dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

C/- Hudson Gavin Martin
Level 16 45 Queen Street
Auckland 1010

hello@dspanz.org
dspanz.org

14 March 2025

Director
Governance and Integrity Policy Unit
Law Division
The Treasury
Langton Crescent
Parkes ACT 2600

Via email: TaxSecrecyReview@treasury.gov.au.

Re: Review of Tax Regulator Secrecy Exceptions

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to make this submission on behalf of our members and the business software industry.

About DSPANZ
Digital Service Providers Australia New Zealand is the gateway for the government into the dynamic, world-class business software sector in Australia and Aotearoa New Zealand. Our members range from large, well-established companies to new and nimble innovators working at the cutting edge of business software and app development on both sides of the Tasman.

DSPANZ supports the government reviewing the tax regulator secrecy exceptions and the opportunities this presents to facilitate information sharing between the ATO and TPB with industry and other government agencies. The outcomes of this review can ultimately deliver better outcomes and experiences across the tax and super system and for taxpayers.

In this submission, we provide the following feedback:

- There are examples where secrecy obligations impact the ATO's ability to provide seamless digital services and interactions for DSPs to support a digital tax and super system;
- DSPANZ recognises that DSPs play a crucial role in every step of the data supply chain from the taxpayer to the ATO and that taxpayers ultimately own this data. Taxpayers should be able to disclose their data directly to third parties through consent driven data sharing. DSPANZ highlights that the Consumer Data Right (CDR) provides an existing framework to capture consent and support data sharing; and

- The ATO should be required to share information with Digital Service Providers (DSPs) when suspected fraud or identity theft has been identified. This information sharing would support their security practices and help detect and mitigate further fraudulent activities.

DSPANZ welcomes the opportunity to provide further feedback on our submission. For more information, please contact Maggie Leese at maggie@dspanz.org.

Yours faithfully,

Chris Denney
President & Director
DSPANZ.

Impacts on Digital Services

DSPANZ recognises the importance of tax secrecy obligations and their role in creating trust in Australia's tax system. There are instances where the current interpretation of secrecy obligations and protected information impacts the ATO's ability to provide wholesale digital services and interactions for DSPs to support a digital tax and super system.

For example, the ATO is unable to provide DSPs with some protected information via the API service as part of the super stapling process that would support payroll and SuperStream processes. These restrictions are intended to protect taxpayers' data. However, the decisions made for the super stapling API have created an experience that many DSPs cannot implement in their software, and taxpayers are forced to use an ATO online web experience that is disconnected from their natural business system or process. As a result, there has been a limited take up of this service.

DSPANZ considers that examples like the above demonstrate how secrecy obligations are impacting the digital services and interactions that the ATO can provide to DSPs. As we move towards a more digital and connected tax and super ecosystem, where software and services provided by DSPs are a taxpayer's main entry point into the system, we need to make these interactions as seamless as possible.

Consumer Consent

DSPs play a crucial role in every step of the data supply chain from the taxpayer to the ATO. DSPANZ recognises that the taxpayer owns their tax data and DSPs act as data custodians in this supply chain.

The Consumer Data Right (CDR) provides a robust framework that outlines requirements for collecting consumer consent and data sharing obligations in a regulated environment.

The ongoing rollout of the government's Digital ID framework will be key to developing a secure verification process for individuals.

DSPANZ recommends that the ATO considers leveraging the Consumer Data Right (CDR) to support consumers in sharing certain ATO-held information safely and securely.

Prevention of Fraud

DSPANZ supports changes to the legal framework that would enable the ATO to share information with Digital Service Providers (DSPs) to support their security practices and help to detect and mitigate fraud.

With the digitisation of the Australian economy, the operation of the tax, payroll, business registration and superannuation benefits system increasingly depends on software products developed by DSPs. DSPs are key stakeholders of the tax ecosystem and are critical to supporting businesses in meeting their reporting obligations to the ATO.

Security Incidents

The ATO has a well developed Operational Security Framework (OSF) that applies to the software products and services that consume ATO Application Programming Interfaces (APIs) and seeks to protect the ecosystem. As ATO registered software providers, DSPs are required under the OSF to report security incidents to the ATO, which is a one-way flow of information from DSPs to the ATO.

Over many years, DSPs have requested that the ATO provide information, even in a summarised form, on the threat landscape and security incidents they experience and that DSPs report to the ATO. With this security incident information, DSPs could implement the appropriate controls or fixes to mitigate against common incidents.

A robust tax system benefits all stakeholders. When the ATO cannot or will not share certain information, this exacerbates risks to all parties.

Fraud Prevention

DSPs are integral to supporting the ATO in detecting, preventing, and mitigating fraud in the tax and super system. In an increasingly digital and interconnected ecosystem, government and industry share the responsibility to prevent, identify, and respond to fraud and uphold the integrity of the tax system.

In a digital world where the operation of the tax system is reliant on DSP software products that interact with the ATO, there is a need for two-way information sharing. With the increased detection of fraudulent activities (including cyber crime, identity theft, and account takeovers), the extended taxation ecosystem is at risk when one party identifies fraudulent actors but is prevented from informing other parties in the supply chain.

Currently, the ATO does not provide information to DSPs when fraud has occurred or key details that could assist them in identifying and mitigating fraudulent activities within their products.

The ATO justifies the lack of information sharing by citing the current secrecy obligations. Without a change in the legal framework and the ATO's willingness to embrace more open and collaborative sharing, DSPs will be prevented from identifying fraud in real time and mitigating the risk of further harm to the tax system before any further interaction with the ATO.

DSPANZ believes that ATO consultation groups such as the Cyber Security Stakeholder Group, DSP Strategic Working Group, and DSP Architecture Reference Group should be considered trusted “networks” where the ATO can facilitate information sharing with DSPs to improve the tax and super system. We also believe that DSPANZ is an appropriate conduit for further information sharing with the wider business software industry.

DSPANZ supports legislation being amended to enable the ATO to provide information on fraud, compromised identity and security incidents to DSPs that are providers of ATO registered products.