Australian Government
Australian Taxation Office

OECD INTERNATIONAL ACADEMY FOR TAX CRIME INVESTIGATION

VAT/GST FRAUD INVESTIGATIONS PROGRAMME

CASE STUDY: VAT/GST REFUND FRAUD AND IDENTITY CRIME

JES DETTERER
AUSTRALIAN TAXATION OFFICE

IDENTITY CRIME | OVERVIEW

The term **identity** encompasses the identity of natural persons (living or deceased) and the identities of body corporate.

Identity Crime: A generic term to describe activities/offences in which a perpetrator uses a fabricated, manipulated or stolen identity.

Identity Fabrication: The creation of a fictitious identity

Identity Theft: The theft or assumption of a pre-existing identity, with or without consent

Identity Manipulation: The alteration of one's own identity

IDENTITY CRIME | COMBATING IDENTITY CRIME

- In Australia, the Australian Federal Police (AFP) is involved in a variety of activities to tackle identity crime and identity theft in collaboration with a number of other government agencies.
- In the ATO, there are a number of ways we assist to combat identity crime:

DETECT

We use intelligent systems to automatically detect tax returns suspected of being lodged using another person's identity.

PARTNER

We are a partner agency in a whole-of-government approach to reducing identity crime.

SUPPORT

Our Client Identity Support Centre supports taxpayers who have had their identity's stolen.

EDUCATE

We provide education to the general public to assist in preventing identity crime.

IDENTITY CRIME | CASE STUDY 1

Australian Government
Australian Taxation Office

> On 4 October 2019, Ryan McCarthy (27) was sentenced in the Brisbane District Court to **5 years imprisonment** with a non-parole period of 18 months for **placing false job advertisements online and stealing the identities of job applicants** in order to lodge false income tax returns.

> Between August 2015 and July 2016, Mr McCarthy created online job advertisements using the names of both legitimate and fictitious companies. **Job seekers would apply for these positions and submit their resumes or CV's**.

> Mr McCarthy would telephone the applicants and conduct phone interviews using various aliases. He would then email the applicant **offering them the job and asking for them to provide further details** including their driver's licence, bank account details and tax file number.

> He then used this information to **assume the identities of some of his victims, and lodged 62 income tax returns online**, resulting in refunds being credited to bank accounts he controlled.

> Many of Mr McCarthy's victims **reported their suspicions to the Australian Cybercrime Online Reporting Network (ACORN)**, after they realised the jobs they had applied for didn't exist. The ATO commenced an investigation in cooperation with Queensland Police.

> Investigations identified 52 victims and discovered that Mr McCarthy had **opened 63 bank accounts with 16 different financial institutions**. Queensland Police also made inquiries into the phone services being used by Mr McCarthy and found that a number of them were subscribed in the names of his victims.

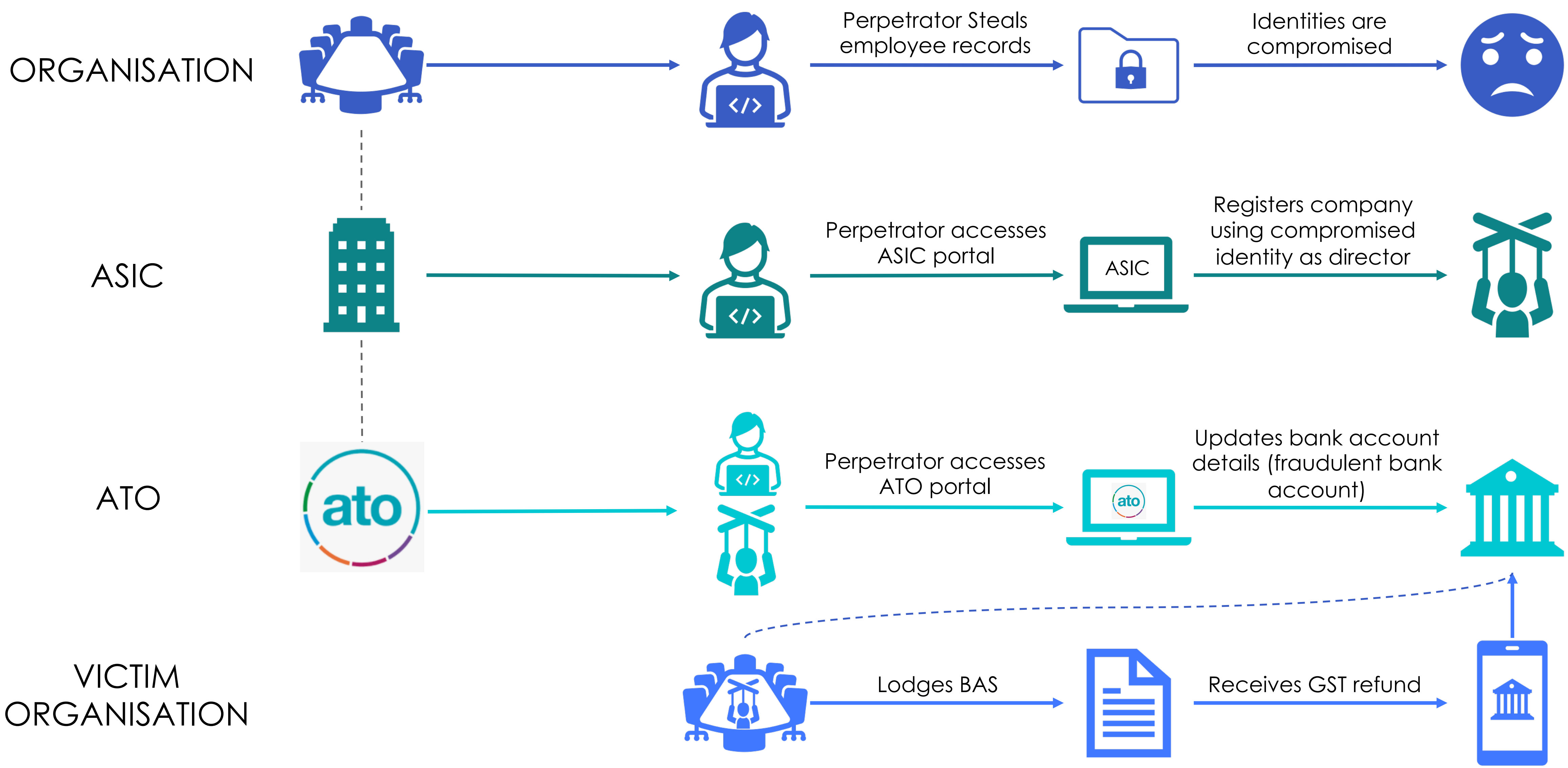
> **Bank records confirmed that ATO refunds were deposited into the various accounts** held by Mr McCarthy and that in the majority of cases the **refund had been withdrawn shortly after it was deposited**. CCTV footage revealed that Mr McCarthy had made four ATM withdrawals from two separate accounts and that the withdrawals coincided with the ATO depositing refunds for two of the victims into those accounts.

> **A total of $558,584.04 was illegally claimed by Mr McCarthy**. Internal bank anti-fraud measures and efforts by the ATO and Queensland Police meant that **$370,787.63 in illegal transactions were stopped**. A total of $187,796.41 was paid into Mr McCarthy's bank accounts.

Brisbane man jailed for identity theft and income tax fraud | Commonwealth Director of Public Prosecutions (cdpp.gov.au)

IDENTITY CRIME | CASE STUDY 2

Australian Government
Australian Taxation Office



IDENTITY CRIME | CASE STUDY 3

Australian Government
Australian Taxation Office

- On 23 November 2020, following a successful joint investigation by the Australian Taxation Office (ATO) and Australian Federal Police (AFP), a 38-year-old fraud syndicate member was convicted in the Melbourne County Court for conspiring to defraud the Commonwealth of **GST refunds totalling over $5 million**.
- Michael Ray was a senior partner in a scheme where **confidential taxpayer information was illegally obtained** and used to create false entities and Australian business numbers (ABNs) and register them for GST. The fraud syndicate then **lodged business activity statements (BAS) claiming false GST refunds**. The refunds were directed to bank accounts that had been created using the stolen identities.
- The scheme was **uncovered by a taxpayer when they conducted a Google search** and discovered their personal details located in a spreadsheet titled 'wolf2012'. The taxpayer reported what they had found to both the police and the ATO. The taxpayer's discovery uncovered a den of deceit for the agencies involved.
- Mr Ray, the last pack member, pleaded guilty to conspiracy with the intention of dishonestly obtaining a gain from the Commonwealth. He was sentenced to five years imprisonment, with a non-parole period of three years, bringing the eight-year long joint investigation to a close.
- Mr Ray's sentencing follows the sentencing of the scheme's orchestrator, Marc Christian, in May 2020. Mr Christian was sentenced to 12 months imprisonment, to be released after six months on a recognizance order, for money laundering and five years imprisonment, with a non-parole period of three years, for **conspiring to dishonestly obtain a gain from the Commonwealth**.
- All convictions in relation to this matter are a successful result under the partnership of the ATO and AFP, who often work together to investigate serious criminal activities.
- **Tax crime affects the whole community**. It reduces the amount of revenue available to fund essential community services.
- This case demonstrates the **power of tip-offs from the community**. A tip-off could be the missing piece of the puzzle we need to successfully prosecute someone who is committing tax crime.

[Financial crime case studies | Australian Taxation Office (ato.gov.au)]

The term 'cybercrime' is used to describe both:

> Crimes directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks), and
> Crimes where computers or ICTs are an integral part of an offence (such as online fraud).

Behaviours (SFCT Fact Sheet):

> They often use illegal marketplaces (facilitated by the dark web) to enable the sale of illicit goods, services and information.
> Crime is provided as a service. For example, some criminals sell names and information related to individuals and criminal syndicates. 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.
> Meanwhile, others provide hacking services, or 'testing services' that seek to compromise the security and information of government agencies, banks, businesses and other organisations.

BREAK-OUT ROOM | ACTIVITY: IDENTITY CRIME

In your groups, consider the following questions:

Group 1:

What sources of information would be at risk of potential identity compromise in your jurisdictions? What would need to be 'stolen' to claim VAT/GST refunds?

Group 2:

What procedures have you in place in your jurisdictions to verify identities of claimants for refunds/credits?

Group 3:

Are there any criminal charges relating to identity crime in your jurisdictions? How should such a crime be prosecuted?

Group 4:

What are some ways to prevent or disrupt possible identity crime related to tax refunds?