Regulatory Impact Statement: Sales suppression software

Coversheet

Purpose	
Decision Sought:	*Introduce penalties for the supply, possession, and use of sales suppression software*
Advising Agencies:	*Inland Revenue*
Proposing Ministers:	*Minister of Revenue*
Date:	*1 June 2021*

Problem Definition

Inland Revenue has been informed that overseas businesses may be selling sales suppression software (software which alters sales data for the purpose of evading tax) is being made available to businesses in New Zealand. This software is relatively new to New Zealand and existing tax law appears insufficient to deter its spread in the New Zealand tax base.

Executive Summary

Sales suppression software appears relatively new to New Zealand, and its distribution is not expressly covered in existing tax law. Using the software is a form of tax evasion, and users could be penalised on that basis. However, it is not currently an offence to make, sell, buy, or possess the software, meaning that the software can spread in the tax base without repercussions, to the point where removing it from the base is likely to be very difficult. Action is required to give authorities the legal tools to deter the spread of the software.

Overseas jurisdictions have employed two broad methods to curtail the spread of sales suppression software. The first approach uses penalties (both civil and criminal) that are targeted at taxpayers who make, sell, acquire, possess, or use the software. The second approach is regulating point-of-sale systems used in the country to ensure that the systems are incompatible with sales suppression software. Given that the problem appears new to New Zealand (and evidence suggests there is little market penetration) and the compliance costs of regulation are high, we currently favour the penalty approach over a regulatory regime.

A penalty regime carries minimal compliance costs for taxpayers who are not using the software, and its administrative costs can be absorbed within Inland Revenue's existing investigation and prosecution functions. Working properly, penalties should sufficiently deter taxpayers from supplying, acquiring, or using sales suppression software that the

software is unable to take a deep hold in New Zealand, thereby maintaining the integrity of the tax base and ensuring a level playing field for taxpayers.

Limitations and Constraints on Analysis

The problem being addressed is new to New Zealand, and as such our proposal is not constrained by Ministers' commissioning or by any prior policy decisions. To some extent, it is constrained by legal norms for offences and imposing penalties.

We do not have data on the existing reach of sales suppression software in New Zealand. Although this software has been around internationally in various forms for some time there is no evidence that it has become prevalent in New Zealand yet. This assumption has been formed from discussions with relevant Inland Revenue staff including staff responsible for review and audit of businesses which would be expected targets of sellers of sales suppression software.

As the subject matter is sensitive, we have not widely consulted on this issue. We have consulted with the Ministry of Justice, the Treasury, the Department of Internal Affairs, and Inland Revenue internal experts on evasion and sales suppression, as well as officials from the Australian Taxation Office. We have also discussed the issue with Chartered Accountants Australia and New Zealand and the New Zealand Law Society. Consulted parties support the Government taking steps to respond to the issue and, in general, are supportive of the preferred option.

Responsible Manager(s) (completed by relevant manager)

Paul Fulton

Principal Policy Advisor

Inland Revenue

1 June 2021

Quality Assurance (completed by QA panel)

Reviewing Agency:	Inland Revenue
Panel Assessment & Comment:	The Quality Assurance reviewer at Inland Revenue has reviewed the *Sales suppression software* RIA prepared by Inland Revenue and considers that the information and analysis summarised in the RIA meets the quality assurance criteria.

Section 1: Diagnosing the policy problem

What is the context behind the policy problem?

1. Inland Revenue has been informed by competent authorities[1] from Australia and the United Kingdom that a UK-based company may be selling sales suppression software to hospitality businesses in New Zealand. Sales suppression software systematically alters point-of-sale data collected by a business in order to understate or completely conceal revenues for the purpose of evading tax.

2. The OECD has identified a number of risks for tax administrations arising from the vulnerability of electronic cash register data to sales suppression software and consequent under-reporting of income. Overseas jurisdictions have reported significant revenue losses to software-enabled tax evasion in cash-heavy business sectors such as hospitality and retail. A 2013 OECD report[2] recommended tax administrations consider criminalising the providing or possession or use of electronic sales suppression software.

3. Sales suppression software appears to be new to New Zealand, and it is not covered by New Zealand's existing regulatory systems. There are only limited mechanisms to prevent the software from spreading through the New Zealand tax base. While its usage is a form of tax evasion and could be penalised as such, it is not illegal to manufacture, sell, supply, acquire, or possess the software. Existing promoter penalties cannot be applied to suppliers of sales suppression software as they only apply to promoters of tax avoidance arrangements, rather than evasion. This means Inland Revenue has limited means of prosecuting or penalising software suppliers, which is likely the most efficient method of deterring the software's spread.

4. Left unchecked, sales suppression software risks becoming embedded in New Zealand businesses. There are strong incentives for businesses in cash-heavy sectors to adopt the software; as businesses using software to suppress their sales data will be able to evade their tax obligations, they will have an advantage over their rivals who are not using software. This will create pressure on businesses to adopt the software to stay competitive with their rivals, which endangers taxpayers' voluntary compliance with their obligations.

---

[1] A competent authority is a person in a revenue agency who, amongst other tasks, can share relevant information with other tax jurisdictions.

[2] https://www.oecd.org/ctp/crime/ElectronicSalesSupression.pdf

What is the policy problem?

5. Sales suppression software presents a threat to the integrity of the New Zealand tax system. It provides an easy-to-use, difficult-to-trace mechanism for businesses to reduce their income tax and GST liabilities. In this way, sales suppression software undermines the principles of voluntary compliance and self-assessment; it provides both method and motive for a taxpayer to be non-compliant and reduces Inland Revenue's ability to detect instances where taxpayers have incorrectly self-assessed their income.

6. As business income tax and GST taken together constitute a major portion of government revenue, spread of the software among businesses may lead to material reductions in revenue. OECD data suggests that revenue losses from sales suppression software can be very high.[3] For instance, Revenu Québec estimated Québec's tax losses to sales suppression software at $CA417 million in 2007-2008, while a professor at Boston University estimated in 2017 that up to $US20 billion of state sales tax revenue may be being lost per annum across US states. During 2006-2010, Sweden's tax agency audited a variety of industries including hairdressers, clothing stores, and food stores, and showed that businesses in these industries were routinely under-reporting 20-40% of their turnover.

7. The spread of sales suppression software throughout the New Zealand tax base could pose similar major revenue losses to those that have been reported in other jurisdictions. The Crown's income tax and GST intake would be reduced as the tax base diminishes, which will have implications for government spending on other issues.

8. The widespread presence of sales suppression software in the New Zealand tax base would also create horizontal equity issues, as the software allows certain taxpayers to artificially reduce their tax bill, creating unfairness between compliant businesses and offending businesses. This would also lead to imperfect competition, as businesses using the software to commit tax evasion would be at an advantage over rival firms which are compliant with their tax obligations. This would create pressure on compliant firms to adopt the software to keep up with their competitors, further eroding the principles of voluntary compliance on which the New Zealand tax system is based.

What objectives are you seeking in relation to the policy problem?

9. Prevent spread of sales suppression software in the New Zealand tax base.

10. Minimise taxpayers' ability to use sales suppression software.

11. Minimise compliance burden on taxpayers who are following the rules.

12. Minimise administrative costs of ensuring compliance.

---

[3] E.g. *Electronic Sales Suppression: a threat to tax revenues (2013)*, pp.6-7 and corrigendum.

Section 2: Deciding upon a preferred option to address the policy problem

What criteria will you use to compare options to the status quo?

13. The criteria being used to consider the options are as follows:
    a. Sustainability of the tax base
    b. Compliance costs
    c. Administration costs

What scope will you consider options within?

14. Our options are not constrained by any previous policy decisions or legislation.

15. We have refined our approach to penalty setting following engagement with the Ministry of Justice. Additionally, we have consulted with the Department of Internal Affairs, the Treasury, Chartered Accountants Australia and New Zealand, and the New Zealand Law Society – these discussions have informed our response.

16. Experience from other countries, particularly Australia, Canada, and the United Kingdom, has been considered in determining our options. We have also considered relevant material published by the OECD.

17. Options considered to address the issue fall broadly into two categories:
    a. a penalty response illegalising various activities in relation to sales suppression software
    b. a regulatory response that places standards on EFTPOS machines sold in New Zealand which prevent taxpayers from using the software.

18. These two options are based on approaches taken by other jurisdictions to address this issue.

What options are you considering?

Option One – Counterfactual

19. The counterfactual is that the government takes no additional regulatory action to prevent the spread of sales suppression software. Although Inland Revenue can to an extent mitigate the spread of software through its existing evasion penalties, this is unlikely to be sufficient to deter its spread altogether. There is a major risk that the software would spread through the tax base and undermine its integrity, potentially leading to significant revenue losses in income tax and GST.

Option Two – *Penalty regime*

20. This option would introduce civil and criminal penalties to make manufacturing, selling, providing, acquiring, or possessing sales suppression software illegal. As usage of the software is inarguably a form of tax evasion, a separate penalty for this is not needed.

The new penalties allow Inland Revenue to target suppliers of software, which is likely to be a more efficient means of preventing the spread of the software than prosecuting end-users under existing evasion penalties. The desired outcome is that taxpayers are deterred from adopting the software, maintaining the integrity of the tax base.

21. The proposed approach introduces criminal penalties on making, selling, or supplying the software of up to $250,000. It also introduces criminal penalties for acquiring or possessing the software of up to $50,000, and a civil penalty for the same behaviour of $5,000. The maximum penalty of $50,000 proposed for the criminal penalty for acquisition or possession is intended to be on par with the maximum penalty for evasion or similar offence,[4] while the criminal penalty of $250,000 proposed for making or selling software is set in line with the Australian model, which imposes a penalty for making or selling at a rate five times that of the penalty for usage.[5]

22. This approach is based on the Australian Taxation Office (ATO)'s experience in applying similar penalties. The ATO's approach is to find users of sales suppression software and charge them with criminal penalties, trace the software back to the seller and charge them as well, and then trace the seller's sales down to other purchasers of the software. However, as the ATO has noted that these purchasers are generally very high in number, they advise us that the cost-effective approach is to levy civil penalties against these users *en masse*, rather than take them individually through the Courts. At its discretion, Inland Revenue can prosecute major offenders identified in this way using criminal penalties, while applying the civil penalty against smaller offenders (in addition to evasion shortfall penalties where applicable). Consistent with existing shortfall penalties, the civil penalty will be reduce or eliminated if a taxpayer with the software makes a voluntary disclosure.

23. It is also proposed to specifically remove eligibility for the existing 50% reduction of the civil evasion penalty for prior behaviour when the evasion included use of sales suppression software. This is because the prior behaviour reduction is intended to take into account situations when a taxpayer has no prior history of non-compliance. However, evasion involving sales suppression software requires the taxpayer to acquire the software (itself a premeditated act of non-compliance) and therefore already establishes a history of non-compliance with their obligations under the Inland Revenue Acts.

24. A sufficiently robust penalty regime increases the financial risk of selling and owning sales suppression software. The purpose of this is to deter taxpayers from engaging in these behaviours. There are limits to this effect, as there will be some taxpayers who will take compliance risks if they perceive the rewards are great enough.

---

[4] Refer section 143B of the Tax Administration Act 1994.

[5] Respectively, 5,000 penalty units for making or selling versus 1,000 for usage. A penalty unit is (as of the time of writing, 25 May 2021) worth AU$222 at the federal level, equating to AU$1,110,000 and AU$222,000.

25. We expect the compliance costs for this option are low to non-existent for taxpayers not engaged in offensive behaviour, as they will not need to change their behaviour. Taxpayers who commit an offence and are caught will face high costs, but this is by design.

26. The option requires Inland Revenue to actively audit taxpayers and prosecute offenders. This will impose some administrative costs on an ongoing basis, but these would fall within Inland Revenue's normal auditing functions, so any additional cost is unlikely to be significant.

Option Three – *Regulatory regime*

27. This option would impose regulations on EFTPOS machines sold in New Zealand to make these machines incompatible with sales suppression software. Businesses would be required to upgrade their systems in line with these new regulations.

28. A number of models exist overseas which we could base our approach on, including so-called "fiscal till" systems (used by jurisdictions such as Argentina, Bulgaria, Lithuania, and Russia) and "certified" cash register systems (used by e.g. Belgium, Greece, and Sweden). There are differences between the two approaches, but in essence they both place requirements on cash registers used in certain industries to store, track, and upload sales data in secured formats and/or to secure servers.

29. The Dutch government has taken a voluntary compliance approach to regulation through its Keurmerk (Quality Mark) system, establishing an industry body with representation from the Belastingdienst (the Dutch tax authority) and point-of-sale system manufacturers to set quality standards for systems sold in the Netherlands. Compliant systems receive a Keurmerk label; businesses using these systems are considered lower risk under the Belastingdienst's fraud risk management systems.

30. A regulatory option is likely to go farthest in preventing the spread of the software and protecting the integrity of the tax base, as it makes the software incompatible with business point-of-sale systems and thereby removes its usefulness. However, the option is likely to impose significant compliance costs on all businesses, even those not using sales suppression software, as all businesses would need to upgrade or replace their systems to meet the new regulatory standards. The option also has relatively high initial administrative costs, as the government must design a set of regulatory standards that meet the policy objective.

How do the options compare to the counterfactual?

	Option One – *Counterfactual*	Option Two – *Penalty regime*	Option Three - *Regulatory regime*
Compliance costs	0	0 *Businesses not using software will not need to alter their behaviour.*	- - *Businesses will need to replace their point-of-sale software, imposing high costs.*
Administrative costs	0	0 *Administrative requirements are largely already met by existing Inland Revenue functions.*	- *Setting regulations will require high upfront effort, but this cost will diminish over time.*
Sustainability	0	+ *A penalty regime will discourage sale or purchase (but some taxpayers may risk it).*	++ *Regulations will greatly reduce utility of the software, discouraging uptake.*
Overall assessment	0	++ *This option is effective while having a low compliance/administrative cost.*	+ *This option is likely to be extremely effective but comes with high costs.*

Key:

++	much better than the counterfactual
+	better than the counterfactual
0	about the same as the counterfactual
-	worse than the counterfactual
- -	much worse than the counterfactual

What is your preferred option?

31. Establishing an appropriate penalty regime (Option Two) should deter the spread and incidence of sales suppression software in the New Zealand tax base, as taxpayers who might otherwise have been inclined to use or sell the software would be discouraged by the penalty rates. It cannot be guaranteed that this will discourage all taxpayers; however, if it is sufficiently robust to discourage enough of them, the ability of vendors of the software to penetrate the New Zealand market will be greatly curtailed and the software may never take sufficient foothold in the tax base to require more substantial (and perhaps more costly) action. This option also has the benefit of having very low compliance costs for taxpayers who are meeting their obligations, as they do not have to change any aspect of their business or behaviour to continue to be compliant with the law. It does impose some administrative costs, as Inland Revenue must expend resources on auditing taxpayers and taking the non-compliant to court (which then ties up the Courts' resources).

32. An effective regime of regulating the quality of EFTPOS systems sold in New Zealand (Option Three) would greatly reduce opportunities for non-compliance through sales suppression software. If the software cannot be used to suppress sales, it becomes valueless to taxpayers, so its spread throughout the tax base is unlikely (but also not likely to cause much damage to the base if it does occur). However, the major drawback of a regulatory regime is its significant compliance costs. Requiring all businesses using EFTPOS systems in New Zealand to upgrade or replace their systems would be imposing a major compliance burden to resolve a problem that is not currently widespread (as far as we know). Compliance costs are also placed on the vendors of EFTPOS systems, who would need to ensure their products are meeting the standard. Option Three also requires a major investment to establish a sensible regulatory framework, as well as ongoing costs to make sure the regulations stay up to date.

33. Officials prefer Option Two. A penalty regime targeted at specific offenders is a more appropriate response to the current scale of the problem than a regulatory response that affects the entire tax base. It is inefficient to impose burdens on all users of EFTPOS systems to resolve an issue where there is no evidence at this time suggesting the issue is widespread in New Zealand. An approach that targets noncompliant taxpayers directly is likely to be more efficient and have smaller economic costs than an approach that targets all users of EFTPOS systems.

34. Stakeholders were generally supportive of Option Two as an approach to deal with the issue. They have not expressed significant support for Option Three, although we have not discussed Option Three in depth with them. Certain stakeholders raised the following concerns:
    a. Some stakeholders were concerned that instituting a penalty for possession in addition to the existing evasion penalty might lead to a double jeopardy situation in which taxpayers are effectively being charged twice for the same offence.
    b. Other stakeholders cautioned against making the proposed offences offences of strict liability, as Australia has done, and suggested that a requirement of criminal intent be added to the offence definitions.

35. Officials will take these comments into consideration when developing the legislation and accompanying Commentary on the Bill giving effect to the preferred option.

What are the costs and benefits of your preferred option?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups (taxpayers who would otherwise use sales suppression software)	Ongoing cost of not being able to use software to suppress sales (therefore higher tax to pay) One-off cost of paying penalties if caught	High	Medium
Regulators (Inland Revenue)	Ongoing cost of auditing and prosecution	Low	High
Taxpayers not using sales suppression software	No costs	None	High
Wider government	Ongoing cost of courts' time in trying offenders	Low	High
Total monetised costs		-	
Non-monetised costs		*Low*	
Additional benefits of the preferred option compared to taking no action			
Regulated groups (taxpayers who would otherwise use sales suppression software)	No direct benefit	None	High
Regulators (Inland Revenue)	Additional tools to use against taxpayers identified using the software	Medium	High
Taxpayers not using sales suppression software	Ongoing benefit of market competition remaining fairer	High	Medium
Wider government	Ongoing benefit of maintaining revenue base and existing taxation levels	High	Medium
Total monetised benefits		-	
Non-monetised benefits		*High*	

36. The major assumption underlying this cost-benefit analysis is that the penalty regime effectively deters taxpayers from adopting or providing sales suppression software. This is a reasonable assumption as the proposed penalty rates are high and are expected to significantly discourage taxpayers.

37. However, some taxpayers may choose to take the risk; whether this will happen in sufficient quantities to pose a problem will be determined by the size of the penalties and taxpayers' perception of their chances of the behaviour being identified. As such, the evidence certainty entry for these effects in the above table has been set at Medium.

38. The table also assumes that the costs of administering the scheme will largely fall within the existing costs of upholding compliance across the tax system and any additional cost will therefore be relatively minor. For this reason, although the individual cost of evasion cases can be quite high, the overall costs for regulators are set at Low; should the penalties work as intended, few cases will need to be taken to court and the overall administrative burden should be low.

39. Inland Revenue conducts compliance work on a risk prioritisation basis. To the extent the introduction of new penalties increases the penalty for a person undertaking this behaviour, it may result in resources being reallocated to identify sales suppression software and away from relatively lower priority work.

Section 3: Delivering the preferred option

How will you implement the preferred option?

40. Enforcement of the new penalty regime will be a matter for Inland Revenue. Inland Revenue also handles tax prosecutions and will therefore be the agency prosecuting offenders. The new penalties thus have minimal implementation costs, as the mechanisms by which it will be implemented (Inland Revenue's auditing and legal functions) are already in place.

41. The penalties will come into effect from the enactment date of the Bill they are included in, which will likely be the next available omnibus taxation Bill. Taxpayers will be notified when the contents of this Bill are publicly announced.

42. As the penalties are not retrospective, there is a risk that notifying taxpayers of the issue before the penalty is in place will lead to an effective grace period in which taxpayers are aware of the issue and can buy, sell, and possess the software without being subject to any legal consequence aside from the existing evasion penalty. This may increase the spread of the software through the tax base before any effective countermeasure can be deployed. However, this is unavoidable under the standard approach that activity that is not illegal at the time it is undertaken will not subsequently become so retrospectively.

43. Inland Revenue runs public awareness campaigns from time to time on areas it considers are a high risk; an awareness-raising action such as a Revenue Alert could be considered as part of its normal prioritisation process.

How will you monitor, evaluate, and review the preferred option?

44. Inland Revenue's existing taxpayer compliance specialists will be responsible for the ongoing monitoring of the effectiveness of the new penalties (as part of their regular work of monitoring taxpayer behaviour and the general level of taxpayer compliance). We will be able to determine the degree to which the penalties succeed in deterring the spread and use of sales suppression software through this work. Monitoring the actual level of business income tax and GST paid to Inland Revenue and comparing it to expected levels will also provide useful insight.

45. The work of reviewing the success of the new penalties will also fall to Inland Revenue's existing compliance specialists, who will inform officials if further measures or development are required. It will likely take some time for the effects (or lack thereof if the regime succeeds) of sales suppression software to be felt in the tax base. Any review of the regime's effectiveness will therefore need to be conducted at some delay.