

Statutory review of the
operation of Schedule 1
to the *Treasury Laws
Amendment
(Black Economy Taskforce
Measures No. 1) Act 2018*

December 2022

© Commonwealth of Australia 2023

ISBN: 978-1-925832-66-2

This publication is available for your use under a [Creative Commons Attribution 3.0 Australia](http://creativecommons.org/licenses/by/3.0/au/legalcode) licence, with the exception of the Commonwealth Coat of Arms, the Treasury logo, photographs, images, signatures and where otherwise stated. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.



Use of Treasury material under a [Creative Commons Attribution 3.0 Australia](http://creativecommons.org/licenses/by/3.0/au/legalcode) licence requires you to attribute the work (but not in any way that suggests that the Treasury endorses you or your use of the work).

Treasury material used ‘as supplied’.

Provided you have not modified or transformed Treasury material in any way including, for example, by changing the Treasury text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Treasury statistics – then Treasury prefers the following attribution:

Source: The Australian Government – the Treasury and the Australian Taxation Office.

Derivative material

If you have modified or transformed Treasury material, or derived new material from those of the Treasury in any way, then Treasury prefers the following attribution:

Based on the Australian Government the Treasury or Australian Taxation Office data.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the Department of the Prime Minister and Cabinet website (see <http://www.pmc.gov.au/government/commonwealth-coat-arms>).

Other uses

Enquiries regarding this licence and any other use of this document are welcome at:

Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Contents

- Foreword 1**
- Introduction..... 2**
- Policy context and background..... 2
 - What is Electronic Sales Suppression Technology? 2
 - Growing international concern..... 3
 - Australia’s Black Economy Taskforce 3
- Deficiencies in previous legislative framework 4
- Government response and legislative amendment..... 6
- The requirement for this Report..... 7
- Enforcement action..... 8**
 - Table 1: Breakdown in penalties and prosecutions for each sub-category (2020–21) 8
 - Table 2: Estimate of amount of revenue recovered or preserved (2021–22) 9
- Australian Observations 10**
 - Evolution of ESST 10
 - Shadow economy behaviours observed 10
 - Impacts of COVID-19 Pandemic..... 11
 - Appropriateness of criminal vs. civil penalties 11
 - Penalty effectiveness 12
 - Use of the Commissioners’ discretion 12
 - Regulatory support 12
- International Developments 13**
 - International Action 13
 - Subsequent OECD research 14
- Summary and Key Findings..... 15**
- Appendix – Summary of relevant provisions 16**
 - Definition of electronic sales suppression tools 16
 - Offences..... 16
 - Production and supply..... 16
 - Acquisition, Possession or Control..... 17
 - Use..... 17
 - Defences 18
 - Civil penalties..... 18
 - Transitional provisions..... 19

Foreword

The Australian Taxation Office (ATO's) Shadow Economy Program is critical to ensuring that our tax system works and businesses are competing on a level playing field: Australian small businesses should have confidence that their competitors are paying their fair share of tax. That is why, at the last election, the Government made a clear and strong commitment to addressing multinational tax avoidance, closing tax loopholes and improving tax transparency.

For this reason, I am very proud that we announced in the 2022–23 October Budget that we were extending the Shadow Economy Program for a further three years from 1 July 2023. This program includes the ATO's actions on sales suppression software. The Government is committed to ensuring the ATO has the resources they need to crack down on tax dodging.

The OECD has been sounding the alarm over sales suppression software for some time. Electronic sales suppression technology and similar tools exist with one purpose in mind – tax evasion. They rob the community of funding for necessary services, and they provide an unfair tax advantage to the few at the cost of the many.

In 2018, Australia passed strengthened penalties to deter the possession, manufacture and distribution of electronic sales suppression technology through the *Treasury Laws Amendment (Black Economy Measures No.1) Act 2018* (the Act). We supported these reforms in opposition, but wanted to ensure that they are effective without inadvertently hurting innocent small businesses or imposing unnecessary handbrakes on genuine business activity.

This Report outlines the early experience of the Act's operation and enforcement, and the results so far are encouraging. The ATO has been successfully cracking down on illegal tax evasion – I am pleased to report that, to date, 46 sales suppression software cases have been completed, with around \$1 million in penalties being applied and raising some \$7.4 million in tax liabilities, with more to come. I thank the ATO for their ongoing efforts.

I commend this Report to the Parliament.



The Hon Stephen Jones MP
Assistant Treasurer and Minister for Financial Services
December 2022





Introduction

This Report will discuss the policy context and background to Electronic Sales Suppression Technology, the previous legislative framework and limitations in enforcement, and the findings of the Black Economy Taskforce review prior to the introduction of new laws and higher penalties in Australia in 2018. The Report will then describe the ATO's enforcement activity under the new laws, include some relevant observations such as developments through the COVID-19 pandemic, outline recent international developments, and present some key findings.

The Report has been prepared jointly by the Treasury and the Australian Taxation Office (ATO).

Policy context and background

What is Electronic Sales Suppression Technology?

The practice of skimming – essentially falsifying sales data – has always existed in one form or another in order to evade taxes and for other reasons. In the past, it could be achieved simply by failing to recognise sales in the cash register through a cash-in-hand transaction or by diverting sales into another cash register which was kept 'off the books'. However, modern technology has allowed both the scale and sophistication of such practices to expand, even in a fully computerised environment which is *prima facie* more auditable.

Modern Point-of-Sale (POS) systems are central to business functions, from sales to inventory management to logistics. This software also generates valuable data needed for accounting, audit and taxation purposes.

Electronic Sales Suppression Technology (ESST) can digitally remove or alter sales data recorded in POS systems, and also can remove, or attempt to remove, evidence that the data has been changed in this way. Some sales suppression software is pre-loaded onto the relevant devices and automatically makes adjustments to recognised sales as they are made, whereas others require the plug-in of devices such as USB sticks combined with activating a hidden menu or combination of keystrokes to be activated and accessed. As such, business owners may not even need to change their observable behaviour whilst engaged in illegal activity.

As with much in the technology field, ESST and the methods used to detect it are in a constant struggle for supremacy akin to an arms race; as efforts to curtail use become more sophisticated, manufacturers innovate to overcome these detection methods, and so on.

POS systems with ESST typically comprise integrated business products and solutions such as online ordering, interactions with web content, registered and unregistered payment platforms, FinTech, and marketing solutions. Advances in marketing and business models reflect an evolution of sophisticated and integrated business offerings in a digital environment. This integration of payment platforms supports the ability to suppress sales and creates a lack of transparency of both cash and electronic records. The technology is constantly evolving, enabled by remote access, cloud-based storage and various anti-detection methodologies that make it hard to identify.

The technology has moved towards a service-based format, typically with ongoing weekly or monthly service fee offerings. Manufacturers are taking deliberate steps to innovate their offerings and remove an audit trail of suppression being undertaken.

Growing international concern

In the early 2000s, the OECD's Taskforce on Taxation Crimes and Other Crimes began to work on the issue and spread awareness to revenue authorities. Similar work was undertaken by the EU Commission. Canada, Germany, the Netherlands and Sweden took early action, and their efforts helped inform a 2013 OECD report *Electronic Sales Suppression – A threat to revenues* (the 2013 OECD Report).

The 2013 OECD Report noted that detecting the scale and prevalence of revenue loss arising from sales suppression software is inherently difficult, like most attempts to quantify illicit activity. In the absence of broad-based data sources, it cited a few examples of countries' audits of then-recent tax evasion behaviours to highlight the scale of the issue:

- Revenu Quebec estimated tax losses from the use of ESST of C\$417 million in 2007–08, in 2008 charging the owners of four restaurants with evasion of nearly 200,000 cash transactions valued C\$4.6 million
- Sweden detected €150 million in 2,000 audits of general tax evasion over four years, finding systematic under-reporting of turnover (in the order of 20–40%)
- South Africa detected the equivalent of €22 million expatriated out of South Africa in a single case.

The 2013 OECD Report also noted that, at publication, several countries (including France, Ireland, Norway and the United Kingdom) had tested their retail sectors and found significant problems. It also noted Ireland and several United States states had moved quickly to put in place legislation to help tackle this abuse by specifically criminalising ESST-related behaviour and support a strategic approach by tax administrations. Other approaches were also noted by various countries, such as the Netherlands creating a “quality mark” certification system for approved POS set-ups, raising awareness, and using project-, electronic- and risk-based mass audits, in addition to criminal investigations.

The 2013 OECD Report further noted that while modern POS software can have built in features that could be used to falsify records, dedicated additional software was often designed as an “add on” specifically to allow a user to falsify or edit records, even if its existence was not immediately apparent (for example, by being only accessible to a business owner who knew it was installed and not by employees processing day-to-day sales).

In the Australian context, ESST can be used most obviously to understate reported GST liability – this was noted by the Black Economy Taskforce (below) – although it can also be used to, for example, delete sales records associated with a person who was unlawfully employed.

The 2013 OECD Report recommended, among other things, that tax administrations should review whether existing legal powers were adequate for audit and forensic examination of POS systems and ESST and consider recommending legislation criminalising the supply, possession and use of electronic sales suppression software.

Australia's Black Economy Taskforce

The Black Economy Taskforce (the Taskforce) was established by the previous Government in December 2016 to:

- Examine evidence on the scope, revenue costs, risks and behavioural factors underpinning black economy activities

- Consider the effectiveness, appropriateness and efficiency of existing policy responses
- Review the black economy efforts of other countries, identifying best practice initiatives which could be applicable to Australia
- Outline an overarching policy strategy to guide current and future policy-making efforts.

In its Interim Report, published March 2017, the Taskforce made several initial recommendations or near-term proposals. The Taskforce noted the 2013 OECD Report and recommended an immediate ban on ESST.

The Taskforce noted that, at the time, the widespread availability and use of such software had been confirmed by a number of international tax jurisdictions and that the OECD had noted legal and technological means to control the proliferation of this software were being used or considered by several countries.

Deficiencies in previous legislative framework

Before the amendments made by Schedule 1 to the *Treasury Laws Amendment (Black Economy Taskforce Measures No.1) Act 2018*, Australia's taxation law contained a variety of offences as well as civil and administrative penalties relating to record keeping and tax evasion (which still exist as supplementary offences that may be relevant to ESST behaviour in particular cases).

These penalties included providing false or misleading information to the Commissioner of Taxation (Division 284 in Schedule 1 to the *Taxation Administration Act 1953*, or TAA 1953) and incorrectly keeping records, including with the intent of misleading the Commissioner (see for example sections 8L, 8Q and 8T, with different fault elements applying to each).

However, the penalties under the TAA 1953 were not considered high enough to adequately reflect the seriousness of the issue – using a tool whose principal function was to misrepresent tax data. For example, an intentional false or misleading statement could under section 8V attract a fine of only 50 penalty units (\$12,600 in 2018) relative to potentially millions of dollars of unreported income. These administrative penalties applied primarily to the users of the sales suppression software, and only if their activity was detected and investigated.

Depending on specific circumstances, manufacturers of sales suppression software could have been prosecuted under other offences, including forgery or providing false documents to the Commonwealth, as well as possessing, making or adapting a device for making forgeries under section 145.3 of the Criminal Code¹ (punishable by imprisonment for up to 10 years).

The Criminal Code also contains more general offences criminalising:

- *General dishonesty*: dishonestly obtaining a gain from or causing loss to a Commonwealth entity, (whether or not the person knew the entity was a Commonwealth entity) (s 135.1)
- *Obtaining financial advantage*: engaging in conduct as a result of which a person obtains a financial advantage from the Commonwealth (whether or not they knew they were receiving it from a Commonwealth entity), which they knew or believed they were not entitled to (s 135.2)
- *Conspiring to defraud*: conspiring with another person with the intention of causing a loss to a Commonwealth entity (whether or not they knew it was a Commonwealth entity) (s 135.4)

1 Contained in Schedule 1 to the *Criminal Code Act 1995*.

- *False or misleading information*: knowingly giving false or misleading information either to a Commonwealth entity or a person exercising powers or performing functions under, or in connection with, a law of the Commonwealth, or in compliance or purported compliance with a law of the Commonwealth (s 137.1)
- *Misleading documents*: producing documents in compliance or purported compliance with a law of the Commonwealth knowing the document is false or misleading (s 137.2)

This suite of offences would appear to provide the Commonwealth with considerable recourse to prosecute ESST-related crimes; however, the practical experience was considerably different.

For instance, these offences have different elements that may or may not be present in a particular case – for instance, electronic point of sale records are not typically Commonwealth documents. These offences normally require the Commonwealth to present sufficient evidence to convict – which is challenging when a key design feature of ESST is the destruction of such evidence. Criminal convictions under these provisions also usually require the Commonwealth to establish some intention or dishonesty on the part of the person.

Further, the mere possession of an ESST was not, prior to the reforms, necessarily an offence until the point that a person used the tool to falsify or destroy tax records, despite that the only function of an ESST by definition is to do this.

Given the destruction of primary evidence, to successfully prosecute a case requires a material resource commitment and significant analysis to establish that a form lodged with the ATO was incorrect, essentially requiring an audit to forensically examine and analyse all relevant systems and financial records to reconstruct the activity, which requires considerable specialist expertise and technical capability.

Where the manufacture and/or supply of an ESST is undertaken from a jurisdiction outside of Australia it is difficult for the ATO or Commonwealth authorities to investigate and apply prosecutions or penalties for those that reside and operate outside an Australian jurisdiction. It can be challenging to obtain evidence on electronic records involving data sources held in offshore jurisdictions or where the money flow involves jurisdictions outside of Australia. This is resource intensive and requires the support of international counterparts.

Different maximum penalties (as well as precedents for setting penalties) also apply to each offence in ways that may not always reflect the seriousness of possessing or distributing ESST; technology that has no other function than to evade taxation.

But, ultimately, the most significant challenge when dealing with penalties associated with electronic sales suppression is the ability to detect. The evolving nature of technology within the shadow economy provides challenges to tax administrators, particularly around detection, which is intrinsically linked to ability to apply penalties. The magnitude of the penalty is less relevant if the public has limited confidence that it will be applied due to the inability to detect the activity. Further, the imposition of a penalty may have limited impact to deter others where the legislation is deficient in requiring the sales suppression functionality from ceasing or being removed.

Government response and legislative amendment

In the 2017–18 Budget, the previous Government announced its decision to accept the Taskforce recommendation and specifically prohibit this technology and software. On 7 February 2018, the Treasury Laws Amendment (Black Economy Taskforce Measures No. 1) Bill 2018 (the Bill) was introduced to Parliament. Schedule 1 to the Bill introduced new offences specifically addressing the production, use and distribution of ESST, defined in the Bill as “electronic sales suppression tools”.²

Specifically, the Bill contained new offences criminalising:

- manufacture, development or publication of electronic sales suppression software (with a maximum penalty of up to 5,000 penalty units, or \$1,050,000 in 2018);³
- acquisition, possession, or control of electronic sales suppression software (500 penalty units, or \$105,000); and
- falsification of tax records using electronic sales suppression software (1,000 penalty units or \$210,000).

Strict liability was to attach to the above offences. This means proof of fault would not be necessary in making a prosecution under them, but a person would not commit an offence if they could prove that they made an honest mistake of fact. Someone who assisted the commission of an above offence could also be charged under the Criminal Code.⁴

The Bill also proposed parallel administrative penalties for manufacture, development or publication (60 penalty units or \$12,600), possession and control (30 penalty units or \$6,300), and falsification of tax records (60 penalty units or \$12,600), as well as aiding, abetting or counselling the course of conduct that would result in an administrative penalty for production, supply, possession or use (with the same penalty as for that course of conduct).

For further information on the provisions as enacted, please see Appendix – Summary of relevant provisions (page 16).

The Senate Standing Committee for the Scrutiny of Bills raised concerns about the appropriateness of imposing strict liability for offences whose penalties could reach \$1,050,000;⁵ however, the Parliamentary Joint Committee on Human Rights, on receipt of a Ministerial response, considered these offences were compatible with the presumption of innocence.⁶

The then-Opposition, now the Government, tabled an amendment that created an obligation to conduct a review of the introduced provisions, given the Parliamentary debate. This amendment was agreed to and incorporated into the final Bill.

The Bill as amended passed both Houses of Parliament on 18 September 2018 and received Royal Assent on 3 October 2018 as the *Treasury Laws Amendment (Black Economy Taskforce Measures No. 1) Act 2018* (the Act). The Act commenced the day after Royal Assent, 4 October 2018.

2 Now contained in section 8WAB of the TAA 1953.

3 In 2018, the value of a penalty unit was \$210.

4 Contained in schedule 1 to the *Criminal Code Act 1995*.

5 Senate Standing Committee on the Scrutiny of Bills, Digest 3 of 2018.

6 Human Rights Scrutiny Report, Report 4 of 2018 [2.230]-[2.231].



The requirement for this Report

Consistent with the amendments referred to above, section 4 of the Act requires the Minister to cause a review of the operation of Schedule 1 to the Act, which introduced these new offences and penalties. The review was to start as soon as practicable after two years after Royal Assent (that is, after 4 October 2020) with a written Report to be prepared.

Accordingly, this Report has been prepared jointly by the Treasury and the Australian Taxation Office (ATO), following a review by both into the administration of the new offences and ATO enforcement action relating to ESST behaviour.

Commencement of the review has been unavoidably delayed alongside a large number of government activities in the context of the response to the COVID-19 pandemic. This has made it impracticable to conduct a review addressing the required topics until this point. However, this delay provided an opportunity to gather additional data that has been presented in this Report.

The Minister is required to cause this Report to be tabled in each House of Parliament within 15 sitting days of each after the day on which the final Report is given to the Minister.

Enforcement action

Before the introduction of new laws, in 2017–18, the ATO conducted a pilot program which, while very small, still successfully confirmed that ESST was being used in Australia. This pilot highlighted the importance of taking a tailored compliance approach to detect, engage with and prosecute ESST users, distributors and manufacturers given concerns regarding the preservation of evidence.

Since the introduction of the new powers in the 2019–20 financial year, the ATO has focused its efforts in addressing ESST behaviour as part of the broader Shadow Economy Program, with specific resources dedicated to address the risk. In the 2022–23 October Budget, the Government extended this Program for three years from 1 July 2023.

These resources have been applied given the strategic intent to address the ESST risk. This has not only supported delivery of compliance cases and tax adjustments but contributed to a range of other tactics that focus on sustainable disruption of the entire ESST supply chain and changing behaviours.

To support these compliance activities, the ATO has required longer cycle times for analysis to identify suppressed income and undertake the necessary examination to gather evidence of possession, use of, and aid/abetting the possession or use of sales suppression technology.

The ATO's compliance activities to date have identified and confirmed a range of shadow economy behaviours predominately across small businesses where POS systems have been identified as supporting suppression.

However, traditional benchmarking and risk modelling alone cannot be relied on to identify highest-risk sectors as they provide a distorted view – that is, since the function of ESST is to alter sales records, widespread use can undermine the reliability of the very benchmarks used to assess particular businesses or industries to identify unusual or problematic behaviour.

The below table breaks down the number and amount of penalties and prosecutions across each sub-category of offence. The data focuses on the specific offences inserted by the Act, rather than the general pre-existing provisions referred to above.

Table 1: Breakdown in penalties and prosecutions for each sub-category (2020–21)

Type	Number	Amount (\$)
Possession	10	63,000
Use	8	489,960
Aid/Abet – Possessions	6	175,960
Aid/Abet – Use	7	252,000
TOTAL	31	971,920

The ATO has found that successfully applying an ESST penalty requires a significant investment in resources and analysis of the taxpayers' affairs. There are significant difficulties in gathering sufficient evidence to support the enforcement decision, given it is common for an ESST itself to delete the audit trail that the ATO would ordinarily rely on to take and justify compliance action. Highly trained ATO officers are required to gather information from many sources to corroborate the existence, manufacture, sale and use of ESST.

The ATO needs to establish whether the software in question meets the threshold definition of "electronic sales suppression tool" which the specific offences in question rely on – as is set out in more detail in Appendix A; to meet the definition, the software must not only be capable of falsifying

relevant records but a reasonable person would conclude this is one of its functions.⁷ This can require detailed forensic analysis and financial record comparison, which can involve computer programming and coding analysis, to identify whether the device, software program or other thing, a part of any such thing, or a combination of any such things or parts, have the capability and principal function of interfering with sales records electronically.

Where the ATO identifies actual or suspected ESST use, detailed compliance action is undertaken to identify both cash and electronic sales suppression across businesses. The use of ESST not only supports the suppression of income across businesses and the individuals associated with them; ESST also can facilitate the payment of cash wages and the subsequent noncompliance with employer obligations such as PAYG withholding and payment of superannuation.

Where ESST behaviour is identified, this makes it more likely that the ATO will identify omitted income risks and tax shortfalls compared to other shadow economy risks or behaviours. Currently, the average expected return per case is also higher when compared to other shadow economy cases. ESST compliance does, however, involve longer cycle times for the ATO, and requires more expertise and capability from audit staff and digital forensic/e-audit staff. There is also a greater workload and level of analysis required to support primary assessments and the application of ESST penalties.

Table 2: Estimate of amount of revenue recovered or preserved (2021–22)

Completed cases	Liabilities raised (\$)
46	7,356,000

The ATO has also identified that businesses possessing or using ESST have a higher propensity, when provided with advance notice of ATO action, to destroy or hide records (e.g. updates to systems are undertaken with a lack of an audit trail) and a higher propensity to exhibit behaviour to dissipate assets. The ATO’s methodology and approaches therefore have evolved to ensure that they assess risk factors and adapt methodologies and approaches accordingly.

The ATO can find it difficult to recover tax revenue with current limitations on its ability to secure and recover debt. Insights across some case work has identified assets held offshore contributing to the complexity and their ability to recover. Further, due to the deliberate efforts to suppress sales, there has been a higher propensity to wind up companies and dissipate assets.

⁷ See section 8WAB of the TAA 1953 as inserted by the Act.

Australian Observations

Evolution of ESST

Traditionally, ESST has been embedded in and focused on manipulating POS software; however, the ATO has also observed ESST which is embedded into other parts of clients' electronic systems, including very sophisticated components and coding to hide the technology that requires analysis of the taxpayer's broader computer architecture and countering the ESST's in-built anti-detection and anti-forensic mechanisms.

More broadly, ESST is constantly evolving and can include:

- cloud based software that works with the POS system
- use of encryption software to conceal documents from the Commissioner
- remote access that can facilitate individual and bulk deletions from mobile devices, such as phones, from anywhere in the world in real time
- concealed phantomware and programs that enable rapid removal or alteration of data by either a portable device (USB) or an external/cloud-based service
- suppression of HR and payroll data (for example within HRIS Systems) which enables falsifying employee and wage records
- digital sources relating to ESST which can be located in computer hard drives, operating systems, servers, software, program coding, log entries, POS Systems, communication, and external devices where most can only be identified by digital forensics experts undertaking imaging activities.

We are particularly concerned with new sales suppression techniques that have emerged that allow for sales suppression through a foreign 'zapper' to operate over the internet, and which allow for the same activities of alteration, deletion, replacement, and manipulation of sales data (zappers are a form of ESST but are not installed on the machine but are stored on removeable media or in this case through the internet, so are not present during normal use). This software also allows for remote crashing of hard drives, making the verification of accurate records extremely difficult for taxation officials.

However, it is evident that these developments represent ongoing and deliberate action by software developers to frustrate the proper administration of the tax system. This is consistent with a premise that ESST is inherently designed to commit tax fraud, and therefore it is reasonable that the onus of proof has been reversed such that the manufacture, distribution, possession or use of this software is due to a general intention to commit tax fraud, unless the taxpayer provides evidence otherwise.

Shadow economy behaviours observed

Unfortunately, the ATO has observed a greater use of sales suppression technology generally, and instances of rapid growth in the number of businesses being supplied and using this technology. The technology facilitates other shadow economy behaviours where the correct amount of tax is not being reported. Such behaviours observed by the ATO include:

- Low household income reported for associates (public officers/family members) that is not commensurate with lifestyle expenditure

- Asset accumulation of associates (public officers/family members) not corresponding with income reported
- Very low cash sales and wages reported compared to income identified through analysis of financial information
- Purchase and/or fit out of new businesses where business income was insufficient to afford costs of upgrades/purchases
 - Some cases included purchases of two or more businesses within a short time period, for example within a year, and in many of those cases, where the business owner had recently arrived in Australia and then rapidly purchased a business without any/sufficient financial assistance
- Some businesses reporting nil to low levels of cash when industry standards and business operating models support higher levels of cash takings.

Beyond shadow economy behaviours, ATO analysis has also identified indications of more serious criminal activity, including some businesses which are suspected of being involved in money laundering activities across multiple related entities, and the questionable movement of funds to and from overseas. In such instances, the ATO has taken appropriate enforcement action.

Impacts of COVID-19 pandemic

The COVID-19 pandemic has had specific effects both on shadow economy behaviour generally within the Australian community, but also on the uptake and use of ESST.

Anecdotally, and working with OECD partners, the ATO is aware of a 4-fold increase in the use of ESST since the pandemic.

Despite lockdown periods where cash was used less and electronic payment methods were preferred, the ATO still finds cash is prevalent in the economy.

Still, the pandemic caused businesses to become more agile by operating in different ways to remain operational or competitive. In particular, the pandemic shifted many business operating models to a digital environment. This provided ESST more opportunities by creating more avenues to suppress electronic transactions.

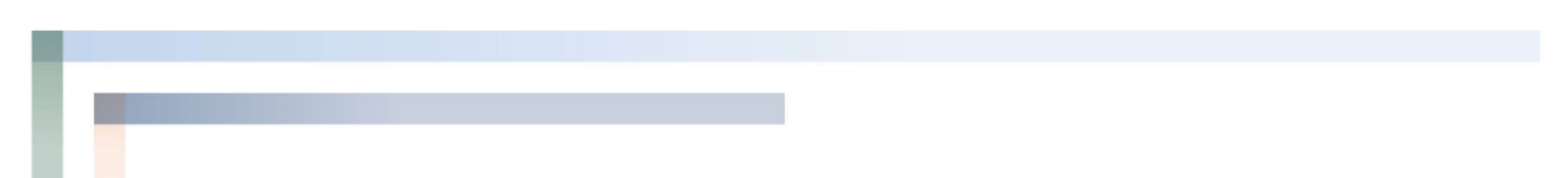
Interestingly, ESST manufacturers also adapted to the post-pandemic operating model by offering more (and more sophisticated) technology that takes advantage of the clients' increased use of electronic payment platforms and their digital operating model.

Overall, particularly since the COVID-19 pandemic, the general risk to tax collection posed by ESST is outside the ATO's risk tolerance.

Appropriateness of criminal vs. civil penalties

When confronting shadow economy risks, including those posed by ESST, there is a critical need to ensure there is a level playing field in order to build confidence that the tax system is fair and applied equally within the community.

The ATO considers it remains important that the ESST risk is addressed by traditional civil compliance action as well as criminal penalties where appropriate. Not only does a traditional compliance strategy ensure the correct amount of tax is paid, it provides leverage to deter others from involvement in such behaviours.



Civil action still deals with those that have used sales suppression and provides valuable insights on vulnerabilities in risk detection, compliance actions, understanding of the rate of growth, the size/scale of the market and aids in developing effective treatment strategies. In more egregious and deliberate situations a complimentary criminal treatment pathway is required to disrupt the entire ESST supply chain to sustainably change behaviours of taxpayers and those who facilitate sales suppression.

This means the ATO considers the administrative penalties accompanying the ESST criminal offences play a crucial role in properly and proportionally managing ESST behaviour and disrupting the supply chain for this technology, by giving the ATO the ability to apply traditional compliance and tax recovery strategies as part of its suite of enforcement tools in a manner targeted to this specific technology.

Penalty effectiveness

To be effective, ESST penalties need to be applied against those supplying, manufacturing, possessing, and using ESST consistently and at all levels throughout the ESST supply chain. As emphasised earlier, a penalty will only be effective if sales suppression can be detected. If there is low community confidence regarding detection, then the deterrence effect of a penalty will be diminished.

A traditional administrative compliance response is not sufficient nor effective in disrupting the entire supply chain or deterring others from engaging in such behaviour alone. The manufacture and supply chain of ESST is well-organised and well-connected. When the ATO considers enforcement action and penalties, therefore, the ATO will generally seek to apply the ESST criminal penalties (as distinct from administrative penalties), but also consider other Criminal Code offences to deal with more serious behaviour and offending. Therefore, a simple compliance response where ESST penalties alone are imposed is not sufficient to deal with the overall risk.

Use of the Commissioners' discretion

The ATO has a general discretion to not seek that civil penalties are imposed by the Courts, as well as the power to remit administrative penalties imposed by law in certain cases, for example in circumstances of genuine mistake.

In the context of ESST, the ATO has not applied its discretion to date (whether because of genuine mistake or otherwise). However, we consider it important that the ATO can assess each situation based on the individual circumstances presented. The ATO may apply the discretion in the future where it is warranted as supported by the associated Practice Statement Law Administration (PSLA).

The ATO has not received any complaints about penalties being applied despite “accidental” possession or use of ESST software.

Regulatory support

The ATO has in place ongoing regulatory strategies that support the prevention of falsifying software and ESST, such as innovative administrative action and consumer messaging campaigns.

ATO web content has been reviewed and updated to provide further awareness and guidance on ESST penalties and the publishing of a PSLA. In addition, a media and communication strategy has been developed and implemented to work with various industry bodies and groups to raise awareness and provide support to the community on where to seek assistance if they suspect a POS system has sales suppression functionality.

International Developments

International Action

Since the OECD's early reporting of this issue, many countries have since implemented new laws, increased penalties and enhanced enforcement.

For example, following advice from Australia and the United Kingdom that a UK-based company may have been selling this software into the New Zealand market, in 2022 New Zealand introduced a suite of new offence provisions imposing criminal penalties on making, selling, or supplying software of up to NZ\$250,000, as well as criminal and civil penalties for possession of up to NZ\$50,000 and NZ\$5,000 respectively. These offences commenced 30 March 2022.⁸

The NZ provisions were explicitly based on the Australian model and the ATO's experience finding users of sales suppression software, charging them with criminal penalties, tracing the software back to the seller, charging the sellers, and then tracing other purchasers of the software.⁹ From an Australian perspective, this is a resource intensive investment but is essential to gather the necessary evidence to undertake either a civil and/or criminal prosecution. Detailed analysis is required to audit businesses suspected or identified as using sales suppression, including analysis of the financial flow of funds for those who have benefited, successful extraction of relevant electronic records (cloud based, remote access and password protected) and subsequent complex and detailed analysis of POS records. This also must take place despite the audit trail of suppressed records often being missing, which makes it more difficult for regulators to pursue criminal charges or commence civil actions.

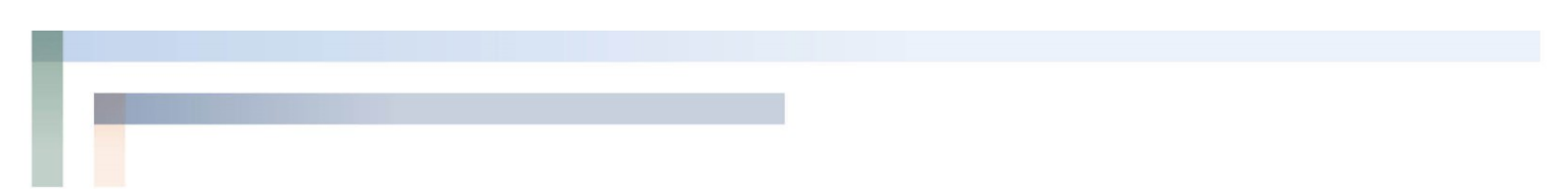
Given the international dimension of the sales suppression software industry, there is accordingly particular benefit in the ATO continuing to work with likeminded countries in investigating and charging offenders who supply such software into Australia. For instance, the ATO has seen the facilitation of sales suppression technology across borders, covering manufacture and/or supply occurring or being supported from overseas. The facilitation of electronic funds transfer suppression often involves the movement of money across borders. This demonstrates a global impact and approach required to disrupt the entire supply chain. However, such operations are particularly sensitive given the technical sophistication of the manufacturers.

Many countries have adapted to the risk presented by ESST and we are aware that a number of other OECD jurisdictions have introduced legislation specifically to ban the use of ESST including:

- New Zealand – introduced new legislation referred to above
- United States – the IRS is now supported by recently-introduced legislation creating monetary penalties, a custodial component and orders to have the technology replaced with a POS that does not contain ESST functionality.
- Canada – the CRA has moved to real time monitoring rather than ESST penalties. Since implementation, they have collected C\$2 billion (about A\$2.3 billion) from the restaurant sector over 8 years with the introduction of sales recording modules.
- United Kingdom – civil based legislation has been introduced that penalises where an ESST is identified.

8 See *Taxation (Annual Rates for 2021–22, GST, and Remedial Matters) Act 2022* (NZ).

9 New Zealand Inland Revenue, Regulatory Impact Statement: Sales suppression software, 1 June 2021 at [21]-[22].



The ATO has been working closely with several OECD partners sharing concerns regarding the growing and global impacts of digital fraud facilitated through ESST. It is a shared view of OECD partner agencies that the complexity and size of the problem is growing as technology rapidly adapts making it harder to detect. It is also evident that, despite inherent difficulties detecting general use of ESST, there is a rate of growth in the number of businesses using the technology. It is also recognised amongst OECD partners that specific skill sets and capabilities are required deal with ESST risk. That includes specialist support and capability with digital forensic staff and audit expertise to effectively identify and deal with sales suppression technology. Shared amongst OECD partners is the growing impact of sales suppression on the respective tax gap.

Subsequent OECD research

OECD research since the 2013 OECD Report has focused predominantly on other non-legislative and innovative technological strategies to address ESST risk.

For example, the OECD's Technology Tools to Tackle Tax Evasion and Tax Fraud,¹⁰ published on 31 March 2017, focused on technological solutions. Based on the principle that tax crime facilitated by technology requires a technology response, this report notes the particular utility of data recording technology, such as fiscal devices, sales data controllers, or sales recording modules. This technology generally connects directly to or integrates directly with POS systems and records and secures sales data immediately as the transaction occurs and in a manner that is tamper proof, with different types available. This technology has potential to raise significant revenue. This report gives several international examples, some notable examples including:

- In Canada, the introduction of sales recording modules in the restaurant industry (see above)
- In Sweden, since 2010 until publication, 135,000 registers had been connected to a fiscal control unit (supported by legislation), causing increased VAT and income tax revenues of SEK3 billion (about A\$425 million) per annum, as well as reportedly leading to better control measures for the Swedish Tax Agency.

On 28 March 2019, the OECD's Forum on Tax Administration followed up the above with a report Implementing Online Cash Registers: Benefits, Considerations and Guidance.¹¹ The more limited objective of this report was to provide insight for tax administrators into implementing online cash registers and other POS software that has direct online connectivity with the tax administration, so sales data is shared in an automated and systematic manner with the tax administration, either pushed by the sales system itself or by the tax administration on demand.

This report, like the previous report, also sets out examples of countries' similar approaches, such as compulsory certification and registration of cash registers (Belgium), voluntary quality-marks signifying cash registers meet regulatory requirements (Netherlands), and compulsorily upload of sales data to central registers accompanied by QR codes on receipts that enable customers to cross-check transactions (Russia). The report details some of the costs accompanying the considerable potential benefits, particularly privacy risks and administrative costs for both business and administrators.

10 Available at <https://www.oecd.org/tax/crime/technology-tools-to-tackle-tax-evasion-and-tax-fraud.htm>.

11 Available at <https://www.oecd.org/ctp/implementing-online-cash-registers-benefits-considerations-and-guidance.htm>.

Summary and Key Findings

In conclusion, this Report has outlined that the introduction of stronger penalties for possessing, manufacturing or distributing sales suppression software arose from growing international concern about the potential scale of tax avoidance, as well as concern of the adequacy of Australia's relevant enforcement laws and mechanisms.

This Report finds that, since the introduction of significantly stronger penalties and relevant law change via the Act, the ATO has conducted significant effective compliance action. As at late 2022, 46 cases have been completed, applying around \$1 million in penalties and raising some \$7.4 million in liabilities. Additional cases are still underway and further enforcement activity is planned.

Despite concerns raised during the parliamentary debate, the ATO has not detected any instances, nor received any complaints about, "accidental" possession of sales suppression software.

Further compliance action is required to bring this risk within tolerance, that includes disrupting entire supply chains, dealing with those who are involved in developing sales suppression technology, providing help and guidance for those who want to do the right thing and influencing/shaping behaviour away from use. The ATO will continue to work proactively with OECD partners to manage and disrupt international behaviour driving ESST manufacture, distribution and use.

The risk and impacts of sales suppression technology continues to exist in the shadow economy and is a contributor to the tax gap. Since the Act was introduced in October 2018, the scale and complexity of ESST use has grown. There is difficulty in investigating ESST; treatment covers prevention through to correction and there needs to be a mix of many tactics to underpin proactive enforcement.

International research and developments have also focused on additional technological solutions to address ESST risks, and as other countries begin implementing these approaches their experiences will be followed closely.

Appendix – Summary of relevant provisions

The offences were inserted into the *Taxation Administration Act 1953* (TAA 1953), with minor consequential amendments to the *Income Tax Assessment Act 1997*. References to sections are to the TAA 1953. For more information, see the Act and the Explanatory Memorandum (EM) for the Bill on the Federal Register of Legislation: www.legislation.gov.au.

Definition of electronic sales suppression tools

The offences and penalties relate to the production, supply, possession and use of “electronic sales suppression tools” (ESST).

Section 8WAB defines this, for the purposes of the inserted offences or penalties, as devices, software programs or other things (or parts of things, or a combinations of any such things or parts), that meet the following conditions:

- it is capable of falsifying, manipulating, hiding, obfuscating, destroying, or preventing the creation of, a record that an entity is required by a taxation law to keep or make, and is, or would be, created by a system that is or includes an electronic point of sale system; and
- a reasonable person would conclude that one of its principal functions is to falsify, manipulate, hide, obfuscate, destroy, or prevent the creation of, such records.

As is explained more fully in the EM, this provision is carefully drafted to ensure that component parts of software with the primary or principal function of falsifying (etc) tax records are considered ESST, while ordinary parts or components of software which could be used to falsify (etc) with effort, but whose primary function was not ordinarily to be used that way, were not (noting this use may be captured by other offences). The definition also captures tools that modify records that are used as inputs in making tax records, for example modifying individual sales records used to aggregate sales data.

Offences

Production and supply

Section 8WAC makes it an offence to manufacture, develop, or publish an ESST. Given the definition of ESST, this also captures the manufacture (etc) or enhancement, e.g. updating, of component parts of ESST. The section also makes it an offence to supply, make available for use, or provide a service involving the use of ESST. This is intended to capture various actions that facilitate the use of ESST (for example, to make ESST available on a website as a ‘zapper’).

The maximum penalty that can be imposed for this offence is 5,000 penalty units. The current value of a penalty unit is set out in section 4AA of the *Crimes Act 1914*, as indexed, and is \$222 per unit; however, the 2022–23 October Budget announced an increase to \$275.¹² Using that amount, therefore, the maximum penalty under section 8WAC is \$1,375,000. This is aligned with the maximum penalty for tax exploitation schemes under Div 290 of the TAA 1953 (for individuals; the maximum for

12 See the measure, “Commonwealth Penalty Unit – increase in amount” in the 2022–23 October Budget, Budget Paper 2, page 6.

companies is 25,000 penalty units, or \$6,875,000), and for breaches of directors' duties under the *Corporations Act 2001*.

The offence applies to persons or entities outside Australia if the ESST is used to modified records required to be kept under Australian law or supplied (etc) to an entity required to keep records under Australian law. For reasons discussed in this Report, it is important for the ATO to be able to trace ESST discovered back "to the source", in order to identify and prosecute other users and/or notify OECD partners.

Under the general criminal law (specifically section 12 of the Criminal Code), someone who assists someone else to commit the above offence themselves commits the offence.

Strict liability applies to both offences. This means, in any prosecution, it is not necessary for the ATO to establish fault if a person has manufactured (etc) or supplied (etc) ESST or a component part, or knowledge about the intended falsifying or fraudulent use of the ESST or component part.

Acquisition, Possession or Control

Under section 8WAD, a person commits an offence if they both:

1. are required under, or pursuant to, a taxation law to keep or make a record; and
2. acquire or have possession or control of an ESST or have a right to use one.

For (1) above, "taxation law" means under the TAA 1953 any law that the ATO has general administration of, with the exception of excise laws (as excise is levied at the point of manufacture and distribution, not sale).

The maximum penalty that can be imposed is 500 penalty units. The maximum penalty is lower for this offence than for production and supply as the latter facilitates the commission of multiple offences.

As with the production and supply offences, someone who assists someone else to commit this offence themselves commits the offence.

Strict liability also applies to this offence.

Use

Section 8WAE makes it an offence where:

1. a person is required under, or pursuant to, a taxation law to keep or make a record; and
2. the record is kept, made or altered with the use of an ESST, or is prevented by the use of an ESST from being kept, made or altered; and
3. as a result of the use, the record does not correctly record and explain the matter, transaction, act or operation to which it relates; or the person does not keep or make the record in accordance with the taxation law.

As the EM explains, this offence is designed so that someone else other than the person who is required to keep records under a taxation law can be the one who actually used the tool to falsify those records. For example, a company under an obligation to keep the records could be charged even if an employee or third party actually caused the tool to falsify the records (although that employee or third party may be captured as well).

As noted above concerning acquisition, possession or control, "taxation law" means under the TAA 1953 any law that the ATO has general administration of, with the exception of excise laws.

The maximum penalty that can be imposed is 1,000 penalty units. This is higher than the acquisition, possession or control offence above as this offence involves actual use of ESSTs to falsify tax records.

This offence operates alongside other general offences in the TAA 1953, including sections 8L, 8Q, 8T and section 382-5 in Schedule 1, but with a higher maximum penalty. This better reflects the seriousness of using software designed to falsify tax records and to supply an increased deterrent effect against acquiring, possessing and using these tools.

As with the other above offences, someone who assists someone else to commit this offence themselves commits the offence.

Strict liability also applies to this offence.

Defences

As noted above, all these offences are strict liability offences. This means that it is not necessary for the prosecution to establish fault (intention, knowledge, recklessness, negligence, or otherwise) – for example, that a person knew that tax records that they were required to keep had been modified with an ESST by someone else.

However, a person would not be criminally responsible if they were able to prove an honest mistake of fact under section 9.2 of the Criminal Code. This would include (section 9.2(1)) where although they were in fact obliged by a taxation law to keep tax records and they physically possessed an ESST (for example, for the purposes of section 8WAD), they had considered whether or not this was the case, and were under a mistaken but reasonable belief that either of those facts weren't the case (in this example, either possessing an ESST or being obliged to keep records).


There is also a defence intended to apply where, for example, a person had reasonably thought their recordkeeping was correct (for instance, following a recent audit of their computer software) but it was ultimately incorrect due to events occurring without their knowledge (such as an employee installing ESST) and there was no reason to believe, and nothing to suggest, that things had changed since the audit (for instance, the business' accounts seemed consistent with real activity). This is because of the general defence in section 9.2(2) of the Criminal Code where, in brief, someone considered circumstances earlier, and thought wrongly that circumstances were the same when the underlying offending occurred.

There are also specific defences against the production, supply or possession offences where the underlying conduct was done for the purpose of preventing or deterring tax evasion or for the enforcing of a taxation law. This is intended to capture where, for example, a third party software developer develops and supplies ESST solely for law enforcement to use for training exercises.

Civil penalties

The Act also added administrative penalties that parallel the above offences, specifically applying where people:

1. manufacture, develop or publish ESSTs or supply or make tools or services involving those tools (up to 60 penalty units, or \$16,500 at 1 January 2023)
2. are required to keep records under a taxation law, and either acquire, possess or control an ESST (up to 30 penalty units, or \$8,250 at 1 January 2023) or keep, make or alter such a record with the use of an ESST in a way that results in the record being incorrectly kept or not being made or kept (up to 60 penalty units, or \$16,500 at 1 January 2023).



Section 8ZE of the TAA 1953 applies to these penalties such that if a criminal prosecution commences in respect of the underlying conduct, these penalties can be applied.

These penalties are higher than pre-existing penalty units that continue to operate alongside the above. The maximum penalty unit for these was only 20 penalty units (only \$5,500 at 1 January 2023), which for the reasons above did not provide sufficient deterrent effect.

The above defence in relation to preventing or deterring tax evasion or enforcing a taxation law also applies to these penalties. There is no defence of honest mistake of fact as with the criminal offences, however the ATO has a general discretion not to impose penalties in these cases.

Penalties can also apply to aiding, abetting, or counselling another entity in undertaking conduct that would result in an administrative penalty for the production, supply, possession or use of an ESST, in a way analogous to how people assisting others to commit the criminal offences can themselves be liable for those criminal offences.

Transitional provisions

The Act contained transitional provisions to provide persons the opportunity to avoid liability for these offences and administrative penalties if they notified the ATO that they had an ESST as soon as practicable after the Act commenced and complied with any ATO direction about how to deal with the tool.

These people may have been liable for any previous offending against pre-existing offence provisions; these transitional provisions were only intended to provide an opportunity to avoid liability under the new offences and penalties if they took reasonable steps after the measure was announced in the 2017–18 Budget.

