



Australian Government
Inspector-General of Taxation
Taxation Ombudsman

Tax Identity Fraud: an own initiative investigation

Interim Report – The importance of bank account integrity

By the Inspector-General of Taxation and Taxation Ombudsman

30 April 2024

Acknowledgement of country

In the spirit of reconciliation, the Australian Government Inspector-General of Taxation acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

© Commonwealth of Australia 2024

Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Creative Commons licence

With the exception of the Coat of Arms (see below), the IGT logo and ATO sourced material, this publication is licensed under a Creative Commons Attribution 3.0 Australia Licence.



Creative Commons Attribution 3.0 Australia Licence is a standard form licence agreement that allows you to copy, distribute, transmit and adapt this publication provided that you attribute the work. A summary of the licence terms is available from: <http://creativecommons.org/licenses/by/3.0/au/deed.en>. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.

The Commonwealth's preference is that you attribute this publication (and any material sourced from it) using the following wording:

Source: Licensed from the Australian Government Inspector-General of Taxation under a Creative

The Australian Government Inspector-General of Taxation does not necessarily endorse third party content of this publication.

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 www.pmc.gov.au/government/commonwealth-coat-arms.

Acknowledgment of contributors

The Inspector-General of Taxation and Taxation Ombudsman (**IGTO**) met with representatives of financial institutions, including the Australia and New Zealand Banking Group, Commonwealth Bank of Australia, Macquarie Bank, National Australia Bank and Westpac Banking Corporation, representatives of the following tax practitioner representative bodies, Chartered Accountants Australia & New Zealand, The Tax Institute, Institute of Public Accountants, CPA Australia and Institute of Certified Bookkeepers, and individual tax practitioners. The IGTO also discussed issues in this investigation with interested external stakeholders.

The IGTO greatly appreciates the generosity of these representatives and practitioners in freely giving their time and sharing their expertise. Their involvement has greatly enhanced the insights and outcomes of this review.

The IGTO also acknowledges the assistance of many volunteer members of the tax profession who assisted by distributing our request for further information and who shared their observations. Without these case studies we would not have been alerted to the significant number of issues and various ways in which taxpayers have been scammed as part of Tax identity fraud (**TaxID fraud**).

The IGT also met with the Commonwealth Ombudsman and Australian National Audit Office staff to form a more holistic understanding of the issues and obtain perspectives and insights from their work. Before officially announcing this investigation and during this investigation, the IGTO also met progressively with Australian Taxation Office (**ATO**) senior management and staff to better understand the administrative issues and distil the scope of improvement.

The IGT also appreciates the ATO's review of the draft of this report to ensure that sensitive content which could be misused by potential fraudsters is not disclosed.

The views in this report are those of the IGTO

It should be noted that the views and recommendations expressed in this report are those of the IGTO after consulting with the community (including individual representatives or practitioners). The views and recommendations were finalised by the IGTO after much deliberation, and are based on the totality of input and documentation received from, and discussions with, private sector representatives, government agency officials and ATO officials. The views expressed in the report were also informed by material received and observations made during IGTO investigations of specific tax official actions and decisions which were examined as part of our dispute investigations (investigations of unresolved complaints) on behalf of dissatisfied taxpayer or tax practitioners.

Table of Contents

Acknowledgment of contributors	iii
Table of Contents	iv
Executive Summary and Key Findings.....	vii
List of recommendations	x
1. Introduction	2
1.1. Background to the investigation	2
1.2. Decision to issue an interim report.....	4
1.3. Initial investigation focus – Changing bank account details	4
1.4. Conduct of investigation	6
1.5. Navigation of report.....	7
2. Background and reference information	9
2.1. Relevant legislative framework and obligations	9
2.2. ATO’s obligations to pay credited accounts as refunds and rights to withhold refunds to verify notified information	11
2.3. Anti Money Laundering and Counter-Terrorism Financing (AML/CTF) obligations	13
2.4. Tax secrecy provisions and relevant exceptions.....	17
2.5. Information sharing between private and public sector bodies to prevent financial fraud.....	20
3. IGTO Dispute Investigation Case Studies.....	24
Case study 1 – Unauthorised access and bank account changes made after ATO had locked the taxpayer’s ATO account.....	24
Case Study 2 – ATO reluctant to garnish funds sitting unclaimed in a Fraudster’s bank account but instead wanted the taxpayer’s consent to do so	25
Case study 3 – ATO asked Legitimate taxpayer to repay \$46,000 refund that was paid to a Fraudster without matching claimed PAYG Withholding credits with employer’s reporting. ATO did not seek any information and concluded that Mr B was not a victim of TaxID fraud after he disclosed that he shared his myGov details	26
Case study 4 – ATO controls did not prevent unauthorised change in bank account details, and taxpayer was not notified of those changes	27
Case study 5 – Taxpayer difficulties in proving they were not complicit in the fraud where a fraudulent bank account was opened in their name	28
IGTO recommendations for taxpayer consent or taxpayer verification solution were rejected by ATO	29

4.	The Importance of Bank Account integrity and related controls	34
4.1.	A bank account is needed to receive tax refunds	34
4.2.	Taxpayers can effectively nominate any bank account to receive tax refunds	34
4.3.	A bank account is an essential ingredient for TaxID fraud	35
4.4.	Expected controls for changing taxpayers’ bank account details in the tax system	36
4.5.	ATO’s risk management regarding bank account changes	37
4.6.	ATO’s authority to retain TaxID fraud refunds, pending verification	41
4.7.	Notifying taxpayers of changes to their nominated bank account.....	46
4.8.	Opening a fraudulent bank account in the taxpayer’s name	49
4.9.	ATO’s eligibility criteria for bank accounts	50
4.10.	ATO verification of taxpayers’ nominated bank accounts.....	51
4.11.	Fraud controls and processes utilised by financial institutions	52
4.12.	Monitoring for known and unknown devices	53
5.	Information Sharing to prevent TaxID fraud	56
5.1.	Key formal partnerships and discussion forums.....	56
5.2.	Information flows between the banks and the ATO on case-specific issues.....	59
5.3.	ATO systems quality may impact its risk management of secrecy provisions and TaxID fraud risk responsiveness.....	62
5.4.	TaxID fraud investigation disclosures in the performance of tax officers’ duties	62
5.5.	IGTO observations and potential solutions to address information sharing limitations.....	64
6.	Information gathering and analysis to identify and address potential TaxID fraud	69
6.1.	Fraud intelligence from affected taxpayers and tax practitioners	69
6.2.	Existing ATO systems data and internal referrals	71
6.3.	Information received by the ATO from other organisations and agencies	73
6.4.	Tax Agent-Client link in ATO systems and notification of de-linking	74
7.	Processes and actual ATO controls.....	78
7.1.	Introduction	78
7.2.	Process and controls for linking myGov accounts to ATO Online accounts	80
7.3.	Process and controls for accessing ATO Online accounts via myGov and for updating taxpayer contact details and bank account details	84
7.4.	Account monitoring controls where fraud or risk of fraud has already been identified.....	87
	Appendix A — Terms of reference.....	91
	Appendix B — ATO response	92

Appendix C — Joint Media Release (29 April 2021) 93

Appendix D — Expected and actual controls to manage change of bank account risks..... 95

Appendix E — Chronology of relevant events leading up to and regarding TaxID fraud..... 97

Appendix F — IGTO information requests to the ATO 104

Appendix G — Glossary and defined terms 108

Executive Summary and Key Findings

This interim report focuses on the Australian Taxation Office's (ATO) risk management controls to prevent fraudsters from changing taxpayers' bank account details that are recorded on their ATO online account. A fundamental step in committing Tax identification (TaxID) fraud is that a fraudster is able to remit money to a bank account controlled by that fraudster. This means that the fraudster must establish access to a relevant bank account that is linked to a legitimate taxpayer's ATO accounts. This is necessary to 'escape' with the money.

Preventing, detecting and responding to TaxID fraud is important to maintain the integrity of the tax system and avoid proliferation that impacts the Revenue. It requires an approach which understands risks presented by the whole of the tax system and considers the activities of the whole of the ATO. A whole of ATO approach requires a co-ordinated framework of individual business units. Further, the nature of TaxID fraud risk mitigation is dynamic. Fraudsters respond to new controls by finding and exploiting control vulnerabilities and finding innovative uses for emerging technologies. As a result, the ATO requires continual vigilance and a commitment to continually fine-tune its controls and quickly redeploy resources in response.

The ATO is progressing a major program of work that was prioritised last year to improve, amongst other things, its ability to address the TaxID fraud risk. Having regard to measures already in progress, this IGTO investigation identifies further work to improve administration in this area.

Accordingly, recommendations are made in the report for the ATO to:

1. make the tax system a less attractive target for TaxID fraudsters, by improving the ATO's systems controls (see Recommendations 1(a) and 1(b)), delaying High-Risk refunds pending authentication and verification (see Recommendation 1(c)), bringing its payment systems up to financial industry standards (see Recommendation 1(d)) and improving its governance and responsiveness in addressing incremental changes to fraud typologies (see Recommendation 1(e));
2. harden the financial system against TaxID fraud (which is a whole of tax system perspective), by directly participating in existing financial forums to combat TaxID fraud (see Recommendation 2(a)) and better engaging with the financial industry on case-specific issues to combat TaxID fraud (see Recommendations 2(a) – 2(c)); and
3. empower taxpayers and tax agents, who are better placed than the ATO to identify and prevent unauthorised changes made on taxpayers' accounts, by requiring taxpayer authentication before making any high-risk changes on their online account (Recommendation 3(a) and 3(b)), notifying tax agents in a timely manner where their clients are removed from their client list (see Recommendation 3(c)) and providing taxpayers with the means to prevent access to their own online accounts and report TaxID fraud (see Recommendations 3(d) and 3(e)).

In total, thirteen (13) recommendations are made for ATO improvement. The ATO had provided the IGTO with its response to each recommendation when they were in draft form. However, it asked that these responses not be reproduced and would provide a consolidated set of responses to all recommendations when the IGTO completes the next phase of this investigation.

Based on ATO indicative responses to date, the IGTO urges the ATO to consult and advocate for legislative authority where it considers this is necessary to implement these critical IGTO recommendations. As with any fraud control framework, robust protection against TaxID fraud risks will require the implementation of a variety of types of controls and an organisational commitment to track and quickly implement the control adjustments and treatments needed to address incremental changes in fraud typologies.

ATO systems need to be fit for purpose and this includes providing 24/7 protection against unauthorised changes to critical confidential taxpayer information that may be used to perpetrate TaxID fraud as the consequences of these changes can have severe impacts on the Revenue, affected taxpayers and their tax agent.

Stakeholders have raised a number of concerns with the IGTO as part of this investigation. Only some of these concerns are addressed in this report. The remainder will be investigated in the second phase of this investigation. For completeness a list of the key issues raised to date is as follows:

- TaxID fraud in many cases appears to be detected by chance and after the event;
- The window for preventing unauthorised payments is too narrow;
- Fraudsters can access taxpayers' online accounts, register for ABN/GST, change personal contact and banking details and then lodge returns/BASs which generate refunds to bank accounts that the fraudster controls, all without being detected by the ATO, ATO systems, taxpayers or their registered agents;
- The perceived lack of ATO support when TaxID fraud occurs;
- Concerns that reports of fraud are not actioned by the ATO (at all or in a timely manner);
- Reports that the ATO did not record information about the fraud when it was reported by some stakeholders, others report that the ATO did make a record, but in accordance with scripting that was inflexible;
- The lack of 24/7 ATO systems support or other mechanisms for taxpayers and their tax agents to prevent or shut down online access to a taxpayer's account – especially over public holidays and weekends;
- Concerns that reported fraudulent bank accounts and addresses are being used to continue to perpetrate TaxID fraud;
- The ATO treatment of Legitimate Taxpayers as Fraudsters when they are in fact the victim of Fraud;

- Concerns about ATO advice to lodge complaints or objections to help expedite investigations or resolve disputes about TaxID fraud;
- Confusion about the requirement for a Legitimate taxpayer to lodge an objection against amendments made fraudulently (ie not by them) to their tax returns and filings;
- The lack of co-ordination between ATO debt recovery action and ATO objections (which can take 3 months before an Objections officer is allocated);
- Concerns with the impact on taxpayers and tax agents, pending ATO investigation and remediation of taxpayers' tax accounts;
- Concerns about the impact of ongoing security settings (ie. Account lockdown) and delays in ATO investigations – some more than 6 months on compromised Taxpayer accounts;
- The ATO treatment of tax debts that arise from financial/ID fraud – that is, the Legitimate Taxpayer remains liable to repay the debt until the ATO completes an investigation and only if that investigation vindicates the taxpayer; and
- Challenges for tax agents representing a client whose identity has been compromised which involves time consuming and unbillable work as well as lack of access to clear guidance, support services and information.

The ATO has governance arrangements in relation to the TaxID fraud risk and made changes in 2023 to improve its ability to respond to a crisis, which necessarily must be at scale. However, TaxID fraud also involves incremental change in methods as typologies evolve and 'displace' themselves from known typologies. This demands a real time response from the ATO. In this respect, the ATO lacks a whole of agency governance structure to respond to the displacement evolution of TaxID fraud. This is especially so in circumstances where TaxID fraud can be facilitated simply by changing taxpayer details within the ATO systems, notably changing their bank account details, and without that taxpayer's knowledge, authorisation or authentication.

The ATO risk management framework for TaxID fraud relies heavily on gateway access controls (such as PORO, mvGov and myGovID). Overreliance on these access controls to provide 24/7 protection against unauthorised changes to details on taxpayer online accounts is inappropriate and inadequate in the circumstances, as demonstrated by the ATO's and taxpayers' experiences. No one type of control is sufficient by itself to effectively mitigate the risk of TaxID fraud. A variety of types of controls are needed.

The ATO has limited automated checks and controls that could operate at scale and in real-time at the very time that (unauthorised) changes are made to taxpayers' ATO accounts. Also, at the time of the IGTO investigation, ATO systems did not monitor for 'known device' identification in real time, so that unknown or suspicious devices could be identified for further investigation and verification as well as the changes made by those devices to taxpayer bank account details on the ATO's systems.

The ATO's risk management framework also relies heavily on post-risk event treatments. The ATO has implemented (since mid-2023) account monitoring to surface suspicious financial institution account changes on ATO systems and the use of the same bank account by multiple unrelated taxpayers.

However, this monitoring requires manual review and processing at critical steps which can take place sometime after the changes on the taxpayers' account have been made. Whilst it may be effective to prevent future unauthorised actions on taxpayers' account, this account monitoring likely has limited effectiveness in mitigating the TaxID fraud risk overall.

The IGTO considers it should not be possible for taxpayers or tax agents to change certain (high risk) contact details within the tax system without the change being verified and authenticated by the taxpayer. Implementation of a number of recommendations in this report would better address these risks and empower the taxpayer or their representative to control access to their ATO online and systems information. These are the very people who are best placed to identify whether activity on their accounts is legitimate or fraudulent.

List of recommendations

The key themes under which these recommendations for improvements are organised is as follows:

1. Improvements to make the ATO less attractive to fraudsters by making it harder for them (and not legitimate taxpayers) to divert monies to the fraudster's bank account;
2. Improvements which harden the financial system against TaxID fraud by introducing more effective collaboration between the ATO and the banks on case-specific issues in real-time; and
3. Improvements to better detect and prevent TaxID fraud by empowering the two key participants in the tax system to assist the ATO, who are much better placed than the ATO to quickly and more reliably determine if a transaction is part of TaxID fraud or not - i.e. Legitimate Taxpayers and their tax agents.

The IGTO's recommendations are listed below. The ATO had provided the IGTO with its response to each recommendation in draft form.¹ However, it asked that these responses not be reproduced in this report and would provide a consolidated set of responses to all recommendations when the IGTO completes the next phase of this investigation. Instead the ATO provided this response for inclusion in the report.

The ATO is pleased that IGTO's interim report recommendations align broadly with ATO-identified work in progress, and agree in principle with the majority of recommendations made. The ATO notes that some recommendations are dependent on matters for Government to consider. The ATO looks forward to IGTO's final report with any remaining findings and recommendations from this investigation, and will provide an ATO response against each recommendation in both interim and final reports as a consolidated set at that time.

The ATO's formal response is reproduced in Appendix B.

¹ On 11 March 2024 and 16 April 2024.

1. Improvements to make the ATO less attractive to fraudsters by making it harder for them (and not legitimate taxpayers) to divert monies to the fraudster’s bank account

1(a) The IGTO recommends the ATO systems monitor for suspicious devices and bank accounts (that is, ‘Known and Unknown Devices’ to allow it to verify that changes made in the ATO systems are authorised by the actual taxpayer and to detect devices and bank accounts associated with TaxID fraud)

The ATO should:

1. identify unknown or suspicious devices and bank accounts for further investigation and verification; and
2. monitor devices and bank accounts known to be associated with fraud.

There should be facilities within ATO systems to monitor for ‘known device’ identification in real time, so that unknown or suspicious devices can be identified for further investigation and verification as well as the changes made by those devices to taxpayer bank account details on the ATO’s systems. Identification of unknown and suspicious devices should result in taxpayer messaging that prompts for verification and authentication. It should also prompt the ATO to investigate any changes made via devices that are known to be associated with fraud.

A device ID catalogue (that is, a list of devices that are known to have been used to perpetrate fraud) is maintained with members of each of the Australian Financial Crimes Exchange (**AFCX**) and the Fintel Alliance. It is understood that the ATO is a member of the latter but not the former. The AFCX receives internet protocol (**IP**) data and device data from some of its members — noting that not all members contribute equally to every catalogue — and this information would be available to the ATO should it choose to join the AFCX. The ATO would also be expected to contribute data to the AFCX were it to become a member. The IGTO also recommends that the ATO join the AFCX (see Recommendation 2(a) below).

1(b) The IGTO recommends that the ATO lodgement and processing controls should be enhanced as part of the self-assessment system so that it does not process suspicious lodgements that may be linked to TaxID fraud without verification

The ATO should develop tighter and more robust controls which pause the processing of suspicious filings – both original and amended lodgements - and suspend related refunds (see Recommendation 1(c) below) for verification where there are suspicious circumstances that indicate potential TaxID fraud. For example, amendments to claim Pay-As-You-Go withholding (**PAYGW**) credits which exceed the

PAYGW amounts recorded against the employee in the employer records should raise suspicion and investigation where the taxpayer's ATO Online account information, such as contact details and bank account, have been changed (especially on an unknown device) before the refund is issued.

1(c) The IGTO recommends that ATO systems delay High Risk refunds unless and until there has been adequate authentication and verification of the bank account details

Refunds that involve a high risk of TaxID fraud (**High- Risk refund**) can include unusual lodgement behaviours (original filings and amendments) and claims which generate refunds and that are coupled with recent changes in the taxpayer's contact and bank account details. The IGTO recommends the ATO develop tighter and more robust controls which pause the processing of original and amended filings and lodgements for verification where the taxpayer's ATO Online account information, such as contact details and bank account, have been changed at the time of or close to the time of lodgement (especially on an unknown device).

The ATO should not pay High Risk refunds unless and until there has been adequate authentication of the bank account details (note that Recommendation 3(a) provides upstream authentication when bank account details are changed).

Authentication of High-Risk refunds may include:

- Verifying any amendments to filed returns and change of bank account details directly with the taxpayer;
- Verifying whether a change of bank account details was made by the taxpayer (or their registered agent);
- Verifying what information the bank has used to comply with the Australian Anti-Money Laundering/Counter-Terrorism Financing's (AML/CTF)'s 'Know Your Client (KYC) requirements as part of the bank account opening process;
- Scanning the ATO systems to identify if the bank account is registered on unrelated taxpayer accounts.

Where the ATO believes it does not have the relevant statutory authority to implement this recommendation, then it should consult with the tax profession to identify the most appropriate legislative reform it could recommend to Government to implement this critical recommendation. For example, whether section 8AAZLGA of the *Taxation Administration Act 1953 (TAA 1953)* should be amended.

1(d) The IGTO recommends that, in the long term, the ATO bring its payment systems up to financial industry standards and develop a dedicated application for trusted devices to allow safe and trusted real time communications between the ATO and taxpayer for verification purposes

Each of the major banks has invested in systems applications to allow secure communications with their customers. The ATO should adopt a similar profile given its major role in the payments system. This would also enhance trust in the community and go some way to addressing the risk of unsuspecting taxpayers being scammed.

1(e) The IGTO recommends the ATO improve its governance and risk management of the TaxID fraud risk, especially with respect to 'displacement' evolutions in TaxID fraud, including by ensuring that:

- i. business units incorporate into their annual planning and budgeting cycle, provision for resources that are needed to give effect to 'rapid response' changes in risk controls which address 'displacement' evolutions in TaxID fraud, and**
- ii. a holistic governance and risk management approach is implemented whereby competing priorities of business units are quickly reconciled in light of the risks to the integrity of the tax system overall.**

The ATO has governance and risk management oversight measures regarding TaxID fraud, for example, the ATO's SES Band 2 Strategy Committee oversees implementation of agreed priority projects and the Deputy Commissioner of the Fraud and Criminal Behaviours business line is now empowered to call a "Fraud Event" to marshal the agency's resources in response to unexpected events. However, these measures would appear to be most effectual when the agency is faced with significant and unexpected events – for example, a crisis.

However, the ATO does not appear to be wholly effective in addressing the need for agile changes in workforce priorities and allocations needed to track 'displacement' evolutions in TaxID fraud typologies.

For example, the ATO's risk management framework does not appear to facilitate quick reconciliation of competing priorities of the business units – i.e. the priorities of the business units that are responsible for tracking fraud evolution and updating fraud controls, those of the business units that are responsible for implementing updated controls and those that are responsible for acting on the cases identified by those models for action. This may ultimately be due to the annual workforce planning and budget allocation cycle for the ATO's business units. In this cycle, annual targets are set at the start of the year that are based on the complete utilisation of the budget allocation for that year, but without provisioning for needed resourcing to accommodate the priorities of other business units that may arise.

Further, the nature of TaxID fraud risk mitigation is dynamic. Fraudsters respond to new controls by innovating to exploit control vulnerabilities and finding new uses for emerging technologies. As a result, the ATO requires continual vigilance and a commitment to continually fine-tune its controls in its response. This is needed to minimise the risk of exponential growth of TaxID fraud activity as organisational inertia to adapt and address weaknesses in its control framework is quickly exploited and usually results in increased activity. Therefore, it is imperative that the ATO not only plan and provision for big urgent changes that are needed, but also ensure that its business units make provision for the ongoing updating of TaxID fraud controls and the quick implementation of those updates to address of 'displacement' changes as well as making provision for resources to quickly accommodate the resulting treatments that flow from these changes.

2. Improvements which harden the financial system against TaxID fraud by introducing more effective collaboration between the ATO and the banks on case-specific issues in real-time

2(a) The IGTO recommends that ATO actively engage with trusted participants in the financial system to combat TaxID fraud and join the AFCX and actively participate in the FRX on case specific issues

The IGTO understands that the ATO has access to the information that financial institutions share with Australian Transaction Reports and Analysis Centre (**AUSTRAC**). The ATO also participates in the Fintel Alliance. Although there are existing communication channels and arrangements that would permit the ATO to share information about case specific issues with banks, these communication processes are limited and not scalable.

Where a new prescribed taskforce was established or one of the existing taskforces, such as the Serious Financial Crime Taskforce (**SFCT**), accepted the TaxID fraud issue as their priority, then the ATO could disclose case-specific information via this taskforce directly to the members of this taskforce. However, this is subject to ATO restrictions and caveats regarding on-disclosure.

There is, however, another forum which would provide a more real-time and effective means of engaging with the banks on case-specific TaxID fraud issues. This is the AFCX's Fraudulent Reporting Exchange (**FRX**), should the ATO become a member of the AFCX and subject to any legislative requirements. The FRX is a safe network that enables its members to efficiently report and address fraudulent activities.

The AFCX, also known as the National Fraud Exchange, is an independent, not-for-profit organisation that was formed by the four major Banks in 2016 to assist businesses combat financial-related crimes. It operates independently of government, law enforcement and its members, although it is funded by its members. The IGTO understands that participants have relevant and appropriate security vetting clearance.

The AFCX has the support of the Commonwealth Attorney-General's Department and is a key limb in the Australian Government's National Organised Crime Response Plan.

The AFCX is the primary channel through which the public and private sector coordinate their intelligence and data-sharing activities for the investigation and prevention of financial and cyber-crime.

The ATO is not a member of the AFCX and so does not access the information shared through the AFCX's FRX. Based on stakeholder consultations, however, ATO membership would be welcome and the ATO is invited to join.

To the extent that establishing real-time communication with the banks via FRX requires industry-agreed data protocols and specific legislative authority, the ATO should actively support and advocate for such initiatives to enable it to more actively and effectively engage with trusted participants in the financial system to combat TaxID fraud.

2(b) The IGTO recommends that the ATO verify taxpayers' bank details with banks and determine whether the process to open those bank accounts creates additional risk factors

The ATO should cross reference bank details with banks to verify bank account details and obtain information to assess the risk of TaxID fraud. That is, information for risk score purposes that may indicate whether the account is at the higher or lower end of the risk spectrum – e.g. how the bank account was opened (in person/online), whether identity documents were sighted by bank employees or whether the documents were verified online through the document verification service.

This would allow bank accounts that are potentially controlled by an identity fraudster to be identified.

2(c) The IGTO recommends that the ATO systems provide banks with real-time verification of Tax File Numbers (TFNs)

The ATO should work with trusted financial institutions to develop systems that permit real time TFN verification as part of bank account opening processes. This would reduce the ATO's exposure to the TaxID fraud risk. Also, financial institutions believe this will assist more broadly to improve fraud controls in the financial system.

3. Improvements to better detect and prevent TaxID fraud by empowering the two key participants in the tax system to assist the ATO, who are much better placed than the ATO to quickly and more reliably determine if a transaction is part of TaxID fraud or not - i.e. Legitimate taxpayers and their agents

3(a) The IGTO recommends that the ATO authenticate change of taxpayer or tax agent contact details which are high risk, which necessarily includes changes of:

- **Bank account details;**
- **Mobile or other telephone contact details; and**
- **Contact email addresses.**

It should not be possible for taxpayers or tax agents to change certain contact details within the tax system without the change being verified and authenticated by the taxpayer. Changes that are high risk events should be determined by the ATO, but in the IGTO's view these events would necessarily include changes to:

- Bank account details;
- Mobile or other telephone contact details; and
- Contact email addresses.

For example: Before accepting a requested change to high-risk details, the ATO should automatically alert the taxpayer via a "Was this you?" message and require their confirmation of the change via multi factor authentication (see recommendation 3(b)), using at least two taxpayer contact details that are recorded on the ATO systems and which pre-exist the requested change. This could include:

- A one-time security number or personal identification number sent to the taxpayer's mobile number or other email/registered device via a dedicated app (see recommendation 1(d));
- An email message sent to the taxpayer's registered email account, or SMS and/or

other non-digital channels for taxpayers who are unable or unlikely to verify digitally (for example, the incarcerated, the elderly and those in aged care, remote communities and victims of domestic abuse).

3(b) The IGTO recommends that the ATO implement systems which allow for multi-factor authentication

The ATO should:

- (a) implement a real-time multi-factor authentication and confirmation system within the tax system for taxpayers; and
- (b) use that system to require taxpayers' confirmation before making any changes to a taxpayer's contact and bank account details; and
- (c) use a dedicated app on the taxpayer's trusted device, pre-existing contact number or email address to alert the taxpayer to any new or overriding myGov linking event to their ATO Online account.

3(c) The IGTO recommends the ATO notify Tax Practitioners in a timely manner if a client has been removed from their tax agent's client listing

Protecting the integrity of the tax system is a shared risk of the ATO, Tax Practitioners' Board (TPB) and practising Tax Practitioners, amongst others. Tax agents likely have the best understanding of their client's financial and tax circumstances and are also well placed to quickly detect suspicious activity, where they are appropriately prompted. Therefore, it is important for the ATO to provide timely and relevant information to notify Tax Agents when a client has been deleted from their client list – so that the agent can identify unscrupulous deletions.

Unless Tax Practitioners are notified that clients have been removed from their list, they cannot monitor for suspicious activity in respect of their client's tax records.

Tax agents have (by chance) been able to identify fraudulent refunds in many cases, but rarely because they received the relevant notifications from the ATO. Accordingly, the fraud is invariably identified by the agent only after the fact. The ATO notification also does not provide sufficient information to identify the relevant client - so the agent does not know which taxpayer account to check.

If tax agents were informed of a client's de-linking in a timely manner it would alleviate the consequences as well as the need to rely on the ATO and taxpayers being able to directly communicate with each other at the very time it is needed. Given the fact that tax practitioners are engaged to represent their clients' best interests and are overall more practised in quickly identifying and diagnosing problems in tax administration, early communication by the ATO of changes to agent client listings would assist to prevent fraudulent filings and claims on the tax system.

Where the ATO considers it is effectively prohibited from advising tax agents that taxpayers have been de-linked from their agent account or removed from their client list, the ATO should:

- a. actively and collaboratively consult with the tax profession to explore how relevant and timely communications could be implemented;
- b. actively and collaboratively consult with the tax profession to ensure that the triggers, method and timeliness of such communications are appropriate and practicable for the tax profession; and
- c. if necessary, advocate for legislative change to ensure this important measure of protection against TaxID fraud is introduced.

3(d) The IGTO recommends the ATO implement controls which better empower taxpayers to protect their own accounts (24/7), by implementing ATO online functionality which allows taxpayers to immediately block online access to their accounts, and which can only be unlocked with their consent

Tax practitioners reported instances where their requests for the ATO to block online access to taxpayers' accounts have not been given effect as and when expected. This has also been observed in IGTO Dispute Investigations. The only means for a taxpayer or practitioner to take action against suspected TaxID fraud is to contact the ATO's call centre to have the account locked. This can sometimes unnecessarily increase the period in which taxpayers' online accounts remain exposed, especially over weekends and public holidays.

Also, many taxpayers only access their online account once or twice per year to fulfill income tax lodgement obligations, which may be far too late to detect suspicious activity on their account which has not been detected by other means. Allowing them to easily lock their accounts in-between lodgement dates will significantly reduce the risk of TaxID fraud, by minimising the potential exposure

times for unauthorised activity on these accounts.

Taxpayers should be empowered to initiate action to lock (and unlock) their account quickly and easily, even if they have no suspicion of any untoward activity on their account. They should also have confidence that the lock can only be lifted when they authorise this, by later passing the necessary authentication or contacting the ATO and passing the necessary proof of identity checks.

3(e) The IGTO recommends that the ATO provide a clearly identifiable and easily accessible online reporting page or contact centre where bank account details associated with TaxID fraud can be reported.

The ATO has webpages that provide guidance for victims of identity fraud and webpages that allow taxpayers or their representatives to report scams, unpaid superannuation and ATO officer corruption. However, those webpages do not allow reporting of TaxID fraud so that the (fraudulent) banking details can be captured and investigated by law enforcement agencies, the ATO fraud team or one of the many private public partnerships that are sharing information for the purposes of combatting financial crimes.

The IGTO has been unable to locate any ATO reporting page or contact centre where bank account details associated with TaxID fraud are specifically reported. The difficulty in locating such a reporting page was also raised as a concern in stakeholder submissions. This is a significant oversight and omission.

1

INTRODUCTION

This Chapter explains the initial focus of the IGTO investigation as set out in this interim report

1. Introduction

This Chapter sets out the background to the IGTO's investigation and its conduct.

1.1. Background to the investigation

The Inspector-General of Taxation and Taxation Ombudsman (**IGTO**) commenced an own initiative investigation into tax identity fraud (**TaxID fraud**) on 15 December 2023². This followed earlier information requests and preliminary discussions with the Australian Taxation Office (**ATO**) which commenced on 18 August 2023 as well as an increasing number of approaches made by taxpayers and tax practitioners to the IGTO regarding unresolved concerns with the ATO's actions and decisions concerning events that appeared to involve TaxID fraud.

The issue of TaxID fraud (e.g. fraudsters using stolen identities to unlawfully obtain refunds through the tax system) is not new but there is a need to constantly renew responses to TaxID fraud as new modes and models of fraud evolve. For example, in 2005, the ATO estimated that over a third of fraud cases involved identity crime and established a dedicated unit to address such issues.

Since that time the ATO has experienced surges of TaxID fraud every few years. For example, in 2008, the ATO's e-tax lodgement system was used by fraudsters to lodge more than 40,000 unauthorised returns with the aim of generating refunds. In response, the ATO implemented an Income Tax Refund Integrity Program model for the purpose of detecting TaxID fraud before refunds were paid on income tax return lodgements. Again in 2013, the ATO experienced an exponential growth in TaxID fraud which required it to again change the way it responded, this time by implementing a Client Identity Watch List which helped reduce the reliance on using "compromised TFN" indicators and alleviate the sometimes disproportionate impact that "lockdown" suppressions had on taxpayers and their representatives.

Again in 2020, the ATO experienced significant growth in more sophisticated identity crime which has challenged the historical reliance on identity credentials as the main preventative control against TaxID fraud. Since that time, it has continued to transform its administrative responses to different typologies that develop.

For example, one of these typologies targeted the representatives of taxpayers. On 29 April 2021, the ATO and the Tax Practitioners' Board (**TPB**) issued a joint media release which noted that both agencies were jointly focused on measures to intercept attempted identity fraud targeted at registered tax practitioners and their clients. A copy of this media release is included at Annexure C. Another one of these typologies became more widely known in 2022 and 2023 through the name of the cross-agency response to this threat: Operation Protego.

² The investigation was conducted pursuant to subparagraphs 7(1)(b) and 7(1)(c) of the *Inspector-General of Taxation Act 2003*

This report does not focus on the type of TaxID fraud perpetrated in Operation Protego, which involved taxpayers who conducted fraud in their own name, albeit with guidance from others on social media, for example. In this report, TaxID fraud means fraud that involves an entity (a **Fraudster**) who impersonates another entity (**Legitimate Taxpayer**) when accessing that taxpayer’s online account on the ATO’s systems to unlawfully generate refunds which are then sent to a bank account controlled by the Fraudster.

Current Dispute Investigations

As at 23 April 2024, the IGTO has commenced 37 Dispute Investigations concerning TaxID fraud. These investigations were commenced where a taxpayer or their representative raised a dispute (i.e. an unresolved ATO complaint) with the IGTO.

Stakeholder Submissions

Following the announcement of the TaxID fraud investigation and our request for public submissions on 15 December 2023,³ the IGTO has received 65 submissions from members of the tax profession and the wider community. This included responses to the ID Fraud response template that was published on our website and distributed with the assistance of many volunteer members of the tax profession and professional bodies.⁴

Many submissions outlined examples and typologies of TaxID fraud which were representative of cases that had been experienced or observed. In particular, more than half of submissions raised instances of alleged fraud where:

- There was an unauthorised change made to the bank account details on the taxpayer’s ATO account in order to perpetrate the fraud.
- The ATO was unsuccessful in preventing the refund being issued to the fraudulent bank account;
- The estimated amount of fraud was more than \$10,000;
- The fraud was identified by the taxpayer or their tax agent, and not the ATO; and
- The fraud appeared to involve unauthorised access to the taxpayer’s myGov account.

Previous Investigations

There have been a number of previous reports following broader investigations into the issue of Tax fraud that encompassed TaxID fraud, including those in the table below.

Table 1: Relevant Reports

Date	Title of Report	Published by:
February 2024	Report No.15 of 2023–24: Australian Taxation Office’s Management and Oversight of Fraud Control Arrangements for the Goods and Services	Auditor-General

³ See IGTO, [‘IGTO launches ‘own initiative’ investigation into tax identity fraud’](#) (Media release, 15 December 2024).

⁴ See [IGTO ‘ID Fraud response template’](#) available on the IGTO’s website at www.igt.gov.au.

	Tax	
2018	Review into the Australian Taxation Office's Fraud Control Management	Inspector-General of Taxation and Taxation Ombudsman
September 2010	Australian Taxation Office: Resolving tax file number compromise	Commonwealth Ombudsman
2002-2003	Report No.55 of 2002-03: Goods and Services Tax Fraud Prevention and Control	Auditor-General

The Auditor-General's most recent report (Report No 15 of 2023-24) identified a number of deficiencies in the ATO's framework for managing Goods and Services Tax (**GST**) fraud and noted that the ATO *"is in the process of clarifying roles and responsibilities for managing fraud risk and making the relevant changes to CEI's"*⁵.

This IGTO investigation is not limited to GST frauds.

The IGTO consulted with the Australian National Audit Office and Commonwealth Ombudsman before commencing the investigation to ensure there was no duplication or redundancy in the terms of reference, given the work program (existing and future) of these agencies.

1.2. Decision to issue an interim report

The full terms of reference are set out in Annexure A. However, because the current IGTO wanted to address several issues as a priority and before her term ends (on 5 May 2024), an interim report was prepared to address the critical issue of concern to the IGTO. Namely the ability to change bank account details in the tax system and hence the relevant checks and controls in the tax system associated with such changes. This is because bank accounts are fundamentally how tax funds may be fraudulently received in the perpetration of TaxID fraud.

Work on the remaining terms of reference will continue, including issues of concern raised with the IGTO regarding the ATO's interactions with taxpayers and tax practitioners.

1.3. Initial investigation focus – Changing bank account details

The bank account is the obvious launching point for understanding how TaxID fraud is perpetrated. Without the ability to change a legitimate taxpayer's bank account details, the fraudulent funds cannot be accessed.

The following figure is a summary of the key steps that are presumed to be necessary to perpetrate the TaxID fraud and the expected type of step-specific and general controls to prevent or identify that fraud.

⁵ Auditor-General, *Australian Taxation Office's Management and Oversight of Fraud Control arrangements for the goods and service tax, Auditor General Report No.15 of 2023 – 24* (February 2024) p 21

Figure 1: Key generic steps to perpetrate TaxID fraud and expected type of controls

Step 1	Step 2	Step 3	Step 4	Step 5
				\$
				Step 5 – ATO to pay the refund to the bank account in Step 1 [or Step 3]
Step 1 – Open bank account	Step 2 – Access Taxpayer’s account on ATO systems	Step 3 – Change the Taxpayer’s contact details, including the Bank account details	Step 4 – Lodge and process amendments and returns that generate refunds	
Control: Identity authentication and document verification	Control: Identity credential authentication	Control: Verification with taxpayer/agent via multi-factor authentication, and authentication of bank account	Control: Detection of combination of unusual claims, lodgement behaviour, and recent changes to bank account details	Control: Authentication of control of bank account with bank (if not checked during step 3 or was changed after)
General Controls:				
Automated scans of ATO’s database to identify where a bank account has been used across multiple unrelated taxpayers’ contact details				
Identification of bank accounts that are reported by ATO, banks or tax practitioners as being associated with fraud, and prevention of their use to perpetrate more frauds				
Scan taxpayer accounts on its systems for suspicious activity, as the banks do when they scan their customer accounts for suspicious transactions.				

Source: IGTO

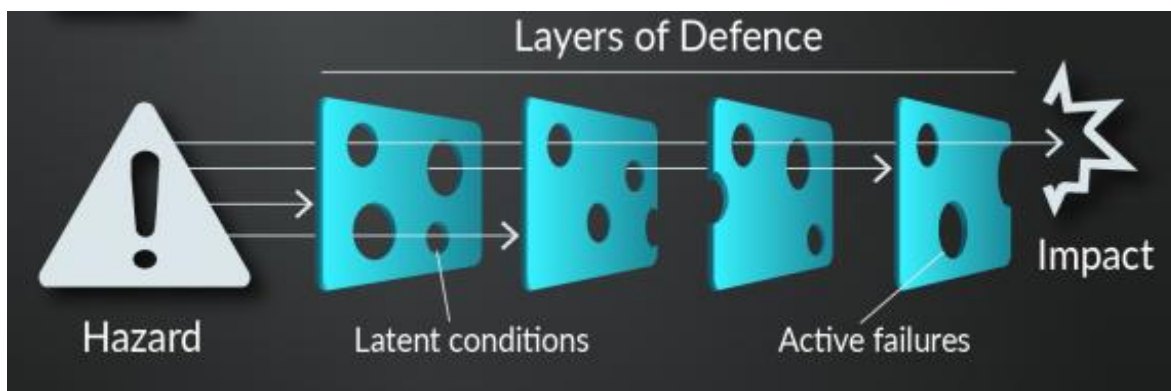
As the focus of this interim report is on changes made to taxpayer’s bank account details on the ATO’s systems, Steps 3 – 5 are examined in further detail in Chapters 4 - 7 which consider:

- What would be the expected Checks and Controls in place for each of these 3 steps?
- What are the actual Checks and Controls in place for each of these 3 steps?

There are also legislative restrictions, currently, which prohibit the sharing of information and prevent these controls from operating effectively or from being implemented. This is discussed in further detail below in the Chapter 4 dealing with bank account integrity.

As a starting point, the IGTO has assumed that no check or control is sufficient on its own to effectively mitigate the risk of TaxID fraud, and that a variety of controls are required. This assumption is illustrated in the figure below (i.e.. the Swiss cheese model), which shows that the control framework should contain a variety of checks and controls. Each check and control operates as a layer of defence, and each has their own latent weaknesses and can potentially fail to operate as intended. Therefore, if all checks and controls are similar or are aimed at a similar risk event, the likelihood of hazards penetrating the control framework is increased. Whereas checks and controls that target different conditions and events decrease that risk as the shortcomings of one layer is more likely to be addressed by another layer.

Figure 2: The Swiss Cheese model



Source: ModelThinkers.com, adapted from James Reason's "The Contribution of Latent Human Failures to the Breakdown of Complex Systems" (1990)

Early in this investigation, it became apparent that the ATO's risk management framework relies heavily on access controls and post-risk event treatments. The ATO has limited automated checks and controls that could operate at scale and in real-time (24/7) at the very time that changes are made to taxpayers' accounts. The ATO has implemented account monitoring (since mid-2023) which could surface suspicious financial institution account changes on ATO systems and use of the same bank account by multiple unrelated taxpayers. However, this monitoring requires manual review and processing at critical steps. Whilst it may be effective to prevent future unauthorised actions on taxpayers' account, this account monitoring likely has limited effectiveness in mitigating the risk overall.

1.4. Conduct of investigation

The IGTO investigation steps included the following:

- meeting with:
 - representatives of the financial institutions including ANZ Banking, Commonwealth Bank, Westpac, National Australia Bank, Macquarie Bank;
 - individual tax practitioners as well as their representative bodies, including Chartered Accountants Australia & New Zealand, The Tax Institute, Institute of Public Accountants, CPA Australia and Institute of Certified Bookkeepers;

- government agencies, including the Australian National Audit Office, Commonwealth Ombudsman, Australian Taxation Office and the Australian Transaction Reports and Analysis Centre (**AUSTRAC**)
- drawing on the observations and information that IGTO investigators had made and gathered in 37 Dispute investigations that raise issues concerning TaxID fraud;
- requesting and considering information from the ATO, together with supporting corroborative or contemporaneous evidence (see below);
- providing to the ATO an advance copy of the draft recommendations on 7 March 2024 to provide it with more time to consider them;
- providing opportunity for the ATO to identify any sensitive material or factual inaccuracies in the draft report — for example, information that could be used by fraudsters to circumvent controls; and
- providing opportunity for the ATO to make submissions in relation to the actions and decisions to which the investigation relates.

The information and documents we requested from the ATO during this investigation is provided in Appendix F.

1.5. Navigation of report

This report contains the following Chapters:

Chapter	Description – This Chapter includes ...
2	Background and reference information on the relevant legislative framework and obligations regarding fraud control, as well as key public and private sector forums
3	Selected case studies from IGTO Dispute Investigations into the actions and decision of tax officials which raised issues of TaxID fraud
4	The importance of bank accounts and the need for integrity to ensure any changes made to taxpayers’ bank account details on the ATO systems are authorised
5	ATO information sharing with other bodies to prevent unauthorised changes of bank account details and TaxID fraud
6	ATO gathering and receipt of information that can be used to conduct analysis to detect unauthorised changes to bank account details and identify potential TaxID fraud
7	The main ATO controls which directly or indirectly operate to reduce the risk of unauthorised changes to taxpayers’ bank account details

2

BACKGROUND AND REFERENCE INFORMATION

This Chapter provides information on the relevant legislative framework and obligations regarding fraud control, as well as key public and private sector forums

2. Background and reference information

This Chapter sets out background information on the legislative framework, related obligations and processes as well as key entities and forums which are discussed in more detail in Chapters 4 - 7.

2.1. Relevant legislative framework and obligations

Public Governance, Performance and Accountability Act 2013 (PGPA Act) and Public Governance, Performance and Accountability Rule 2014 (PGPA Rule) requirements to prevent Fraud and Corruption

Accountable authorities of Commonwealth entities are responsible for managing the risk and incidents of fraud, in accordance with the *Public Governance, Performance and Accountability Rule 2014 (PGPA Rule)* as follows:

Fraud Rule – this applies until 30 June 2024

The purpose of this section [section 10 of the PGPA Rule] is to ensure that there is a minimum standard for accountable authorities of Commonwealth entities for managing the risk and incidents of fraud. It is made for paragraphs 102(a), (b) and (d) of the [PGPA] Act.

Public Governance, Performance and Accountability Rule 2014

Part 2-2—Accountable authorities and officials

Division 1—Requirements applying to accountable authorities

10 Preventing, detecting and dealing with fraud

Guide to this section

The purpose of this section is to ensure that there is a minimum standard for accountable authorities of Commonwealth entities for managing the risk and incidents of fraud. It is made for paragraphs 102(a), (b) and (d) of the Act.

The accountable authority of a Commonwealth entity must take all reasonable measures to prevent, detect and deal with fraud relating to the entity, including by:

- a) conducting fraud risk assessments regularly and when there is a substantial change in the structure, functions or activities of the entity; and*
- b) developing and implementing a fraud control plan that deals with identified risks as soon as practicable after conducting a risk assessment; and*
- c) having an appropriate mechanism for preventing fraud, including by ensuring that:*

- i) officials in the entity are made aware of what constitutes fraud; and*
- ii) the risk of fraud is taken into account in planning and conducting the activities of the entity; and*
- d) having an appropriate mechanism for detecting incidents of fraud or suspected fraud, including a process for officials of the entity and other persons to report suspected fraud confidentially; and*
- e) having an appropriate mechanism for investigating or otherwise dealing with incidents of fraud or suspected fraud; and*
- f) having an appropriate mechanism for recording and reporting incidents of fraud or suspected fraud.*

Fraud and Corruption Rule – this applies from 1 July 2024

The purpose of this section [section 10 of the PGPA Rule] is to ensure that there is a minimum standard for accountable authorities of Commonwealth entities for managing the risk and incidents of fraud and corruption. It is made for paragraphs 102(a), (b) and (d) of the [PGPA] Act.

Public Governance, Performance and Accountability Rule 2014

PART 2-2—ACCOUNTABLE AUTHORITIES AND OFFICIALS

Division 1—Requirements applying to accountable authorities

10 Preventing, detecting and dealing with fraud and corruption

The accountable authority of a Commonwealth entity must take all reasonable measures to prevent, detect and respond to fraud and corruption relating to the entity, including by:

- a) conducting assessments of fraud and corruption risks regularly and when there is a substantial change in the structure, functions or activities of the entity; and*
- b) developing and implementing control plans to deal with fraud and corruption risks, and updating the plans as soon as practicable after conducting an assessment mentioned in paragraph (a); and*
- c) conducting periodic reviews of the effectiveness of the entity's fraud and corruption controls; and*
- d) ensuring that the entity:*
 - i) has governance structures and processes to effectively oversee and manage risks of fraud and corruption relating to the entity; and*
 - ii) has officials who are responsible for managing risks of fraud and corruption relating to the entity; and*

- iii) *keeps records identifying those structures, processes and officials; and*
- e) *ensuring that the entity has appropriate mechanisms for preventing fraud and corruption, including by ensuring that:*
 - i) *all officials of the entity are made aware of what constitutes fraud and corruption; and*
 - ii) *risks of fraud and corruption are taken into account in planning and conducting the activities of the entity; and*
- f) *ensuring that the entity has appropriate mechanisms for:*
 - i) *detecting fraud and corruption, including processes for officials of the entity and other persons to report suspected fraud or corruption confidentially; and*
 - ii) *investigating or otherwise responding to fraud or corruption or suspected fraud or corruption; and*
 - iii) *recording and reporting incidents of fraud or corruption or suspected fraud or corruption.*

2.2. ATO's obligations to pay credited accounts as refunds and rights to withhold refunds to verify notified information

ATO's obligations to pay credited accounts as refunds

The Commissioner of Taxation (**Commissioner**) is required to refund net credits which are posted on taxpayer's accounts (running balance account), as follows:⁶

8AAZLF Commissioner must refund RBA [Running Balance Account] surpluses and credits

(1) The Commissioner must refund to an entity so much of:

- (a) an RBA surplus of the entity; or*
- (b) a credit (including an excess non-RBA credit) in the entity's favour;*

as the Commissioner does not allocate or apply under Division 3.

Voluntary payments only to be refunded on request

(2) However, the Commissioner is not required to refund an RBA surplus or excess non-RBA credit that arises because a payment is made in respect of an anticipated tax debt of an entity unless the entity later requests, in the approved manner, that the Commissioner do so.

⁶ Taxation Administration Act 1953, s 8AAZLF

(3) On receiving such a request, the Commissioner must refund so much of the amount as the Commissioner does not allocate or apply under Division 3.

Effect of refunding RBA surplus

(4) If the Commissioner refunds an RBA surplus under this section, the Commissioner must reduce by the same amount excess non-RBA credits that relate to the RBA.

Effect of refunding credit that relates to an RBA

(5) If, under this section, the Commissioner refunds an excess non-RBA credit that relates to an RBA, the RBA is adjusted in the Commissioner's favour by the same amount.

ATO's right to withhold refunds

The Commissioner has a statutory power to retain a refund owing to a taxpayer in order to verify certain *notified information*. The relevant statutory provision provides as follows:⁷

RETAINING REFUNDS WHILE COMMISSIONER VERIFIES INFORMATION

The Commissioner may retain an amount that he or she otherwise would have to refund to an entity under section 8AAZLF, if the entity has given the Commissioner a notification that affects or may affect the amount that the Commissioner refunds to the entity, and:

(a) it would be reasonable to require verification of information (the notified information) that:

(i) is contained in the notification; and

(i) relates to the amount that the Commissioner would have to refund; or

(b) the entity has requested the Commissioner to retain the amount for verification of the notified information, and the request has not been withdrawn.

(2) In deciding whether to retain the amount under this section, the Commissioner must, as far as the information available to the Commissioner at the time of making the decision reasonably allows, have regard to the following:

(a) the likely accuracy of the notified information;

(b) the likelihood that the notified information was affected by:

*(i) **fraud or evasion**; or*

(ii) intentional disregard of a taxation law; or

⁷ Taxation Administration Act 1953, s 8AAZLGA

- (iii) recklessness as to the operation of a taxation law;*
- (c) the impact of retaining the amount on the entity's financial position;*
- (d) whether retaining the amount is necessary for the protection of the revenue, including the likelihood that the Commissioner could recover any of the amount if the notified information were found to be incorrect after the amount had been refunded;*
- (e) any complexity that would be involved in verifying the notified information;*
- (f) the time for which the Commissioner has already retained the amount;*
- (g) what the Commissioner has already done to verify the notified information;*
- (h) whether the Commissioner has enough information to make an assessment relating to the amount (including information obtained from making further requests for information);*
- (i) the extent to which the notified information is consistent with information that the entity previously provided;*
- (j) any other relevant matter.*

2.3. Anti Money Laundering and Counter-Terrorism Financing (AML/CTF) obligations

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)*, and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules)* aim to prevent money laundering and the financing of terrorism by imposing a number of obligations on the financial sector, gambling sector, remittance (money transfer) services, bullion dealers and other professionals or businesses (known as 'reporting entities') that provide particular services (known as 'designated services'). These obligations include collecting and verifying certain 'know your customer' (KYC) information about a customer's identity when providing those services.

Businesses that are required to comply with the AML/CTF Act are also required to comply with the *Privacy Act 1988* when handling personal information collected for the purposes of compliance with their AML/CTF Act obligations.

The Australian Transaction Reports and Analysis Centre (**AUSTRAC**) is the Australian Government agency responsible for ensuring compliance with the AML/CTF Act.

‘Know Your Customer’ obligation and safe harbour

The following summary of the KYC requirements are taken from the AUSTRAC website:⁸

As a reporting entity you must apply customer identification procedures to all your customers. Part B of your AML/CTF program is solely focused on these ‘know your customer’ (KYC) procedures.

You must document the customer identification procedures you use for different types of customers. The procedures you use must be based on the level of money laundering/terrorism financing risk that different customers pose.

*You must check a customer’s identity **by collecting and verifying information** before providing any designated services to them. You must identify both individual customers (people) and non-individual customers (such as companies, associations or trusts).*

After checking a customer’s identity you must be satisfied that:

- *an individual customer is who they claim to be*
- *a customer who is not an individual is a real entity (a business or organisation that actually exists) and you know the details of its beneficial owners.*

KYC and being familiar with your customers’ typical financial transactions makes you aware of any unusual or suspicious activity and reduces the risk of your business or organisation being exploited for money laundering or terrorism financing purposes.

Most financial institutions indicated that it would be insufficient to rely upon KYC compliance requirements as the sole or primary means to combat financial crimes. Stakeholders have indicated that additional models are required including:

- Behavioural models such as device identification,
- Biometrics such as face recognition and fingerprint identification,
- Typology libraries, and
- IP addresses.

Many banks’ KYC procedures with respect to customer identification are publicly available. An example of one such procedure is as follows:

⁸ AUSTRAC, ‘Customer identification: Know your customer (KYC)’ (accessed on 12 March 2024) <https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/customer-identification-know-your-customer-kyc>

CUSTOMER IDENTIFICATION PROCESS (CIP) – ACCEPTABLE IDENTIFICATION DOCUMENTS

In order to comply with Anti-Money Laundering and Counter-Terrorism Financing Legislation (AML/CTF), [Bank] has a Customer Identification Process (CIP) for individuals seeking banking services.

The standard requirement is for a person to provide:

At least One Primary identification document - Government issued photographic identification

or

At least any Two Secondary identification documents

Details of acceptable identity documents within each category are shown below.

Please refer to [a bank] representative for identification procedures for organisations.

Acceptable categories of documents

All identification must be current unless specified.

The following is the list of acceptable identity documents:

Primary Government Issued Photographic ID Documents

Australian photographic driver's licence or learner's permit

Australian Passport (current, or one that has expired within the past two years)

*Foreign Passport**

Australian State/Territory Government issued Proof of Age card

*Foreign Government issued National Identification card**

Australian Firearms/Shooting Licence

Australian Explosives Licence

Australian Waterways/Boat Licence

Secondary ID Documents

Maximum of ONE of each Document type:

*Birth certificate, birth card, birth extract issued by an Australian State or Territory, or Foreign Government**

Australian Medicare card

*Foreign driver's licence**

*Australian or Foreign citizenship certificate**

Australian Government card or notice issued by Centrelink to concession holder.

Includes any ONE of:

DHS Commonwealth Seniors Health Card or Health Care Card

DHS or DVA Pensioner Concession card

Benefits Notice (less than 12 months old)

Australian ImmiCard. Includes any ONE of:

Evidence of Immigration Status (EIS) ImmiCard

Permanent Resident Evidence (PRE) ImmiCard

Residence Determination ImmiCard (RDI)

Australian School attendance letter issued by principal to person under 18, recording residential address and period of attendance (less than 3 months old)

Australian Tax Office (ATO) assessment notice (less than 12 months old) with name and residential address

Notice issued by approved Australian Aged Care facility (less than 12 months old) with name and residential address

Letter issued by the Australian Electoral Commission (less than 3 months old) with name and residential address

Although the CIP operate at the time of establishing a service, the KYC requirements extend to being familiar with your customers' typical financial transactions. This allows financial institutions to identify any unusual or suspicious activity and reduce the risk of being exploited for money laundering or terrorism financing purposes. However, it is also useful for identifying financial fraud, which may or may not be associated with money laundering or terrorism financing but is nonetheless a crime.

2.4. Tax secrecy provisions and relevant exceptions

All tax officials have a statutory obligation to keep protected information confidential.

355-25 Offence—disclosure of protected information by taxation officers

(1) An entity commits an offence if:

- (a) the entity is or was a *taxation officer; and*
- (b) the entity:*
 - (c) makes a record of information; or*
 - (d) discloses information to another entity (other than the entity to whom the information relates or an entity covered by subsection (2)) or to a court or tribunal; and*
- (e) the information is *protected information; and*
- (f) the information was acquired by the first-mentioned entity as a taxation officer.*

Penalty: Imprisonment for 2 years.

Protected information is defined to mean⁹ information that:

- (a) was disclosed or obtained under or for the purposes of a law that was a *taxation law (other than the Tax Agent Services Act 2009) when the information was disclosed or obtained; and*
- (b) relates to the affairs of an entity; and*
- (c) identifies, or is reasonably capable of being used to identify, the entity.*

Note: Tax file numbers do not constitute protected information because they are not, by themselves, reasonably capable of being used to identify an entity. For offences relating to tax file numbers, see Subdivision BA of Division 2 of Part III.

⁹ Section 355-30(1) of Schedule 1 to the *Taxation Administration Act 1953*

Disclosure in performing duties

There are several exceptions to the above secrecy provisions, including where the disclosure is in the performance of a taxation officer’s duties under a taxation act¹⁰, as follows:

355-50 Exception—disclosure in performing duties

(1) Section 355-25 does not apply if:

- (a) the entity is a *taxation officer; and*
- (b) the record or disclosure is made in performing the entity’s duties as a taxation officer.*

Note 1: A defendant bears an evidential burden in relation to the matters in this subsection: see subsection 13.3(3) of the Criminal Code.

Note 2: An example of a duty mentioned in paragraph (b) is the duty to make available information under sections 3C, 3E and 3H.

*(2) Without limiting subsection (1), records or disclosures made in performing duties as a *taxation officer include those mentioned in the following table:*

<i>Records or disclosures in performing duties</i>		
<i>Item</i>	<i>The ... disclosure is to ...</i>	<i>And the ... disclosure ...</i>
<i>1</i>	<i>any entity, court or tribunal</i>	<i>is for the purpose of administering any *taxation law.</i>
<i>2</i>	<i>any entity, court or tribunal</i>	<i>Is for the purpose of the making, or proposed or possible making, of an order under the Proceeds of Crime Act 2002 that is related to a *taxation law.</i>
<i>...</i>		
<i>6</i>	<i>any entity</i>	<i>Is for the purpose of enabling the entity to understand or comply with its obligations under a *taxation law</i>
<i>...</i>		

¹⁰ Refer item 1 - 11 in the Table in s355-50 of Schedule 1 to the *Taxation Administration Act 1953*

Prescribed Taskforces

Another exception to tax secrecy and confidentiality is disclosure for the purposes of law enforcement and related purposes¹¹.

355-70 Exception—disclosure for law enforcement and related purposes

(1) Section 355-25 does not apply if:

- (a) the entity is the Commissioner or a *taxation officer authorised by the Commissioner to make the record or disclosure; and*
- (b) an item in the table in this subsection covers the making of the record or the disclosure; and*
- (c) if the entity is not the Commissioner, a *Second Commissioner or an SES employee or acting SES employee of the Australian Taxation Office—one of the following has agreed that the record or disclosure is covered by the item:*
 - (i) the Commissioner;*
 - (ii) a Second Commissioner;*
 - (iii) an SES employee or acting SES employee of the Australian Taxation Office who is not a direct supervisor of the taxation officer.*

Item 4 of section 355-70 (of Schedule 1 to the TAA 1953) authorises disclosure for or to a taskforce officer of a prescribed taskforce or a court or tribunal and is made for or in connection with a purpose of the prescribed taskforce. Regulation 67 of the *Taxation Administration Regulations 2017* sets out the relevant taskforces, as reproduced in the table below.

Table 2: Prescribed taskforces

Item	Prescribed Taskforce
1	Criminal Assets Confiscation Taskforce
2	National Criminal Intelligence Fusion Centre
3	National Anti-Gang Taskforce
4	Trusts Taskforce
5	Phoenix Taskforce
6	Fraud and Anti-Corruption Centre
7	Taskforce Cadena
8	Black Economy Standing Taskforce
9	Illicit Tobacco Taskforce
10	Serious Financial Crime Taskforce
11	Fraud Fusion Taskforce

¹¹ Refer section 355-70 of Schedule 1 to the *Taxation Administration Act 1953*

Source: Taxation Administration Regulations 2017

The ATO advised the IGTO that two of these taskforces are no longer in operation (see the shaded Items 3 and 6 in the Table above).

A taskforce officer must hold an office in, be employed in, or is performing the services for an agency in the taskforce.

2.5. Information sharing between private and public sector bodies to prevent financial fraud

Australian Financial Crimes Exchange (AFCX)

The AFCX also known as the National Fraud Exchange is an independent, not-for-profit organisation that was formed by the four major Banks to assist businesses combat financial-related crimes. It operates independently of government, law enforcement and its members, although it is funded by its members.

The AFCX has the support of the Commonwealth Attorney-General's Department and is a key limb in the Australian Government's National Organised Crime Response Plan. The AFCX is the primary channel through which the public and private sector coordinate their intelligence and data-sharing activities for the investigation and prevention of financial and cyber crime.

AFCX members currently include:

- ANZ
- Westpac
- CBA
- NAB
- Macquarie
- Bendigo Bank
- Latitude Financial
- Optus
- Eftpos
- Customer owned banking association financial crimes
- Australian Department of Home Affairs

The Fintel Alliance

The Fintel Alliance is a world-first public-private partnership established in 2017 between Australian federal and state government intelligence and law enforcement agencies, private sector businesses and AUSTRAC – Australia's financial intelligence unit and anti-money laundering and counter terrorism financing regulator. Established under AUSTRAC, the Fintel Alliance brings together government, industry, academic and international partners to harness a collaborative approach to combat and disrupt complex and emerging financial crime, money laundering and terrorism financing. There are currently 30 member organisations that are part the Fintel Alliance, including the ATO and each of the Big 4 Banks.

Fintel Alliance has a Members' Protocol, which details the agreed information-sharing arrangements between government and non-government members. As Fintel Alliance is a conglomerate of public and private sector partners, it does not usually 'collect' information under its own initiative. Rather, information, including personal information, is collected by individuals in the course of performing their

daily functions in accordance with their own governing legislation (for public partners) or business operations (for private partners). Information is then shared within Fintel Alliance in accordance with the agreed information-sharing arrangements in the Protocol.

Fintel Alliance Partners agree that information disclosed to them within the Fintel Alliance will only be used for the purposes for which the information was provided. Under the Protocol, each partner agrees that it is responsible for ensuring there is no mishandling or inappropriate use (including unauthorised copying, reproduction and storage of any kind) or disclosure of information they access within the Fintel Alliance.

The Protocol requires all Fintel Alliance partners to comply with their privacy obligations under applicable privacy legislation and with any common law confidentiality obligations. Public sector Fintel Alliance partners are also required to adhere to the secrecy provisions of the relevant legislation that governs their functions and activities. They may only disclose and share information (which may include personal information) in accordance with any restrictions imposed by their governing legislation.

ATO Fraud Forum

During Operation Protego, the ATO and Commonwealth Bank of Australia (CBA) established an ATO Fraud Forum. This public-private partnership forum was set up to allow senior fraud officers from seven (7) major banks to come together to share information on fraud typologies and emerging threats related to tax refund fraud. This forum is the primary mechanism for the ATO to directly engage with financial sector teams dedicated to addressing fraud within the banks.

The ATO Fraud Forum is held quarterly and is currently chaired by the CBA.

Interbank Forum

The Interbank Forum is a quarterly forum attended by financial institutions, cryptocurrency exchanges, law enforcement and government agencies to share insights and intelligence relating to fraud and eSecurity. This forum involves the discussion of fraud typologies, emerging trends, scam typologies, potential controls, detection and diagnostic techniques. Information discussed among participating organisations is not disclosed outside of the Interbank Forum.

Joint Chiefs of Global Tax Enforcement (J5)

Established on 1 July 2018,¹² the J5 is an international, intelligence-sharing alliance against tax crime and money laundering. The J5 is made up of the following agencies:

- Australian Taxation Office
- His Majesty's Revenue and Customs from the United Kingdom
- Internal Revenue Service Criminal Investigations from the United States

¹² ATO, [Joint Chiefs of Global Tax Enforcement](https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/joint-chiefs-of-global-tax-enforcement) (last updated 20 November 2023) <https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/joint-chiefs-of-global-tax-enforcement>

2. Background and reference information

- Canada Revenue Agency from Canada
- Dutch Fiscal Information and Investigation Service from the Netherlands

The ATO's involvement in the J5 is supported through the ATO-led Serious Financial Crime Taskforce (**SFCT**).

The J5 Global Financial Institutions Partnership (**GFIP**) is a newly established public-private partnership, which brings together tax authorities, financial intelligence units and international financial institutions from the J5 jurisdictions, to share typologies and indicators to help detect and prevent tax crime, including identity-based crime.

3

CASE STUDIES AND SOLUTIONS RAISED PREVIOUSLY WITH THE ATO

This Chapter summarises some case studies to illustrate the experience of the community when TaxID fraud was suspected and previous IGTO recommendations for ATO improvement as part of Dispute Investigations

3. IGTO Dispute Investigation Case Studies

As at 23 April 2024, the IGTO has commenced 37 Dispute Investigations concerning TaxID fraud. The IGTO also received 67 responses from members of the tax profession which outlined their experience with and typologies of TaxID fraud which were representative of those they had observed in their practice. These responses were received following a request for information by the IGTO on 15 December 2023 that was distributed with the assistance of many volunteer members of the tax profession and professional bodies.

In addition, the IGTO investigated ATO actions and decisions that were the subject of unresolved complaint (or dispute) raised by dissatisfied individuals and their representatives (**Dispute Investigations**). The following is a small selection of case studies from these dispute investigations which demonstrate and illustrate the experience of people in the community who believe they have been the subject of, or have observed, TaxID fraud.

They illustrate some of the concerns raised by the IGTO in this TaxID fraud investigation and demonstrate the urgent need to implement the recommendations set out in this report.

Case study 1 – Unauthorised access and bank account changes made after ATO had locked the taxpayer's ATO account

On 3 July 2023, Miss S attempted but could not access her ATO online account. She called the ATO call centre and was told that her account was locked. The ATO officer did not provide any reasons why. However, they did unlock her ATO online account temporarily, for 48 hours, so that she could access it.

Two days later, on 5 July 2023, the ATO temporarily unlocked Miss S' ATO Online and Miss S accessed that account on the same day. She discovered that her income tax returns for FY21 and FY22 had been amended without her knowledge. She called the ATO call centre immediately. She was told that the bank account details registered on her account had been changed three times: on 26 June 2023, 27 June 2023 and 3 July 2023. She was also told that her email address had been changed. Miss S advised that she had not made these changes. Due to this, the ATO officer advised that they would add extra security on Miss S's account, but she would have to provide both a secret question and the answer when she contacted the ATO in future so that she could establish her identity to enable her to access her account.

When Miss S called the ATO again, on 7 July 2023, however, the ATO officer did not follow procedures correctly and ask for any secret question or answer prior to giving Miss S access her account. When Miss S reminded the ATO officer about what she had been told before, the ATO officer incorrectly disclosed the secret question that Miss S was supposed to give as part of her proof of identity.

Later, on 18 July 2023, Miss S obtained access to her ATO online account again and discovered that her bank account had been changed yet again without her authorisation. When she contacted the ATO, she was told that a fraudulent myGov account had been linked to her ATO Online account on 11 July 2023.

This was despite the ATO having locked her ATO online account and adding extra security measures before that date to the ATO.

Miss S complained about these events via the ATO formal complaint process. However, it did not result in any change or better explanation. The ATO advised Miss S to approach the IGTO if she remained dissatisfied, which Miss S did.

After reviewing Miss S' dispute with the ATO, the IGTO commenced an investigation into the ATO's actions. Through the IGTO's investigation, it was discovered that Miss S' account was left unlocked for six days from 5 July 2023 to 11 July 2023, which was longer than the expected 2-business day window, and that further unauthorised activity had occurred during this period. The ATO explained that the delay in re-locking the account was due to system issues and it remediated Miss S' account. The ATO also advised that the process taken during Miss S' 7 July 2023 call was not the approved process for ATO staff and steps have been taken to ensure the staff member is aware of the correct procedure to follow.

As at the date of this report, the IGTO's investigation into this dispute was continuing.

Case Study 2 – ATO reluctant to garnish funds sitting unclaimed in a Fraudster's bank account but instead wanted the taxpayer's consent to do so

Mr H lodged his income tax returns for FY22 and FY23, but he did not receive his expected refunds. When he contacted the ATO, he was advised that this was because his refunds had been offset against a \$30,000 GST debt that had arisen from an ATO audit of his BAS. The ATO officer advised him that he had lodged BASs which reported a \$30,000 credit and the ATO had paid this sum to his bank account. Later, the ATO audited those BASs and assessed them as incorrect and reduced the credit to NIL. So, now the ATO required repayment of that refund. Mr H did not believe he had ever lodged any BASs or received any GST refunds. However, he did remember that the police had previously contacted him to advise they had found a person in possession of his identity documents and bank cards. He also remembered that he had reported this to the ATO earlier in 2022.

An ATO officer reviewed the matter and obtained information about the bank account to which the refunds had been paid. They also found that, prior to the BAS lodgements, Mr H's ATO account had been linked to a new myGov account before his contact details and bank account details had been changed on his ATO online account. Despite this information, the ATO officer maintained that Mr H was liable for the GST debt on the basis that the bank had confirmed that the bank account which received the refunds was in his name.

Mr H complained and the ATO reviewed the matter via its formal complaint review process which ultimately affirmed the original officer's decision. The ATO complaints officer advised Mr H to approach the IGTO if he remained dissatisfied, which Mr H did. The IGTO then reviewed the information and commenced an investigation.

The IGTO's investigation revealed that the ATO had obtained information from the bank which confirmed that the bank account was in the name of Mr H. However, that information also indicated that the bank account had been opened without the bank sighting any original or certified copies of Mr H's identity documents. Also, and more importantly for Mr H, there was still money in that bank account - the balance was approximately equal to the amount of GST refund that the ATO had paid. The IGTO also found that the ATO had issued a letter to Mr H earlier, advising him that it may issue a garnishee notice to recover the refund that was paid. However, that letter was issued to the [wrong] address that had been registered on Mr H's account after the myGov linking event occurred and not the [correct] address that was registered on his account before that linking event.

Further, the IGTO also found that the ATO was aware that there were funds remaining in the same bank account into which the ATO had paid the GST refund. However, the ATO had not taken any action to recover those amounts, contrary to the letter it had sent to the wrong address.

During the investigation, the ATO advised that the ATO would ask the bank for the money if Mr H gave his written consent for the ATO to do so. This suggestion was rejected, as Mr H had professed no knowledge of this bank account. Also, Mr H had previously urged the ATO to take the monies in that account so that he wasn't pursued for the debt. Giving his consent in these circumstances could be viewed by the ATO as an acknowledgement that Mr H was complicit in the fraud.

The IGTO recommended that the ATO garnish the funds from the bank account and the ATO undertook to commence a retrieval of those funds from the bank account. The IGTO's investigation into this matter is continuing.

Case study 3 – ATO asked Legitimate taxpayer to repay \$46,000 refund that was paid to a Fraudster without matching claimed PAYG Withholding credits with employer's reporting. ATO did not seek any information and concluded that Mr B was not a victim of TaxID fraud after he disclosed that he shared his myGov details

Mr B went to a tax agent to lodge his income tax returns for FY19, FY20 and FY21. However, they were both surprised to discover that returns for those years had already been lodged when they looked at his ATO online account. They were even more surprised to see that the returns as lodged included salary and wage income (\$80,000) from a large corporate employer that Mr B had never worked for and PAYG-Withholding credits totalling \$37,000 against that income. The ATO had paid a refund of around \$46,000 for these returns.

Mr B immediately contacted the ATO. During the call, Mr B said that he had given his myGov login details to a person on a social media site, who he did not know, to help him claim a COVID economic support payment. Based on this, the ATO officer concluded that the lodgements were not lodged by an

unauthorised party, that no fraud had taken place and that it was a civil matter. The officer concluded that Mr B had authorised the returns because he had knowingly disclosed his myGov login details to the unknown third party. They also advised that as a refund had been on incorrect information, Mr B was now liable to repay the \$46,000, notwithstanding the fact that Mr B said that he did not receive the refund.

Mr B complained and the ATO reviewed the matter via its formal complaint review process which ultimately affirmed the original officer's decision. The ATO complaints officer decided not to take any further action. They advised Mr B to approach the IGTO if he remained dissatisfied, which Mr B did.

After reviewing the case, the IGTO commenced an investigation. During the investigation it became apparent that both the original and complaints ATO officers did not agree that Mr B may have unknowingly been the subject of TaxID fraud, albeit he appeared to have acted recklessly in giving his details to a person who had never met physically. The officers had not considered the possibility of there being other motivating reasons for the taxpayer to act that way and that the bank account which received the refund may have been opened by someone who had duped him and stolen his identity. If there was no evidence of his active and deliberate involvement in the TaxID fraud, was a \$46,000 tax bill a proportionate penalty for his reckless decision?

As a result of the IGTO's investigation, the ATO agreed to reconsider the matter if Mr B was able to provide a police report and evidence that the bank account (which received the refund) did not belong to him. Mr B provided the requested evidence. After the ATO carefully considered this evidence, it agreed to rectify his ATO account. The \$46,000 debt was expunged from his account and, after Mr B lodged the tax returns he had originally intended to lodge, the ATO released the legitimate tax refunds that were generated by those returns.

Case study 4 – ATO controls did not prevent unauthorised change in bank account details, and taxpayer was not notified of those changes

Miss G attempted to access her ATO Online account as she wanted to get things ready to lodge her income tax return for FY22. However, Miss G was unable to do so as her myGov account had been delinked from her ATO online account. She called the ATO and got her account relinked. However, when Miss G went onto her ATO online account one month later to complete her tax return, she found that there was a debt of more than \$23,000. She was not aware of this debt before. Miss G also noticed that her bank account and contact details were wrong, so she corrected them.

Miss G called the ATO and an ATO officer advised her that the debt arose from an ATO audit of BASs that had been lodged on her account and had generated GST refunds that the ATO had paid. The auditor had reversed the GST credits that were claimed in those BASs. This gave rise to a GST debt that the ATO now sought to recover. The ATO view was that as the GST refunds had been paid, Miss G was now liable to repay these amounts. Miss G explained that she had never applied for an ABN, lodged BASs, or received the refunds.

The ATO officer advised Miss G that if she was claiming that she was the victim of fraud she would need to lodge an objection together with supporting evidence to have the debt extinguished on her account. Miss G did as the ATO advised and lodged an objection. She provided documents in support of her fraud claim, including a letter from the bank which confirmed that the bank considered the refunds were sent to a bank account that had been set up due to identity takeover fraud. The ATO, however, disallowed Miss G's objection on the basis **that there was insufficient evidence to support her claim that the BASs were lodged by an unauthorised third-party.**

Miss G complained to the ATO. However, the ATO declined to change its decision. Miss G then asked the IGTO to look into her dispute with the ATO.

The IGTO commenced an investigation, including for the reason that the objection process would appear to be ill-suited to resolving questions of TaxID fraud. It would be a rare case that a Legitimate Taxpayer could satisfy the onus of proof required, given the significant barriers that would be faced in obtaining evidence to support any claim that they did not access or lodge the returns in question.

Case study 5 – Taxpayer difficulties in proving they were not complicit in the fraud where a fraudulent bank account was opened in their name

Mr C was made aware of unusual activity on his ATO account when he was contacted by an ATO officer to discuss Business Activity Statements (**BAS**) which had been lodged on his account. Mr C explained that he had never owned a business or applied for an Australian Business Number (**ABN**). Therefore, he would never need to lodge a BAS. The officer explained that, notwithstanding this, an application for an ABN and GST registration had been made in his name and BASs had been lodged, which had generated approximately \$50,000 in GST credits.

As a result, the ATO investigated suspected fraudulent activity on Mr C's account. The ATO contacted the bank the refund was paid to and issued notices that required the bank to disclose who held that account. The bank responded by confirming that the account was in the name of Mr C and that the bank account had been opened using Mr C's driver's licence details and address. The bank's advice to the ATO also recorded that "No copies of [Mr C's] identification documents [were] available for production".

The ATO informed Mr C that it was satisfied that Mr C was the owner of the bank account as the bank had provided information that the account was opened using his identity documents.. Mr C explained that he had no knowledge of the bank account and did not open it, which if correct, would mean that he was a victim of identity fraud as a third party had used his details to open a bank account in his name.

The ATO refused Mr C's request to remove the debt until he provided a statutory declaration, police report and letter from a bank that confirms that the fraudulent bank account does not belong to him, or that bank account was created for fraud purposes under client's identity. Mr C advised that he could not take off time at work to get this information. As a result, he lodged a formal complaint with the ATO. As he was not satisfied with the ATO's response to his complaint, he lodged a dispute with the IGTO.

The IGTO then commenced an investigation into Mr C's dispute.

During the investigation, the IGTO raised concerns with the ATO regarding the difficulties that any victim of TaxID fraud would face in obtaining a letter from a bank saying that the account did not belong to them when it had been opened in their name using their stolen identity documents. The ATO considered this issue **was hypothetical** and insisted on its documentary requirements. Mr C eventually complied with this ATO request – it took more than a year to satisfy the evidence required.

The IGTO has made recommendation for ATO investigations to take further steps to assist taxpayers. For example, the ATO and the bank can exchange information about account ownership and opening processes, to establish if the bank account is associated with alleged fraudulent activities.

The Case illustrates the importance of taking investigatory steps to not only rely on the name and address of the bank account owner but also obtain corroborative evidence about the circumstances in which that account was established where ownership is disputed.

IGTO recommendations for taxpayer consent or taxpayer verification solution were rejected by ATO

In January 2023, the IGTO identified that the ATO's controls and process could be improved by empowering the taxpayer to intervene where changes made on their account were unauthorised. This improvement opportunity was based on insights gleaned during one of the IGTO's Dispute Investigations that was conducted at the time. The opportunity was formally put to the ATO formally (as a Business Improvement Opportunity (**BIO**) – see the IGTO's Annual Report for a description of this process and its importance in making systemic improvements in the tax system). The IGTO considered the improvement would not only better protect taxpayers against being victims of TaxID fraud but also improve the ATO's control framework overall. In particular, the IGTO recommended that the ATO improve their controls to alert Legitimate Taxpayers to changes made to their contact details on their tax account:¹³

Business Improvement Opportunity

We [the IGTO] recommend that an additional step be added at the end of [the ATO's] procedure for changing client's contact details to alert the client to the change. The following are some examples how it can be done. You may develop your own potential solutions considering your business requirements and constraints. Examples: Once a mobile number is updated, a text message is sent to the original mobile about the change. A letter is posted to the original postal address to advise a postal address change. An alert is sent to the original email address after the email address is updated.

The ATO effectively declined the BIO recommendation as no commitment was given to the implement changes. The ATO also indicated that it had already commenced work on a proposal for a new project,

¹³ IGTO, Communication to ATO, Business improvement opportunity: R/23/001 (2023)

the 'Event-Driven Communication project' which would address the identified issues. The ATO gave a brief description of the project in its response to the IGTO's BIO recommendation, as follows:

The ATO has already commenced work on a new project called 'Event-Driven Communication'. This project is aimed at providing the capability to communicate with clients in real-time via secure and personalized messages, to enable them to safely and effectively manage their tax and superannuation affairs. One of the key aspects of this project, is to steer away from communicating with clients via unsecured channels (such as traditional SMS and email), so that clients can have a high-level of trust/confidence that the communications are genuinely with/from the ATO. Existing methods for informing clients of changes to their account, such as the 'Was This You?' program, where-by notifications are sent to clients via SMS or email (and also suggested in this BIO), tend to not be very effective, as clients either ignore the information or think that it may be a scam message, and consequently take no action.

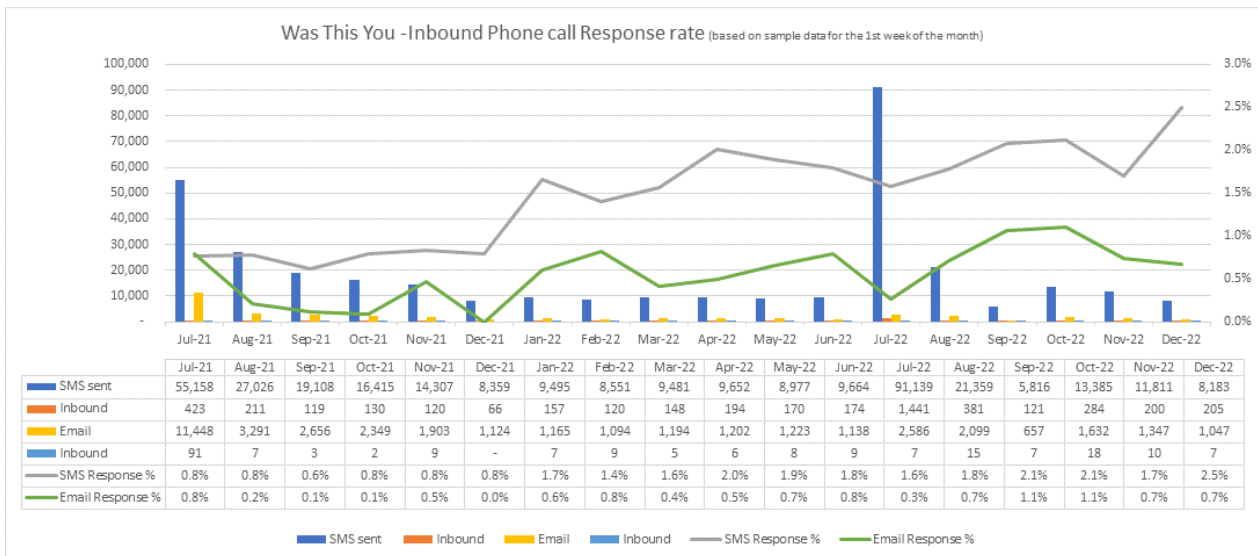
The ATO proposal is that we move to secured (and authenticated) communication channels, in combination with improved client verification processes, so that we can have a much higher level of confidence that we are always dealing with the genuine client. Implementation will be dependent on funding and resourcing for this to happen, and currently no firm commitment to can be made, due to budget constraints. In the interim, we will investigate possible updating of the existing 'Was This You?' platform, but given the known constraints of that system, and lack of any development budget, any improvements are likely to be very limited.

The IGTO asked clarifying questions to better understand the reasons for the ATO's rejection of the IGTO's BIO recommendation and the ATO responded with data indicating a low level of trust in ATO WTY messages:

[IGTO questions:] You mentioned that the "Was this you?" notifications tend to not be very effective, as clients either ignore the information or think that it may be a scam message, and consequently take no action. Would you please be able to provide evidence supporting the above finding?

ATO Response: Please refer to the table below in relation to Was This You (WTY) and the Inbound phone call response rate captured from July 21 to Dec 22. When matching the data against clients who actually became compromised, it demonstrates a low response rate. Comments from clients who acknowledge receiving the WTY notification advised they did not realise the importance at the time, or thought it was a scam message and consequently took no action.

3. IGTO Dispute Investigation Case Studies



The IGTO persisted with the BIO recommendation and referred to a similar practice that the ATO had already adopted elsewhere in support of the IGTO’s improvement opportunity. Again, the ATO expressed commonly agreed aspirations but would not commit to taking action to realise them:

[IGTO Questions:] Also, I noticed that the ATO sends an email or text message alert (or both) when changes are made to SMSF information. Could this be expanded to mobile numbers for individual taxpayers? The reason I am asking is that the mobile phone is heavily used for authentication purposes, at least currently. An alert would give the taxpayer an opportunity to contact the ATO if the change to the mobile number was not made or authorized by the taxpayer.

ATO Response: The ATO has a current WTY process for individuals where there is a subsequent linking event in myGov. We are working on expanding this to include a WTY message when updates are made to financial institution account information and mobile numbers. There is currently no time frame available, however the work includes automating the WTY process by building a new operations analytics model to identify potential ID fraud and proactively cancel possible fraudulent returns.

The current WTY process includes the following steps:

Criteria for an e-mail or SMS to be sent

The client record has had a second or subsequent link to their ATO Online account from a myGov account.

Timeframe

Notification via E-mail or SMS sent the next day except for Friday Saturday and Sunday, where 31he message is sent on the Monday.

Where is the message sent to

A notification is issued to the client (via SMS or email) to alert them of the event, in case it was not them.

This will go to the e-mail or SMS number existing prior to the change. i.e. If the alleged change is done by a fraudster and they change either channel, the SMS or e-mail will go to the number/address already existing on the account..

If the client did not create the new link they are advised to contact the ATO due to the potential identity crime and fraud.

No evidence has been made available to the IGTO that the ATO has committed any resources to an ‘Event-Driven Communication’ project which was referred to in the ATO’s responses.

Further, the ATO material that has been made available to the IGTO indicates that this project is unlikely to be resourced. This is based on the SES Band 2-sponsored “Counter Fraud Investment Program of Work’ which encapsulates 21 “above the line” major projects (for which identified ATO Band 2 SES officers are responsible). All of the 21 ‘above the line’ projects are resourced and prioritized (with the exception of one in which the Second Commissioner has expressed reservations), where 102 ‘below the line’ items are not:¹⁴

*Below the line items relate to recommendations that have generated from previous vulnerability assessments, some of which are aged. **The relevance and status of these recommendations requires investigation** with relevant recommendation owners.*

The January 2024 update on the ATO’s Program of Work:¹⁵

- does not refer to any ‘event-driven communication project’ being “above the line”;
- but does refer to the following as being one of the 102 items that are “below the line” and not receiving priority of resources:

ATA - Deliver a secure two-way notification capability (event driven notifications) through authenticated self-service channels that allow clients to validate high-risk transactions...

¹⁴ ATO, Response to IGTO’s 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

¹⁵ ATO, Response to IGTO’s 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

4

THE IMPORTANCE OF BANK ACCOUNTS

This Chapter discusses the importance of bank accounts and the need for integrity to ensure any changes made to taxpayers' bank account details on the ATO systems are authorised

4. The Importance of Bank Account integrity and related controls

4.1. A bank account is needed to receive tax refunds

In most cases the ATO's method of issuing refunds is by electronic funds transfer to the taxpayer's nominated bank account. The ATO does not provide direct financial benefits through many other means, apart from issuing paper cheques which must be physically deposited into bank accounts that match the name printed on the face of the cheque.

4.2. Taxpayers can effectively nominate any bank account to receive tax refunds

According to the ATO's website, a bank account must either be in the taxpayer's name (as sole or joint account holder) or in the name of their authorised representative.¹⁶ However, the ATO has advised the IGTO during our dispute investigations that it is not able to verify the name of bank accounts with the relevant bank unless it is conducting an investigation.

As a result, taxpayers can effectively instruct the ATO to pay their refunds to any Australian bank account, including any account that is **NOT** held in their own name or their representative's name — that is, the bank account which is registered against the taxpayer's account in the tax system (and is therefore nominated as the account to receive taxpayer refunds) is not required to be in the name of that taxpayer. This creates additional **known** risks in managing TaxID fraud.

An extract from the ATO website¹⁷ is set out below:

Your financial institution details

We can only pay refunds into an Australian bank account. The quickest way to update your financial institution details is online. To do this, you need a myGov account linked to the ATO.

The account must be held by:

- *you under your legal or trading name, either solely or jointly*
- *your registered tax or BAS agent*
- *a legal practitioner acting as your trustee or executor.*

¹⁶ ATO, 'Update your financial institution details' (Webpage last updated 14 October 2022) <https://www.ato.gov.au/individuals-and-families/tax-file-number/update-your-tfn-registration-details/update-your-financial-institution-details>

¹⁷ Ibid.

4. The Importance of Bank Account integrity and related controls

When providing your account details, we require the:

- *bank state branch (BSB) number – this number has 6 digits*
- *account number – this number has no more than 9 digits*
- *account name.*

There are legitimate reasons why a taxpayer may not want refunds to be paid into a bank account that is in their name. It would be usual, for example, for a corporate group to have a single ‘working capital’ style bank account for all entities in the group. It is also not unusual that couples may hold funds jointly in a bank account held in their joint names (with or without single authorisation operating instructions). However, it is also possible (notwithstanding the ATO’s website guidance) for a bank account to be in another person’s or entity’s name.

There is nothing inherently wrong in the lack of any requirement for the bank account name to match the taxpayer’s name. However, this fact does increase the risk of TaxID fraud occurring. That increased risk of TaxID fraud will not be mitigated unless further checks to authenticate the bank account and any change of bank account are conducted before paying a refund.

4.3. A bank account is an essential ingredient for TaxID fraud

To perpetrate TaxID fraud, a Fraudster must:

- control an Australian bank account which can be used to receive and remit monies, and
- access a legitimate taxpayer’s online account on the tax systems, and
- redirect monies from a legitimate taxpayer’s nominated bank account by replacing that bank account on that taxpayer’s online account with the fraudster’s bank account.

Therefore, gaining control of a bank account (for example, opening a new bank account), accessing a taxpayer’s online tax account and changing the bank account on the ATO online systems are the transactions which present the greatest risk of TaxID fraud occurring. The first two risks may be mitigated by strengthening the identity credentials required. Whereas effective mitigation of the last risk (i.e. changing the bank account details within ATO systems) requires a different control – for example, authenticating that bank account and verifying the change was authorised by the legitimate taxpayer.

4.4. Expected controls for changing taxpayers’ bank account details in the tax system

Table 3: Expected controls for changing bank account details

Changing bank account details		
Description of how this can be achieved	Expected Checks and Controls	Actual ATO Checks and Controls
<p>Taxpayers can change their personal contact details, including their bank account details within the ATO systems as follows:</p> <ul style="list-style-type: none"> ▪ Using myGov ▪ Using Online Services for business ▪ Via a registered tax agent who uses Online Services for Agents ▪ Lodging an income tax return or amendment ▪ Lodging a Business Activity Statement (BAS) form or BAS revision <p>These are explored in further details in Appendix D</p>	<p>The details at high risk of TaxID fraud at the time of their change, include changes to:</p> <ul style="list-style-type: none"> ▪ Bank account details; ▪ Mobile or other telephone contact details; ▪ Contact email addresses. <p>it should not be possible to change bank account and contact details within the tax system without the change being verified and authenticated with the taxpayer.</p> <p>For example: Prompting the taxpayer via a ‘Was this you?’ message and requiring taxpayer confirmation of the change via multi-factor authentication, with at least two of the original taxpayer contact details – that is, those that were registered on the ATO systems before the request was made to change details. This could include:</p> <ul style="list-style-type: none"> ▪ A one time security number sent to the taxpayer’s mobile number or other email/registered device; and ▪ An email message or SMS sent to the taxpayer’s registered email account or mobile. <p>There should be automated facilities within ATO systems to monitor in real-time (24/7) for known and unknown device identification, so that changes made on unknown, suspicious or devices which are known to be associated with fraud raise red flags, blocks and the need for further investigation.</p> <p>A device ID catalogue (that is, devices known to be used to perpetrate fraud) is maintained by the AFCX. It is understood that the ATO is not a member of the AFCX but could join and, if it did, it would have access to this information.</p>	<p>Currently, there are limited ATO controls which operate contemporaneous with the change made to a taxpayer’s bank account or other high risk contact details.</p> <p>Instead, the ATO advises that it relies upon checks and controls which permit or restrict access to the taxpayer’s account on the ATO’s systems.</p> <p>These are explored further below.</p>

4.5. ATO's risk management regarding bank account changes

Currently, there are limited ATO checks or controls which operate in 'real time' (24/7) — i.e. at the time a change is made to a taxpayer's bank account or other high risk contact details within the ATO systems.

Instead, the ATO advises that it relies upon checks and controls which permit or restrict access to the taxpayer's account on the ATO's systems. The information made available by the ATO evidences that the risk is currently managed, in summary, as follows:

- Tax officials manually review reports of changes to bank account details for taxpayer accounts that have already been flagged as being potentially involved in, or at risk of TaxID fraud (that is, placed on the Client Watchlist which is generally after the fact), against a list of 'barred bank accounts' that is updated weekly¹⁸;
- Automated identity crime models are run over each tax filing or lodgement;
- Outside sources alert the ATO to unauthorised changes to bank account details (again this would be presumed to be after the fact); and
- Other measures which, while focussed on other risk events, indirectly contribute to decreasing the risk of unauthorised changes to taxpayers' bank account details.

Each of these components of the ATO's risk management framework (their actual controls) is discussed below.

Limited real-time monitoring of suspicious bank account changes

The ATO advised that real-time monitoring of bank account changes that are registered on taxpayers' accounts on the ATO systems is limited:¹⁹

As such, the ATO has opportunities to increase client notifications of changes to their ATO online account details and to conduct additional verification checks prior to making those changes.

Manual reviews are generally conducted after the fact

The ATO's barred bank account list is a list of bank accounts that tax officials believe are connected with fraud. The list is updated weekly and checks against this list are conducted by manually reviewing a report of bank account details that were changed for taxpayers whose accounts are already placed on the Client Watchlist. Tax officials conduct the checks by inputting the BSB number from the report into the spreadsheet to determine if that number is already entered on that spreadsheet.²⁰

¹⁸ ATO, Response to IGTO's 12/12/2023 request for information – Q2 (received 15 February 2024) p 2.

¹⁹ ATO, Response to IGTO's 12/12/2023 request for information – Q3 (received 15 February 2024) p 2.

²⁰ ATO, Response to IGTO's 12/12/2023 request for information – Q3 (received 15 February 2024) p 4; ATO, Response to IGTO's 12/12/2023 request for information – Q2 (received 15 February 2024) p 2.

4. The Importance of Bank Account integrity and related controls

The ATO has a report that monitors suspicious financial institution account changes on client accounts. Business analysts actively monitor the output of the tool to assess whether the bank account is suspicious and potentially linked to identity takeover or is likely legitimate. Where the analyst deems the update to the client's bank account(s) as suspicious and/or linked to potentially fraudulent transaction(s) and/or behaviours, compromised treatments are applied to both the bank account and the client account.

No information was made available to the IGTO to indicate when the manual review and reporting of bank account changes was started, apart from that indicated by the 22 August 2022 original creation date of the electronic document that contains the procedure which the ATO made available to the IGTO.²¹ There have, however, been modifications to that document since that original creation date.

Also, no evidence has been made available to the IGTO to confirm that the barred bank account list will flag an account for manual review. The IGTO is aware of internal ATO research which, in 2022²², found weaknesses in the operation of that account list as a control. The research found that the list did not flag lodgements which generated refunds in cases where a fraudster had first tried to enter a bank account number but was unsuccessful because that account was on the barred bank account list, but then had successfully entered a bank account number which was not on that list before lodging the return. Also, the researchers found that the operation of this barred bank account list could be bypassed altogether in certain types of cases. They recommended changes to address these weaknesses and to consolidate into one bank account watchlist the variety of different bank account watchlists which were being used by the ATO at that time. No information has been made available to the IGTO to confirm that the recommendations made by the researchers were implemented.

ATO's internal monitoring of same bank account used for multiple (unrelated) taxpayers is essentially a manual process

Based on information made available to the IGTO, fraudsters had used the same bank account to perpetrate frauds on a number of different and unrelated client accounts as far back as early 2022.²³ However, it appeared that it was not until early March 2023, that the ATO started weekly internal reporting to detect this.²⁴

In tax practitioner submissions to the IGTO, this fraudster practice was also observed, with one practitioner expressing surprise that the ATO's systems did not detect this before refunds were issued or after that practitioner had reported the issue to the ATO. After making that report and giving the ATO the bank account numbers that were used by the fraudster, they later observed that one of their clients had their bank account details changed to the very number that the practitioner had previously reported to the ATO.

²¹ ATO, Response to IGTO's 12/12/2023 request for information – Q3 (received 15 February 2024) p 4; ATO, Response to IGTO's 12/12/2023 request for information – Q2 (received 15 February 2024) p 2.

²² ATO, Internal Research Paper (2020)

²³ ATO, communication to the IGTO during Dispute Investigation (3 July 2023)

²⁴ ATO, Response to IGTO's 12/12/2023 request for information – Q2 (received 15 February 2024) p 2.

4. The Importance of Bank Account integrity and related controls

The IGTO sought to confirm the incidence of such events by requesting, on 19 January 2024, a copy of the ATO's pre-existing analysis of TaxID fraud events as well as data that the IGTO could independently analyse, including that which would enable the IGTO to estimate the number of instances where the same bank account was used to perpetrate multiple frauds. This request followed an 11 January 2024 request for the provision of the ATO's risk assessment and treatment plan of the TaxID fraud risk. The IGTO expected that such information would have been readily available and provide a comprehensive insight into the ATO's understanding of the TaxID fraud risk, given the ATO's ongoing oversight of these risks.

On 2 February 2024, the ATO indicated that the data would take 4 weeks to provide and, the IGTO met with relevant tax officials on a weekly basis from 23 February 2024 to settle the data fields and progress the request. The data was made available for IGTO to access on 26 March 2023. The IGTO analysed the data and provided indicative findings to the ATO on 12 April 2024 with opportunity to test and correct it before observations on that data were provided to the acting Auditor-General for her consideration.

On 23 March 2024, the ATO provided its response to the information request for its pre-existing analysis. The IGTO expected a more fulsome and more timely response to this information request, given the nature of this risk. Some of the information regarding the ATO's understanding of the risk remains outstanding at the time of this report.

Lodgement risk models are run over tax returns and activity statements before refunds are paid. These models are mainly focused on determining whether information has been accurately reported, although there are 3 models that analyse characteristics that are likely to be attributed to identity crime:

- one for income tax returns;
- one for business activity statements and
- one implemented in 2023 for income tax returns where the account is linked to a myGov account.

These risk models give a risk score that indicates the likelihood of incorrect payment and identity crime. The risk models which generate risk scores, however, are set at thresholds to manage workloads. Therefore, the models are set so that the number of cases that are selected for action are restricted to the resources that are available to action those cases – i.e.. conduct a review or audit of the lodgement prior to the assessment being issued or refund paid.

There are also risk models that do not give risk scores but are rule-based. They run rule-based queries to select cases for action where they have certain attributes, such as by suspending a lodgement from further processing, pending tax official action. Relevant identity crime rule-based models suspend lodgements via the prior application of a 'compromised accounting treatment', generally by a tax official who previously identified the taxpayer's account as potentially compromised. Where the lodgement is suspended, a tax official aims to verify with the relevant taxpayer or tax agent that the lodgement is genuine before removing the suspension and allowing the lodgment to continue processing.

4. The Importance of Bank Account integrity and related controls

In April 2023, the ATO piloted an additional identity crime model, the High-Risk Linking Model, which runs across each lodgement for accounts that are linked to a myGov account. This model does not prevent unauthorised changes to bank account details. However, it will prevent a refund from issuing, where a lodgement meets certain risk criteria. The model has had teething issues with respect to its integration into the lodgement risk model framework, and updates to the model made in October 2023 resulted in more first party fraud being detected than predicted, requiring review of treatment pathways. Also, there are early indications that TaxID fraud typologies are transforming in response to this model.²⁵ This is to be expected as the fraud-control relationship is dynamic and usually responds to address changes made by the other.

The ATO lodgement risk models, however, do not appear to be adequate in detecting all fraud patterns.

For example, the ATO failed to either select for review or suspend a number of self-lodged income tax returns with highly unusual Pay As You Go Withholding (**PAYGW**) credit claims that were made by taxpayers who had a history of tax practitioner representation, and lodged soon after the taxpayer's bank account and contact details were changed. This was observed by tax practitioners in their submissions to the IGTO. It was also observed by the IGTO in January 2024 during inquiries in a Dispute Investigation, which indicated that there may be a fundamental failure in the ATO's models as the PAYGW credit claims made in the Income Tax Return (**ITR**) were far in excess of the ATO's pre-fill data (which would have been sourced from Single Touch Payroll reporting made throughout the year by the large business employer in this case). The return should have been either automatically adjusted on assessment, suspended pending verification of the claim or at least flagged for audit post-assessment. It is noted that the taxpayer in this case had neither lodged income tax returns before nor been represented by a tax agent nor entitled to any PAYGW credits.

The ATO 16 January 2024 responses to the IGTO's 9 November 2023 questions sought to give assurance that this case was a result of the ATO's risk-based approach to selecting cases for pre-issue action (i.e. lodgement of the ITR in this case was not selected for review under the risk-based approach), and there had been a fundamental change to address these cases for the future. However, those ATO responses raised further issues for IGTO examination. Also, the IGTO had received tax practitioner submissions to this investigation which reported similar cases occurring as late as October 2023. As at the date of this report the IGTO is progressing its enquiries.

The ATO should develop tighter and more robust controls which pause the processing of suspicious filings – both original and amended lodgements - and suspend related refunds (see also Recommendation 1(c)) for verification where there are suspicious circumstances. For example, amendments to claim PAYGW credits which exceed the PAYGW amounts that would have been deducted for the reported income or recorded against the employee in the employer (single touch payroll) records should raise suspicion and investigation. A further example would include where the taxpayer's ATO Online account information, such as contact details and bank account, have been changed at the time of or close to the filing or lodgement (especially on an unknown device) which results in the refund.

²⁵ ATO, Response to IGTO's 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

Recommendation 1(b)

The IGTO recommends that the ATO lodgement and processing controls should be enhanced as part of the self-assessment system so that it does not process suspicious lodgements that may be linked to TaxID fraud without verification

4.6. ATO's authority to retain TaxID fraud refunds, pending verification

The ATO advised the IGTO that it had limited scope and time to retain refunds. The operation of the relevant taxation provisions in circumstances of TaxID fraud requires further consideration.

The Commissioner must pay credited accounts as refunds to entities according to section 8AAZLF of the TAA 1953²⁶.

The Commissioner also has a discretion to retain refunds under section 8AAZLGA, which operates "**if the entity has given the Commissioner a notification that affects or may affect the amount that the Commissioner refunds to the entity**" (see the Relevant legislative framework section in Chapter 2).

- It could be argued that this discretion is not available to the Commissioner in circumstances of TaxID fraud because the Legitimate Taxpayer has not given the Commissioner any notification. It is the fraudster who gave the notification.
- However, it is also arguable that section 8AAZLGA is available to the Commissioner because the notification (including a notification to pay refunds to a different bank account) is a notification that fraudulently affects the refunds due (or not due) to the entity. Furthermore, subsection 8AAZLGA(2) clearly states that 'fraud' as well as 'the likelihood of recovering amounts' (should the notified information be later found to be incorrect) are both factors that must be taken into account when deciding to exercise the discretion to retain refunds under this provision.

The ATO should carefully consider if the taxation administration provisions, including section 8AAZLGA, provides sufficient discretion to permit retention of a refund to allow the Commissioner to verify taxpayer contact details, including the taxpayer's bank account details in cases of suspected TaxID fraud.

Additionally, the obligations on an accountable authority and statutory requirements under the PGPA Act and PGPA Rule must also be considered.

²⁶ *Taxation Administration Act 1953*

Resolving competing statutory requirements

The above two tax administration provisions (i.e. sections 8AAZLF and 8AAZLGA) may present the Commissioner with competing statutory requirements which need to be resolved – i.e.:

- a statutory obligation to pay credited accounts as refunds; and
- statutory rights to retain refunds to verify notified information.

The Commissioner's obligations under the PGPA Act and PGPA Rule²⁷, however, are reasonably clear (even if the above tax administration provisions are not) – as they effectively authorise an accountable authority to take the appropriate steps in taxation administration which are necessary to detect and prevent fraud, including for the purposes of investigating suspected fraud.

Where this PGPA Act and PGPA Rule requirement and the right to retain refunds is not considered by the ATO to be sufficiently clear enough to permit retention of refunds for investigation for suspected TaxID fraud, then legislative remediation would appear simple to achieve. However, noting that legislative amendments can take considerable time and resources to implement, the IGTO encourages the Commissioner to consider if an exercise of his remedial power may be appropriate in these circumstances.

The ATO could improve its agility to more quickly adapt to changes in fraud typologies

Based on information made available to the IGTO, the majority of suspected TaxID fraud that the ATO had detected from these models appears to be due to cases selected for action that are based on the incorrect reporting models and not the identity crime model. This appears mainly due to a combination of the following:

- a lack of a dedicated work unit to action cases which the identity crime model detects as involving higher risks and a lack of suitable governance or co-ordinated oversight structure that is able to quickly reconcile competing priorities and refocus business line resources to enable a cohesive and effective fraud response – that is, unless there is a situation where a Deputy Commissioner-announced 'Fraud Event' is warranted;
- the ATO's existing processes were established during a time of minimal fraud, but do not appear to efficiently deal with the larger volumes of fraud that are more recently being experienced. The identity crime risk score effectively competes against other models' risk scores for ATO business line resources as the cases selected by both types of models are allocated back to the business lines (that have already allocated their resources to fulfill their annual commitments) which have primary responsibility to address compliance risks; and

²⁷ *Public Governance, Performance and Accountability Act 2013*, ss 102(a), (b) and (c), and *Public Governance, Performance and Accountability Rule 2014*, rule 10.

4. The Importance of Bank Account integrity and related controls

- a lack of a model which scans lodgement behaviours and account detail changes (including changes to bank accounts) in combination with suspicious claims made in the lodgement form.

These issues indicate there is room for further improvement in the ATO's governance and risk management of the TaxID fraud risk. This is echoed in the Auditor-General's recent findings²⁸ and his report, as well as the ATO's Internal Auditor's report which is referred to in that report.

The ATO has some measures aimed at governance and risk management oversight of TaxID fraud, for example, an SES Band2 Strategy Committee chaired by a Second Commissioner meets to progress agreed priority projects into implementation and the Deputy Commissioner of the Fraud and Criminal Behaviours (**FCB**) business line is now empowered to call a "Fraud Event" to marshal the agency's resources in response to unexpected events. However, these measures would appear to be most effectual when the agency is faced with significant and unexpected events. The ATO gave the IGTO an overview of one example in which that approach had been effective in generating an early response to an emerging new typology that involved a number of external bodies.²⁹

However, the ATO does not appear to be wholly effective in addressing the need for agile changes in workforce priorities and allocations that are needed to track 'displacement' evolutions in TaxID fraud typologies.

For example, the ATO's risk management framework does not appear to facilitate quick reconciliation of competing priorities of those business units that track fraud evolution and update fraud controls with the priorities of those business units that implement updated controls or those business units that act on the cases identified by those models for action. This may ultimately be due to the annual workforce planning and budget allocation cycle for the ATO's business units. In this cycle, annual targets are set at the start of the year, based on the complete utilisation of the budget allocation for that year. It appears that no provision is made to accommodate the overriding priorities that may arise during the year from other business lines.

Further, the nature of TaxID fraud risk mitigation is dynamic. Fraudsters respond to new controls by finding new innovative methods and new uses for emerging technologies. As a result, the ATO must be continually vigilant and continually fine-tune its controls in order to avoid exponential growth of fraud events, which is growth that usually occurs where an organisation is slow to track 'displacement' evolutions or adapt its controls to address weaknesses in its control framework. Therefore, it is imperative that the ATO not only plan and provision for big urgent changes that are needed, but also ensure that its business lines' provision for ongoing incremental updates to its TaxID fraud controls as well as quickly accommodate the resourcing to carry out the treatments that flow from these changes.

²⁸ Auditor-General, *Report No.15 of 2023–24: Australian Taxation Office's Management and Oversight of Fraud Control Arrangements for the Goods and Services Tax* (February 2024)

²⁹ ATO, Response to IGTO's 25/1/2024 request for information – Q(h) (received 21 February 2024).

Recommendation 1(e)

The IGTO recommends the ATO improve its governance and risk management of the TaxID fraud risk, especially with respect to 'displacement' evolutions in TaxID fraud, including by ensuring that:

- i. business units incorporate into their annual planning and budgeting cycle, provisioning for resources that are needed to give effect to 'rapid response' changes in risk controls which address 'displacement' evolutions in TaxID fraud, and
- ii. a holistic governance and risk management approach is implemented whereby competing priorities of business units are quickly reconciled in light of the risks to the integrity of the tax system overall.

Reliance on outside sources to report TaxID fraud, which is often post-event

The ATO advised that the outside sources that alert the ATO to TaxID fraud include:

- taxpayers or their tax agents reporting alleged TaxID fraud which usually includes reporting of an unauthorised change to the taxpayer's bank account; and
- banks that alert the ATO to payments it has made to suspicious bank accounts.

The ATO requires the banks to send their notification by email via the Reserve Bank of Australia (RBA) and the RBA in turn notifies the ATO. Once received, the ATO allocates the referrals to the relevant ATO compliance area for review or audit.³⁰

Heavy reliance on access controls as a means to prevent unauthorised bank account changes

The ATO has advised the IGTO that it relies on the following access controls to prevent unauthorised bank account changes. Proof of Record Ownership (PORO) checks are conducted when a myGov account is initially linked to a taxpayers account on the ATO systems via the ATO Online for Individuals platform³¹.

³⁰ ATO, Response to IGTO's 12/12/2023 request for information – Q3 (received 15 February 2024) pp 4-5.

³¹ ATO, Response to IGTO's 12/12/2023 request for information – Q2 (15 February 2024), p 2.

4. The Importance of Bank Account integrity and related controls

Services Australia provides a report to the ATO with myGov account details that have been compromised. The ATO will identify the affected taxpayer's record, investigate the breach and contact the taxpayer.³²

Where the ATO detects a myGov account is delinked from a taxpayer's ATO online account because of a new myGov account linking to that online account, tax officials will manually send a 'Was this you?' message to that taxpayer during business hours where a valid mobile number or email address is registered on that taxpayer's account immediately prior to the delinking event.³³ No information was made available to the IGTO to indicate when such a measure commenced.

In March 2023, the ATO proposed to implement a 'playbook' to define responsibilities and coordinate action in the event that the ATO becomes aware that bulk personal information held by an organisation outside of the ATO is subject to unauthorised access or misuse. According to this playbook, if the ATO considers there is at least a low-medium risk that affected taxpayers' identity credentials have been potentially compromised, the ATO would add on compromised alert on those taxpayers' records (Siebel Alert) which would increase the PORO that the ATO would require for account access and place the account on a client identity watchlist that may result in the retention of a refund until its validity is confirmed.³⁴

Various suppressions and indicators may be applied where TaxID fraud is suspected or confirmed

'Compromised accounting treatment'

The ATO advised that it may apply a range of security measures on the account, known as 'compromised accounting treatment' (CAT), which are aimed at protecting the account against the risk of fraud occurring again in the future. These measures include:

- Adding compromised indicators and alerts to the taxpayer's account on the ATO's Integrated Core Processing and Siebel systems, respectively;
- Adding the taxpayer to the 'client identity watchlist'; and
- Increasing the PORO requirements to access the account (such as verification of identity documents, secret questions and voiceprint);
- Restricting the taxpayer's access to the account via ATO Online and only providing temporary access after the taxpayer passes extensive PORO (accounts are flagged during this period for monitoring); and
- Suspending the processing of income tax return (ITR) lodgements, pending confirmation of their validity.

³² ATO, Response to IGTO's 12/12/2023 request for information – Q3 (received 15 February 2024) p 5.

³³ ATO, Response to IGTO's 12/12/2023 request for information – Q3 (received 15 February 2024) p 5.

³⁴ ATO, Response to IGTO's 12/12/2023 request for information – Q3 (received 15 February 2024) p 8.

4. The Importance of Bank Account integrity and related controls

The ATO advised that CATs are currently applied to client accounts where the account:

- has been identified as having been accessed by a third party,
- is suspected to have been accessed by a third party, or
- has been assessed as being at high risk of being accessed by a third party.

Compromised tax agent

The ATO advised that when it suspects that a tax agent has been compromised, it can:

- report fraud that involves myGovID to myGovID, who can then suspend the credential, and
- withdraw access to online services for tax agents.

Compromised business account

The ATO advised that when it suspects that a business account has been compromised, it must rely on the suspension of the myGovID credential as a control, as it does not have the capability to withdraw access to online services for business.

4.7. Notifying taxpayers of changes to their nominated bank account

Currently, there are limited dedicated ATO controls which check whether a change made to a taxpayer's bank account details involves a risk of TaxID fraud or not – e.g. changing the nominated bank account to one controlled by the fraudster and changing contact details to those of the fraudster. Instead, the ATO relies on the checks it conducts when access is attempted to the taxpayer's account (such as PORO checks when a person telephones the ATO, accesses ATO Online for Agents, logs on to a myGov account and linking it to the taxpayer's ATO Online account) and the control checks it conducts when processing a lodgement that generates a refund.

The ATO has previously identified that taxpayer confirmation of certain transactions should be obtained, such as payment of refunds. These recommendations have not always been implemented:³⁵

Below the line items relate to recommendations that have generated from previous vulnerability assessments, some of which are aged. The relevance and status of these recommendations requires investigation with relevant recommendation owners.

... CCPP – delay and get greater assurance on client activity via notification of payment made to client's account and seeking confirmation

³⁵ ATO, Response to IGTO's 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

4. The Importance of Bank Account integrity and related controls

The ATO has also confirmed, during IGTO inquiries in Dispute Investigation cases, that it does not automatically verify or vet the name provided as part of the taxpayer's bank account details. The ATO indicated that to do so would impose increased administrative costs:³⁶

The ATO does not automatically verify or vet the name provided on financial institution account details. This is because names may be authorised to receive refunds but are written differently than the legal name on ATO systems. Examples: including or excluding a middle name or initial or using a bank account which includes their partner's name. The administration to check the name provided in all circumstances would be untenable.

The absence of device identification and other (24/7) 'real time' checks for bank account changes increases the risk of TaxID fraud and is also inconsistent with the controls used in the financial sector more generally. As a result, there is a risk that unauthorised changes to bank account details will remain undetected on the ATO's systems until it is too late for effective action to be taken. Changes to the ATO's systems to implement such checks, however, may take time.

In the interim, the IGTO considers that the ATO's initial focus should be to empower the person who is best placed to verify the change – the taxpayer. Accordingly, the ATO should consider measures that would allow a taxpayer to be notified in real-time (24/7) that someone has changed their banking details in the tax system and measures that would allow taxpayers to confirm whether that change was authorised as it should not be possible for taxpayers or tax agents to change certain contact details within the tax system without that change being verified and authenticated by the taxpayer. Changes that are high risk events should be determined by the ATO, but in the IGTO's view would necessarily include changes to:

- Bank account details;
- Mobile or other telephone contact details; and
- Contact email addresses.

As noted in Section 4.4 ('Expected checks and controls...') and Table 1 in Appendix D, the IGTO considers that the ATO should update its checks and controls to:

- ensure that it is not possible to make more than one change to the taxpayer's contact details within ATO online or other systems, unless and until the change has been verified and authenticated (using the taxpayer's pre-existing contact details for authentication);
- ensure that the ATO notifies taxpayers (or their representatives) when a change is sought to be made to taxpayers' bank accounts and/or contact details on the ATO's systems. This would include a multi-factor authentication with the taxpayer using at least two of the taxpayer's pre-existing contact details – that is, those that were registered on the ATO systems before the requested change of details.

³⁶ ATO, communication to the IGTO in dispute investigation (dated 17 January 2024).

4. The Importance of Bank Account integrity and related controls

For example: Before accepting a requested change to high-risk details, the ATO should automatically alert the taxpayer via a “Was this you?” message and require their confirmation of the change via multi factor authentication (see Recommendation 3(b)), using at least two of the taxpayer’s contact details that were recorded on the ATO systems prior to the change request. This could include:

- A one-time security number or PIN sent to the taxpayer’s mobile number or other email/registered device via a dedicated app (see Recommendation 1(d)); and
- An email message sent to the taxpayer’s registered email account, or SMS.

Accordingly, the ATO should:

- (a) implement a real-time multi-factor authentication and confirmation system within the tax system for taxpayers; and
- (b) use that system to require taxpayers’ confirmation before making any changes to a taxpayer’s contact and bank account details; and
- (c) use the taxpayer’s pre-existing contact number or email address to alert the taxpayer to any new or overriding myGov linking event to their ATO Online account.

Each of the major banks have invested in systems applications to allow secure communications and authentication with their customers. The ATO should adopt a similar profile given its major role in the payments system. This would also enhance trust in the community and go some way to addressing the risk of unsuspecting taxpayers being scammed.

Recommendation 3(a)

The IGTO recommends that the ATO authenticate change of taxpayer or tax agent contact details which are high risk, which necessarily includes changes of:

- **Bank account details;**
- **Mobile or other telephone contact details; and**
- **Contact email addresses.**

Recommendation 3(b)

The IGTO recommends that the ATO implement systems which allow for real time (24/7) multi-factor authentication

Tax practitioners reported instances where their requests for the ATO to block online access to taxpayers' accounts have not been given effect as and when expected. This has also been observed in IGTO Dispute Investigations. The only means for a taxpayer or practitioner to take action against suspected TaxID fraud is to contact the ATO's call centre to have the account locked. This can sometimes unnecessarily increase the period in which taxpayers' online accounts remain exposed, especially over weekends and public holidays.

Also, many taxpayers only access their online account once or twice per year to fulfill income tax lodgement obligations, which may be far too late to detect suspicious activity on their account which has not been detected by other means. Allowing them to easily lock their accounts in-between lodgement dates will significantly reduce the risk of TaxID fraud, by minimising the potential exposure times for unauthorised activity on these accounts.

Taxpayers should be empowered to initiate action to lock (and unlock) their account quickly and easily, even if they have no suspicion of any untoward activity on their account. They should also have confidence that the lock can only be lifted when they authorise this, by later passing the necessary authentication or contacting the ATO and passing the necessary proof of identity checks.

Recommendation 3(d)

The IGTO recommends the ATO implement controls which better empower taxpayers to protect their own accounts (24/7), by implementing ATO online functionality which allows taxpayers to immediately block online access to their accounts, and which can only be unlocked with their consent

4.8. Opening a fraudulent bank account in the taxpayer's name

Stakeholder discussions suggest that it is not difficult for fraudsters to set up a new bank account in the name of a taxpayer using stolen documents, intercepted information or fake documents. This can be easily achieved where the taxpayer's personal identity information has been accessed or stolen by an unauthorised third-party (i.e. through widescale data breaches, identity theft or phishing scams).

4. The Importance of Bank Account integrity and related controls

It is possible for an individual to create a bank account and provide their personal information and identity documentation online without physically going to a bank. The banks use the online Document Verification Service (DVS) (which is administered by the Department of Home Affairs) to verify identity documents such as a driver's licence and passport.³⁷ However, the DVS only verifies the existence of the identity document and does not verify whether the identity document belongs to the person using the DVS. Accordingly, many online banks rely on additional information and checks for bank account opening purposes. However, it is still possible for a fraudster to use stolen identities and identification numbers to establish a bank account.

The ease at which a bank accounts can be created also mirrors the fact that it is far too easy for fraudsters to create a false myGov profile and link it to the ATO. This is discussed in later sections but noting that myGov is not administered by the Commissioner but rather Services Australia. As such, the Commonwealth Ombudsman has an interest in and has been provided with progress reports throughout this investigation.

Banks also obtain TFN information from an individual when a new bank account is opened but cannot verify at that time whether the TFN is correct or belongs to that individual, meaning it cannot be used for identification purposes during the bank account application process.

The ATO should work with trusted financial institutions to develop systems that permit real time TFN verification as part of bank account opening processes. This would help reduce the risk faced by the ATO's online access controls and make it more difficult for fraudsters to complete one of the essential steps needed to perpetrate TaxID fraud. Financial institutions believe this will assist to improve fraud controls in the financial system as well.

Recommendation 2(c)

The IGTO recommends that ATO systems allow for real time verification by banks of Tax File Numbers

4.9. ATO's eligibility criteria for bank accounts

The IGTO understands that, currently, the ATO stipulates that only Australian bank accounts can be registered on its systems for refund purposes. The IGTO considers that the ATO should review this risk and consider whether additional criteria for eligible bank accounts may be required for the purposes of receiving refunds. This might include (for example) whether:

³⁷ see: AUSTRAC, 'Customer identification: Know your customer (KYC)', (Last updated 15 January 2024) <https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/customer-identification-know-your-customer-kyc>

4. The Importance of Bank Account integrity and related controls

- the bank account must be held in Australia and by a financial institution that is registered and complying with Australian AML/CTF requirements;
- for individual taxpayers, whether the bank account must be held in the name of the taxpayer;
- whether the financial institution must be a participant in the AFCX or some other relevant fraud prevention forum.

4.10. ATO verification of taxpayers' nominated bank accounts

The ATO considers that it currently does not have the Information and Communications Technology systems capability or legal framework to support verification of a taxpayer's bank account (as recorded on their ATO account) with the relevant bank to confirm the identity of the bank account holder.

When the ATO makes a payment to a taxpayer's bank account, the ATO transmits the bank account name (as reported on the taxpayer's ATO record) and payment reference number to the recipient bank. No further verification of the bank account or payment occurs.

The ATO should cross reference bank details with banks to verify bank account details and assess the potential risk of TaxID fraud. That is, the ATO should obtain relevant information for the purposes of calculating risk scores that it uses in its pre-lodgement model to indicate whether the account is at the higher or lower end of the risk spectrum – e.g. how the bank account was opened (in person/online), whether identity documents were sighted by bank employees or whether the documents were verified through the DVS.

This would allow bank accounts that are potentially controlled by a Fraudster to be identified.

Recommendation 2(b)

The IGTO recommends that the ATO verify taxpayers' bank details with banks and determine whether the process to open those bank accounts creates additional risk factors

Refunds that involve a high risk of TaxID fraud (**High-Risk refunds**) can include unusual lodgement behaviours (original filings and amendments) and claims which generate refunds and that are coupled with recent changes in the taxpayer's contact and bank account details. The ATO should not pay High-Risk refunds unless and until there has been adequate authentication of the bank account details (note that Recommendation 3(a) provides upstream authentication when bank account details are changed).

Authentication of High-Risk refunds may include:

4. The Importance of Bank Account integrity and related controls

- Verifying any amendments to filed returns and change of bank account details directly with the taxpayer;
- Verifying if change of bank account details were made by the taxpayer (or their registered agent);
- Verifying the information relied upon by the bank to comply with AML/CTF's KYC requirements as part of the account opening process;
- Scanning the ATO systems to identify if the bank account is registered against other unrelated taxpayers' accounts.

If the ATO believes it does not have the relevant statutory authority to implement this recommendation, it should consult with the tax profession to identify the most appropriate legislative reform it could recommend to Government to implement this critical recommendation. For example, whether section 8AAZLGA of the TAA 1953 should be amended.

Recommendation 1(c):

The IGTO recommends that ATO systems delay High-Risk refunds unless and until there has been adequate authentication and verification of the bank account details

4.11. Fraud controls and processes utilised by financial institutions

Over many years, financial institutions have made significant investment in their information and technology systems to ensure their fraud and security controls are able to prevent and detect fraudulent and unauthorised activity.

Both within the banking industry as well as more broadly, multi-factor authentication and secure messaging systems (such as dedicated and authenticator apps) are widely accepted as best practice in preventing unauthorised access to any account or system that contains private and sensitive information. Multi (or two) factor authentication is bound to an original and trusted device (usually a mobile phone) for that account. This device is used as an additional factor of identification by requiring a one-time passcode from that very device.

For bank accounts held with most financial institutions, the client is required to complete multi-factor authentication when undertaking high-risk actions or changes on their account (such as a change in mobile number or email address). Fraud detection controls implemented by banks also rely on the

analysis of transaction data and unique behavioural patterns, for example, IP addresses, device data, geolocation and biometrics.

A key consideration when developing fraud detection controls and processes is the organisation's level of fraud loss appetite (i.e. what is pre-determined to be an acceptable level of loss for that risk) and the amount of friction and inconvenience they wish to impose on the user. While minimising the inconvenience for taxpayers when interacting with the ATO is important, this should not be at the expense of the security of taxpayer accounts or the integrity of the tax system.

Given the significant role of the ATO within the domestic payments ecosystem, the ATO should aspire to adopt a suite of information technology systems, similar to the banks, that would allow for secure communications with taxpayers. This would also enhance trust in the community and go some way to addressing the risk of unsuspecting taxpayers being scammed.

Recommendation 1(d)

The IGTO recommends that, in the long term, the ATO bring its payment systems up to financial industry standards and develop a dedicated application for trusted devices to allow safe and trusted real time communications between the ATO and taxpayer for verification purposes

4.12. Monitoring for known and unknown devices

There should also be facilities within ATO systems to monitor for device identification, so that red flags are raised and the ATO is prompted to investigate any change made on devices that are known to be associated with fraud.

The ATO should:

1. identify unknown devices and bank accounts for further investigation and verification; and
2. monitor devices and bank accounts known to be associated with fraud.

There should be facilities within ATO systems to monitor real time for 'known device' identification, so that it can identify unknown or suspicious devices for further investigation and verification as well as changes made to taxpayer bank account details using such devices. Identification of unknown and suspicious devices should result in taxpayer messaging and prompts for verification and authentication, and also prompt the ATO to investigate any changes made via devices that are known to be associated with fraud.

A list of devices that are known to have been used to perpetrate fraud (**device ID catalogue**) is maintained by the AFCX whose members are also members of the Fintel Alliance (refer to Chapter 2, section 2.5 'Information sharing ...'). The IGTO understands that the ATO aims to use the AFCX's

4. The Importance of Bank Account integrity and related controls

device ID catalogue in a proof of concept project in early October 2023³⁸ and is awaiting legal advice before proceeding. Notwithstanding this, the IGTO recommends the ATO equip its systems with the capability to capture device IDs as well as join the AFCX (see Recommendation 2(a) below). The IGTO understands that there is no legal prohibition to doing so and recommends that the ATO engage the community in consultation to ensure that any sensitivities relating to the capture of device ID information are surfaced and considered appropriately.

Recommendation 1(a)

The IGTO recommends the ATO improve its systems monitoring for suspicious devices and bank accounts (that is, 'Known and Unknown Devices' to allow it to verify that changes made in the ATO systems are authorised by the actual taxpayer and to detect devices and bank accounts associated with TaxID fraud)

³⁸ ATO, Response to IGTO's 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

5

INFORMATION SHARING TO PREVENT TAXID FRAUD

This Chapter identifies the ATO's key formal partnerships and discussion forums which relate to TaxID fraud as well as the limitations in the information flows between the ATO and the banks, and the IGTO's potential solutions

5. Information Sharing to prevent TaxID fraud

A collaborative and holistic approach between the ATO and trusted financial institutions is critical to combat TaxID fraud in a rapidly evolving digital environment. This is facilitated through the sharing of information between relevant public and private sector entities, either by way of direct information exchange between the parties or through formally established partnerships and forums.

5.1. Key formal partnerships and discussion forums

There are a number of forums, including private and public forums that are established for the purposes of preventing financial crime. These are described in more detail in Chapter 2 Background and Reference Information.

Some of the key formal partnerships and discussion forums used to share information about or which relates to TaxID fraud are discussed below. The partnerships and forums that the ATO and the major banks are participants in is shown in the figure below. With the exception of the Fintel Alliance Tax Crime and Evasion Working Group, the ATO does not share any case-specific actionable information with other agencies or organisations in these forums.

Table 4: TaxID fraud-related forums with financial institutions and ATO participation

Forum	Purpose	Membership	ATO participation	Type of information sharing
AFCX (incl FRX)	Financial and cyber crime	Financial institutions and Dept Home Affairs	None	Typologies, data sets, case-specific actionable data
Fintel Alliance Tax Crime and Evasion Working Group	Areas of Tax Crime	AUSTRAC, Financial institutions, ATO	Joint-lead	Typologies, case-specific actionable data
ATO Fraud Forum	Tax fraud	Financial institutions, ATO	Member	Typologies, emerging threats
Interbank Forum	Financial Fraud and e-Security	Financial institutions, Australian Federal Police	Participant	Typologies, controls
J5 (GFIP)	Financial crime	Financial institutions and intelligence units and tax authorities from 5 countries	Participant	Typologies

Source: ATO, IGTO and open source

Australian Financial Crimes Exchange (AFCX)

The AFCX is the primary channel through which the public and private sector coordinate their intelligence and data-sharing activities for the investigation and prevention of financial and cyber crime.

The ATO is not a member of the AFCX but the IGTO understands it would be welcomed as a member and is invited to join. As the ATO is not a member, it does not currently access the information shared through the AFCX Fraudulent Reporting Exchange (**FRX**) (see below).

AFCX Fraudulent Reporting Exchange (FRX)

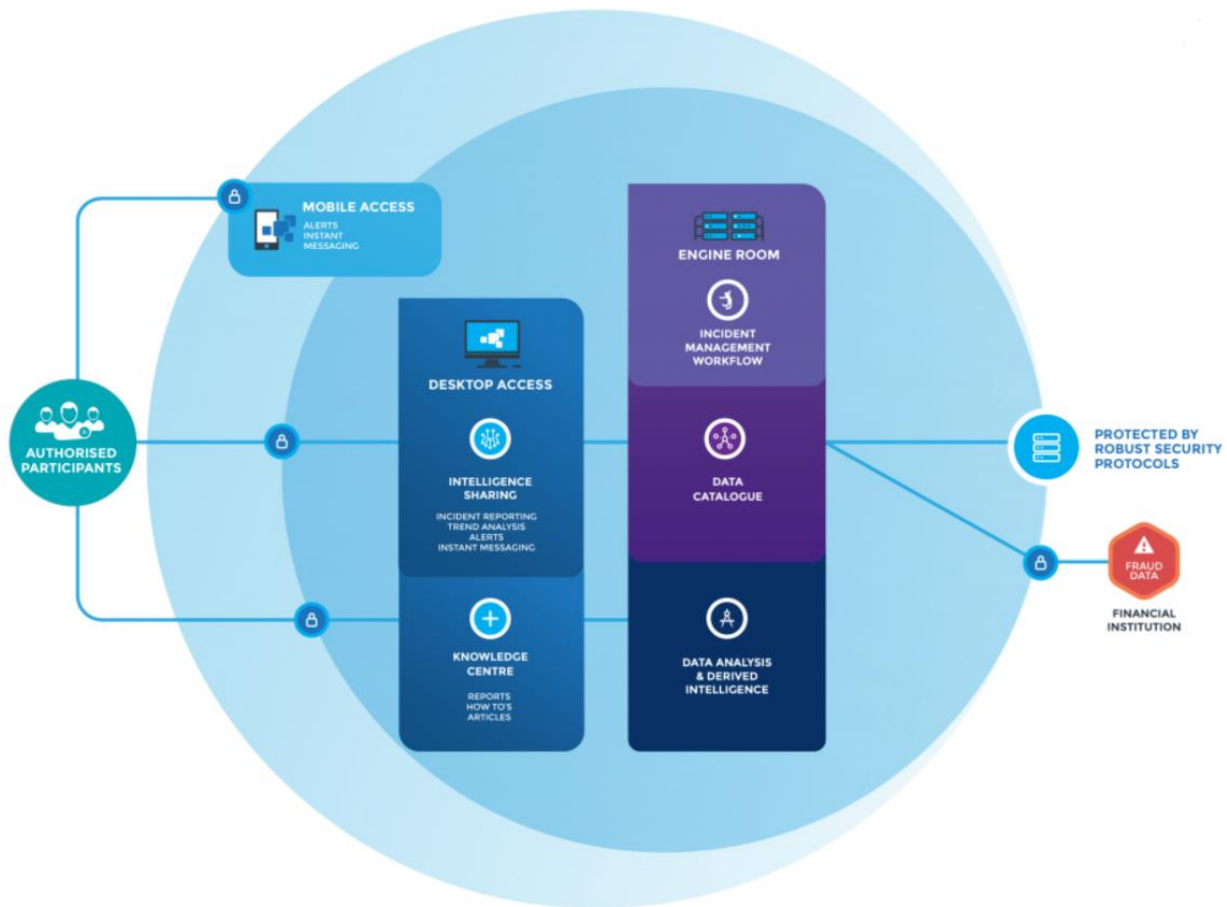
The FRX is a safe network that enables financial institutions to efficiently report and address fraudulent activities via a trusted platform which facilitates sharing of data and collaboration. The IGTO understands that the FRX currently provides 9 datasets that would be useful for fraud detection and prevention purposes. The following explanation about the utility of the FRX is given on the AFCX's Linked-In account³⁹ and the following diagram of the FRX platform is given on the AFCX's website:

By sharing information, analytic capability, and evidence-based insights, AFCX members create a powerhouse of financial and cybercrime intelligence that takes the fight beyond simply policing transactions and investigating irregularities. Working outside traditional silos creates the ability to identify criminal trends, activity and networks that operate across different businesses.

Cooperating with similar organisations overseas also allows the AFCX to identify criminal activity and networks that operate across international boundaries.

³⁹ <https://au.linkedin.com/company/afcx>

Figure 3: AFCX's Exchange platform



Source: AFCX website

The Fintel Alliance

Established under AUSTRAC, the Fintel Alliance, brings together government, industry, academic and international partners to harness a collaborative approach to combat and disrupt complex and emerging financial crime, money laundering and terrorism financing. There are currently 30 member organisations that are part the Fintel Alliance, including the ATO and each of the Big 4 Banks.

Information is shared within Fintel Alliance in accordance with the agreed information-sharing arrangements in the Members' Protocol. Under this Protocol, Fintel Alliance Partners agree that information disclosed to them within Fintel Alliance will only be used for the purposes for which the information was provided. The Protocol also requires all Fintel Alliance partners to comply with their privacy obligations under applicable privacy legislation, any common law confidentiality obligations and any secrecy provisions of legislation which govern their functions and activities.

The IGTO understands that the ATO's view is that tax secrecy and confidentiality provisions may only permit the ATO to share relevant information with the banks (TFNs, taxpayer names and bank account details) for the purpose of identifying fraudulent accounts through AUSTRAC and relevant prescribed

taskforces. This would indicate that a more direct sharing of information may better assist to identify, detect and prevent harmful financial practices, including tax fraud and crimes. The IGTO suggests that this conclusion requires closer consideration – see Sections 5.3 to 5.5.

ATO Fraud Forum

The ATO Fraud Forum is a public-private partnership forum that was set up to allow senior fraud officers from seven (7) major banks to come together to share information on fraud typologies and emerging threats related to tax refund fraud.

This forum is the primary mechanism for the ATO to directly engage with teams dedicated to addressing fraud within the banks.

Interbank Forum

The Interbank Forum is a quarterly forum attended by financial institutions, cryptocurrency exchanges, law enforcement and government agencies to share insights and intelligence relating to fraud and e-Security.

This forum involves the discussion of fraud typologies, emerging trends, scam typologies, potential controls, detection and diagnostic techniques.

Joint Chiefs of Global Tax Enforcement (J5)

The J5 is an international, intelligence-sharing alliance against tax crime and money laundering and made of agencies from Australia, the United Kingdom, the United States of America, Canada and the Netherlands.

The ATO's involvement in the J5 is supported through the ATO-led SFCT.

J5 Global Financial Institutions Partnership (GFIP)

The J5 GFIP is a newly established public-private partnership, which brings together tax authorities, financial intelligence units and international financial institutions from the J5 jurisdictions.

This forum shares typologies and indicators to help detect and prevent tax crime, including identity-based crime.

5.2. Information flows between the banks and the ATO on case-specific issues

Information provided through collaborative partnerships and forums

As outlined above, there are several established partnerships and forums for public and private organisations to discuss and share information related to tax crime and identity fraud. Both the ATO and

the major Australian banks are participants in many of these groups, namely the Fintel Alliance, ATO Fraud Forum and Interbank Forum.

Whilst these partnerships and forums share intelligence on typologies and trends associated with tax identity fraud, the ATO has explained that its view is that there are existing secrecy provisions that prevent the ATO exchanging operational information that relates to individual taxpayers. As a result, the ATO's engagement with banks and other entities through these groups has been limited to sharing high-level information on fraud risks identified and developing strategies to address issues of fraud. For the reasons given further below, the IGTO considers this ATO view may be overly conservative.

Information provided by the banks to the ATO

The banks proactively provide the ATO with a significant volume and range of information on transactions that they have identified as suspicious or fraudulent. This primarily occurs through the ATO's Financial Institution Referral (**FIR**) process where banks can make referrals to the ATO via the Reserve Bank of Australia. Further details of the FIR process is provided in Chapter 6 'Information gathering and analysis...'.

The information that the ATO receives from the banks through the FIR process includes:

- ATO payment reference number
- Payment amount
- ABN (if applicable)
- BSB
- Account number
- Account name (as provided by the bank)
- Account balance
- Whether the bank account is frozen
- Whether the bank account is a joint account
- Whether there are any signatories on the account
- Any other information the bank considers to be relevant to the referral

There are some restrictions on what information banks can provide to the ATO through the FIR process, which depends on the bank's terms of customer service, application of the *Privacy Act 1988* and the AML/CTF laws. Stakeholders have advised the IGTO that AML/CTF legislation permit the proactive sharing of certain information with AUSTRAC and its employees only. There are law enforcement exemptions provided in Chapter 75 of the AML/CTF Rules but these exemptions are limited to the following 'eligible agencies':

- (a) the Australian Crime Commission;
- (b) the Australian Federal Police;
- (c) the Immigration Department;
- (d) the NSW Crime Commission; or
- (e) the police force or police service of a State or the Northern Territory.

There is no exemption for the ATO. This suggests a need for a more co-ordinated approach to ensure information sharing to combat financial crimes is able to be shared in appropriate circumstances and through appropriate forums.

Banks can disclose instances of identity crime with AUSTRAC by lodging a Suspicious Matter Report (**SMR**). The ATO then obtains SMR data from AUSTRAC under the terms of an agreement between the two agencies. Specific reporting codes have been established to allow the ATO to easily detect matters relating to refund fraud (and their source and typology).

Outside of these processes which facilitate bank-initiated disclosures, the ATO receives information from the banks in response to statutory notices issued by the ATO under section 353-10 of Schedule 1 to the TAA 1953 which require the bank to provide information to the ATO. However, the ATO notices do not disclose the reason for needing information, including whether there is a suspected fraud that relates to the account or account holder.

Information provided by the ATO to banks

The ATO considers that there is no legislative provision or direct avenue for it to make a disclosure of taxpayer specific information connected to identity fraud to financial institutions for the purpose of alerting those institutions to the fraud.

Under section 355-70 of Schedule 1 to the *Taxation Administration Act* 1953, the ATO can disclose protected information to prescribed cross-agency taskforces, but only for or in connection with the specific purpose of that taskforce. Privately-owned organisations, such as financial institutions, are not members of these taskforces.

Taskforce partner agencies may choose to on-disclose protected taxpayer information to financial institutions for the purpose of achieving the objectives of the taskforce and the specific agency. However, the ATO advised that it cannot (and does not) disclose fraud specific taxpayer information to taskforces for the purpose of on disclosure to financial institutions.

Due to secrecy provisions, the ATO advises that it is also unable to provide the banks with any confirmation of whether any identity fraud has occurred. This includes circumstances where the ATO has investigated a referral received from the bank. After the ATO has completed investigating a bank referral, it will only advise the bank that it either has no interest in the refund amount that remains in the bank account or to retain that amount as it has an interest.

Also, the ATO advised that it cannot use a section 353-10 statutory notice for the purpose of informing the bank that the ATO suspects the account holder to be connected with TaxID fraud or that the ATO has confirmed those suspicions.

5.3. ATO systems quality may impact its risk management of secrecy provisions and TaxID fraud risk responsiveness

The ATO's conservative view on the secrecy provisions is understandable from a personal-risk perspective. Section 355-25 (of Schedule 1 to the TAA 1953) provides a sanction of up to 2-years imprisonment for a tax official that discloses protected information to another entity without excuse. Protected information includes information that was disclosed or obtained under or for the purposes of a taxation law (see Section 2.4 'Tax Secrecy provisions and relevant exceptions').

Accordingly, bank account information for a specific taxpayer could be protected information. If so, there is an inherent risk to be managed in disclosing suspected fraudulent bank account information – what if the ATO gets it wrong? What if their suspicions are incorrect? The weighing up of these risks and the Commissioner's obligations under the PGPA Act and Rule to take all reasonable measures to prevent, detect and deal with fraud need to be considered in light of the reliability of existing ATO controls and systems for detecting potentially fraudulent activity.

Where the existing ATO systems are not advanced, sophisticated, or reliable, then there is a likelihood that the ATO will manage this risk conservatively – that is, there is a reasonable basis to consider that tax officials will under report and/or under investigate potential fraudulent activity because there is a high personal cost of getting it wrong.

Investment in ATO systems that can accurately and expeditiously detect potential TaxID fraud is therefore necessary and warranted to adequately manage this risk. It is also necessary to protect the integrity of the tax system as well as taxpayer and tax practitioner trust and confidence in the integrity of the tax system and the ability of tax officials to fulfil their statutory obligations.

5.4. TaxID fraud investigation disclosures in the performance of tax officers' duties

One of the relevant exceptions to the tax secrecy provisions is a disclosure made in the performance of the taxation officer's duties under a taxation act. This exception appears to provide a more reasonable basis for the Commissioner to make lawful disclosures to the banks for the purposes of dealing with TaxID fraud. This exception⁴⁰ is as follows: in:

355-50 Exception—disclosure in performing duties

(1) Section 355-25 does not apply if:

⁴⁰ *Taxation Administration Act 1953*, Item 1 in the Table in section 355-50 of Schedule 1

5. Information Sharing to prevent TaxID fraud.

(a) *the entity is a *taxation officer; and*

(b) *the record or disclosure is made in performing the entity's duties as a taxation officer.*

... (2) *Without limiting subsection (1), records or disclosures made in performing duties as a *taxation officer include those mentioned in the following table:*

<i>Item</i>	<i>The record is made for or the disclosure is to</i>	<i>and the record or disclosure ...</i>
<i>1</i>	<i>any entity, court or tribunal</i>	<i>is for the purpose of administering any *taxation law</i>

The applicability of this section will primarily depend on whether the disclosure is sufficiently related to the purpose of administering any taxation law. In the case of TaxID fraud, an essential element of that fraud is for the Fraudster to access a Legitimate Taxpayer's ATO online account for the purpose of perpetrating the fraud. Obtaining information about that taxpayer is an inherent necessity as the Fraudster must be able to pass themselves off as that taxpayer for ATO access control purposes. Such action, if proven, would amount to a breach of section 8XA of the TAA 1953:

8XA Unauthorised access to taxation records

A person **must not take action with the intention of obtaining information about another person's affairs that:**

(a) **is contained in records in the possession of the Commissioner;** and

(b) *is held or was obtained by the Commissioner under or for the purposes of a taxation law;*

unless the person takes the action:

(c) *under the Freedom of Information Act 1982; or*

(d) *in accordance with the processes of a court or the Tribunal; or*

(e) *in the course of exercising powers or performing functions under or in relation to a taxation law.*

Penalty: 100 penalty units or imprisonment for 2 years, or both.

A Fraudster also breaches section 8WB of the TAA 1953 if it is proven that they have used a Legitimate Taxpayer's TFN when opening a bank account, used that TFN to link a myGov account to the Legitimate Taxpayer's ATO online account or used that TFN to pass the ATO's PORO controls:

8WB Unauthorised recording etc. of tax file number

(1) A person must not:

- (a) record another person's tax file number or maintain such a record; or*
- (b) use another person's tax file number in a manner connecting it with the other person's identity; or*
- (c) divulge or communicate another person's tax file number to a third person.*

Penalty: 100 penalty units or imprisonment for 2 years, or both.

If administering the taxation laws involves investigating suspected non-compliance with the tax laws or suspected breaches of specific prohibitions in those laws, then this appears to be reasonable grounds for the ATO to make disclosures of bank account details and their suspicions to the banks for the purposes of dealing with that non-compliance and breaches of sections 8XA and 8WB of the TAA 1953. Disclosure of information that identifies taxpayers, such as name and bank account numbers, and the ATO's suspicions would be reasonably necessary if the ATO were to obtain information from the banks that would assist it to determine whether the bank account and its controller were connected to TaxID fraud.

Investigation of suspected TaxID fraud necessitates, at the very least, disclosure of the investigation hypothesis to ensure that the banks provide information that is material to the investigation of that hypothesis. Not disclosing the hypothesis significantly increases the risk of jeopardising the investigation. This is because it substantially increases the likelihood that needed evidence will not be obtained due to ill-informed questions by the ATO or that evidence will be overlooked due to the bank not considering it relevant or important to include in its answer of the ATO's questions.

5.5. IGTO observations and potential solutions to address information sharing limitations

Making Disclosures in the performance of duties

The IGTO considers that the ATO should carefully reconsider its view and obtain independent legal advice regarding the application of the 'in the performance of duties' tax secrecy provision exception⁴¹ to the facts and circumstances of TaxID fraud cases and tax secrecy provisions.

Other agencies such as AUSTRAC can notify the banks of suspicious accounts, which then allows the banks to take action by blocking or freezing those accounts. If the ATO disclosed its suspicions to the bank, the bank could similarly consider taking appropriate action. However, if the bank itself does not suspect the account is involved in fraud, it may not have reason to examine the account to determine if there is a reasonable basis to freeze the account.

⁴¹ *Taxation Administration Act 1953*, Item 1 in the Table in section 355-50 of Schedule 1

It may be that the ATO is conservative with what information it believes can be disclosed without breaching tax secrecy and confidentiality. However, to the extent the ATO considers it is prohibited from making disclosures for the purposes of preventing TaxID fraud, it should advocate for a specific exception to the tax secrecy provisions to facilitate such disclosures (for example, to the Fintel Alliance and AFCX) and ensure that appropriate criteria and controls are imposed on those disclosures.

Administrative workarounds in the absence of legislative change

In the interim, there may be some useful non-identifying information that could be disclosed at present that may assist banks with identifying and addressing suspicious bank accounts. Examples of such non-identifying information may include:

- Non-identifying details that are relevant for the bank's KYC obligations, such as IP address used, and
- Patterns that would allow the bank to refine searches of its records, such as large numbers of entities at the same address with the same bank account.

Prescribed taskforces

The IGTO also observes that, according to the ATO's website, one of the focuses of the SFCT is to combat cybercrime and identity theft that is perpetrated through the tax and superannuation systems.⁴² As such, there may also be scope for the ATO to leverage this existing taskforce to facilitate the disclosure of protected information to banks in order to achieve the SFCT's purpose of addressing tax crime involving identity-related fraud.

The other alternative would be to create a new prescribed taskforce specifically for the purpose of addressing TaxID fraud. However, it is acknowledged there are administrative burdens for establishing a taskforce and it may not be the most effective or timely way to improve information sharing between public and private entities. There may also be concerns with the inclusion of private entities, such as financial institutions, in government agency taskforces.

Additionally, the functions and existence of the taskforce may be linked to the continued funding of that taskforce. This taskforce approach appears suited to ephemeral or transient focus areas whereas the need to continuously monitor and respond to evolving TaxID fraud is becoming generally accepted as necessarily an enduring and persistent effort. However, the inclusion of the AFCX which is already self-funded by its members may offer an alternative.

Improving collaboration and the use of 'fusion cells'

Stakeholder feedback indicates that the information shared by the ATO at collaborative forums, such as the Fintel Alliance, is high-level and not actionable, which is consistent with the ATO's responses to this

⁴² ATO, "Serious Financial Crime Taskforce: We're targeting: Cybercrime affecting the tax and superannuation systems (Fact Sheet) (3 June 2021) [497b1534-17d2-418c-8240-229a1caa94dd_SFCT_Cybercrime_Fact_Sheet_pdf \(sitecorecontenthub.cloud\)](https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/serious-financial-crime-taskforce) available from <https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/serious-financial-crime-taskforce>

investigation. There may also be question marks on how quickly information is able to be exchanged through such forums in order to address emerging fraud typologies in (close to) real time.

Collaborative forums such as the Fintel Alliance are intended to be a 'fusion cell' to share information between banks and government agencies in a safe space. The use of fusion cells to safely share protected information as part of public and private sector partnerships has been explored previously in the IGTO's 2018 Review, *The ATO's Fraud Control Management*⁴³. The IGTO understands that participants have relevant and appropriate security vetting clearance.

Improving information sharing via AFCX membership and participation in the FRX

The AFCX's FRX appears to be a useful source of fraud thematics, typologies, fraud data and, more importantly, could facilitate information sharing for case specific issues. In addition to sharing bank account information, the FRX could be used to facilitate the exchange of other information that may be indicative of identity fraud, such as name mismatches and payee or income information. Since the ATO is currently not a member of AFCX and does not have access to the FRX, it would be beneficial for the ATO to become a member.

There is also a device ID catalogue, amongst other datasets, that are shared between AFCX members. The IGTO understands that the ATO aims to use the AFCX's device catalogue in a proof of concept project in early October 2023⁴⁴ and is awaiting legal advice before proceeding. Notwithstanding this, the IGTO recommends the ATO equip its systems with the capability to capture device IDs as well as join the AFCX (see Recommendation 2(a) below). The IGTO understands that there is no legal prohibition to doing so (See Section 6.2 Existing ATO systems, data and internal referrals – Device and IP address data) and recommends that the ATO engage the community in consultation to ensure that any sensitivities relating to the capture of device ID information are surfaced and considered appropriately.

Real-time monitoring and flagging of bank accounts and TFNs may be possible using the information that could be shared through the AFCX. The FRX would be best placed for real time investigation and exchange of information between the ATO and the banks, as it is said to provide a protected platform through which information can be exchanged automatically via agreed parameters and rules. This would help the ATO overcome the issue of differing data protocols that it would face in directly dealing with the banks on an individual level.

Furthermore, the AFCX has the support of the Commonwealth Attorney-General's Department and is a key limb in the Australian Government's National Organised Crime Response Plan. The AFCX is the primary channel through which the public and private sector coordinate their intelligence and data-sharing activities for the investigation and prevention of financial and cyber crime.

The ATO is not a member of the AFCX, but based on stakeholder consultations, the ATO would be welcomed as a member and is invited to join. Accordingly, ATO membership would facilitate access to

⁴³ Available from <https://www.igt.gov.au/investigation-reports/ato-fraud-control-management/>

⁴⁴ ATO, Response to IGTO's 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

5. Information Sharing to prevent TaxID fraud.

information shared through the FRX to enable it and financial institutions to more efficiently report and more effectively address fraudulent activities.

To the extent that establishing real-time communication with the banks via FRX requires industry-agreed data protocols and specific legislative authority, the ATO should actively support and advocate for such initiatives to enable it to more actively and effectively engage with trusted participants in the financial system to combat TaxID fraud.

Recommendation 2(a)

The IGTO recommends that ATO actively engage with trusted participants in the financial system to combat TaxID fraud and join the AFCX and actively participate in the FRX on case specific issues

6

INFORMATION GATHERING AND ANALYSIS TO IDENTIFY AND ADDRESS POTENTIAL TAXID FRAUD

This Chapter discusses the main sources of information that the ATO uses to identify potential TaxID fraud and the Tax Agent-Client link on ATO systems

6. Information gathering and analysis to identify and address potential TaxID fraud

The ATO's fraud prevention and detection controls rely on the gathering and analysis of ATO and third-party information to be effective. This includes utilising information received from the following sources:

- Affected taxpayers and tax practitioners who have reported a fraud to the ATO
- Existing ATO systems data, such as bank account details, IP addresses, some device details and third-party income data matching
- Financial institutions, by way of referrals received or responses to statutory information requests made by the ATO
- Other Commonwealth or government agencies

6.1. Fraud intelligence from affected taxpayers and tax practitioners

Collecting information on fraudulent bank accounts

Although the ATO does appear to record information that is reported by the taxpayer about the fraud, including details of the fraudulent bank account that is used, it is unclear how the ATO uses this information to prevent and detect fraud. For example, the ATO does not cross-check or blacklist these accounts to help prevent and detect further frauds.

There is also a link to the ATO website's fraud page⁴⁵ to the Commonwealth Fraud Prevention Centre webpage.⁴⁶ While that ATO fraud web page allows taxpayers or their representatives to report scams, unpaid superannuation and ATO officer corruption, it does not allow reporting of TaxID fraud so that the relevant (fraudulent) banking details can be captured and investigated by either a law enforcement agency, the ATO fraud team or one of the many private public partnerships that are sharing information for the purposes of combatting financial crimes.

⁴⁵ <https://www.ato.gov.au/about-ato/contact-us/report-fraud-tax-evasion-a-planning-scheme-or-unpaid-super>

⁴⁶ <https://www.counterfraud.gov.au/find-where-report-fraud>

6. Information gathering and analysis to identify and address potential TaxID fraud.

There are ATO webpages that provide guidance for victims of identity fraud.⁴⁷ However, the IGTO has been unable to locate any ATO reporting page or contact centre where bank account details associated with TaxID fraud are specifically reported. This is a significant oversight and omission.

The difficulty in locating such a reporting page was also raised as a concern in stakeholder submissions.

Recommendation 3(e)

The IGTO recommends that the ATO provide a clearly identifiable and easily accessible reporting page or contact centre where bank account details associated with TaxID fraud can be reported.

The ATO's Client Identity Support Centre

The ATO's website⁴⁸ instructs taxpayers who are (or suspect they have been) a victim of tax identity fraud to contact the Client Identity Support Centre (CISC) and report any (suspected) fraudulent activity on their ATO account. The type of information that is obtained by CISC includes details of:

- Relevant lodgements
- Compromised personal identity information
- Suspicious/unusual activity relating to digital channels, such as myGov and myGovID
- Tax agents that are linked to the taxpayer's record
- Suspicious/unusual changes to the taxpayer's contact and bank account details
- Suspicious/unusual activity on the taxpayer's account on ATO systems, including any ABN and GST registration
- Suspicious/unusual activity linked to the taxpayer, such as that relating to superannuation, non-individual entities and economic stimulus measures.

The above information is captured in a template by CISC, is stored in the ATO's client relationship management system and is made available for internal reporting purposes.

Additionally, where a tax agent provides information regarding a data breach or cyber incident, the ATO advised that this information is captured by frontline staff in a template and referred to a management and support team within CISC for support to be provided. In 2023, the CISC unit has implemented a procedure which allocates responsibilities for initial risk assessment and a pre-defined pathway for

⁴⁷ For example, <https://www.ato.gov.au/online-services/identity-security-and-scams/help-for-identity-theft>

⁴⁸ ATO, 'Help for identity theft' (a webpage on www.ato.gov.au) (last updated 27 July 2021)
<https://www.ato.gov.au/online-services/identity-security-and-scams/help-for-identity-theft>

6. Information gathering and analysis to identify and address potential TaxID fraud.

treatments that are based on this risk assessment which include identification of the roles and responsibilities of the relevant ATO business units in these pathways.

The ATO explained that its Tax Integrity Centre (**TIC**) scans new tip-offs received from the community to identify possible fraudulent activity related to identity takeover and will check the relevant taxpayer's account. The IGTO's *Review into the ATO's Fraud Control Management (2018)*⁴⁹ provides more information on the ATO's TIC system (or Tax Evasion Referral Centre (**TERC**) as it was called then).

The ATO's Fraud and Criminal Behaviours Triage Centre

The ATO's Fraud and Criminal Behaviours (**FCB**) Triage Centre collects internal intelligence on potential fraud from ATO business lines.

The ATO advised that the Triage Centre also receives external referrals from law enforcement and partner agencies of potential, suspected or known identity crime or unauthorised ATO or myGov account access. Referrals received from law enforcement agencies often includes information provided in the police reports that are made by taxpayers or their representatives.

It should be noted that although the FCB business line was created on 1 July 2023, it continues with the essentially the same responsibilities that the now defunct Integrated Compliance business line had before that date.

6.2. Existing ATO systems data and internal referrals

Bank account data

As discussed in Chapter 4, the ATO captures BSB and account numbers as well as the account name of bank accounts that are registered on taxpayer's accounts on ATO systems. The ATO does not currently obtain any further information regarding taxpayers' bank account, unless it does so during an investigation or had received it from external parties in reporting their concerns.

As discussed in Section 3.5 'ATO's risk management regarding bank account changes', the ATO does not automatically check whether a single bank account is linked to multiple (unrelated) taxpayer ATO accounts. This check requires manual intervention at critical stages in the process and is only undertaken if a taxpayer's account has previously been identified as compromised or potentially compromised, i.e. the ATO system does not automatically monitor or scan for taxpayer accounts that have bank accounts which are registered on other (unrelated) taxpayer accounts.

Device and IP address data

The ATO advised the IGTO that it collects some data in relation to a taxpayer's interaction with their ATO account online. This includes the IP address that is used. The ATO also noted that it has identified a list of IP addresses that have been used by fraudsters to access taxpayers' online accounts. However, the ATO

⁴⁹ Available from <https://www.igt.gov.au/investigation-reports/ato-fraud-control-management/>

6. Information gathering and analysis to identify and address potential TaxID fraud.

also advised that it does not have the technology to integrate the IP address data into its current systems so that it can be used in real-time to detect suspicious interactions.

The ATO also advised that, unlike financial institutions, it does not collect the unique device ID from all types of devices used by the taxpayer to access their ATO account. This device data is limited to the type of device used (i.e. a phone, computer or laptop) and the operating system or software used on that device. For mobile phones, the International Mobile Equipment Identity (**IMEI**) number is unique to each device.

During the investigation, the ATO advised that it did not collect device ID because of legislative restrictions. However, the ATO has not identified the specific restrictive provisions it referred to.

The IGTO considers that there is no legislative prohibition on the ATO collecting device ID data. In fact, such data would likely assist investigations into TaxID fraud a great deal. Collection of device ID data would need to comply with the *Privacy Act 1988* requirements. However, it is unclear that these requirements would effectively prohibit collection of this information given the wealth of evidence that TaxID fraud is being perpetrated by unknown actors. Further, it is noted that the ATO is pursuing a trial with the AFCX to use their device ID data sets.

Notwithstanding this, public perceptions are important to the confidence in the administration of tax and therefore the ATO would be prudent to start engaging with the community over this potentially sensitive, but necessary, data collection need.

Notwithstanding the absence of real-time integration of such data, there is scope for the ATO to actively consider and improve how it uses the data it already obtains.

Third-party data matching

The ATO obtains information from third parties such as employers, financial institutions, investment bodies and other government agencies to pre-fill tax returns and verify the accuracy of information reported by taxpayers in their tax returns and activity statements.⁵⁰ The ATO's use of this information in its lodgement risk model is discussed in Section 4.5 'ATO's risk management regarding bank account changes'.

Internal ATO referrals

ATO officers can make a referral to CISC for account protection and remediation where they identify suspected third-party fraud on a taxpayer's account.

⁵⁰ ATO 'Third-party reporting' (a webpage on www.ato.gov.au, last updated 14 December 2022)
<https://www.ato.gov.au/businesses-and-organisations/preparing-lodging-and-paying/third-party-reporting>

6.3. Information received by the ATO from other organisations and agencies

The ATO receives a wealth of information from a range of entities, both private sector and public sector. Some information is routinely required under statute, some is proactively provided without the ATO's prior knowledge.

With respect to bank accounts that are used in TaxID fraud, the organisations with some of the most valuable and actionable information are the financial institutions.

Chapter 4 'Information sharing to prevent TaxID fraud' discusses the issues relating to information sharing between the ATO and financial institutions. Additional factual material is set out below.

Financial institution referrals

Where tax refunds have been issued to taxpayers' nominated bank accounts, the recipient bank itself may identify potentially fraudulent arrangements connected with the refund via its own fraud detection models.

Where this occurs, the bank can provide information to the ATO about the transaction and its suspicions through the ATO's FIR process. This FIR process involves:

1. The bank completes an approved reporting template with relevant information including identification and payment details.
2. The bank sends the template via email to the Reserve Bank of Australia (**RBA**).
3. The RBA forwards the bank referral template to the ATO's FIR team.
4. The FIR team manually records all reported transactions.
5. An internal reporting tool allocates the transaction to the relevant business line for risk assessment and further compliance action (if deemed appropriate). Transactions which were GST refunds are manually allocated.
6. The relevant business line conduct reviews, audits or risk assessments to ascertain the level of risk for the reported refund.
7. After the business line has investigated the referral, they are required to advise the FIR team whether the refund should be retained or released.
8. The FIR team will then inform the RBA whether the ATO has an interest in the account or wishes for the refund to be retained.
9. The RBA will then forward the FIR team's email to the bank for action.

The ATO advised that, since December 2023, its FIR team tracks scheduled disbursements within 3 days for some institutions for potential identity fraud issues. This information is passed on to the relevant risk

6. Information gathering and analysis to identify and address potential TaxID fraud.

areas for their analysis and decisions. The process includes identifying instances where the taxpayer's name and bank account name on ATO systems do not match and changes of bank account details which occur before refunds are due to issue.

Requiring information from banks – section 353-10 statutory notice

The ATO can require the banks to provide the ATO with information by issuing a statutory notice under paragraph 353-10(1)(a) in Schedule 1 to the TAA 1953:

(1) The Commissioner may by notice in writing require you to do all or any of the following:

*(a) to give the Commissioner any information that the Commissioner requires for the purpose of the administration or operation of a * taxation law; ...*

This statutory notice, known as a section 353-10 notice, allows authorised officers to require any person to provide the information requested to the ATO.

The ATO advised that when issuing a section 353-10 notice for the purpose of investigating suspected TaxID fraud activity, the ATO will require the bank to provide information relating to the bank account in question, including identity documents used to open the account and copies of bank statements. IGTO dispute investigations have confirmed that the identity documents themselves are not made available to the ATO. Instead, the ATO receives details of the type of identity document and the document number.

myGov/Interim Oversight Authority referrals

Another source of actionable information is that received from Services Australia by reason of myGov's connection with the ATO's Online services.

The ATO advised that one of the terms and conditions of use of myGov by partner agencies is that when another member's service advises myGov that fraud is committed on their client account and the ATO is also linked as a service for that member, the ATO is required to report suspected fraud to myGov Operations. Where the ATO suspects ID takeover via a myGov account this is referred to Services Australia for investigation and suspension of the myGov account. Services Australia also provide a report to the ATO with myGov account details that have been compromised. CISC staff will then identify the affected client's record from data provided by Services Australia, investigate the breach and contact the client. An incident will be created with a Siebel alert attached, and relevant treatment determined following investigation, using various tools for analysis. Following investigation, CISC recommend remediation action for the client's ATO account, or taking no further action where the account has not been compromised or where the ATO has already identified the client as having compromised records and security measures have previously been applied.

6.4. Tax Agent-Client link in ATO systems and notification of de-linking

Approximately 70 per cent of individual taxpayers use a registered tax agent, mainly to assist in meeting their annual income tax return reporting obligations. The remainder self-lodge their income tax returns.

6. Information gathering and analysis to identify and address potential TaxID fraud.

There are approximately 15.1 million individual taxpayers in Australia in the 2020–21 income tax year.⁵¹ Based on ATO information, the vast majority of these taxpayers, approximately 14.6 million, also have linked their myGov account to their ATO Online accounts.⁵²

A number of reported instances of TaxID fraud involved a fraudster delinking Legitimate Taxpayers from their tax agent's client list and then lodging amendments or original returns which resulted in unauthorised refunds. Neither the Tax Agents nor the taxpayer (their clients) currently receive any notification from the ATO that a client has been removed from their agent listing.

Tax agents have (by chance) been able to identify fraudulent refunds in many of the IGTO dispute investigations, but rarely because they received the relevant notifications from the ATO. Accordingly, the fraud is invariably identified by the agent only after the fact. The ATO notification also does not identify the relevant client – so the agent does not know which taxpayer account to check.

The ATO considers use of the highest strength of myGovID identity verification (which involves matching a live face against a photo on an accepted identity document) would be among the better solutions at this point in time. However, draft digital identity legislation before the Parliament at the moment⁵³ would, if passed without amendment, prohibit the mandated use of a digital identity. Accordingly, the ATO has chosen to embark on a project to implement Agent-Client linking for small businesses and individuals as the next optimal remedial measures. The ATO had successfully piloted Agent-Client linking arrangements with large businesses and began to implement the process to new small business clients of tax agents in November 2023.

The IGTO understands that tax professionals have raised concerns during this roll-out to small businesses and the ATO is currently in the process of resolving these concerns and issues. Practitioners have told the IGTO that they agree with the reason for the initiative, however, expressed concerns that the process that the ATO is seeking to implement does not adequately take into account the practical difficulties that are faced by different clients and the disproportionate amount of time taken to resolve them. For example, one practitioner explained that in helping their client to set up their myGov and myGovID accounts, they could not link the accounts to the client's ATO Online account. After a number of successive phone calls to the ATO Helpline, it was discovered that the client's myGov account had been incorrectly registered with an extra letter in the client's name. So, the attempt to link the myGov account was rejected by ATO Online. Given that this was part of the client's engagement meeting with the tax agent, first impressions were formed and the systems problems were [unfairly] attributed to the agent's level of [in]competence.

⁵¹ ATO, 'Snapshot' (webpage on www.ato.gov.au, last updated 8 June 2023) <https://www.ato.gov.au/about-ato/research-and-statistics/in-detail/taxation-statistics/taxation-statistics-2020-21/statistics/snapshot?anchor=Snapshot#Snapshot>

⁵² ATO, Response to IGTO's 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

⁵³ Parliament of Australia, Digital ID Bill 2023 (Introduced into the Senate on 30 November 2023)

6. Information gathering and analysis to identify and address potential TaxID fraud.

As at the date of this report, the IGTO understands that the ATO is engaged in discussions with the tax professional bodies to resolve these Client-Agent linking concerns. It is hoped that these discussions will resolve the issues that threaten agents and client's ongoing engagement in this initiative.⁵⁴

Notwithstanding this, it is also important to note the critical role that tax practitioners play in the high levels of voluntary compliance in Australia's tax system. Protecting the integrity of the Tax system is a shared risk of the ATO, the Tax Practitioners' Board and practising Tax Practitioners, amongst others. Tax agents likely have the best understanding of their client's financial and tax circumstances and are also well placed to quickly detect suspicious activity, where they are appropriately prompted. Therefore, it is also important for the ATO to provide timely and relevant information to notify Tax Agents when a client has been deleted from their client list – so that the agent can identify unscrupulous deletions (that may be associated with TaxID fraud).

The Tax Agent is arguably best placed to identify if the amendments are authorised and reasonable but because they have been delinked, there is no visibility of the unauthorised amendments or their reasonableness. Although Tax Agents can manually monitor their complete client listing to identify discrepancies, a more efficient reporting system would be to ensure that Tax Agents receive notification on a regular basis (daily or weekly) of amendments (additions but importantly deletions) to their Tax Agent client listing.

Unless Tax Practitioners are notified that clients have been removed from their list, they cannot monitor for suspicious activity in respect of their client's tax records. Sole reliance on client-initiated nominations, would lessen the level of controls that could reasonably be employed to mitigate the risk of TaxID fraud.

Early communication by the ATO of changes to agent client listings could assist to prevent fraudulent filings and claims on the tax system.

To the extent that ATO notification to tax agents of client de-listing (or 'de-linking') requires specific legislative authority, the ATO should consult with the tax profession to identify the most appropriate legislative reform it could recommend to Government to implement this critical recommendation which would better empower the tax profession to assist the ATO to combat TaxID fraud.

Recommendation 3(c)

The IGTO recommends the ATO notify Tax Practitioners in a timely manner if a client has been removed from their tax agent's client listing

⁵⁴ ATO, Response to IGTO's 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

7

PROCESSES AND ACTUAL ATO CONTROLS

This Chapter describes key processes that are exposed to the risk of TaxID fraud and ATO controls which relate to those processes and the risk of unauthorised bank account change

7. Processes and actual ATO controls

7.1. Introduction

This Chapter summarises ATO-provided information that describes the main processes and controls that are connected to TaxID fraud.

The Table below gives a high-level summary of the current ATO actions or processes and controls that are relevant to the changing of taxpayers' bank account details on the ATO's systems.

Table 5: Actions or processes to access taxpayer accounts and bank account change-related controls

Action or process	ATO control	ATO controls in operation since...
Creating a myGov account	<ul style="list-style-type: none"> N/A – myGov is managed by Services Australia 	<ul style="list-style-type: none"> N/A
External Bulk Data breach of taxpayer information	<ul style="list-style-type: none"> Client Account Services (CAS) Data Breach Playbook (established end-to-end workflows and responsibilities) Updated March 2023 (to address Critical Third Party Data Breach events) 	<ul style="list-style-type: none"> No evidence made available, but records indicate between March 2023 and January 2024
Financial institution's provision of actionable information	<ul style="list-style-type: none"> Financial Institution Referral (FIR team triage and action) 	<ul style="list-style-type: none"> No evidence made available, but records indicate approx. 2020 communication step implementation and December 2023 FIR team 3-day triage standard and action implementation
Taxpayer/tax practitioner or other Internal/external referral of actionable information	<ul style="list-style-type: none"> CISC recording, risk assessment and allocation 	<ul style="list-style-type: none"> Since 2018, in one form or other January 2024 work process redesign proposal to deal with backlogs
Creating a myGov account	<ul style="list-style-type: none"> N/A – myGov is managed by Services Australia 	<ul style="list-style-type: none"> N/A
Using a myGov account	<ul style="list-style-type: none"> N/A, however interagency myGov Agreement requires Partner agency reporting and dissemination of account compromise cases 	<ul style="list-style-type: none"> No evidence made available, but records indicate no later than March 2022
Linking a myGov account to ATO Online	<ul style="list-style-type: none"> PORO required 	<ul style="list-style-type: none"> Since inception, however amendments have been made to PORO requirements on a periodic basis to

Action or process	ATO control	ATO controls in operation since...
		address risks
	<ul style="list-style-type: none"> • ‘Was this you?’ messaging (if there’s a valid email or mobile on file, sent manually during business hours at least the following business day after the even number) 	<ul style="list-style-type: none"> • No evidence made available, but records indicate between July 2021 and 25 January 2024
Accessing ATO Online via myGov	<ul style="list-style-type: none"> • Two factor authentication when logging in to an ATO-linked myGov account 	<ul style="list-style-type: none"> • No evidence made available
	<ul style="list-style-type: none"> • Two factor authentication required when using myGovID 	<ul style="list-style-type: none"> • No evidence made available
Accessing ATO Online services for Business	<ul style="list-style-type: none"> • Two factor authentication required when using myGovID 	<ul style="list-style-type: none"> • 2019-20 • Update in early 2023 to allow user to see all devices connected to myGovID account • Update in late 2023 to message user’s mobile device if new device added to their myGovID account
Accessing ATO Online services for Agents	<ul style="list-style-type: none"> • Two factor authentication required when using myGovID 	<ul style="list-style-type: none"> • 2019-20 • Update in early 2023 to allow user to see all devices connected to myGovID account • Update in late 2023 to message user’s mobile device if new device added to their myGovID account
Updating contact details on ATO Online	<ul style="list-style-type: none"> • None 	<ul style="list-style-type: none"> • N/A
Updating bank account details on ATO Online	<ul style="list-style-type: none"> • Barred bank account list (prevents input of that BSB and account number again) 	<ul style="list-style-type: none"> • No evidence made available, but records indicate no later than August 2022⁵⁵
Lodging tax returns and/or activity statements	<ul style="list-style-type: none"> • Income Tax Refund Integrity suite 	<ul style="list-style-type: none"> • No evidence made available, but records indicate initial implementation in 2008 with alterations made since
	<ul style="list-style-type: none"> • Income tax ID crime model (if threshold reached, CAT applied and allocated for audit) 	<ul style="list-style-type: none"> • No evidence made available

⁵⁵ ATO, Response to IGTO’s 12/12/2023 request for information – Q3 (received 15 February 2024) p 4; ATO, Response to IGTO’s 12/12/2023 request for information – Q2 (received 15 February 2024) p 2.

Action or process	ATO control	ATO controls in operation since...
	<ul style="list-style-type: none"> Contemporary GST risk model (incl. ID crime and incorrect reporting models - if threshold reached, allocated for case officer management) 	<ul style="list-style-type: none"> No evidence made available
	<ul style="list-style-type: none"> High-Risk Linking Model (applied to myGov linked accounts – if rules met) 	<ul style="list-style-type: none"> Piloted in April 2023 Updated in October 2023⁵⁶
Where fraud or fraud risks have been previously identified for that account	<ul style="list-style-type: none"> Compromised account indicator (enacts various automated functionality, including credit suppression (i.e.. refund retention) ATO Online access prevention, suspension of lodged form pending verification; once CAT is enacted, it is usually permanently retained) 	<ul style="list-style-type: none"> No evidence provided, but no later than January 2024
	<ul style="list-style-type: none"> Client identity watchlist (officer decision to place account on list, facilitates reporting and increased PORO, used as risk attribute) 	<ul style="list-style-type: none"> No evidence provided, but records indicate 2013 implementation, with additions implemented since
	<ul style="list-style-type: none"> FIR Report monitoring (report generated for recent suspicious financial institution account changes on client accounts, manually reviewed) 	<ul style="list-style-type: none"> No evidence made available, but records indicate no later than January 2024
	<ul style="list-style-type: none"> model (if a return is lodged, CAT applied, then allocated for risk assessment and action; if no CAT, then refund retained) 	<ul style="list-style-type: none"> No evidence made available

Source: ATO, IGTO and Open Source

The main processes and controls are described below.

7.2. Process and controls for linking myGov accounts to ATO Online accounts

The process for creating a myGov account and linking a myGov account to ATO Online (which is the portal used by individuals to access their online ATO account), and the relevant controls for linking myGov to ATO Online are detailed below.

⁵⁶ ATO, Response to IGTO's 12/12/2023 request for information – Q7 (received 15 February 2024) p 4.

Creating a myGov account

myGov is an Australian Government portal for accessing government services online. It is managed by Services Australia.

To access a government agency service online, an individual is required to create a myGov account and link that account to the government agency (such as the ATO) in order to access that service. There is also no limit on how many myGov accounts can be created for an individual. An individual can create more than one functional myGov account to access their services, however, each of these different accounts must use different email addresses.

An individual only requires a valid email address to create a myGov account. A confirmation code is sent to the email address to progress registration of the myGov account. The individual can also provide a mobile phone number when setting up an account, however this information is optional.

As part of the account registration process, individuals are required to select and answer three secret questions. Upon registering, a username is allocated to the individual and they can choose a password.

The user must also select a second sign-in option to secure their myGov account, either two factor authentication (an SMS code or a code from the myGov code generator) or secret questions and answers. Where the user downloads and uses the myGov app, they may also select to use a biometric identifier that their device is enabled to confirm – for example, a fingerprint. Alternatively, individuals with an existing digital identity (known as myGovID) may use this to establish a myGov account.

At this stage in the setup process, the individual has yet to link their myGov account to any agency services and has not had their identity verified by those agencies. Details used to establish a myGov account are held by myGov and not updated on the ATO client record for that individual, in accordance with myGov policy and standards.

Linking a myGov account to ATO Online

A myGov account must be linked to ATO Online before an individual can access their ATO account online. Although myGov is managed by Services Australia, the ATO is responsible for determining how an active myGov account can be linked to the ATO.

To link a new (and ATO-unverified) myGov account to ATO Online, the individual is required to provide:

- Name
- Date of birth
- TFN
- Address as known to the ATO
- Answers to a series of security questions, referred to as ‘passing’ Proof of Record Ownership (PORO)

For an individual to pass PORO, they must provide two (2) items of proof relating to information on their tax record.

As an alternative to passing PORO online, the individual can contact the ATO by phone to provide PORO and, if successful, obtain a code which they may use to link their myGov account to their ATO Online account (**linking code**). To pass PORO over the phone, the individual must provide:

- a minimum of two (2) items of proof by responding to randomly generated PORO questions; and
- an identity document, such as a driver's licence or passport, that can be verified with the **DVS**.

The individual is required to pass PORO, either online or by phone, when linking their first myGov account to ATO Online as well as linking any further myGov accounts (known as 'relinking' or an 'overlinking event').

Overlinking of a myGov account to ATO Online

Due to myGov requirements, a myGov account that is linked to an individual's ATO Online account is not permanently linked to that account. This means that a new myGov account can be linked to ATO Online for that individual (if it meets the required linking criteria) which disconnects and overrides the previously linked myGov account. This is referred to as overlinking.

Where a fraudster has obtained or stolen an individual's identity information and is able to pass the ATO's PORO protocols, there is a risk they can override a genuine user's myGov link (or create a new link if one does not previously exist) and connect to that individual's ATO online record.

'Was this you?' messaging

The ATO can send a 'Was this You?' (**WTY**) message for new overlinking events from myGov to ATO Online where the ATO has a valid mobile number or email address for the individual immediately prior to the event. This message is to confirm if the link was created by the individual or whether it is likely to be fraudulent.

A copy of the WTY text message sent when a linking event occurs is provided below:⁵⁷

*Hi [insert name],
On [insert date/time] a new link to your Australian Taxation Office (ATO) record was created in myGov, and changes to your account details have been made. If this wasn't you, call our Client Identity Support Centre on 1800 467 033 (choose Option 3).
Australian Taxation Office*

WTY messages are not sent in real time. In most instances, WTY messages are sent by ATO officers manually to the individual on the following business day after the linking event has occurred. As WTY messages are manually issued by ATO officers they are unable to be sent after business hours, on

⁵⁷ The WTY email provides the same information as the text message but in an email format.

weekends or on public holidays. This can result in some messages only being issued a few days after the linking event. This delay defeats the purpose of the WTY message.

The WTY process relies on the individual keeping their contact details on their ATO account up to date. There may also be difficulties where the contact details on the ATO account belong to a tax agent rather than the individual themselves. The ATO advises that in 2022 approximately 202,000 individual taxpayers have listed their tax agent's mobile number as their contact number and that it has advised tax agents to not put their own number on the taxpayer's account as there is no provision to specify which contact number to send the WTY message to.⁵⁸

IGTO observations

Based on submissions, ATO provided material and IGTO Dispute Investigations, myGov appears to be the preferred vector for fraudsters to access taxpayers' ATO Online accounts. Fraudsters with sufficient personal information about a taxpayer are able to create a myGov account using contact details, such as email addresses and phone numbers, that they control and link it to the taxpayer's ATO Online account. Since an ATO Online account can be linked to more than one myGov account, the fraudulent link can be created regardless of whether the Legitimate Taxpayer has already established an existing link.

In principle, WTY messages are aimed at empowering taxpayers and their representatives to prevent unauthorised access and lodgement occurring on their account and under their name. In principle, they aim to prompt taxpayers and their representatives to the event and give opportunity to intervene if they did not authorise that action. After all, taxpayers and their representatives are best placed to determine if the action is authorised or if it is an attempt to perpetrate TaxID fraud.

In practice, however, some taxpayers did not receive the WTY message. If the taxpayer has a tax agent, the fraudster is able to sever the connection between the taxpayer and the tax agent (without detection and notification). Based on submissions, some taxpayers received prompts to check their account which allowed the fraud to be identified, some received prompts far too late and some did not receive any at all. Some tax practitioners also advised the IGTO that they had received WTY messaging, but because there was no identifying information in the message (as shown above) they did not know which of their clients was affected. This creates a considerable burden on tax agents with hundreds of clients.

The ATO's current WTY messaging is well-intentioned, however, it has very limited effectiveness as a control on TaxID fraud. It does not place sufficient onus on the taxpayer to approve the action. The delay in notifying the taxpayer means that the taxpayer may only receive the WTY message after the fraud has been perpetrated. Overlinking is an extremely high risk event and therefore, without a trusted and real-time (24/7) verification system to verify the link is legitimate, additional controls that are proactive are required to operate as an effective control.

⁵⁸ ATO, Response to IGTO's 25/1/2024 request for information – Q3 (received 21 February 2024).

7.3. Process and controls for accessing ATO Online accounts via myGov and for updating taxpayer contact details and bank account details

Accessing myGov and ATO Online

An individual is required to enter their username and password and complete the second sign-in option to log in to their myGov account.

For an individual to access ATO Online via their linked myGov account, the second sign-in option must be two factor authentication (either an SMS code or a code from the myGov code generator).

Historically, myGov users could link to ATO Online where their myGov account was set up with secret questions and answers instead of two factor authentication. The ATO has since ceased allowing new links to ATO Online for myGov accounts with secret questions and answers, however any links that occurred originally are permitted to remain. If these users unlink, they must register with two factor authentication in order to re-link with the ATO.

Once the individual logs in to their myGov account, they can access ATO Online without any additional security requirements (i.e. the individual does not need to pass PORO each time they access their ATO online account).

Using myGovID to access myGov and ATO Online

myGovID is the Australian Government's digital identity app that is used across multiple government services for online log in and access. In order to use myGovID, the individual must have a smart phone and download the myGovID app. Once myGovID is successfully set up, it provide a means for the user to give an independent factor of authentication when accessing other on-line services.

myGovID offers three different identity strengths which require different levels of identification information and documentation and provide different levels of access to government online services. These identity strengths and the level of identification required is outlined in the table below.

Table 6: myGovID identity strengths

myGovID identity strengths	Level of identification required
Basic	<ul style="list-style-type: none">• Personal details
Standard	<ul style="list-style-type: none">• Personal details• Verification of two (2) of the following Australian identity documents: driver's licence, passport (not more than three years expired), birth certificate, visa (using foreign passport), citizenship certificate, ImmiCard or Medicare card
Strong	<ul style="list-style-type: none">• Personal details• Verification of an Australian passport (not more than three years expired)

myGovID identity strengths	Level of identification required
----------------------------	----------------------------------

- Verification of one (1) of the following Australian identity documents: driver's licence, birth certificate, citizenship certificate or Medicare card
- A one-off face verification check

Source: ATO

Individuals can use myGovID as an alternative way to log in to their myGov account and access ATO Online.

Businesses and tax agents must use myGovID to access Online Services for Business and Agents.

In November 2023, the ATO introduced changes to myGovID for individuals who use myGovID to access ATO Online.⁵⁹ This involves locking the myGovID identity strength (either standard or strong) for an individual as the minimum online access strength for all future access to ATO Online – i.e. the individual cannot elect to downgrade their identity strength.

Controls for updating contact details on ATO Online

An individual can update their phone number, email address, residential and postal address and authorised contacts by logging in to an myGov account that is linked to their ATO Online account.

Besides the log in requirements to access myGov (assuming the myGov account has been linked to the ATO), there are limited no additional controls or verification checks prior to updating an individual's contact details through their ATO Online account.

For phone numbers, email addresses and residential and postal addresses, the individual can also update these details on their ATO account via myGov directly (without accessing ATO Online). This can occur using myGov's 'Update Your Details' service which allows users to update their contact details for all linked services (including the ATO) at once. These changes are then imported into the ATO's systems and reflected on the taxpayer's ATO account.

Controls for updating bank account details on ATO Online

An individual can also update their bank account details by logging in to myGov and accessing their ATO Online account.

When a bank account is added to the taxpayer's account, the ATO does not validate bank account details (i.e. BSB and account number) beyond confirming that the BSB is a valid number and the account number meets basic syntax requirements in accordance with Australian payment system standards.

The ATO maintains a register of bank accounts that have been identified as having been used for fraudulent purposes before – the 'barred bank account register'. This register is updated weekly with accounts that tax officials' believe are used to perpetrate TaxID fraud. The ATO advised that once a bank

⁵⁹ ATO, '[ATO launches new protections against rising tide of fraud](https://www.ato.gov.au/media-centre/ato-launches-new-protections-against-rising-tide-of-fraud)' (last modified 28 November 2023) <https://www.ato.gov.au/media-centre/ato-launches-new-protections-against-rising-tide-of-fraud>

account number is uploaded onto this register, that number is unable to be entered on any taxpayer account via ATO Online and will result in an error message if there is an attempt to do so.

Apart from myGov log in requirements (assuming the myGov account has been linked to the ATO), the ATO conducts limited controls or verification checks before updating an individual's bank account details through their ATO Online account.

In addition, multiple changes can be made to a taxpayer's account within the same ATO Online session (i.e. both contact details and bank account details can be updated at the same time) and there are currently limited controls or restrictions to prevent this from occurring.

Identification and notification of changes to contact details and bank account details

With the exception of some limited monitoring which requires manual review, the ATO currently does not monitor in real time for any anomalous behaviour when taxpayers use their ATO Online account, including where changes are made to contact details. As a result, the ATO does not conduct any verification checks prior to changes being made to taxpayers' contact details.

The ATO also does not notify a taxpayer or their authorised tax agent of any changes made to their account details.

The ATO relies on its lodgement risk models to detect unusual account activity and suspected fraud. These models are run over a tax return or activity statement when they are processed for assessment. Further details on these are given in Section 4.5 ATO's Risk Management regarding bank account changes.

Other methods to update contact details and bank account details

In addition to the above processes, the ATO will also update contact and bank account details if requested during phone calls, subject to the caller passing PORO.

Requests to change contact and bank account details can also be made by sending a request to the ATO in writing via the post. The ATO will implement these changes where a signature and sufficient identification information is given.

Lodgement of paper income tax returns also provide space on those forms for contact and bank account details to be updated. These forms require signatures that confirms the lodger declares the information they have given on the form is true and correct.

Tax agents may also update a client's contact and bank account details via their access to Online Services for Agents.

IGTO observations

The ATO's risk management framework relies heavily on access controls and post-risk event treatments. The ATO does not have any automated checks and controls that could operate at scale and in real-time

at the very time that changes are made to taxpayers' accounts. The ATO has implemented account monitoring (since mid-2023) which could surface unauthorised changes to taxpayers' bank account details on ATO systems and use of the same bank account by multiple unrelated taxpayers. However, this monitoring requires manual review and processing at critical steps which can take place sometime after the changes on the taxpayers' account have been made. Whilst it may be effective to prevent future unauthorised actions on taxpayers' account, this account monitoring likely has limited effectiveness in mitigating the risk overall.

Updating contact details and bank account details are extremely high risk events and there is no real time controls for making such changes, including multi-factor authentication. The only control identified at this stage is the barred bank account list – which provides limited protection as that list only comprises bank account numbers that the ATO identified as having been used previously in perpetrating TaxID fraud. It would be reasonable to expect fraudsters to use new bank accounts to prevent detection.

Once a fraudster is able to link to ATO Online, they can change the taxpayer's contact details, bank account details and lodge fraudulent returns without detection from the ATO or notification to the taxpayer. Multiple high risk events are able to occur in quick succession on the ATO's systems without detection. In many cases the taxpayer and/tax agent identified the unauthorised activity by chance and then notified the ATO. Unless prompted to check their account, taxpayers will remain unaware of unauthorised access to their tax account and any unauthorised changes and lodgements made. More concerning is the fact that taxpayers are not even aware that their ATO account has been compromised and that amended returns have been lodged in their name, with bank account details changed so their refund is directed elsewhere.

Leveraging 'strong' myGovIDs is a sensible and reasonable approach. However, in the absence of strong myGovIDs being mandatory, other more secure preventative controls are required.

7.4. Account monitoring controls where fraud or risk of fraud has already been identified

External data breach

External data breaches are unauthorised disclosures or access to the personal information of numbers of people – for example, a hacker stealing a large employer's HR and payroll information database.

The ATO advised that it is dependent on the breached entity advising and cooperating with the ATO and other government regulators such as the Office of the Australian Information Commissioner (OAIC) for the ATO to assess the extent of client data exposure, and whether that data, if misused, could enable unauthorised access to ATO client accounts. For example, assessing whether a fraudster could pass the ATO's PORO with the breached data or could use that data to establish other credentials which would be accepted for PORO purposes.

Accordingly, the ATO's account monitoring controls which are aimed at preventing TaxID fraud are usually applied after the ATO becomes aware of:

- a risk of unauthorised activity, for example, the taxpayer’s personal information being stolen or potentially exposed in a data breach of third party systems;
- a fraud event taking place on the taxpayer’s account, such as being alerted to unauthorised changes made to taxpayer account details and the lodgement of fraudulent returns.

Recently, the ATO’s CAS business line has implemented a “Playbook” which establishes workflow pathways and assigns responsibilities for work-step outcomes. This is aimed at ensuring that all affected tax officials know the ‘rules’ of that playbook when such an event occurs and therefore operate confidently without seeking clarification or assuming that others were responsible for tasks.

The ATO also provided the IGTO with descriptions of its account monitoring controls (see below). Generally, no contemporaneous documentary evidence to support these descriptions was made available to the IGTO.

Compromised accounting treatment

The ATO advised that it may apply a range of security measures on the account, including a ‘compromised accounting treatment’ (**CAT**), which are aimed at protecting the account against the risk of fraud occurring in future. (See section 4.6 for more information)

Compromised tax agent

The ATO advised that when it suspects that a tax agency has been compromised, it can:

- report fraud that involves myGovID to myGovID (which is administered by the ATO) who can then suspend the credential, and
- withdraw that agent’s access to Online Services for Agents.

Compromised business account

The ATO advised that when it suspects that a business account has been compromised, it must rely on the suspension of the myGovID credential as a control, as it does not have the capability to withdraw the businesses access to Online Services for Business. It should noted, however, that this suspension will practical prevent access to that business’ online account because, according to the ATO, access to the Online Services for Business platform requires authentication via myGovID for access to be granted.

Client identity watchlist

The ATO advised that it maintains a client identity watchlist (**CWL**) for taxpayers whose ATO account the ATO has identified as having been compromised or potentially compromised (including those who have had their personal information exposed or potentially exposed due to external data breaches).

This watchlist does not restrict access to the taxpayer’s ATO account. Rather, it serves as a risk attribute that is used by other ATO risk models and processes, which in turn can prioritise certain high-risk transactions for additional scrutiny before completion.

The CWL is also taken into consideration when applying PORO, with an 'Alternate PORO – potentially compromised' Siebel alert applied to all compromised and potentially compromised taxpayer records.

Financial institution account monitoring

The ATO advised that it generates reports of taxpayer accounts where bank account details have been recently updated as well as where the bank account is linked to multiple taxpayers. ATO officers assess whether the bank account is suspicious and potentially linked to TaxID fraud or is likely legitimate. If those ATO officers deem the updated bank account to be suspicious or linked to potentially fraudulent transactions and behaviours, the ATO will:

- end date the suspicious bank account on the taxpayer's ATO account;
- add the bank account to an internal monitoring watchlist or the 'barred bank account list'; and
- apply the CAT to the taxpayer's ATO account.

The ATO advised that where an ITR is lodged by a taxpayer where a confirmed CAT has been applied to that taxpayer's account, an activity will be created and risk assessed by tax officials to determine further treatment required by manual or automated processes. Where the taxpayer is on the CWT but no CAT has been applied to their account, the model will hold the refund if the account has been identified as potentially compromised or at a high risk of the taxpayer's identity being compromised until CAS staff can confirm the refund's validity.

8

APPENDICIES

Appendix A — Terms of reference

To investigate the ATO's systems that prevent, detect and respond to identity and related financial fraud, and the impact of those measures on affected taxpayers and their representatives including:

1. What controls and security measures the ATO has in place, including modifications implemented since Operation Protego, to prevent and detect identity and financial fraud or identity theft from occurring on taxpayers' ATO accounts;
2. What communication measures and tools are relied upon to prevent, detect and respond to treating identity and related financial fraud;
3. Whether the ATO makes effective use of information that taxpayers and tax practitioners provide which indicate potential weaknesses in the ATO's approach to addressing identity and related financial fraud, for example:
 - a. quickly acting on taxpayers' enquiries that indicate potential compromise of accounts, and analysing them to detect potential new and emerging fraud methodologies;
 - b. quickly acting on concerns raised by tax practitioners about potential weaknesses in administration and inter-agency interactions and using them to test and update the ATO's fraud detection methods;
4. Whether the ATO quickly and effectively treats instances of identity and related financial fraud when notified, for example, by:
 - a. immediately stopping any affected refunds that are due to issue;
 - b. immediately preventing further unauthorised dealings with the taxpayer's account and protecting it against future financial damage;
5. Whether the ATO has appropriately considered the impact that security settings (especially ongoing security settings) placed on compromised ATO accounts may have on affected taxpayers and their representatives, such as:
 - a. where the ATO imposes protection measures on a compromised account, the ease with which affected taxpayers and tax practitioners can access their accounts to fulfill their tax obligations, and the alternative measures that are open to the ATO;
 - b. the speed at which tax returns and notices issued for affected taxpayers will be assessed; and
 - c. the treatment of debts on affected taxpayer accounts pending the outcome of investigations into the alleged identity and related financial fraud.

Appendix B — ATO response

Second Commissioner of Taxation



Australian Government
Australian Taxation Office

Karen Payne
Inspector-General of Taxation and Taxation Ombudsman
GPO Box 551
Sydney NSW 2001

Dear Ms Payne,

Re: Own Initiative Investigation into Tax Identity Fraud

Thank you for the opportunity to comment on the Inspector-General of Taxation and Taxation Ombudsman (IGTO) draft interim report on *Tax Identity Fraud: an Own Initiative Investigation*, which was provided to us by email on 15 March 2024.

The ATO welcomes the investigation given the priority we place on addressing identity fraud in Australia's tax, super and registry system. The IGTO's investigation provides a timely and constructive review of the ATO's management and response to this issue. In particular, the ATO acknowledges additional consideration the IGTO has given to balancing the need for transparency and ATO accountability, with prudent handling of sensitive content that could be misused by potential fraud actors.

The ATO continues to work closely with government agencies, financial institutions, tax professionals, and others, in an interdependent fraud ecosystem to harness and improve fraud management efforts together. The recently created National Anti-Scam Centre demonstrates government commitment and recognition of the need for collective efforts in combatting fraud amongst a fast-changing threat environment.

While the draft report contains potential recommendations and identifies some areas for improvement, we are pleased that it aligns broadly with ATO-identified work in progress and does not appear to identify any significant systemic concerns around the ATO's systems, processes and risk management controls to prevent, detect and respond to tax identification fraud.

We agree in principle with the majority of the interim recommendations, noting some are matters for Government to consider, particularly in relation to law reform and investment.

We would like to acknowledge the IGTO's collaborative and professional approach to the review and look forward to receiving the report, and considering the finalised recommendations once the investigation is completed.

Yours sincerely


A handwritten signature in black ink, appearing to read 'Jeremy Hirschhorn'.

Jeremy Hirschhorn
Second Commissioner of Taxation

17 April 2024

Appendix C — Joint Media Release (29 April 2021)

ATO and TPB target identity fraud in partnership with tax profession

1. 
2. News and Events
3. [News and Media](#)
4. ATO and TPB target identity fraud in partnership with tax profession

Media releases

Issued: 29 April 2021

Last modified: 29 April 2021

Joint media release between the Australian Taxation Office and the Tax Practitioners Board

The Australian Taxation Office (ATO) and the Tax Practitioners Board (TPB) are focused on measures to intercept attempted identity fraud targeted at registered tax practitioners and their clients. New guidelines will strengthen and modernise the practices and controls that registered tax practitioners follow when verifying the identity of their clients.

The ATO has seen an increase in attempts by criminals to commit refund fraud by stealing the identities of taxpayers which has coincided with an increased reliance on technology and remote working practices. Having your identity compromised can have devastating financial consequences.

A lack of consistency to verifying the identity of clients has left individual tax practitioners vulnerable to attack. Practices that retain client identity documents insecurely are also at greater risk of having these documents stolen through physical break-ins.

The ATO's draft guidance encourages tax practitioners to voluntarily start adopting the new client verification standard immediately, with the view for the standards to become compulsory in the future following an initial transition period and further consultation with the tax profession.

ATO Assistant Commissioner Sylvia Gallagher confirmed there is not an expectation that tax practitioners need to go back and verify the identity of their entire client base as part of the transitional approach. 'We're asking that they perform identity checks from this point on, at the next opportunity in their normal dealings with clients.'

Inviting feedback on the TPB's draft guidance, the TPB Chair Mr Ian Klug AM said, 'We value the support of the tax profession in implementing these important controls to better protect the Australian community from tax fraud through identity crime.' Mr Klug further said the TPB's guidance will apply to all registered tax practitioners regardless of whether they use the

ATO's online services or not.

'The *Tax Agent Services Act 2009* does not expressly set out minimum requirements for tax practitioners to verify a client's identity. However, there are implications under this Act if tax practitioners fail to take reasonable steps to ensure the identity of their clients is established. Our draft guidance provides practical guidance and examples so tax practitioners do not fall foul of their obligations and put their registration and business at risk,' Mr Klug said.

Tax practitioners who are unable to successfully verify a client's identity and suspect potential fraud should contact the ATO immediately on **1800 467 033**.

The ATO's draft guidance is available on the [ATO website](#). The ATO is seeking feedback from tax practitioners. Submissions can be emailed to TaxPractitionerConsultations@ato.gov.au.

The TPB's draft practice note is available on the [TPB website](#). Submissions can be emailed to tpbsubmissions@tpb.gov.au or sent by mail to GPO Box 1620, Sydney NSW 2001.

Submissions are due to the ATO and the TPB by **10 June 2021**.

Appendix D — Expected and actual controls to manage change of bank account risks

Tax Compliance Step	Description of how this can be achieved	Expected Checks and Controls	Actual ATO Checks and Controls
Changing Bank account details			
Changing Bank account details	<p>Taxpayers can change their personal contact details, including their bank account details within the ATO systems as follows:</p> <ul style="list-style-type: none"> Using myGov Using Online Services for business Via a registered tax agent who uses Online Services for Agents Lodging an income tax return or amendment Lodging a BAS Form or BAS revision Calling the ATO Call Centre 	<p>It should not be possible to change certain contact details within the tax system without the change being verified and authenticated. The changes of high risk include changes to:</p> <ul style="list-style-type: none"> ▪ Bank account details; ▪ Mobile or other telephone contact details; ▪ Contact email addresses. <p>For example:</p> <p>Prompting the taxpayer via a ‘Was this you?’ message and requiring taxpayer confirmation of the change via multi-factor authentication, by using at least two of the taxpayer’s contact details that were registered on the ATO systems before this request to change of details.</p> <p>This could include:</p> <ul style="list-style-type: none"> ▪ A one time security number sent to the taxpayer’s mobile number or other email/registered device; and ▪ An email message or SMS sent to the taxpayer’s registered email account or mobile. <p>There should be facilities within ATO systems to monitor for device ID, so that ATO changes made with devices that are known to be associated with fraud raise red flags and the need for investigation.</p> <p>A device ID catalogue (that is, devices known to be used to perpetrate fraud) is</p>	<p>There are limited controls specific to changing of bank account or contact details. However, checks and controls exist with respect to accessing the taxpayer’s account on the ATO’s systems.</p> <p>It is possible to change ALL contact details within the ATO online systems ALL at once.</p>

Appendix D — Expected and actual controls to manage change of bank account risks

Tax Compliance Step	Description of how this can be achieved	Expected Checks and Controls	Actual ATO Checks and Controls
		<p>maintained by the AFCX and members of the Fintel Alliance. It is understood that the ATO is a member of the latter but not the former and so should have existing access to this information.</p>	
Lodging Amendments – ITRs and BAS			
	<p>Original tax lodgements and amendments to income tax returns (ITRs) and Business Activity Statements (BAS) may be lodged either through: ATO Online; or paper forms.</p>	<p>The lodgement should be verified using two factor authentication using at least two taxpayer contact details in the ATO systems. This could include:</p> <ul style="list-style-type: none"> ▪ A one time security number sent to your mobile number or other email/registered device; and ▪ An email message or SMS sent to your registered email account <p>A receipt to acknowledge the lodgement should be sent via email to the taxpayer.</p>	<p>Before any refund is sent, there is currently no verification or investigation conducted unless the lodgment is flagged by one of the ATO’s lodgement risk models or the account has been previously identified as exposed to potential or confirmed TaxID fraud.</p>
Paying Tax Refunds			
	<p>The refund is paid to the bank account registered in the ATO systems.</p>	<p>The ATO should not pay refunds to a bank account that is not subject to Australian AML or KYC requirements (as part of the account opening process). It should be noted that this is not a guarantee that the bank account is held by a genuine taxpayer.</p> <p>The ATO systems should automatically scan taxpayers accounts to identify if there is more than one bank account registered against unrelated taxpayers.</p> <p>Where the bank account details have been changed within (say) 2 months of the amendment or filing, there should be a delay of 2 – 3 business days at least from the relevant filing to allow for the taxpayer’s verification or report of suspicious transactions.</p>	<p>The ATO no longer pay to Superannuation fund bank accounts – which are not subject to the AML/CTF’s KYC requirements at the time of opening (but are subject to them at the time of release from those accounts).</p>

Appendix E — Chronology of relevant events leading up to and regarding TaxID fraud

2005 Australian Financial Review interview of ATO Assistant Commissioner, “Billion-dollar bust”⁶⁰

“The Australian Taxation Office is cracking down on fraud, and no one is immune. The use of fake and stolen identities to perpetrate tax crimes is increasing rapidly. ... The deputy commissioner with responsibility for serious non-compliance, Michael Monaghan, says his 273-officer unit, comprising investigators and special auditors, has been building up its resources over the past two years.

...Identity fraud

Identity fraud is the growth area of tax crime. Monaghan estimates that 38% of detected tax frauds are committed using fake identities - up from 14% just three years ago. Monaghan says a reason for this growth is the ready availability of technology ... Identities are stolen from wallets, rubbish piles and the internet. A favoured strategy involves lodging many fraudulent tax returns in fake names.”

2009 Commissioner of Taxation’s Annual Report 2009–10 (p 79):

“In 2008–09, we risk assessed the returns being lodged through e-tax... We also identified organised groups stealing or buying tax file numbers and using them to receive large refunds...”

2011 Commissioner of Taxation’s Annual Report 2010–11 (p74):

“During 2010-11 there was 31,249 cases of potentially fraudulent use of tax file numbers, compared to 12,669 in 2009-10. We attribute the increase to a range of factors, including an increase in the incidence of identity crime, growing community awareness and our improved fraud-detection processes...”

2012 Commissioner of Taxation’s Annual Report 2011–12 (p40):

“The incidence of compromised TFNs has risen from about 31,000 in 2010–11 to over 43,000 in 2011–12. We attribute the rise to improved detection, growing community awareness and of the risks of compromised TFNs, and the increased use of electronic financial transactions.”

2013 IGTO observations of the ATO’s identity crime model⁶¹

2.21 The identity crime model strike rates for the years 2010–11 and 2011–12 ...[2.22] ... shows that of all the returns stopped by the [Income Tax Refund Integrity Program], only a

⁶⁰ Laurence M, ‘Billion dollar bust’, *Australian Financial Review* (8 September 2005).

⁶¹ IGTO, *Review into the ATO’s compliance approach to individual taxpayers – income tax refund integrity program* (September 2013) https://www.igt.gov.au/wp-content/uploads/2021/07/158_income-tax-refund-integrity-program.pdf

fraction were as a result of risks identified by the identity crime and network detection model. In 2010–11, this accounted for 7,269 cases (being 21 per cent of total returns reviewed by the ATO). In 2011–12, 7,924 cases were stopped by the identity crime and network detection model, accounting for about 10 per cent of total returns reviewed by the ATO.

2.23 Of those returns which were stopped by the identity crime model, the ATO reports that it made adjustments in 6,427 cases (or 88 per cent) in 2010–11 and 4,894 cases (or 62 per cent) in 2011–12. The average adjustment rate, however, has increased between the two years from an average of \$2,349 to \$4,413 per case.

2013 Commissioner of Taxation’s Annual Report 2012–13 (p42):

“This year, approximately 47,000 tax file numbers (TFNs) were compromised... In response, we have created a new unit to deal more effectively with the emerging incidence of identity crime in the online environment.” [which was the CISC area]

2014 Commissioner of Taxation’s Annual Report 2013–14 (p60):

“We have significantly improved how we approach, manage and address identity crime and refund fraud. Our approach focuses on better protecting our business practices, enhancing our detection processes, improving our incident response ... Our actions supported over 30,000 clients with potentially compromised identities and contributed to protecting over \$2.5 million in revenue this financial year.”

2015 Commissioner of Taxation’s Annual Report 2014–15 (pp 50–51):

“Refund fraud is becoming more elaborate and the methods more complex. Our analytical models are also increasing in sophistication. For example, now we are able to identify where the same invoice is being presented by different taxpayers and use this evidence to identify potential creation of false identities and fraudulent refund claims....Identity crime is a key focus area and we continue to face sophisticated and organised attempts to claim fraudulent refunds... To protect people’s identities, we undertake checks at the time of registration to address errors and detect identity crime...”

2017 Commissioner of Taxation’s Annual Report 2016–17 (p 61):

“Our priority has been to detect identity crime to prevent refund fraud impacting the tax and superannuation systems. Organised crime syndicates engage in attempted refund fraud often using stolen identities...”

2018 Commissioner of Taxation’s Annual Report 2017–18 (p 56):

“... Along with shifting community expectations, there is a need to increase security and assurance around identification, in the face of increasingly sophisticated methods of identity theft and related fraudulent activity. ... In partnership with the Digital Transformation Agency, we are developing GOVPass – a way to manage identity digitally across government. GOVPass forms the government’s client identity programme, allowing individuals to securely and easily identify themselves, connect with government digital services and authorised people to act on their behalf. Soon, this technology will enable

citizens to manage a range of online transactions with government where verification of identity is required. During 2017- 18, we focused on developing two critical components to GOVPass:

- *myGovID clients to prove their identity via an app on their smart device*
- *the Relationship Authorization Manager (RAM) for clients to authorise who can transact on behalf of their business*
- *... the current AUSkey business credential ...will end in 2019-20 together, myGovID and RAM will replace AUSkey and will be available over multiple releases during 2018- 19..."*

2019 Commissioner of Taxation’s Annual Report 2018–19 (p 22):

“With rapid growth in online activity there is greater opportunity for fraudsters to steal and sell personal data. The ATO will continue to invest in securing taxpayer information through robust identity, authentication and authorisation platforms...”

October 2020 Commissioner of Taxation’s Annual Report 2019–20 (p 31):

“With rapid growth in online activity, there is greater need for governments to be able to verify the digital identity of individuals and businesses. It also brings greater opportunity for fraudsters to steal and sell personal data. The ATO continues to invest in securing taxpayer information through robust identity, authentication and authorisation platforms.

In June 2019, we delivered myGovID and RAM as a new whole-of-government identity solution for individuals and businesses. This enabled the replacement of AUSkey as the log-in credential for businesses by March 2020. Access to participating online services now requires an individual to obtain a verified digital identity (myGovID) and establish who is authorised to act on behalf of a business online (via RAM). In the future, this will provide the option for people to use digital identity as an alternative to the legacy myGov credential for individual services...”

April 2021 TPB and ATO jointly announce consultation on new guidelines to help tax agents verify the identity of their clients

“... New guidelines will strengthen and modernise the practices and controls that registered tax practitioners follow when verifying the identity of their clients.

The ATO has seen an increase in attempts by criminals to commit refund fraud by stealing the identities of taxpayers which has coincided with an increased reliance on technology and remote working practices. Having your identity compromised can have devastating financial consequences.

A lack of consistency to verifying the identity of clients has left individual tax practitioners vulnerable to attack. Practices that retain client identity documents insecurely are also at greater risk of having these documents stolen through physical break-ins.

The ATO's draft guidance encourages tax practitioners to voluntarily start adopting the new client verification standard immediately, with the view for the standards to become compulsory in the future following an initial transition period and further consultation with the tax profession..."

June 2021 Serious Financial Crime Taskforce issues a Fact Sheet

Financial crime is constantly evolving, and technology plays an increasingly significant role.

... Criminals we are on the lookout for: Cyber Criminals use technology to gain access to information and sensitive data which can be used to facilitate a range of crimes, including tax crime and identity theft. There are a range of different kinds of cyber criminals including:

... • data thieves | hackers | phishers | code writers | data buyers

These criminals could be anyone from a teenage hacker living next door to a member of an offshore crime syndicate.

Behaviours to look out for:

.. • Crime is provided as a service. For example, some criminals sell names and information related to individuals ... Other criminals buy and then use these identities and information to carry out serious financial crimes that harm people, businesses, banks and government agencies (and therefore the Australian public).

• Stolen identities and information, and phishing schemes can be used to steal from superannuation and share trading accounts, and purchase goods and services using the victim's funds and ID..."

April 2022 Operation Protego commences

June 2022 Second Commissioner's speech to the Tax Summit⁶²

.... criminals are seeking to access the broader tax system both directly and through other channels, like tax agent systems, superannuation funds or even taking over the identity of directors. Increasingly we are seeing cascading penetration attempts, where criminals attempt to obtain information from different places before putting it together for fraud attempts. The recent Optus data breach has really brought home how vulnerable many businesses and organisations are to attack and the need to evolve our controls as threats arise. We continue to strengthen our safeguards in preparedness for the increased threat and urge you to take this very seriously."

October 2022 Commissioner of Taxation's Annual Report 2021-22

"Strengthening digital identity and increasing adoption

⁶² ATO, Commissioner's address to the Tax Institute's Tax Summit 2022 (Address to The Tax Institute Tax Summit on 20 October 2022 by Second Commissioner) <https://www.ato.gov.au/media-centre/commissioner-s-address-to-the-tax-institute-s-tax-summit-2022>.

In 2021–22 we delivered a significant upgrade to myGovID, implemented a real-time digital tax file number (TFN) application, and upgraded the Relationship Authorisation Manager (RAM) service. We also enhanced our fraud, security and detection capability across the ATO digital identity products.

Strong myGovID with biometrics was introduced. This technology uses liveness detection to verify whether an individual is real and present, and a face verification service (provided by the Department of Home Affairs) – to enable a user to complete a face verification against their passport image.”

November 2022 **ABC news article “Cyber black market selling hacked ATO and myGov logins shows Medibank and Optus only tip of iceberg”⁶³**

“... An ABC investigation has identified large swathes of previously unreported confidential material that is widely available on the internet, ranging from sensitive legal contracts to the login details of individual myGov accounts, which are being sold for as little as \$1 USD.

... One of the main hubs where stolen data is published is a forum easily discoverable through Google, which only appeared eight months ago and has soared in popularity ... ABC Investigations found users selling personal information and log-in credentials to individual Australian accounts which included myGov, the ATO and Virgin Money for between \$1 to \$10 USD.

... CyberCX's Ms Mansted said the "black economy" in stolen data and hacking services was by some measures the third largest economy in the world, surpassed only by the US and Chinese GDP... "It's a buyer's market."

Cyber threat investigator Paul Nevin monitors online forums where hundreds of Australians' login data are traded each week... "In the past, we'd see small scatterings of accounts but now, this whole marketplace has been commoditised and fully automated.

... Australian Federal Police (AFP) Cybercrime Operations Commander Chris Goldsmid, told the ABC personal data was becoming "increasingly valuable to cybercriminals who see it as information they can exploit for financial gain". "Cybercriminals can now operate at all levels of technical ability and the tools they employ are easily accessible online," he warned. He added the number of cybercrime incidents has risen 13 per cent from the previous financial year, to 67,500 reports — likely a conservative figure...”

⁶³ Rubinsztein-Dunlop S, Hui E, Curnow S and Nguyen K, Cyber black market selling hacked ATO and MyGov logins shows Medibank and Optus only tip of iceberg, ABC News (28 November 2022) www.abc.net.au/news/2022-11-28/cyber-black-market-shows-medibank-optus-hack-just-the-surface/101700974

December 2022 **ABC news article ‘Fake myGov profiles are being used to hack ATO accounts.’⁶⁴**

"Congratulations on selling your Footscray house," an accountant told Sue ... while the pair were discussing a routine tax return. The comment was baffling. Sue didn't own a house in Footscray. But according to her ...ATO records, not only did her supposed inner-Melbourne home go under the hammer but her return had already been lodged.*

In fact, more amendments had been put through on previous years' tax returns and one more was still pending. As Sue and her accountant pored over the details on his screen, a horrifying realisation set in. Someone had accessed her account, impersonated her, and fraudulently lodged five refunds from the ATO amounting to \$25,000.

... Through Sue, ABC Investigations has uncovered a vulnerability in the myGov and ATO systems which is being exploited by cybercriminals to defraud the taxpayer. It's a loophole which no amount of careful management of your online activity can prevent. ... The Melbourne woman is what cyber security and information experts would characterise as the model citizen for digital hygiene.

... Whenever a user logs into myGov to access their ATO account, a two-factor authentication (2FA) is triggered; in Sue's case, she was supposed to be sent a code to her phone. She had not received any such account authorisation request in recent months. "We found that the address, the [bank] account number, the telephone number, the email had all been changed," Sue said.

Sue had been an Optus breach victim. She initially thought the hacker must have used that information to help crack into her ATO account — but ABC Investigations found this wouldn't have been enough for the perpetrators to get in. ... Sue was told the fraudster created a bogus myGov account and ... they linked this new profile to her ATO account using her tax file number (TFN), her date of birth, and another credential which the agency didn't specify.

After changing her personal details, the fraudster severed Sue's ATO account from her genuine myGov account which prevented her from seeing any refund assessment notices — it also bypassed the extra layer of protection provided by a two-factor authentication.

Sue was told by an ATO officer this was not uncommon and was advised "there are lots of fraudulent myGov accounts accessing tax files".

... The hackers had repeatedly changed the bank account details in her ATO profile between refunds. The UBank account Sue saw on November 15 was just the last in a string of accounts which were used to perpetrate the fraud."

⁶⁴ Sarah Curnow and Kevin Nguyen, Fake myGov profiles are being used to hack ATO accounts. Sue found this out the hard way, ABC News (18 December 2022) <https://www.abc.net.au/news/2022-12-18/ato-tax-hacked-via-mygov-services-australia-exploit/101781656>

2023 Commissioner of Taxation's Annual Report 2022-23

"Enabling digital identity, security and take-up

... Together, myGovID and RAM are used to access over 130 services across 39 government agencies. At 30 June 2023, over 8.2 million verified myGovIDs were enrolled, up from 5.8 million the previous year. This usage is expected to increase as more government services are added.

... The ATO continues to see growth in identity crime-enabled fraud and scaled fraud attacks through individual and entity lodgments. These attacks are promoted through social media – they are agile, prolonged, persistent and further amplified by increased data breaches in the community. We are addressing these challenges by supporting and encouraging our clients to be vigilant in protecting their identity and building awareness of scams that lead to identity crime....

... Client-agent linking

We are strengthening our security controls to protect taxpayers from increasing efforts by criminals to lodge fraudulent returns or traffic their data to other criminal networks. Our client-agent linking project is changing the way taxpayers authorise their nominated tax professional to access their ATO account through our online services.

This will further limit the ability of cyber criminals to harvest taxpayers' data and ensures clients retain control over who accesses their data. In its pilot phase, the project has already protected around 200,000 entities and has successfully prevented fraud attempts. In 2023–24, we will continue to work with stakeholders and extend this project to include more taxpayer groups, including small business and individuals."

Appendix F — IGTO information requests to the ATO

The table below sets out the IGTO’s requests for the ATO to provide information supported by contemporaneous and pre-existing documentation where applicable. IGTO request and ATO response dates (as at 22 April 2024) are also set out in the table.

Table 7: IGTO requests for information and documentation

Date of request	IGTO request for information supported by contemporaneous and pre-existing ATO documentation	Date of ATO response
12 December 2023	The current end-to-end systems and processes for a taxpayer to establish or change their personal details on their ATO account by either online, phone and post (including the process for establishing a myGov account and/or myGovID then ‘linking’ to ATO Online.	15 February 2024
	The current ATO identity and financial fraud prevention or detection controls at all stages of the end-to-end processes for all methods to establish or update a taxpayer’s personal details (including contact numbers, email addresses and bank accounts) on their ATO account.	15 February 2024
	The ATO detection controls that exist to proactively inform the ATO that a taxpayer’s identity or account is compromised, including: <ul style="list-style-type: none"> • controls to detect whether a fraudulent tax return or activity statement has been lodged; • sources of information and risk models relied on by the ATO and; • controls where multiple myGov accounts are linked to a single taxpayer ATO account. 	15 February 2024
	The current ATO controls to deal with taxpayers who have, or are at risk of having, their identity or ATO account compromised, including how often the compromised account is reviewed and what is communicated to the taxpayer following a review.	15 February 2024
	Details of how fraud and identity theft, including fraud relating to Operation Protego matters, were able to bypass the ATO’s fraud prevention and detection controls.	15 February 2024
	Details of projects and improvements the ATO is currently undertaking to address the risks of fraud and identity theft.	15 February 2024
	Steps taken to implement or progress the recommendations from the January 2023 <i>Critical National Infrastructure myGov User Audit</i> (in particular recommendations 6 and 7).	15 February 2024
	An explanation of how the new <i>Digital ID Bill 2023</i> (currently in Exposure draft) affect the way in which the ATO verifies taxpayers using their online ATO services.	15 February 2024
11 January 2024	Provision of the ATO’s risk assessment and treatment plans regarding the ‘threat’ aspect of Identity Fraud	Outstanding as at 22 April 2024
19 January 2024	Data extracted from the ATO systems of all refunds issued from 1 July 2021 to present where a change was made to a taxpayer’s BSB and/or account number within a two (2) month period prior to the issue of the refund, including the following data for each transaction identified:	26 March 2024

	<ul style="list-style-type: none"> • taxpayer details i.e. unique identifier and type of taxpayer; • date and channel of bank account change; • refund issue date and amount; • updated bank account details; • lodgement details i.e. type of lodgement, whether the lodgement was original or an amendment, whether the lodgement was made by the taxpayer or tax agent; • date of GST registration where the lodgement was an activity statement; • whether the updated bank account details were changed back to the pre-existing bank account; • whether the refund was flagged by ATO controls for further analysis; • whether a tax identity fraud allegation was raised by the taxpayer; and • details of additional security measures placed on the taxpayer’s account. 	
	Pre-existing copies of any ATO research and/or analysis of the specific (or similar) scenario outlined above, including any observations or conclusions and the ATO business units that considered the research/analysis.	20 March 2024
	Copies of briefings to the Commissioner(s) which refer to the type of fraud scenario described above (i.e. where the fraudster changes the bank account details of taxpayers to divert refunds into their own bank accounts) or which relate to it.	20 March 2024
25 January 2024	Details of the ATO’s interactions with the banks/financial institutions in relation to identity crime, including: <ul style="list-style-type: none"> • what automated interactions are there to verify bank account details (if any); • what are the dedicated channels to share information on identity fraud in specific cases in real time (if any); and • what are the forums, meetings or channels of communication that the ATO uses to discuss identity fraud related issues with the banks. 	22 February 2024
	Details of the information that is shared between government authorities and banks in countries that are part of the J5 (Joint Chiefs of Global Tax Enforcement).	1 February 2024 and 21 February 2024
	Explanation of the verification (if any) that currently occurs when the contact details and bank account details are changed in the ATO systems (by a taxpayer or their representative) including: <ul style="list-style-type: none"> • whether these details be changed simultaneously; and • whether confirmation of any changes is provided back to the pre-existing contact details. 	21 February 2024
	An explanation of the ATO’s process for capturing and analysing information about potential/alleged identity fraud events which are reported by taxpayers and tax agents.	21 February 2024
	The proportion of taxpayers with tax agents who have changed their contact details to those of the tax agent and whether it is possible for the tax agent to provide their client’s mobile number for the sole purpose of sending a ‘Was This You?’ message.	21 February 2024
	Details of the previous alert/s the ATO sent to the ‘Fusion Cell’ and its related discussions with the banks, especially those concerning bank accounts, real-time arrangements for information sharing and account matching, and related identity verification of the account owners.	21 February 2024
	Copies of any current ATO advocacy briefs to Treasury in relation to tax	15 March 2024

	identity fraud.	
27 February 2024	The ATO's capacity to receive encrypted information and emails from financial institutions, including the potential cost of further system upgrades to improve capacity to receive encrypted information.	27 March 2024
	Details of whether the ATO has the ability to withhold refunds beyond the 14-day statutory timeframe (under sections 8AAZLG, 8AAZLGA and 8AAZLH of the <i>Taxation Administration Act 1953</i>) in the case of suspected fraud, including ATO General Counsel advice on: <ul style="list-style-type: none"> • whether these sections apply for any type of refund; • if not, whether there are any other provisions that give the ATO the power to hold up refunds; and • whether these sections give the ATO the power to investigate suspicious bank accounts. 	15 March 2024
	Copies of ATO submissions to parliamentary inquiries on telecommunications legislation regarding the ATO's ability to access telecommunications data for the purpose of criminal investigations, such as fraud.	6 March 2024
	An overview of what the ATO currently provides to banks when it becomes aware of bank accounts used in fraud.	15 March 2024
	Information on how the ATO manages clients who believe bank accounts have been opened fraudulently in their name, as well as how recovery of funds works in this scenario.	14 March 2024
	Further details and a timeline of the ATO's improvements to notify taxpayers of suspect details and lodgements, with respect to the Business Improvement Opportunity identified by the IGTO.	14 March 2024
	An update on internal design workshops with Enterprise Solutions and Technology to connect ATO and bank verification processes.	15 March 2024
	A copy of the PowerPoint presentation on the ATO's potential future focus of fraud management.	27 March 2024
	Confirmation of whether the Trust Taskforce and Taskforce Cadena are still funded and operational.	15 March 2024
	An overview of Client Agent Linking notifications provided to agents who are or have been de-linked from a client.	15 March 2024
29 February 2024	A copy of the ATO's fraud victim remediation procedures and dates of changes to these procedures.	10 April 2024
	The number of identity crime disclosures made by the ATO to law enforcement agencies since 1 July 2021.	20 March 2024
	A copy of a pre-existing process map for victim remediation and third-party fraud investigation by the ATO's Client Identity Support Centre (CISC).	14 March 2024
	The criteria used by the CISC support and processing team to determine whether third party fraud has occurred, including details of what information is requested and obtained from banks under s353-10 of Schedule 1 to the TAA.	14 March 2024
12 March 2024	Confirmation that s355-25 of Schedule 1 to the TAA 1953 is the legislative provision the ATO considers would prevent notification to agents where the client has left them). Also, copies of any legal advice (internal/external), either in relation to this or similar issues.	27 March 2024
18 March 2024	Copies of templates for s353-10 notices that Client Account Services (CAS) issue to banks with respect to suspected identity fraud cases from 1 July 2021 to present.	18 April 2024
	Copies of all Operational Policy, Assurance and Law (or other internal) advice and instructions regarding CISC identity fraud-related activities.	Outstanding as at 22 April 2024

	CISC's Average Handling Time and cases per hour data for identity fraud victim remediation cases from 1 July 2021 to present.	18 April 2024
	Copies of the Minutes, Agendas and agenda attachments (relating to identity fraud) for the CAS business line executive meetings held from July 2021 to March 2024.	18 April 2024
	Where CISC considers an alleged identity fraud case may involve first party fraud and referred for investigation, copies of referral templates and instructions/guidance provided to Client Engagement Group (CEG) auditors for investigating such cases.	Partially provided on 18 April 2024
19 March 2024	A copy of the General Counsel advice received on whether notifications to agents who have been delinked from a client would be considered as an unauthorised disclosure of protected information under s355-25 of Schedule 1 to the TAA 1953.	2 April 2024 and 10 April 2024
20 March 2024	Copies of all project documentation and timeline/details of any improvements made in relation to the Secure Messaging Capability program of work and other projects relating to the notification to taxpayers of suspicious changes to account details and lodgements.	Outstanding as at 22 April 2024
3 April 2024	Details on the operation of ATO risk models, including a timeline of key updates, and other fraud detection processes (such as the monitoring of ATO accounts).	Outstanding as at 22 April 2024
	Information on the stages of processing and cancelling credits and refunds.	Outstanding as at 22 April 2024
	Information relating to the use of IP address data and the potential collection of telecommunications data for the purposes of investigating potential identity fraud.	Outstanding as at 22 April 2024
	Copies of pre-existing documentation on the organisational and governance structure for the relevant ATO business lines with respect to identity fraud.	11 April 2024
	Pre-existing information and documents shared internally and/or externally relating to the use of myGov to perpetrate potential identity fraud.	Outstanding as at 22 April 2024
	Pre-existing internal research and analysis on the level of fraud risk posed by the Online Services for Agents (OSfA) and Online Services for Business (OSfB) platforms.	Outstanding as at 22 April 2024
	ATO policy or legislative basis for requiring an ATO-linked bank account to be held in Australia.	Outstanding as at 22 April 2024
8 April 2024	Copies of the ATO's risk assessment and treatment plans regarding the threat of identity fraud.	Outstanding as at 22 April 2024
12 April 2024	ATO risk model presentation slides and case-specific details of how risk models detect lodgements, including amendments.	Outstanding as at 22 April 2024
	Copies of the charter, membership details, agenda items, agenda attachments and minutes from past meetings of the relevant ATO External Fraud Committees.	Outstanding as at 22 April 2024
	ATO Executive endorsed documentation on the process for escalating external fraud risk events for consideration.	Outstanding as at 22 April 2024
	Copies of previous requests to (and responses from) the ATO Executive Committee for contingency funding for external fraud response.	Outstanding as at 22 April 2024
	Copies of the internal audit assessment of ATO fraud event response.	Outstanding as at 22 April 2024

Appendix G — Glossary and defined terms

Abbreviation	Defined term
AFCX	Australian Financial Crimes Exchange
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
AML/CTF Rules	<i>Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)</i>
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
BAS	Business Activity Statement
CAS	ATO's Client Account Services business line
CAT	compromised accounting treatment, which denotes a range of security measures applied to a taxpayer's account
CISC	ATO's Client Identity Support Centre
Commissioner	Commissioner of Taxation
Complaint	A complaint is defined AS/NZS 10002:2014 Guidelines for complaint management in organizations: <i>Expression of dissatisfaction made to or about an organization, related to its products, services, staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.</i>
Device ID	A number that is unique to a particular device and can be used to identify that device. For example, with respect to mobile phones, the International Mobile Equipment Identity (IMEI) number is unique to each mobile phone device and can be used to identify devices on a network.
Dispute	A dispute is defined AS/NZS 10002:2014 Guidelines for complaint management in organizations: <i>Disputes - Unresolved complaints escalated internally or externally, or both.</i>
Dispute Investigation	IGTO investigation of specific tax official actions and decisions which were the subject of unresolved complaint (or dispute)
DVS	online Document Verification Service managed by Department of Home Affairs
Entity	an entity as defined in section 960-100 of the <i>Income Tax Assessment Act 1997</i> , i.e.: an individual, a body corporate, a body politic, a partnership, any other unincorporated association or body of persons, a trust, or a superannuation fund
FCB	ATO's Fraud and Criminal Behaviours business line
FIR	ATO's Financial Institution Referral process, in which the banks make referrals to the ATO via the Reserve Bank of Australia
Fraudster	an entity who impersonates another entity
FRX	Fraudulent Reporting Exchange
GST	Goods and Services Tax
High-Risk refund	Refunds that involve a high risk of TaxID fraud
HRLM	High-Risk Linking Model
ID	identity
IGT Act 2003	<i>Inspector-General of Taxation Act 2003</i>
IGTO	Inspector-General of Taxation and Taxation Ombudsman. The acronym "IGTO" is

	used throughout the submission to denote both the “Inspector-General of Taxation”, as named in the enabling legislation, and “Inspector-General of Taxation and Taxation Ombudsman” as recently adopted due to recent calls for greater understanding and awareness of our dispute investigation function.
ITR	Income tax return
KYC	Know Your Client (obligation and requirements which are imposed by the AML/CTF Act)
Legitimate Taxpayer	an entity who a Fraudster impersonates when accessing that entity’s tax account
NOA	Notice of Assessment
PAYGW	Pay As You Go Withholding
PGPA Act 2013	<i>Public Governance, Performance and Accountability Act 2013</i>
PGPA Rule 2014	<i>Public Governance, Performance and Accountability Rule 2014</i>
PORO	Proof of Record Ownership. PORO is a control the ATO uses to verify a person's authority to access information that relates to the tax affairs of a taxpayer. Successfully answering a series of security questions is referred to as ‘passing PORO’. For an individual to pass PORO, they must provide at least two items of proof relating to information on their tax record.
SFCT	Serious Financial Crime Taskforce
SMS	Short Message Service, commonly known as texting
TAA 1953	<i>Taxation Administration Act 1953</i>
Tax Official	<p>The term ‘tax official’ is defined in section 4 of the IGT Act 2003 to mean:</p> <ul style="list-style-type: none"> (a) an ATO official; or (b) a Board member of the Tax Practitioners Board; or (c) an APS employee assisting the Tax Practitioners Board as described in section 60-80 of the <i>Tax Agent Services Act 2009</i>; or (d) a person engaged on behalf of the Commonwealth by another tax official (other than an ATO official) to provide services related to the administration of taxation laws ... <p>For the purpose of this report, the term ‘tax official’ is also used to refer to a ‘taxation officer’ to whom subdivision 355-B of Sch 1 to the TAA 1953 applies.</p>
TaxID fraud	means fraud that involves a Fraudster who impersonates another entity when accessing that entity’s online account on the ATO’s systems to unlawfully generate refunds which are then sent to a bank account controlled by the Fraudster.
TFN	Tax File Number
TPB	Tax Practitioners Board
WTY	Was This You? message