Australian Government
Inspector-General of Taxation
Taxation Ombudsman

20th anniversary 2003–2023

Tax Identification (TaxID) Fraud

Interim Report - Bank account integrity is critical to prevent and detect TaxID fraud

April 2024

Stakeholder Concerns

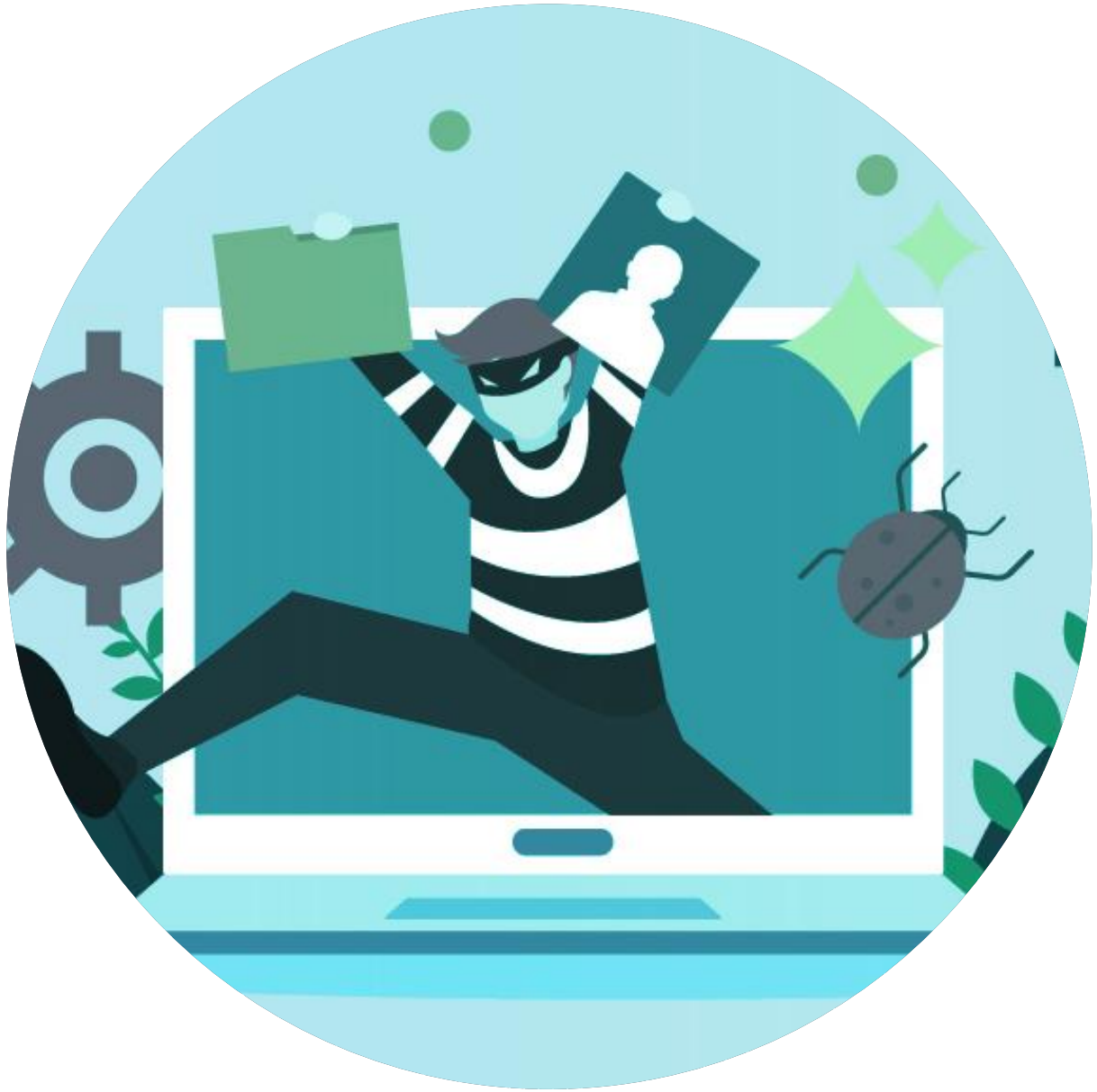
- TaxID fraud in many cases appears to be detected by chance and after the event;
- The window for preventing unauthorised payments is too narrow;
- Fraudsters can access taxpayers' online accounts, register for ABN/GST, change personal contact and banking details and then lodge returns/BASs which generate 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;

Stakeholder Concerns

- 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.

Bank Account Details

- Banking and financial eco-systems are only as good as their weakest link
- Big 4 + Macquarie have invested heavily in technology, systems and teams to combat financial fraud
- Banks rely upon known devices, multifactor authentication, Was This You, Secure Applications and Security PINs for high risk change of contact details. This includes:
  - Mobile phone contacts
  - Banking details



IGTO Concerns – changing bank account details in tax system permits fraud

- ATO systems permit change of banking details without taxpayer verification
- ATO not alerting banks to bank accounts involved in fraud [based on discussions with Big Banks]
- ATO not matching bank accounts involved in fraud to taxpayer details
- ATO not acting swiftly to block or garnishee fraudulent amounts – even when reported by taxpayer or agents
- Agents can be victims or complicit in committing fraudulent lodgements for the purposes of securing tax refunds

Phase 2

- The Taxpayer experience
  - ATO involvement in investigating and remediating reported fraud
  - Communicating progress on ATO investigations
  - TFN and 48 hour access
  - Collection of debts

Case Studies – Chapter 3

- 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 Studies – Chapter 3

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

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

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

Case Studies – Chapter 3

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

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

Improvement Themes

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;

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 – especially through the Australian Financial Crimes Exchange (AFCX) and the Fintel Alliance;

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;

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

Make it harder to exploit the system using fraudster accounts

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

Make it harder to exploit the system using fraudster accounts

- 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.

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

Effective Collaboration

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
- that the ATO verify taxpayers' bank details with banks and determine whether the process to open those bank accounts creates additional risk factors
- that the ATO systems provide banks with real-time verification of Tax File Numbers (TFNs)

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

Empower taxpayers and tax agents

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.
- that the ATO implement systems which allow for multi-factor authentication
- the ATO notify Tax Practitioners in a timely manner if a client has been removed from their tax agent's client listing
- 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

www.igt.gov.au
enquiries@igt.gov.au
(02) 8239 2100

Facebook Linkedin Twitter