digital investigation of the system, such as changing the time stamps for the data files, etc.

The legal powers and technical ability to secure the contents of electronic cash registers and computers are critically important in the detection of Phantomware and the use of electronic sales suppression software. Although the sales suppression software may be able to create credible evidence for a reduced turnover and remove all traces of the actual turnover, one must work on the assumption that electronic evidence will remain in the underlying layers, such as in the operating systems and file systems. These are areas that in many cases can only be investigated through digital forensics.

The use of Zappers can also leave traces in data in operating systems and file systems. Unlike Phantomware, a Zapper is removed from the system after its use and cannot be analyzed on the basis of the material that is normally accessed in digital forensics. If a Zapper is found, it would be analysed; in most cases, this would require the use of legal powers to seize personal belongings.

Digital forensic investigations are carried out by the controlled collection and analysis of data. Collection of data involves seizing verifiable copies of the data sources that may be related to the business. The analysis of data comprises the investigation methods and measures used in order to interpret the seized digital information.

Seizing digital sources

While the prime focus for seizure of data will be on the POS system, there are other sources for digital information in a business that may be relevant to the investigation. In addition to the POS system, there may be computers with back office systems and external storage media that could be related to the use of Zappers and Phantomware. Provided it is legally authorised to seize and review such sources, the challenge is to access the information so that it can be copied. There is a risk of harming or deleting information, which can cause serious consequences for the business being investigated, and reduce the ability to investigate the turnover. This risk can be avoided by caution and the skilled use of tools and techniques, which are described below.

A range of tools, equipment and software, suitable for such data collection is available. In essence these tools ensure that changes are not made on the business's digital information, and that the copy can be verified against the original source.

Where there is a need to secure content in proprietary systems, such as ROM-based[1] cash registers, it can be necessary to carry out preliminary tests on the same type of equipment prior to the actual collection. This demands good intelligence on the business's use of technology prior to the tax investigation.

Tools for securing digital information include the following systems.

- EnCase from Guidance Software, which has the capability to collect data from various storage media and is often used in conjunction with hardware-based write blocking. The purpose of the write blocking is to protect the integrity of the original data.
- Forensic Toolkit Imager from Access Data, which can be used with hardware-based write blocking and the data collection carried out on systems that are running.

These are some of the current examples and while the products may change the principles will remain the same. There may be cases where the tools mentioned above are not sufficient in themselves and the competence to carry out forensic analysis procedures is crucial. This places great demands on the available documentation and procedures should be carried out under the principle that tasks must be verified and able to be reproduced at a later date.

Analysis of digital information

The procedures for analysing the secured information will vary based on the needs of the case, access to resources and expertise, and laws governing such work. It is therefore difficult to give a general representation of the general analysis to be done, but a good starting point would probably be to find and read entries related to the sales.

A forensic investigation must start with a review and evaluation of all the information relevant to the tax audit. This may be information contained in the system for storage, in the operating system, software, or contained in various other files. The analysis will be focused on uncovering evidence of the use of electronic sales suppression software and to uncover the actual software used (the Phantomware or Zapper).

Files that contain registered sales can be checked against timestamps[2] in the storage system / file system. If the sales were changed at a time period when they normally would not be written to, this can indicate the use of electronic suppression of sales software. The log files may also contain data that can further substantiate traces of suppression that have been indicated. Normally, the information in the file system can be a good source for determining the timing of when a file is created, modified, or last used. Other sources can be log entries in security applications such as antivirus programs, which may include information about names and size of files. If there are differences between the file size that is logged by the antivirus program and the size of the files in the seized system, this may be proof that the content is changed. The analysis of such files is aimed mainly at identifying the use of electronic sales suppression software.

Typical tools used in the analysis of digital information include the following.

- EnCase from Guidance Software is a program that has broad support for different storage systems and is suitable for a general analysis of collected digital information (*www.guidancesoftware.com/*).
- Forensic Toolkit from Access Data is a program that supports the most common types of storage systems and simplifies the search process through the use of indexing of the contents of the collected digital information (*www.accessdata.com/*).
- IDA from Hex-Rays is a program that has broad support in order to decompile application files (*www.hex-rays.com/idapro/*).
- Forensics WinHex from X-Ways Software Technology is a hex editor with many forensic functions (*www.x-ways.com/*).

If the focus of the digital analysis is on detecting the existence of electronic sales suppression software, analysis will largely focus on program files and entries in the operating system. The procedure of such analysis can vary and can combine a range of expertise. One approach that has been used frequently and with good results is to obtain application software from the secured materials and review them. This can be done by running the program on another physical computer or on a *virtual machine*. There are several examples where this has resulted in the discovery of hidden functionality. This is also a good way to discover a program's ability to reduce turnover (sales) through the use of other functions, which are not hidden. A more complex approach is to use methods of decompiling the program files. This means that the contents of program files, which largely consist of instructions for the machine, are interpreted into a programming code that is readable by the investigator. This is very time consuming and can give greatly varying success. One approach that can yield good results is to bring out the dialog boxes and graphics from the program files. These are items that can reveal hidden functionality and hold references to the functionality related to the reduction of the sales data.

Notes

1. Read Only Memory (ROM) is computer memory that can permanently store data and applications within it.
2. A timestamp is the current time of an *event* e.g. sales transaction that is recorded by a computer.

Government Responses

Electronic sales suppression on POS systems has been developing for some years now, and awareness among governments and tax administrations has steadily risen. Work by the TFTC has helped to raise awareness among countries and to stimulate action in a number of them. A presentation at the first Tax and Crime Forum in Oslo in March 2011 brought the tax risks to the attention of a wider audience of tax and law enforcement officials.

The TFTC carried out a survey of the government responses from a number of countries where the information was available. This has contributed to an analysis of the range of government responses that can be effective in tackling the challenges and risks of electronic sales suppression.

The responses can be summarised under the following categories:

- strengthen compliance;
- raise awareness;
- detection, audit and investigation;
- intelligence; and
- fiscal tills and certified POS systems.

The issue of electronic sales suppression is a complex one and needs a solution addressing some or all of these categories. For that reason it is important that a strategic approach is taken to developing an appropriate set of responses.

Strategic approach

Some tax administrations have seen their work in this area as part of a wider strategy on whether to tackle the "tax gap" or to address the grey economy.

To develop a strategic response to electronic sales suppression a tax administration can identify the nature of risks to which it might be exposed; that could draw on some of the information in this report and valuable information can also be obtained from experienced contacts in other tax administrations that are further along the path in dealing with sales suppression.

Risks can be identified by some special audits targeted on a range of businesses; both ones already with a risk factor and without. This approach has been followed in a number of countries and the presence of electronic sales suppression has been found in both types of case. Extending these sample audits could help identify which retail and service sectors were most at risk. In many countries the focus is on restaurants but high risks have also been identified in small supermarket chains, retail pharmacies, hairdressers and other service providers.

It is also useful to understand the nature of the POS business market, who the POS suppliers are, both domestically and internationally owned, and their relative shares of the market.

A number of tax administrations have made clear through legislation their strategic intent to combat electronic sales suppression. Legislation criminalising the supply, possession or use of electronic sales suppression software should be available for prosecutors as this may speed up the often lengthy process of tackling the rogue suppliers as well as provide a powerful signal to manufacturers and suppliers. Ireland has recently introduced such legislation[1] and it is being introduced at state level in the United States (including Florida, Maine and New York).

Strengthen compliance

The Forum on Tax Administration's report *Monitoring Taxpayer's Compliance*[2] states that "in an ideal world, all citizens and businesses would satisfy their obligations under the tax law to register where specifically required, and to voluntarily declare and pay on time their tax liabilities, all calculated fully and accurately in accordance with the law". Compliance by taxpayers with these basic obligations can also be viewed in terms of whether such compliance is achieved voluntarily (i.e. *voluntary compliance*) or corrected by verification/enforcement actions carried out by the tax administration (i.e. *enforced compliance*). In a tax administration context, this distinction is highly relevant as "enforced compliance" has a cost, and very often a significant one.

Voluntary compliance

OECD tax guidance on record keeping[3] describes the benefits of achieving voluntary compliance thus:

"Enforcing compliance via frequent checks, substantive audits and prosecutions is an expensive way of ensuring adequate compliance levels, so most tax administrations attempt to maximize voluntary compliance where the taxpayer is encouraged to co-operate and actively comply with the tax regulations. This reduces the cost of administering the tax system but is only practicable when the requirements of the tax system are well understood, relatively easy to comply with, and generally accepted by businesses". "Voluntary compliance is best enabled ...where tax requirements integrate with existing business record and accounting systems. Providing such systems are reliable, the costs of compliance for both businesses and tax administrations are likely to be minimised."

Working to improve "co-operative compliance", the Forum on Tax Administration's Guidance Note "Guidance and Specifications for Tax Compliance of Business and Accounting Software" provides recommendations to both tax administrations and software developers. These recommendations apply to all accounting and business software and therefore include cash registers and POS systems. As the Guidance Note states, each tax administration is faced with a different environment in respect of factors such as policy, legislation, administration and culture and these factors will need to guide their responses.

Many tax administrations seek co-operative compliance relationships, or enhanced relationships, with their largest business taxpayers. These relationships are based on mutual trust, transparency and understanding. Commercial awareness, impartiality, proportionality,

openness and responsiveness by tax administrations and disclosure and transparency by taxpayers underpin these relationships. Certainty on tax issues in a timely manner is one of the advantages for businesses engaging in these relationships. Tax administrations will consider the internal control framework of large businesses when entering into enhanced relationships. Accounting software (including electronic cash registers and point of sale systems) forms part of the internal business control framework. For small and medium-sized enterprises, tax administrations will often look at specific business sectors and their associations in discussing compliance issues and seek to provide certainty in advance on tax issues. Examples here include Canada and the Netherlands where the tax administrations have engaged the restaurant sector at local levels on compliance discussions.

A very important group of stakeholders are software developers and suppliers of electronic cash systems. A number of tax administrations are examining the possibility of enhanced relationships with developers and suppliers of POS systems. The intention would be to create a business environment where the vast majority of cash systems were free from the use of sales suppression techniques. Tax administrations seek to establish co-operative relations with these stakeholders and challenge them to remove suppression software. It is therefore not only important to influence taxpayers' behaviour but also to influence software developers and suppliers; such an approach might be more effective as it is a collective, proactive one instead of individual audits. It is important to determine standards as regards electronic cash registers and to have software developers' and distributors' commitment to these standards.

The tax administration in Ireland has set out a clear example of this approach. They launched a compliance campaign on the use of cash register systems, focusing on three major stakeholders: the business owners (end-users), the suppliers of the cash register systems and/or the cash register software; and their respective representative bodies. The stakeholders were sent a letter enclosing the new leaflet on the subject that was published by the Irish Revenue Commissioners. The leaflet explains clearly what is expected from every stakeholder, to comply with the VAT Regulations of 2008, and in particular how the obligation to keep records applies to the use of cash registers. The information is also highlighted on the tax administration website at *www.revenue.ie/en/tax/vat/leaflets/cash-registers.html*.

Quality mark

An innovative approach to voluntary compliance by the Dutch tax administration has led to the creation of an industry body set up to certify the quality of POS systems marketed in the Netherlands. The Quality Mark[4] system is currently unique to the Netherlands and it would appear that it may be adaptable by other jurisdictions. It is worth examining when the process is fully established whether there may be the possibility of applying this with an international scope. Specific standards for POS systems should be applicable internationally and this could have far reaching benefits – substantially reducing the open market for electronic sales suppression, providing tax administrations, software developers and users with certainty on compliance quality of POS systems and reducing compliance costs for all.

The Dutch tax administration and the manufacturers participate in this project, on a voluntary basis. The project is now operational, has the support of many manufacturers; and the Quality Mark organisation functions as a fully independent group. The idea is that cash registers systems that comply with the standards will obtain a Quality Mark label. The Quality Mark body sets standards to which a reliable system should comply and monitors that manufacturers keep to the standards (and correctly use the Quality Mark label).

Figure 3. Quality Mark introduced in the Netherlands

Source: *www.keurmerkafrekensystemen.nl*

The Dutch tax administration will take into account within its risk management system for audits that quality marked systems represent a lower risk regarding fraud.

Raise awareness

Raising the awareness of the impact of electronic sales suppression in a planned and stepped manner can be beneficial. Sometimes the awareness-raising can be assisted or even initiated by the media and investigative journalists as has been the case in Canada, the Netherlands and Norway.

Tax administrations may want to consider establishing a series of dialogues with key stakeholders, such as manufacturers, suppliers and business sector representatives. Through dialogue, they can ensure the stakeholders understand:

- how legislation applies to the hardware and software they use;
- what the government expects of their behaviour in this matter;
- how they can comply with the legal requirements; and
- the possible results of non-compliance.

When the focus for awareness is on the end-user, the dialogue can specifically address:

- the accounting and legal requirements for maintaining books and records;
- the use of cash register systems and how it complies with these laws; and
- the benefits of compliance for both sides (win-win): providing entrepreneurs with up-to-date business information and providing tax authorities with both the knowledge about the systems used and ensuring the taxpayer is "lower" risk (and so keeping audit capacity free for "higher" risks).

The communication tools used in this approach may be specific leaflets about the use of cash register systems, specific web pages on the official website of the tax administration and more targeted awareness campaigns.

When the focus is on the supply side, communication can mostly deal with:

- the accounting and legal provisions for the development, installation and use of cash register systems;
- the specific requirements of the cash register system to comply; and
- the benefits of compliance for every involved party (win-win): for example, developers/suppliers can compete on equal terms, while the compliant behaviour provides the tax administration some insurance (lower risk, keeping more audit capacity for the "higher" risks).

The main communication tools are here the meetings with the representative bodies and individual meetings with the suppliers.

There is also the possibility of focusing awareness on the generality of taxpayers by using the media to publicise results of successful convictions, thereby encouraging compliance. In Canada, media coverage and publication of successful prosecutions is a cornerstone to the success of the Criminal Investigations Program. In some instances, such as the Zapper cases, media coverage may be sought at the time search warrants are executed and the criminal investigations are ongoing. Publicising prosecutions and convictions are an integral part of the self-assessment system and it acts as deterrence to others who may be contemplating tax evasion. An example of some of the media coverage obtained is shown in figure 4. This story was picked up and reported in the nightly television news programmes.

Figure 4. Zappers – Media coverage

Source: The Province, "Tax – Cheating software bust – Something's fishy at these restaurants (… and it's not the sushi)", Front Page, The Province, 11 December 2008.

Audit and investigation

Tax administrations not only audit individual cases but also use project-like approaches to review and audit possible electronic suppression of sales cases. Selection of cases for these campaigns can be based on a number of different factors. Risk analysis software (such as IDEA described earlier) plays an important role as well as knowledge about business and cash-intensive sectors. A variety of signals coming to the tax administration can lead to the discovery of electronic sales suppression software and techniques and their suppliers.

Through audits and investigations of suppliers of systems who are suspected of using electronic suppression of sales techniques, it is possible to obtain client lists and identify the users of the software. This can be used to develop audit projects on specific types of electronic cash registers. This can also serve to gain more knowledge on changes to the systems being audited.

The most serious cases should be pursued through prosecutions and publicity should be sought to encourage others to correct their actions. Many tax administrations have voluntary disclosure programs aimed at encouraging taxpayers to come forward and correct their tax position.

A key element for all tax administrations in combating sales suppression is the reliance on the skills of frontline compliance officers (the tax auditor, e-auditor, computer forensic investigator and criminal investigator) to carry out the strategy. Resources will need to be found and skills developed for the roles set out below.

The Tax Auditor

Under the 'principle' based approach to combating sales suppression, where tax administrations rely on taxpayers to comply with their tax obligations, maintain accurate and complete books and records, and file accurate reports, the auditor needs to complete a variety of traces during the course of the audit including a tour of the taxpayer's premises where observations on the presence of POS systems are noted (e.g. noting the manufacturer's name, any old POS systems 'no longer in use' etc.), conducting interviews (e.g. interviewing the taxpayer and staff on the various functions/usage of the POS, questioning the roles and responsibilities of the taxpayer and staff regarding the business's processes and internal controls), indirect testing of income (e.g. a source and application of funds test, a net worth analysis) and a review of the outputs of the POS itself (e.g. comparing reported sales in the past to those at the time of the auditor's visit).

Furthermore, as with detecting possible cases of tax evasion and making referrals to the criminal investigations program of the tax administrations or to the appropriate law enforcement agency, the auditor also needs to be mindful of the possibility of the use of sales suppression software and make the appropriate arrangements for the electronic commerce auditor or e-auditor to review the POS itself.

Where a 'rules' based approach (rather than principles based) is utilised, the role of the auditor is expanded. Under this approach, the government requires the users to utilise certain "government approved" physical hardware and software and to maintain certain records. Along with the traditional traces mentioned above, the auditors may have to closely monitor and regulate the electronic cash registers and the POS for physical tampering as well as audit the records produced. In some countries, this may also be a function shared with the e-auditor.

Auditors will provide referrals to the criminal investigations area or the appropriate law enforcement agency for all likely cases of tax evasion, including those that are based on the use of sales suppression software.

The E-Auditors & Computer Forensic Investigators

E-auditors have an important support role to tax auditors where POS are used by taxpayers. It is the e-auditors who have the expertise to access the taxpayers' systems and provide the tax auditor with copies of the taxpayers' electronic POS records.

However, with the discovery of the first sales suppression software back in the 90's, the role of the e-auditor has evolved from one of passive support to active auditing. In the countries where they have created such positions, they have developed the skills to perform sophisticated computer traces (e.g. decryption of passwords, exposing management function keys, detecting changes to codes). They will also conduct interviews of business owners and their staff in relation to the operation of the POS. Their findings are generally passed on to tax auditors who will then be able to incorporate these findings into their audits.

In serious cases of abuse, the file may become a criminal investigation and the role of the computer forensic investigator comes to the fore. These specialists, like their e-auditor counterparts, have developed an expertise to forensically seize and investigate the electronic data. They gain access to the taxpayer's POS and computers and use various forensic traces (e.g. analysing time stamps, checksums & counts, cloning systems to perform testing, reviewing for incriminating emails and recovering deleted emails & files/data etc.) to help criminal investigators establish the *mens rea* or the 'criminal mind' element usually required for criminal charges to be pursued. Again, their findings are generally passed on to the criminal investigator who will then be able to incorporate these findings into their investigation.

Regardless of the approach adopted by the tax administrations, e-auditors and computer forensic investigators are key to ensuring tax administrations are successful in their fight against electronic sales suppression. It is also important that e-auditors and computer forensic investigators are able to co-operate effectively in combating electronic sales suppression, both with each other and with the tax administration.

Criminal Investigation

The threat of criminal investigation and prosecution represents the strongest deterrent that most tax administrations can bring to the fight against taxpayers engaged in serious tax non-compliance, including those opting to use sales suppression techniques. As with other law enforcement agencies, it must gather evidence to support *mens rea* as well the determination of the unreported revenues.

Investigators will use traditional investigative techniques (e.g. gathering evidence through the use of judicially authorised search warrants, production orders as well as interviewing key staff both at the taxpayer's place of business, at the sales suppression software manufacturer's place of business, etc.) to gather evidence. However, other techniques may be appropriate such as the use of undercover operations (described earlier) or joint operations with other law enforcement bodies and regulators aimed at securing key evidence to demonstrate the use of sales suppression to underreport revenues. The secondary goal is to create deterrence by raising public awareness of the growing threat of electronic sales suppression and the unfair advantage it places on others in the industry. Publicity gained also lets those who are engaging in this form of tax evasion or fraud, know that the tax administration is aware of this behaviour and will not tolerate it. Those who participate will face stiff penalties and fines and even possibly jail sentences.

Sources of intelligence

In addition to the frontline officers mentioned above, there are those working 'behind the scenes' that help support the activities of the frontline officers involved in the fight against sales suppression. They range from intelligence officers who use public (open source) and internally-generated information gathered by auditors and investigators (e.g. suppliers' client lists) in the field and produce intelligence reports for management to action; to train staff who have the expertise to provide all four types of frontline officers with the appropriate training required to carry out their tasks.

Detailed knowledge on the operation of POS systems is required to support detection and investigation. The knowledge that is gathered about the various systems can be:

- openly gathered and collected from open sources; or
- gathered in a clandestine way (e.g. by anonymously purchasing technical manuals).

The legal basis of information-gathering is a national legislative matter. There are many systems built on legal traditions and understanding of public rights. Most OECD member countries have a division between law enforcement legislation and tax legislation. The flow of information between the tax administration and law enforcement agency is usually tightly regulated. Information gathering and sharing increasingly happens where there is a reasonable suspicion a crime is being or has been committed. It is vital in the cases regarding manipulation and fraud using digital systems like POS systems, that law enforcement and governmental bodies have a sufficient legal basis to gather and analyse information. This is needed so that the best response can be chosen and that systems that are misused are identified.

Relevant information gathered by tax administrations can be shared with other tax administrations using the range of tax exchange information measures that are available. In particular the use of spontaneous exchanges of information on manufacturers operating internationally has already proved useful. The use of the Convention on Mutual Administrative Assistance in Tax Matters to enable exchange of information between several countries at the same time has been successful in pursuing recent cases. This convention is not yet signed by all member states, but the numbers are growing steadily.

Intelligence gathering

Intelligence gathering provides a basis for the investigator to scope their investigation. Intelligence is not used as evidence in a prosecution but helps the investigator to obtain evidence that can be used. The benefit for the case investigator is that they know what to look for (and what it looks like).

Electronic sales suppression systems have many attributes that make them good candidates for intelligence gathering. Useful methods in such cases are the following.

- Undercover operations – this method is used by a number of tax criminal investigation sections to carry out covert investigations. These require very detailed legal, technical and operational planning. The outcome of such techniques may be shared, but legal obstacles such as privacy issues may render the delivery, the acceptance and the use of such information non-usable in a criminal proceeding in some jurisdictions.

- Technical methods to *gather* information include communication control/wire taps, logging of cars, room monitoring and other "passive technical" operations (passive in the sense that they do not presuppose a covert break-in or such like steps). These techniques are used to *obtain* information and could include measures like installing key loggers in computers, hacking computers and other more aggressive measures.
- Use of confidential sources and informants.

Library of information

Several countries have been developing a library of relevant information to support audit and investigation of POS systems. At a national level the library may contain not only publically available information on manufacturers and suppliers and the POS systems marketed but also technical information obtained from audits and investigations. This has raised the possibility of whether such a library could be maintained at an international level and made available to tax administrations. This could face some challenges in terms of data protection and exchange of information. An alternative would be to design a template for exchanges of information on the use of POS systems for sales suppression which could be used under the normal exchange of information instruments between countries who managed their own libraries.

Fiscal tills and certified POS systems

In combating the abuse of POS systems by taxpayers to evade tax, governments have sought different approaches. The range of solutions has increased and evolved from the original Italian 'fiscal till' (where the sales data is saved to a recording device at the end of the working day) to the Portuguese 'certified POS software' (where the system is required to produce encrypted sales data with digital signatures that validate a genuine transaction). One of the key evolutions in these technical solutions is that the POS data is now secured upon creation of the data rather than in early systems at the end of the day's business. A detailed description of the features of fiscal tills and certified POS systems is included in the Annex.

The report does not make recommendations about specific technical solutions. Rather it seeks to provide information on the range of solutions adopted. There appears to be a growing trend towards a solution that secures cash register data upon its creation and includes new techniques such as data encryption and digital signatures.

Notes

1. The legislation introduced in 2011 added the following offences to the statute:

''(ba) knowingly or wilfully possesses or uses, for the purpose of evading tax, a computer programme or electronic component which modifies, corrects, deletes,

cancels, conceals or otherwise alters any record stored or preserved by means of any electronic device without preserving the original data and its subsequent modification, correction, cancellation, concealment or alteration,

(bb) provides or makes available, for the purpose of evading tax, a computer programme or electronic component which modifies, corrects, deletes, cancels, conceals or otherwise alters any record stored or preserved by means of any electronic device without preserving the original data and its subsequent modification, correction, cancellation, concealment or alteration.

The penalty for such offences are on summary conviction of an offence committed on or after 14 March 2008, a fine not exceeding EUR 5,000 (EUR 3,000 for offences committed before that date) – which may be mitigated to not less than one fourth part of such fine – or at the discretion of the court, a term of imprisonment not exceeding 12 months, or both, and on conviction on indictment, a fine not exceeding EUR 126,970 or at the discretion of the court, a term of imprisonment not exceeding 5 years, or both."

2. OECD (2008) *www.oecd.org/dataoecd/51/13/40947920.pdf*.

3. Tax Guidance Series-Record Keeping: *www.oecd.org/dataoecd/29/25/31663144.pdf*.

4. The brochure on the Quality Mark approach, also available in English, can be found at *www.belastingdienst.nl/download/1419.html*.

Conclusions

Since the OECD's Task Force on Tax Crime and Other Crime began raising awareness of the issue of electronic sales suppression among tax administrations, there has been significant increase in action by them in identifying and addressing the tax revenue threats posed. But alongside this there has been an increase in the sophistication of the techniques used by the suppliers of POS systems to conceal the operation of this form of tax evasion. This report provides advice to tax administrations on developing strategies to combat sales suppression and provides specific information to help tax auditors and investigators in detecting, investigating and disrupting tax evasion.

It is for each tax administration to assess the risks and devise the most appropriate and effective strategy in tackling this issue. A series of recommendations for action that should be part of such a strategy is presented below.

The work of the group of experts who have come together to make this report has had a significant number of benefits during the process. The sharing of experiences has highlighted additional areas for research and in some cases has led to international co-operation in tackling crime – even to the point of co-operation on the raiding of premises and the issue of cross-border arrest warrants. This has started to redress the imbalance whereby the providers of Phantomware and Zappers operate internationally and have been able to exploit the lack of communication between countries.

Recommendations

Tax administrations should develop a strategy for tackling electronic sales suppression within their overall approach to tax compliance to ensure that it deals with the risks posed by electronic sales suppression systems and promotes voluntary compliance as well as improving detection and counter measures. Ideally, this will include gaining prior knowledge of customer systems prior to engagement, to identify potential risk areas and allocate resources.

A communications programme should be developed aimed at raising awareness among all the stakeholders of the criminal nature of the use of such techniques and the serious consequences of investigation and prosecution.

Tax administrations should review whether their legal powers are adequate for the audit and forensic examination of POS systems.

Tax administrations should invest in acquiring the skills and tools to audit and investigate POS systems including developing the role of specialist e-auditors and recruiting digital forensic specialists where appropriate. Mechanisms should be in place to ensure that different experts co-operate effectively in combating electronic sales suppression.

Tax administrations should consider recommending legislation criminalising the providing or possession or use of electronic sales suppression software.

Annex: Fiscal Tills and Certified POS systems

Fiscal Tills

Fiscal tills were introduced by legislation in a number of countries more than twenty five years ago and there has been a recent increase of interest in their use. Essentially, they are cash registers that are required to conform to a set of specified technical requirements to secure data storage and to monitor events within the system. They were first introduced in Italy back in 1983, when the Government created the obligation for certain businesses to issue a fiscal receipt by means of a fiscal electronic cash register in an attempt to reduce the size of the shadow or underground economy. This approach was also adopted by Greece and a number of other countries. Each country's government determined what the system should record, how it should store the data, and what kind of output (reports/files and receipts) the system should be able to produce in specified formats in order to secure the data for tax audits.

Specific requirements include:

- electronic preservation of the detailed data of transactions in specified formats, encrypted in specified ways and on specified storage devices;
- detailed records that are only available for the tax auditor when required;
- preservation of a complete audit trail and in some cases event monitoring;
- the system is equipped with some kind of a monitoring apparatus; and
- other technical measures to guard against subsequent alterations in a manner that will assure that data-integrity is maintained.

In early versions fiscal tills secured the sales data at the end of day operations, while the approach now generally taken is to secure data at the time of the data creation.

The working method can be described as follows. At the end of every working day, the entrepreneur has to generate a Z-report (daily financial report). The total sales reflected in that report are then written to a protected memory, where the counters are updated with the sales totals of that particular day. Later on, in some countries, the counters were expanded to include ticket counters, refund totals and other items.

Originally, the protected memory (ROM) was sealed and secured in the machine itself, by fixing it to the chassis with resin or epoxy. When cash registers became more and more sophisticated and became more and more pc-based systems, it was no longer mandatory for the protected memory to be placed inside the chassis of the terminal, but it could be placed instead in the separate printer of the system (then called a fiscal printer).

The issued receipt specifically states whether it is a genuine fiscal receipt, representing a recorded sale, or is produced for training, as a *pro forma* invoice, or a copy ticket. The fiscal receipts also have a stamp in the footer, containing a fiscal logo that must meet some specific requirements, regarding the font and lay-out.

Figure 5. Examples from left to right: Italy, Bulgaria, Greece, and Hungary.

Source: Information provided by Italy, Bulgaria, Greece, and Hungary.

Depending on the country, the certification (showing the compliance of the system with the law) is carried out either by the tax administration or by private certification bodies.

'Fiscal till' solutions were introduced in various countries, including Argentina, Brazil, Bulgaria, Greece, Hungary, Latvia, Lithuania, Malta, Poland, Russia, Turkey and Venezuela. Such systems are still appropriate in certain circumstances. In some developing countries such systems are put in place with data transactions being automatically uploaded to the tax administration's computer system.

Certified POS systems

More recently, a growing number of countries is seeking to improve taxpayers' compliance by making the use of 'certified' cash register systems mandatory, for all cash related business or for all business in some specified economic activities (e.g. restaurants). This approach is characterised by the use of additional equipment which adds a digital signature to some or all of the data items on a receipt using encryption technology. This can include a monitoring device for storing receipt and signature data and updating grand totals in secure memory.

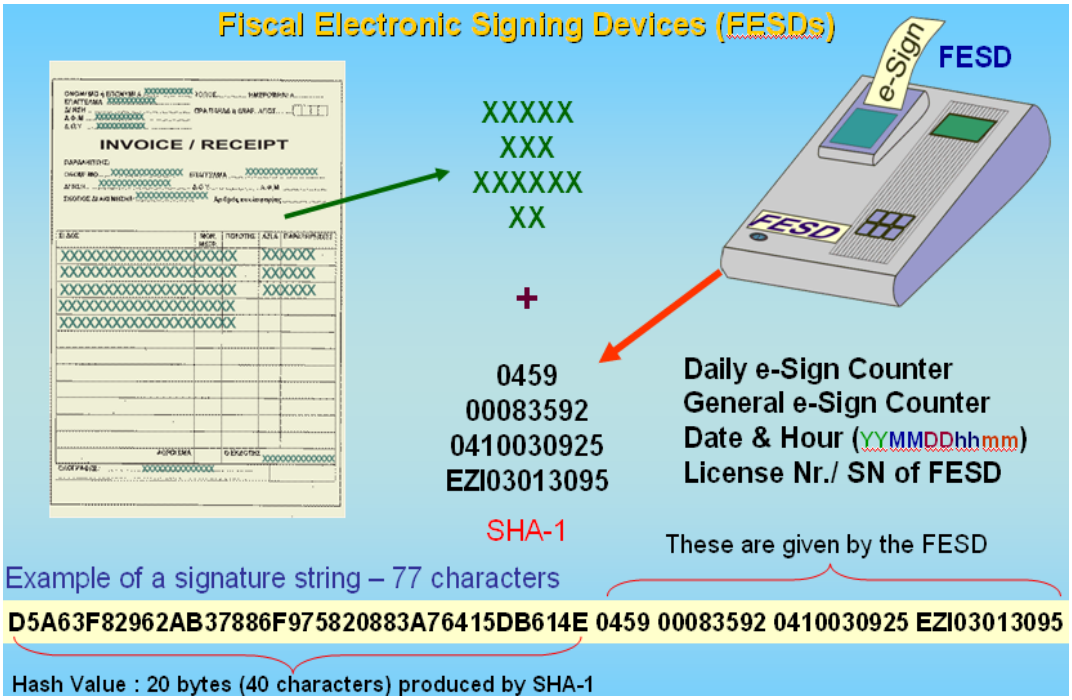
Signing receipt data and storing relevant data in monitoring device

Technical solutions of this kind not only add a digital signature to some sales receipt data, they additionally keep track of the tax relevant data of these receipts. Among tax administrations that are implementing or have implemented this kind of approach are Belgium, Greece, Québec province of Canada and Sweden.

Greece

The Greek Ministry of Finance was the first to introduce the digital signing[1] of data on receipts and invoices. When this is printed on the receipt/invoice and stored in the original data, it provides a significant tool to check and enforce the data integrity of the POS system.

Figure 6. The Greek Fiscal Electronic Signing Device



Source: Information provided by Greece

Québec

The Québec Provincial Government designed a monitoring device, the Sales Recording Module, which stores the relevant receipt data and produces a digital signature.[2] The signature is also printed on the client's receipt, in a 2D bar code. The public key is held by the tax administration (the supplier of the Sales Recording Module).

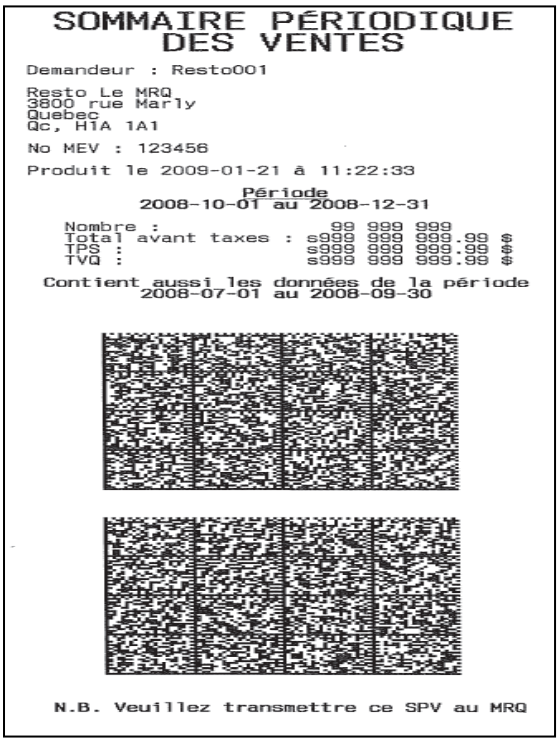
Figure 7. The Québec Sales Recording Module

Source: Information provided by the Québec tax administration

Scanning this bar code with a hand scanner (including software with public key) makes it very easy to check whether the signature is valid. A non-valid signature can only mean that the content of the receipt was manipulated.

Furthermore, the Sales Recording Module is able to produce a periodic report, also presented in a 2D bar code. This report can be transmitted to the Québec tax administration by normal post or electronically, copying it on a USB key and uploading it through their secure electronic services.

Figure 8. Example of bar-coded report of sales data produced by the Québec Sales Recording Module


SOMMAIRE PÉRIODIQUE DES VENTES

Demandeur : Resto001

Resto Le MRQ
3800 rue Marly
Québec
Qc, H1A 1A1

No MEV : 123456

Produit le 2009-01-21 à 11:22:33

Période
2008-10-01 au 2008-12-31

Nombre :	99 999 999
Total avant taxes :	s999 999 999.99 $
TPS :	s999 999 999.99 $
TVQ :	s999 999 999.99 $

Contient aussi les données de la période
2008-07-01 au 2008-09-30

N.B. Veuillez transmettre ce SPV au MRQ

Source: Information provided by Canada.

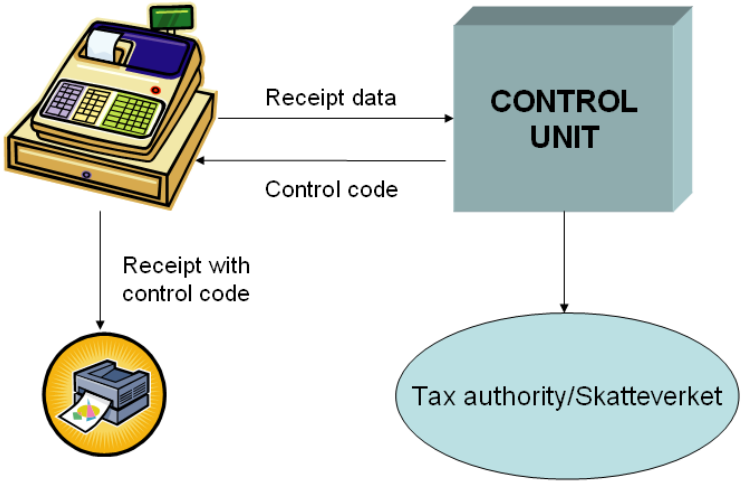
This device has been introduced only in the restaurant sector. More information can be obtained on the website[3] of Québec Revenue.

Sweden & Belgium

Sweden's new legislation became fully active in 2010, introducing the mandatory use of cash register systems in cash intensive businesses (with some exemptions: e.g. very small business, open air markets, large companies with good internal controls).

The legislation requires that POS systems must meet strict technical requirements, including both mandatory functions and forbidden functions. The cash register has to be declared by the manufacturer to the tax administration.

Figure 9. The Swedish control unit



Source: Information provided by Sweden.

Furthermore, a control unit has to be connected to the system. It produces a digital signature,[4] based on the content of the receipt. The signature (which is printed on the receipt) allows for an easy check on the integrity of the receipt data. Relevant receipt data is kept in a secure database in the control unit, which also contains a large number of counters that are updated each time a receipt is issued. An easy copying procedure allows the auditor to get a full copy of the control unit's database, allowing for an easy audit with special software.

Belgium is set to introduce a similar system in 2013 that, at this point in time, is to be limited to the restaurant sector. More specifically, it will target restaurants with at least 10 % of their annual sales turnover consisting of meals to be served on the premises.

The main difference is that the monitoring device will consist of two parts - the sales data controller which is similar to the Swedish control unit and a VAT signing card (VSC). The certificate with the private key, provided by the tax administration, will be embedded on the VSC, which will be personalised by connecting the VAT number to the card, producing the pair of keys and storing the public key in the tax administration's database. The manufacturers of the sales data controller will have no knowledge of the key.

Figure 10. The Belgian 'Certified Cash Register System'

Source: Information provided by Belgium.

This approach not only focuses on the technical aspects, but will also implement a full certification of each part of the 'certified cash register system', making every stakeholder involved (manufacturer, distributor, user, tax administration) fully aware of their responsibility.

Just as in Sweden and Québec, the issuing of the (fiscal) receipt is made mandatory and certified systems will be published on the website of the tax administration.

Variations on both concepts are currently being considered in other EU Member States including the introduction of a semi-online function to the control module.

Signing receipt data, storing relevant data in monitoring device and secure online data transfer to government

Signing the receipt data, storing it in a monitoring device and making it available for remote access by the tax administration (e.g. using GRPS), may be an appropriate and economic solution for some governments. The remote access may be automatic, that is, at some fixed time a full copy is sent to a central server in the tax administration, or it can be 'on demand' when an audit is being carried out. An automatic upload may be considered as an official tax return.

Signing receipt data with certified POS software

The most recent example of adding a digital signature with certified POS software is the system introduced in Portugal. This approach, which does not require a monitoring device, is based on an encryption process, which signs the documents by using an asymmetric pair of keys and an RSA algorithm. The software developer hands over the public key to the tax administration and the private key may only be known by the software developer. The tax administration verifies if the software meets the requirements and if so, it certifies the software and makes this certification public.

Since 2008 Portugal has made mandatory the use by POS systems of a Standard Audit File for Tax purposes (SAF-T). This includes the signature of the following fields in each document: receipt date; system entry date; receipt number; gross total; and the signature of the previous document of the same series.

As a result:

- it is easy to see on the receipt whether or not certified software is used;
- digits of the signature printed out must correspond with the hash signature on the SAF-T (when requested by auditor); and
- based examining on the public key, the receipt data and the receipt signature, the SAF-T Analyser is able to determine:
  - whether the receipt was manipulated;
  - if the signature was generated with the correct private key; and
  - whether the receipt sequence was broken.

More information and a free signature analysis can be found on the website of the Portuguese tax administration (*http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/news_saf-t_pt.htm*). This includes an English translation of the software certification law.

Notes

1. The algorithm used is an open source SHA-1.
2. This uses a public key infrastructure and a RSA algorithm.
3. *www.revenuquebec.ca/en/a-propos/evasion_fiscale/restauration/secteur.aspx*
4. RSA based algorithm, public key infrastructure, private key on certificate in the control unit.

ELECTRONIC SALES SUPPRESSION: A THREAT TO TAX REVENUES

Electronic sales suppression techniques facilitate tax evasion and result in massive tax loss globally. In the retail sector, point of sales systems are an important business tool and are expected to contain reliable data. In reality such systems not only permit skimming of cash receipts, much like a manual cash box, but once equipped with specialised "sales suppression" software they facilitate far more elaborate frauds. Tax administrations are losing billions of dollars through unreported sales and income hidden by the use of these techniques.

This report describes the functions of point of sales systems and the specific areas of risk to tax administrations. It sets out in detail the electronic sales suppression techniques that have been uncovered, in particular "Phantomware" and "Zappers", and shows how such methods can be detected by tax auditors and investigators. The report also considers a number of strategies adopted in different countries to tackle electronic sales suppression and highlights best practices. In particular, it makes a number of recommendations to countries for addressing this important area of risk

Table of Contents:

www.oecd.org/ctp/taxcrime