**EXECUTIVE SUMMARY**

To support tax fairness and a level playing field for all businesses, the government is examining options to address sales suppression schemes at cash registers (i.e. point-of-sale or electronic cash registers terminals). The Ontario government is seeking input from the business community and other stakeholders on technology-based approaches that would help to address the practice of electronic sales suppression while minimizing the burden for businesses.

Electronic sales suppression (ESS) involves the manipulation of a point-of-sale (POS)/electronic cash registers (ECR) terminal to hide sales records, including the taxes that customers have paid. This reduces the amount of revenue a business reports and prevents tax revenue from being collected and used for essential public services. Many governments have already implemented technology-based solutions to address this illicit activity, and other governments, including Ontario, have begun to examine ways of detecting and preventing these practices.

The 2015 Budget amended the *Taxation Act, 2007* to make the use, possession and manufacturing of software or devices that electronically suppress sales an offence. This amendment supports measures introduced by the federal government, as well as recommendations from the Commission on the Reform of Ontario’s Public Services and the Organisation for Economic Co-Operation and Development (OECD) on how to address ESS.

Ontario’s legislative amendment penalizes those caught using sales suppression software and helps deter individuals that may use this software in the future. As this software can be difficult to detect in some instances owners may not even be aware of employees using it in their establishments, exposing them to unforeseen liabilities from tax authorities and a potential loss of revenue.

That is why the government is consulting with the public and the business community to identify the scope of this problem and additional actions that may further limit the use of these illegal practices.

**OBJECTIVES**

The Province is examining an approach that will minimize the burden to businesses, promote a level playing field and support an innovative and dynamic business environment that enables Ontario businesses to thrive.

The key components under consideration include:
- an electronic device to secure sales transaction data and prevent the use of sales suppression software;
- requiring the mandatory printing of receipts; and
- undertaking targeted inspections of devices and receipt printing to ensure compliance.

Engaging key stakeholders is essential to help ensure any solution considered by the Province takes into account the impact on businesses, consumers and the broader economy.
By addressing electronic sales suppression in collaboration with industry and stakeholders, Ontario aims to:

- enhance the fairness and competitiveness of Ontario’s business environment by helping to ensure everyone pays their fair share of taxes;
- enhance the integrity of POS/ECR systems in Ontario; and
- reduce participation in the underground economy.

**Electronic Sales Suppression – Overview**

*Organization for Economic Co-Operation and Development (OECD)*

In 2013, the OECD released a report titled “Electronic Sales Suppression: A Threat to Tax Revenue”, in which it outlines the growing evidence of tax evasion over the course of the past decade related to ESS, and outlines attempts made by tax authorities to address this issue. The report made five recommendations that governments should consider:

1. having tax authorities develop a strategy for tackling ESS that states the risks posed by ESS, and promotes voluntary compliance as well as improving detection and counter measures;
2. developing a communications strategy aimed at raising awareness among stakeholders;
3. ensuring the adequacy of tax authorities’ legal powers;
4. investing in acquiring the skills and tools to audit and investigate POS/ECR systems; and
5. developing legislation criminalizing the supply, possession and use of ESS.¹

**Electronic Sales Suppression Software**

There are two types of ESS software:

- programs stored within a POS/ECR system are known as *phantom-ware*.
- programs added on via a USB, CD or Internet link are known as *zappers*. Zappers are more difficult to detect due to the lack of integration with the businesses’ operating system.

As pictured below, when ESS software is installed, it deletes select items from the electronic record, falsifying the number of taxable sales and allowing an individual to pocket the difference in cash. The program also reorganizes the order of receipts so that nothing seems amiss to the owner or tax authorities. For example, if a day’s transactions are numbered one through 10 and transaction number four is removed, the zapper will align the remaining transactions to show only a total of nine records in the correct order. The software can apply to cash, debit and credit card transactions² and may be moving into mobile payments.

---


² Ibid., pg. 13
Evidence of the use of such software is very difficult to establish and, to do so, requires the use of specialized forensic tools by highly trained audit specialists. Tax authorities that have implemented a technological solution were able to detect ESS software and streamline their audit and inspections process. In most cases, ESS software was identified in sectors traditionally considered to be at a high risk of underground economic activity.

**Other Electronic Suppression Schemes**

In addition to ESS software, tax authorities have discovered additional schemes used to conceal sales. For example, all POS/ECR systems are embedded with specific functions for different purposes. Auditors have found that some individuals may use these functions to avoid reporting a sale. In this scenario, an employee may enable the “training mode” function on a POS/ECR and pretend to ring up a sale. As a result, the system considers the transaction a training exercise, allowing the individual to appropriate the funds from the sale.

Additional schemes include using inappropriate accounting methods. This includes, but is not limited to, having multiple sets of invoices, developing false reports for the owner or tax authorities or deleting business records.

Through these schemes, it is possible for individuals to conceal sales transactions from unsuspecting managers or owners, appropriate funds for themselves and leave owners vulnerable to unforeseen liability from tax authorities.

Owners who participate in these schemes create an unfair advantage for themselves (e.g. offering lower prices) over those businesses that pay their fair share of taxes. These practices also reduce tax revenues that are used to fund essential services such as education and health care.

**JURISDICTIONAL PERSPECTIVE**

Electronic sales suppression is not unique to Ontario. Several jurisdictions report significant revenue losses due to ESS and have taken various methods to address the issue.

Tax authorities around the world have identified tax revenue losses due to the use of ESS. For example:

- Sweden recovered €150 million (approximately $200 million CAD) between 2006 and 2010;

---

3 Ibid pg. 7
Norway found €7 million (approximately $10 million CAD) in one underreported case; South Africa recovered over €22 million (approximately $30 million CAD); and Quebec recovered over $940 million CAD as a result of measures aimed at addressing ESS.

**Ontario**

Statistics Canada estimates the province’s underground economy to be 2.3 per cent of annual gross domestic product. This results in approximately $15.3 billion in annual economic activity lost to the underground economy. Much of this activity is believed to occur in the construction, retail and hospitality sectors where cash payments are common.

The 2015 Ontario Budget amended the Taxation Act, 2007 to make the use, possession and manufacturing of ESS software an offence punishable by fine, or imprisonment for the most serious activity.

Businesses that use, possess or acquire ESS software will be fined:

- $5,000 on the first infraction; and
- $50,000 on subsequent infractions.

Anyone who designs, develops, manufactures, possesses for sale, offers for sale, sell or otherwise makes available to another person will face $10,000 on the first infraction and $100,000 on subsequent infractions.

In addition, any person that uses, acquires, manufactures, supplies or participates in ESS is guilty of an offence and, in addition to the above penalties, is liable on conviction to a fine of not less than $10,000 and not more than $500,000 or imprisonment for a term not exceeding two years, or both.

The 2015 Ontario Budget also committed to examine options to stop sales suppression at POS/ECR terminals.

**Canada Revenue Agency**

In 2014, the federal government enacted an amendment to the federal Income Tax Act and the Excise Tax Act to make the use, possession and manufacturing of ESS software an offence. The amendments included new monetary penalties under each act:

- $5,000 on the first infraction and $50,000 on subsequent infractions for the use, possession or acquisition of ESS; and
- $10,000 on the first infraction; and $100,000 on any subsequent infraction for the manufacture, development, sale, possession for sale, offer for sale or otherwise making available of ESS.

The federal government also made the use, possession, acquisition, manufacture, development, sale, offer for sale, or making available of ESS software a criminal offence under the Criminal Code. The criminal fines are:

---

• on summary conviction, a fine of no less than $10,000 and no more than $500,000 or imprisonment for a term of no more than two years; and
• on conviction by indictment, a fine of no less than $50,000 and no more than $1,000,000 or imprisonment for a term of no more than five years.

As announced in the federal 2015 Budget, the government will invest $118.2 million over five years to enhance the CRA’s audit capacity by expanding its Underground Economy Specialist Teams. These new specialist teams will use advanced data analysis to identify and adopt new approaches to combat the underground economy and, working with provincial colleagues, target UE activity in high risk sectors of the economy.

**GERMANY – SMART CARD**

In 2005, Germany identified evidence of technology-assisted fraud amounting to around 50 per cent of cash receipts.  

Germany has since mandated that all POS/ECR systems be fitted with a smart card containing a crypto processor that e-signs designated tax relevant data. With this device, an electronic journal can be signed on a regular basis, or each transaction open or closed could be designated as tax relevant and signed whenever entered into the POS/ECR.

With this digital solution, audits are done remotely with the store owner emailing a data feed from the POS/ECR to the tax authority.

**NETHERLANDS – DETAILED AUDITS AND CERTIFIED CASH REGISTERS**

To address the issue of sales suppression, the Netherlands focussed on detailed and comprehensive audits. Its “deep audit” is a simultaneous and comprehensive review of a business’s accounting records (including income tax, consumption tax and employment taxes) with a strong focus on the interrelationships between these taxes.

In addition, the government is working with industry to establish a set of standards for reliable cash registers, a “Quality Mark” for all POS/ECR terminals (certification), and a commitment by the producers and traders that:

• no POS/ECR system would be sold that could not achieve a “Quality Mark”; and
• all simple cash registers would have settings verified by the producers.

---

5 Working Group on Cash Registers: Interim Report 5 (Mar. 16, 2005) (Ger.)
**Sweden & Belgium – Mandatory Use of Certified Cash Register Systems**

In 2010, Sweden introduced legislation requiring the mandatory use of cash register systems in cash-intensive businesses. The legislation requires that POS systems meet strict technical requirements including both mandatory and forbidden functions. A control unit must be connected to the system, which produces a digital signature, based on the content of the receipt. The signature allows for an easy check on the integrity of the receipt data. Relevant receipt data are 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.

Certification is provided by an independent company appointed by the Swedish Board for Accreditation and Conformity Assessment.

In 2013 Belgium followed Sweden’s lead by introducing the certification of third-party devices	extsuperscript{9}. As of 2015, devices are required in hotels, restaurants and bars.

**Quebec – Sales Recording Module**

Quebec identified more than 230 cases of underground economy activity at POS/ECR systems in the restaurant sectors between 1997 and 2008, with an estimated tax loss of over $420 million for the 2007-08 fiscal year alone.

Quebec amended the *Act Respecting the Quebec Sales Tax* mandating that all restaurants install a SRM (in French: module d’enregistrement des ventes (MEV)). The SRM records data from transactions, produces an encrypted numerical signature, and transmits it to the printer where it is printed on the receipt. Both the e-signature and the recorded data are preserved within the memory of the SRM for seven years. Restaurants are required to submit sales summaries generated by the SRM when they submit their tax declarations.

Through the use of SRMs, in its first year (2011/12) Quebec recovered more than $160 million. In total, the government has recovered over $940 million in tax revenue, with a projected total of $2.1 billion by 2018/19.

**Potential Solutions**

To ensure all businesses play by the rules and to enhance the government’s ability to detect and mitigate illegal practices meant to underreport sales revenue, the province is examining additional measures to detect and prohibit the use of ESS devices. Ontario is seeking to work with key stakeholders to identify a solution that enhances the competitiveness of the business community and ensures the integrity of Ontario’s tax regime without being overly burdensome.

---

	extsuperscript{9} Ibid, OECD report
Research from academics and tax authorities have highlighted the sophistication of ESS and its ability to evolve as tax authorities adapt. Jurisdictions that have identified the problem and are committed to reducing its effect on tax revenues appear to focus on a technological solution to combat the technological problem.

The underlying premise to the technology solution is to have sales transaction information encrypted and stored in a separate secure device to prevent any tampering. Most solutions create two sources of records, one on the POS/ECR and one in the secured device. Aggregate data from establishments would be used by tax authorities to ensure the integrity of revenue reporting.

This allows tax authorities to conduct targeted audits where a discrepancy exists between the revenue reported and aggregate data from the device. Tax authorities that have used this approach have identified a drastic reduction in audit hours and costs, thus reducing the invasive burden on legitimate businesses.

Although different methods to address the issue of sales suppression are currently being assessed by the province, consideration is being given to solutions that satisfy the following criteria:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Device</td>
<td>To secure sales transaction data and prevent the use of sales suppression software.</td>
</tr>
<tr>
<td>Mandatory Receipts</td>
<td>Require printing of receipts with an e-signature from the electronic device to ensure a transaction is recorded.</td>
</tr>
<tr>
<td>Periodic Inspections Access</td>
<td>Inspections to verify that a device is not tampered with and establishments are providing receipts to customers.</td>
</tr>
</tbody>
</table>

PROVIDING YOUR INPUT

The Ontario government is asking for your feedback to help develop a solution to respond to the use of ESS software. **Send your response via letter or email to the addresses below by December 16, 2015.** Discussion questions are posed below for consideration.

**QUESTIONS:**
- Do you identify ESS as a concern in your sector?
- How can the government effectively reduce the use of sales suppression software?
- What are your thoughts about the technological approaches outlined in this paper?
- What impacts do you anticipate?
- What other areas of the underground economy should the government seek to address?
- Other questions or comments?