



Australian Government
Australian Taxation Office

Welcome back to day two of our Presentation: Complex Money Laundering and the Role of Tax Investigators

Delivered by Carla Grist and Mark Robinson

With a supporting session from Austrac representative Sam Lamour

Day Two

- Participant Presentation, a selected case study or insight from a participant is shared to build knowledge and connections
- AUSTRAC (Australian Transaction Reports and Analysis Centre) presentation
- Presentation and discussion on ML, money flows, methodologies and reporting suspicions. Case studies.
- Money laundering legal framework, Practical Exercises (“Catch me if you can”)
- Tax Evasion, what it is, with case studies
- Participant Presentation
- Case Study - how tax crime fits in to predicate offences to money laundering.
- Case Study - future focus

Breaks may occur sooner or later depending on topic and conversation.

Please share freely of your knowledge – we are all here to learn.

Tuesday	Wednesday
24-May-22	25-May-22
Starting Time 13:00 pm (Tokyo Time GMT+9)	
Participant Presentation (13:00 - 13:30)	Participant Presentation (13:00 - 13:30)
Fighting Tax Crime: The 10 Global Principles	Austrac
What is Money Laundering? *Breakout session	
Virtual Break	
Entry/mid/high level examples.	Money laundering legal framework - Practical Exercise ("Catch me if you can")
Enablers	Tax evasion: what it is and case studies
Lunch Break at 16:00 pm, Return to Class 17:00	
Recent and Emerging Trends	Participant Presentation (13:00 - 13:30)
The role of tax investigators in the fight against ML / Enablers	Case Studies - predicate offences to money laundering and how tax crime fits in.
Virtual Break	
Case Study - Enablers - accountants - role of tax investigators.	Case Study - future focus
Extra Time as Needed	Extra Time as Needed
Wrap up	Wrap up
Ending Time 19:00	

Participant Presentation

We are very
pleased to
hear from....



Australian Government

AUSTRAC

/FIGHTING FINANCIAL CRIME TOGETHER/

AUSTRAC

Sam Larmour
Serious Financial Crime Team
May 2022

Overview

- **The Australian Transaction Reports and Analysis Centre (AUSTRAC)**
- **Money Laundering Intelligence at AUSTRAC**
 - Case Study
- **Public-Private Partnerships and Fintel Alliance**
 - Case Study
- **AUSTRAC's Regulatory Role**
 - Case Study

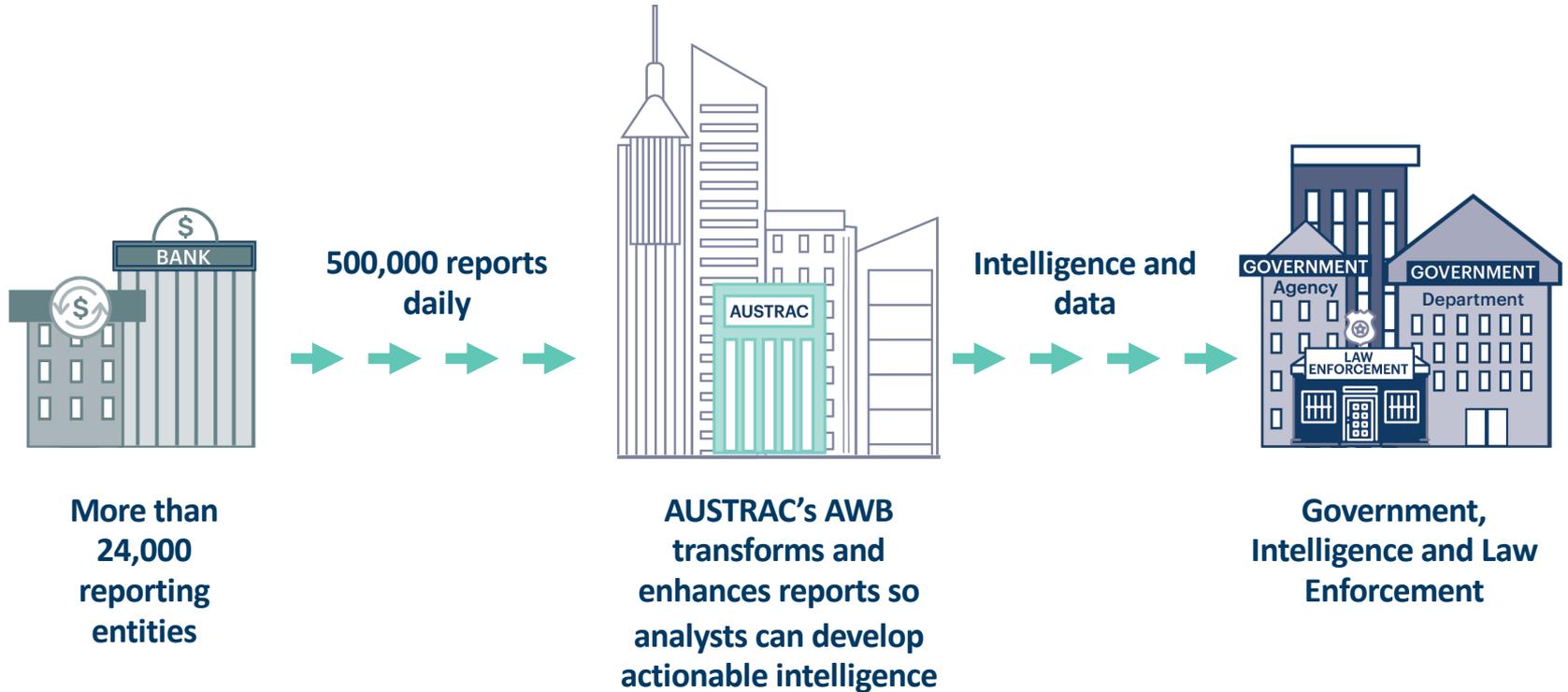


The Australian Transaction Reports and Analysis Centre (AUSTRAC)

AUSTRAC

- AUSTRAC is Australia's financial intelligence agency, with regulatory responsibility for anti-money laundering and counter-terrorism financing.
- AUSTRAC is responsible for preventing, detecting and responding to criminal abuse of the financial system to protect the community from serious and organised crime.

Australia's Reportable Transactions



Analyst Workbench

Usage

3
Partner agencies
7
of AWB growing

1.
BILLIO
3
Transaction reports

30
Internal
0
Users

19
MILLION
6
Entities

More than
1,000,00+
queries in the past 4 months



Australian Anti-Money Laundering Reporting Requirements

Australian AML in the 1990s

- 100 point check to open bank account
- Reporting transactions to AUSTRAC
 - Suspicious transactions
 - Large cash transactions
 - International funds transfers
 - Taking cash into/out of Australia
- Ok to do business with criminals so long as you report it to AUSTRAC



Australian AML today

- Identify, rectify and monitor vulnerabilities that could be exploited by criminals (risk-based approach)
- Verify their customer's identity
- Monitor transactions to spot suspicious activity/customers
- Scrutinise high-risk customers and potentially suspicious activity further
- Submit transaction reports to AUSTRAC



Money Laundering Intelligence at AUSTRAC

Money Laundering Intelligence

- Criminal Assets Confiscation Taskforce
- Money Laundering Operations
- Taskforce Vanguard



Taskforce Engagement

- AUSTRAC is a member of a diverse range of taskforces, providing **specialist financial intelligence** to support national security and law enforcement outcomes.
 - Victim based crime – child exploitation
 - Drugs
 - Firearms
 - Outlaw Motor Cycle Gangs
 - Economic crime
 - Cyber crime
 - Serious Financial Crime
 - Criminal Asset Confiscation
 - Illicit tobacco
 - High Volume Crime
- Cooperation mechanisms include:
 - MOU underpins the purpose and focus
 - Analyst secondments
 - Senior agency representatives contribute to strategic direction
 - Leveraging networks of Fintel Alliance, Data Analytics and Regulatory Operations

Taskforce Benefits and Challenges

Benefits:

- Enhanced information and intelligence exchange
- Build trust and develop collaborative working relationships
- Better understanding of money laundering risks around predicate offences
- Leverage resources
- Greater agency buy-in and support of financial intelligence
- Promote unified messaging
- Joint training opportunities and capability development

Challenges:

- Legislative restrictions - information sharing provisions
- National taskforces operating at a state level
- Limited capabilities of a non-law enforcement agency
- Resourcing



FIU Continuous Improvement



THREATS & ENABLERS

Expand our detection, analysis and assessment to include the enablers of financial crime including facilitators and technology.



ENRICH OUR PRODUCTS

Enhanced 'discovery' and actionable real-time intelligence through multi-source data and analysis, data modelling, and AI.



EXPAND OUR OFFERING

Strengthen 'understand' outcomes through new strategic intelligence offerings, and lead community action in niches areas.



WORLD-LEADING TRADECRAFT

Enhance methods beyond entity analysis, integrate data analytics into tradecraft, and normalise data analysts in FININT teams.



ADVANCED TOOLS & SYSTEMS

New technologies leveraged to enhance visualisation, reduce manual processes for analysts, and support cutting edge analysis.



Case Study: ML in Casinos

Overview – Case Study

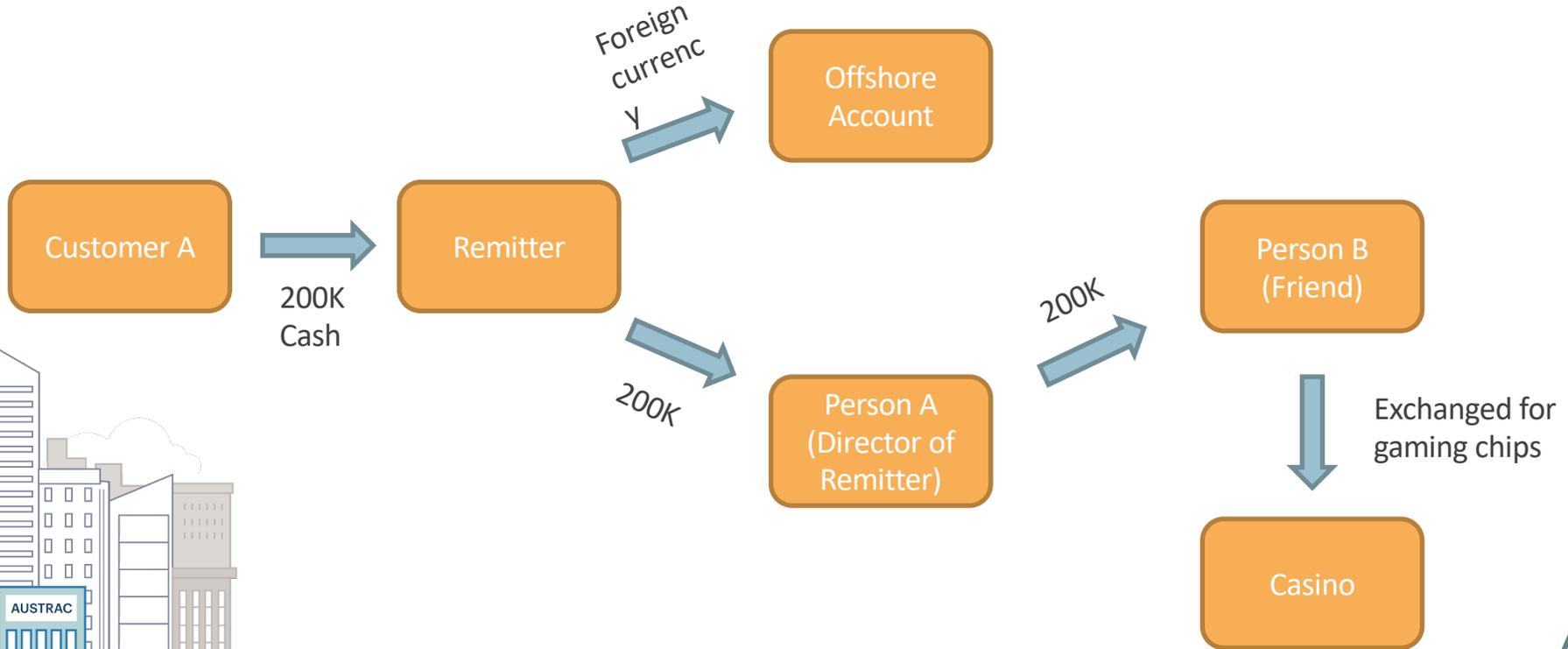
“Serious crime is motivated by profit, and no matter the size, most criminal acts leave a financial trail.”

- Multiple government agencies
- Use of cash
- Remittance company
- Transfers to offshore entities
- Gambling at casino
- ML convictions



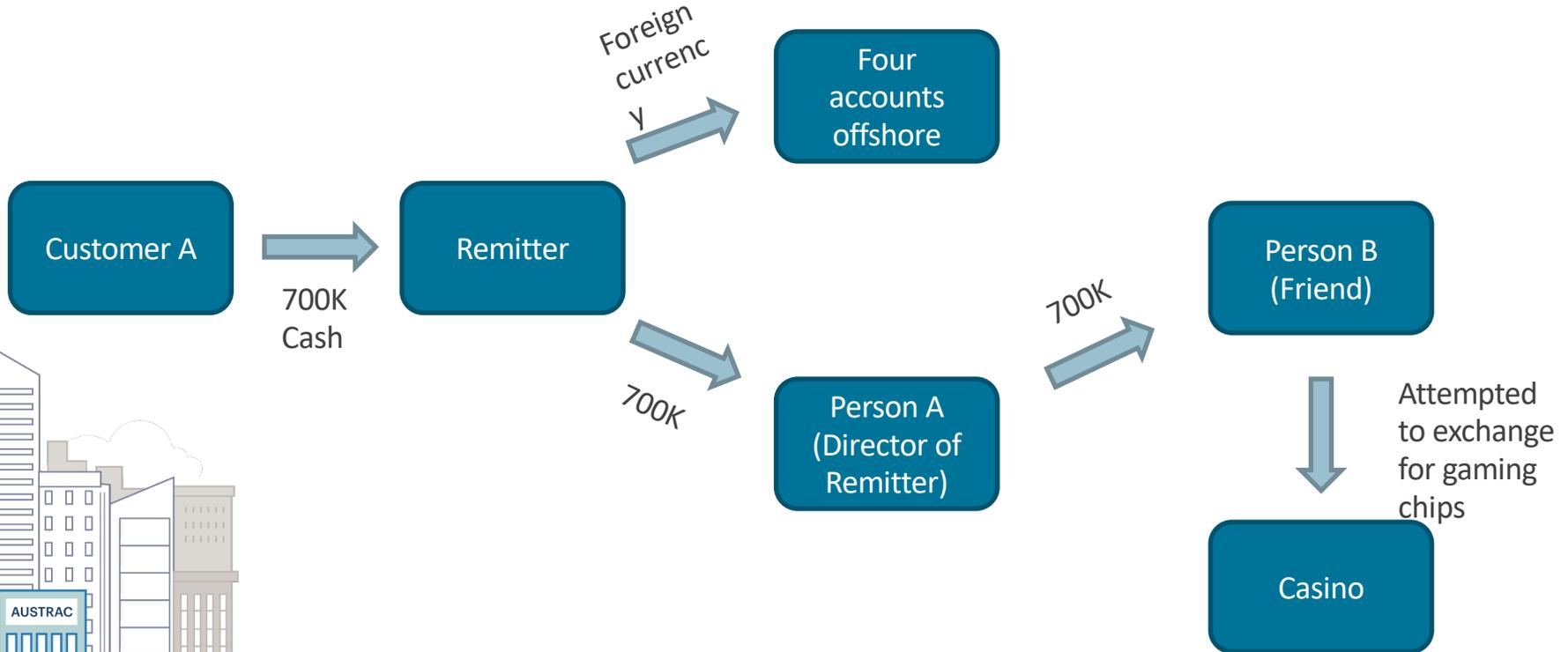


Flow of Funds – Example One





Flow of Funds – Example Two





Interagency Cooperation

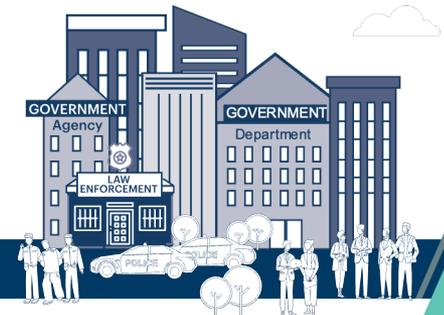
- Suspicious cash deposits identified by casino
- Requests for further information to AUSTRAC
- Financial intelligence
- Issued information gathering notice
- Additional analysis





Why was the money suspicious?

- Customer's wealth inconsistent with occupation
- Undocumented large amounts of cash
- Structured transfers to offshore countries
- Instant messaging and paper ledger





Outcome

- Person B arrested at casino
- Cash seized and later forfeited
- Person A arrested at later date
- Convictions for dealing with proceeds of crime
- Remitter de-registered with AUSTRAC





Public-Private Partnerships

Fintel Alliance

An AUSTRAC initiative, Fintel Alliance brings together government and private sector organisations who work together to increase the resilience of the financial sector and contribute to law enforcement investigations.

Government and private sector members work together to:

- **increase the resilience** of the financial sector to prevent it being exploited by criminals
- **support law enforcement** investigations into serious crime and national security matters
- **protect the most vulnerable** members of the community from criminal exploitation

A public private partnership



Fintel Alliance: Themes

Theme	Types of matters
Crimes affecting the most vulnerable community members	Children, the elderly and people with a disability.
Exploitation of government revenues	Protecting Australia's tax system, national disability scheme, education, child and day care services, aged services and other government programs from abuse.
Networked and complex financial crime	Disrupting organised criminal enterprises that seek to exploit multiple businesses and industries e.g. money mules, black economy and trade-based money laundering.
Nationally significant task forces and campaigns	Supporting national operations including targeting Australia's most wanted criminals, illicit drugs, transnational and serious organised crime, illegal firearms and support to other national effort.
Responding to regional and community harms	Helping to address localised crime, address regional programs, and collaborate with regional partners
Technology and sophistication	Responding to the most complex money laundering efforts through innovative approaches to data and information.

Fintel Alliance working groups

Tax Crime and Evasion Working Group



The Tax Crime and Evasion Working Group brings together Commonwealth Government agencies and banking partners. The working group presents a forum for the sharing of information to identify, disrupt and prevent tax crime and evasion, with an additional focus on engaging with international partners.

Trade-Based Money Laundering Working Group



The Trade-Based Money Laundering Working Group has established a program of work to drive educational uplift and knowledge exchange, the development of shared operations, and support international efforts to combat and disrupt trade-based money laundering.

Fintel Alliance working groups

National Security Working Group



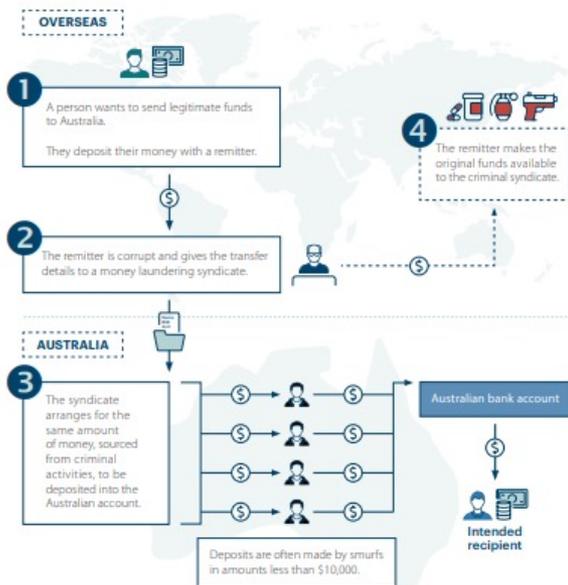
The Fintel Alliance National Security Working Group promotes engagement between AUSTRAC, federal government, the Big Four banks and PayPal, to share and exploit information and financial tools to better understand, detect and disrupt major national threats.

Virtual Asset Working Group



The Fintel Alliance Virtual Asset Working Group brings together experts from digital currency exchange providers and law enforcement in the fight against money laundering, terrorism financing and other serious crime through the use of digital currencies.

Fintel Alliance education material



Cuckoo smurfing

How to spot, avoid and protect yourself from this money laundering scheme

If you send or receive money from overseas using a money transfer business, you may be at risk of criminals targeting your bank account using 'cuckoo-smurfing'.

Cuckoo smurfing is a method of money laundering used by criminals to make money generated by criminal activities appear to have come from a legitimate source. Organised criminals use professional money laundering syndicates to target the bank accounts of people receiving money transfers in Australia.

Protect yourself from this criminal activity by learning the warning signs and reporting suspicious activity.

What are the warning signs?

Look out for and report unexpected and suspicious activity occurring in your bank account, including:

- multiple cash deposits in amounts under \$50,000
- multiple cash deposits made on the same day or within a short period
- cash deposits made across various branches and ATMs, including across different states
- cash deposits from multiple third parties.

Who is a target?

You could be at risk if you are expecting a money transfer from overseas involving a money transfer business. This includes:

- Australian expatriates
- Australian exporters
- international students studying in Australia
- international investors
- migrants wishing to settle in Australia.

How to protect yourself

Only deal with, or request funds be sent through, legitimate financial institutions or money transfer businesses.

If you're expecting to receive funds from overseas, review your bank account activity and report any suspicious transactions.

Here's how it works:



The deposits into the Australian account (the 'cuckoo's nest') are often made by cash mules ('smurfs') in amounts less than \$50,000. It is a criminal offence to deliberately split large transactions into smaller amounts of less than \$50,000 in an attempt to avoid threshold transaction reporting.

Reporting suspicious account activity

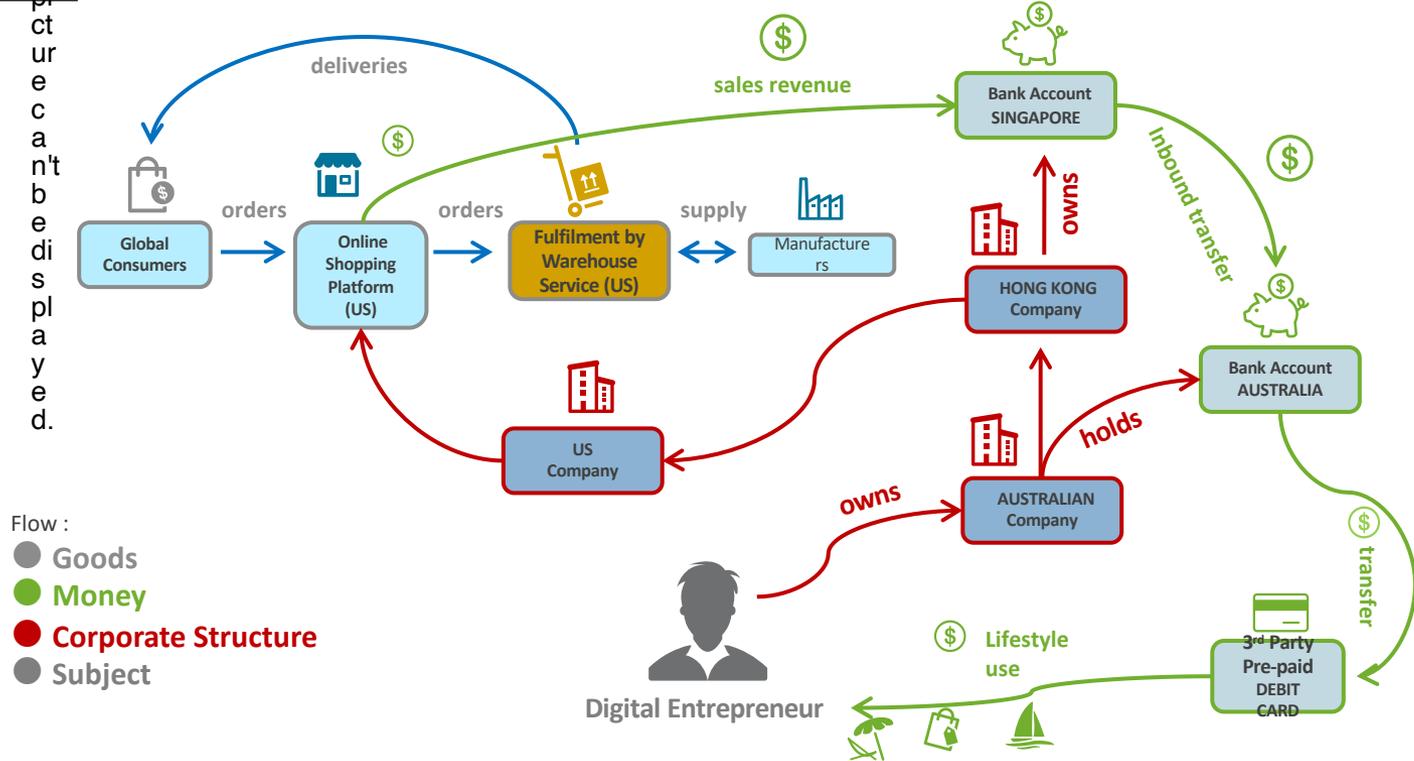
If you notice any suspicious activity occurring in your bank account, including the warning signs above, you should immediately report it to your bank in the first instance, or call Crime Stoppers on 1800 333 000.

If you become aware of this activity, it is important to report it. Failure to report this activity means you could face the prospect of criminal prosecution, confiscation of these funds or your bank closing your account(s).

For more information visit www.afp.gov.au/proceeds-crime

The picture can't be displayed.

Case study: Partnerships identify tax evasion across four countries



✗ No Tax Returns – US or HK ✗ Aust. Company – Losses Only ✗ Individual – minimal income ✗ No IDS and Minimal FSI declared ✗ No BAS Lodgements



AUSTRAC's Regulatory Role



AUSTRAC case study: CBA Regulatory Action

Case Study: AUSTRAC Regulatory Action against the CBA

- CBA ordered to pay pecuniary penalty of \$700 million.
- Largest civil penalty at the time.
- Second time AUSTRAC has taken civil penalty action.
- CBA admitted to 53,750 breaches of the AML/CTF Act.
- Most contraventions related to the intelligent deposit machines (IDMs).
- The Court considered the contraventions serious, and found that millions of dollars had been laundered through CBA, included proceeds of crime.



AUSTRAC detects non-compliance by CBA

- 11 August 2015 AUSTRAC contacts CBA about 2 missing threshold transactions referred to in an SMR
- 24 August 2015 CBA submits 2 TTRs to AUSTRAC and identifies that 53,506 threshold transactions are reported late
- 24 September 2015 53,504 late TTRs are reported

AUSTRAC's investigation of non-compliance

- AUSTRAC gathered evidence from CBA in respect of the alleged non-compliance
- AUSTRAC worked with LEAs to investigate the non-compliance
- AUSTRAC applied to the Federal Court

Enforcement Criteria

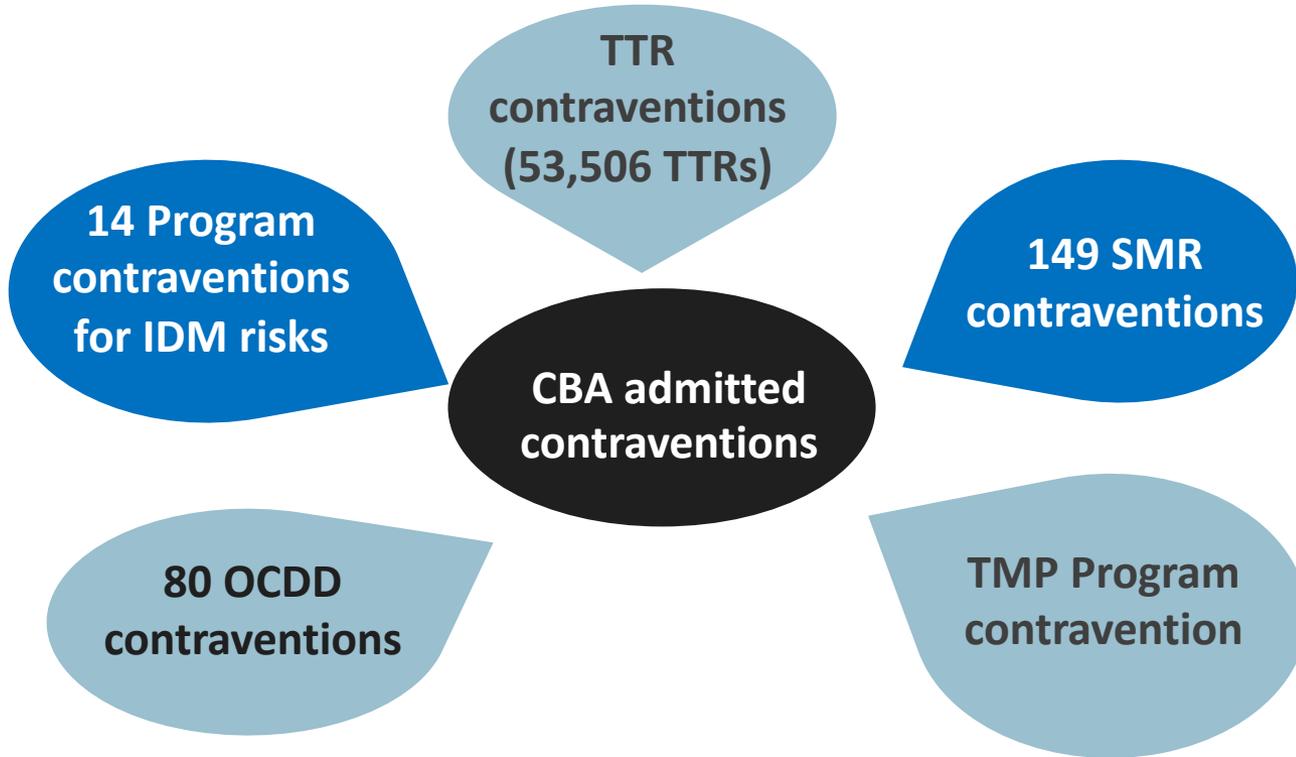
- i. The nature of the non-compliance;
- ii. The ML/TF risk associated with the reporting entity;
- iii. The reporting entity's willingness and effort to comply;
- iv. Whether the reporting entity voluntarily disclosed the non-compliance; and
- v. The likely consequences of an enforcement action, e.g. achieving remediation and deterrence and/or establishing legal precedent.



Further contraventions

- Further investigation by AUSTRAC identified and alleged:
 - CBA failed to report 2 SMRs relating to TF
 - CBA failed to report 54 SMRs in relation to accounts and individuals subject to LEA operations
 - 38 instances of not appropriately monitoring after becoming aware of suspected TF, ML and structuring
 - 6 breaches of its AML/CTF program

CBA Admissions and Judgement



Impact of non-compliance on the community

- Exploitation by Criminals
 - Money Laundering
 - Terrorist Financing
- Intelligence loss
 - TTR and SMR failures/delay



Questions?



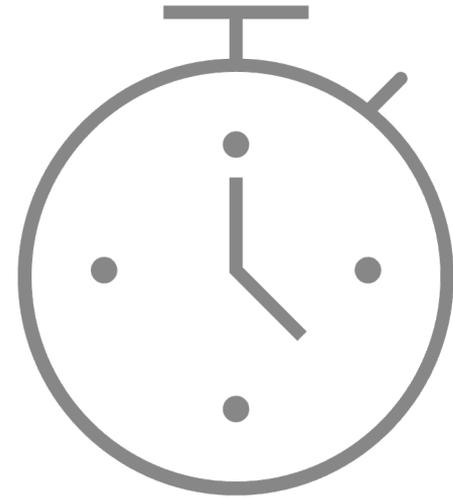
Australian Government

AUSTRAC

www.austrac.gov.au

DISCLAIMER: The information contained in this document is intended only to provide a summary and general overview on these matters. It is not intended to be comprehensive. It does not constitute nor should it be treated as legal advice or opinion. This presentation contains statements of policy which reflect AUSTRAC's administration of the legislation in carrying out its statutory functions. The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication, including any errors or omissions therein. AUSTRAC recommends that independent professional advice be sought. The information contained herein is current as at the date of this document.

BREAK



Money laundering legal framework



Avoidance vs Evasion vs Fraud

The difference between Tax Avoidance and Tax Evasion is legality.

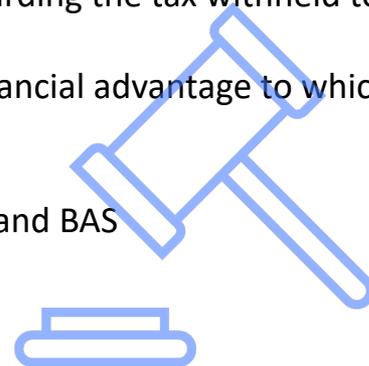
Tax Avoidance is legally exploiting the tax system to reduce current or future tax liabilities by means not intended by parliament. It often involves artificial transactions that are contrived to produce a tax advantage. Part IVA of the Income Tax Assessment Act 1936 holds the treatment provisions for dealing with Tax Avoidance schemes.

Tax Evasion is where a person makes blameworthy acts or omissions on Income Tax Returns or Statements to the ATO. Examples of Tax Evasion include:

- Not reporting all income
- Not reporting cash wages
- Not withholding tax from a worker's wages, or withholding tax and not forwarding the tax withheld to the ATO.

Tax Fraud occurs when individuals or organised groups cause a loss or claim a financial advantage to which they aren't entitled, including:

- Claiming false tax refunds using false or stolen identities
- Knowingly claiming GST credits for goods or services based on false invoices and BAS
- Knowingly claiming deductions for expenses which were never incurred.
- Using dishonest methods to transfer tax debts to an insolvent entity.



Indicators an arrangement is more than Tax Avoidance

- Circular Movement of Funds or No Movement of Funds
- Accounting Book Entries, No Accounts or Financial Statements
- “Questionable” invoices, receipts, paperwork
- Reliance on hidden relationships, secrecy, tax havens
- Nominee or Straw Directors and Shareholders
- Post Dating or Backdating of Documents



Practical Exercise: Catch me if you can

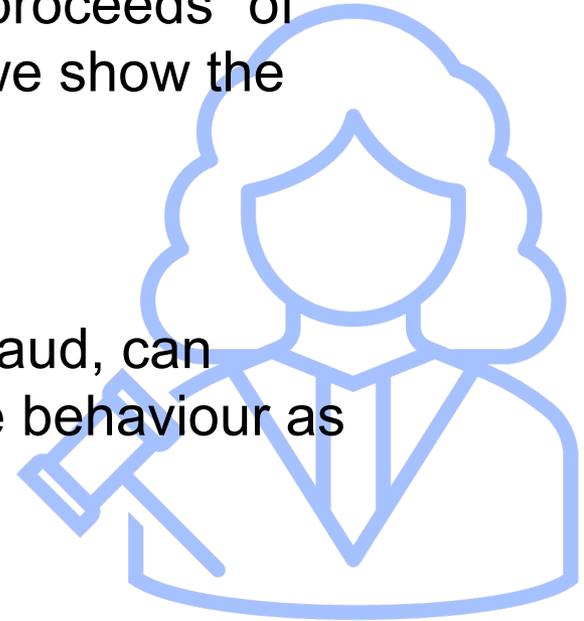
- Circular Movement of Funds or No Movement of Funds
- Accounting Book Entries, No Accounts or Financial Statements
- “Questionable” invoices, receipts, paperwork
- Reliance on hidden relationships, secrecy, tax havens
- Nominee or Straw Directors and Shareholders
- Post Dating or Backdating of Documents



Does the predicate offence need to be proven?

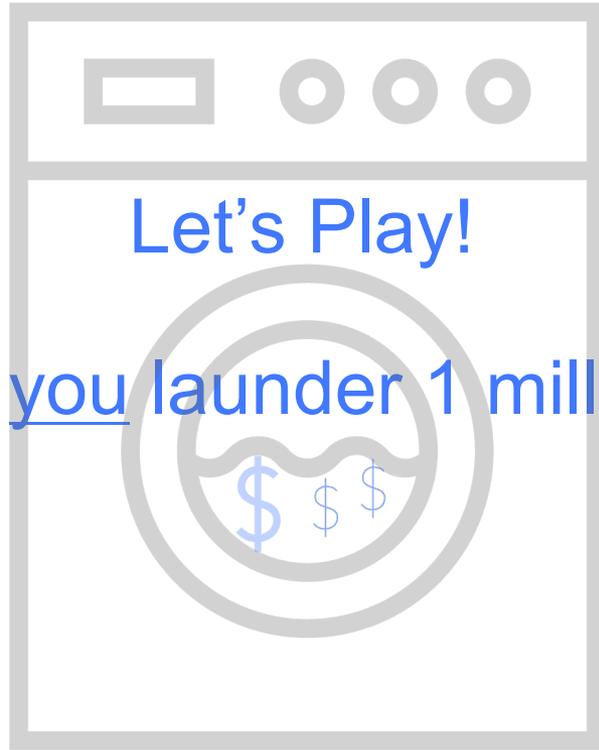
Money laundering relates to the “proceeds” of the predicate offence so how do we show the “proceeds” are criminal profits?

For financial crimes such as tax fraud, can money laundering cover the same behaviour as the fraud?



\$

\$



€

£

₪

How would you launder 1 million dollars?

\$

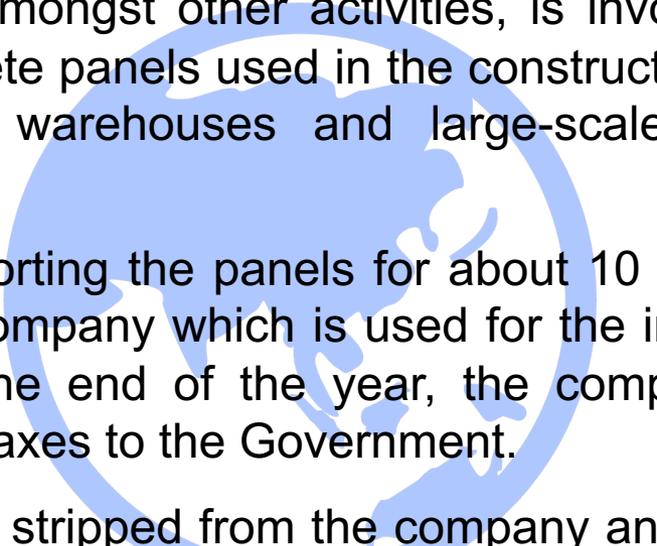
¥

₹

\$

\$





Your syndicate is an organised crime group based in South East Asia. Your group, amongst other activities, is involved in importing prefabricated concrete panels used in the construction of commercial buildings such as warehouses and large-scale accommodation buildings.

You have been importing the panels for about 10 years. Every year you incorporate a company which is used for the importing and sale of the panels. At the end of the year, the company is liquidated without paying any taxes to the Government.

All of the assets are stripped from the company and a new company is incorporated. For the last year, you have been using a company called '*Dragon Panels*'* to import the panels.

**(This is a made up business name, and similarities to any real companies called this is purely coincidental)*

You have a corrupted high-ranking official in the governments Revenue Department. They provide information about any interest taken in your company by authorities and you pay them \$10,000 every year.



Construction companies are happy to enter into contracts on a yearly basis with your new companies. They do it because you sell the concrete panels to the construction companies cheaper than anyone else - you do not pay VAT or company tax to the Government.



Each month, the construction companies pay the amounts owing into bank accounts operated by Dragon Panels with a Commercial Bank.



Once payment has been received, cash runners employed by your syndicate attend various branches of the bank and withdraw the money **in cash**. This is then taken to a secret location and stored. The cash is used to pay the wages of each employee of Dragon Panels.

Due to COVID you now have \$1 million US dollars stored in your secret location. Previously, the cash was simply divided up between the syndicate members, with each member taking their share of the cash and doing whatever they wanted to with the money.

Your high-ranking official in the Revenue Department has told you that a joint agency investigation is about to start which will be investigating your company. You agree to pay him \$10,000

As a result, you want to develop a plan to launder the money prior to each member getting their share.

Group Task

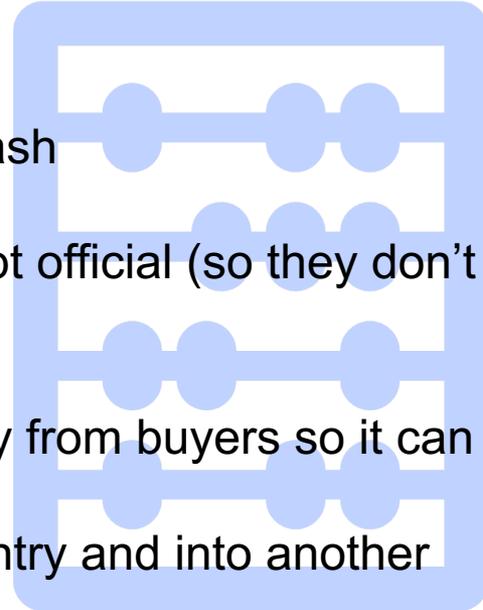
Your syndicate is to design a money laundering plan that addresses the following issues:

Group 1. The laundering of the US \$1 million cash

Group 2. Payments of US \$10,000 to the corrupt official (so they don't get caught).

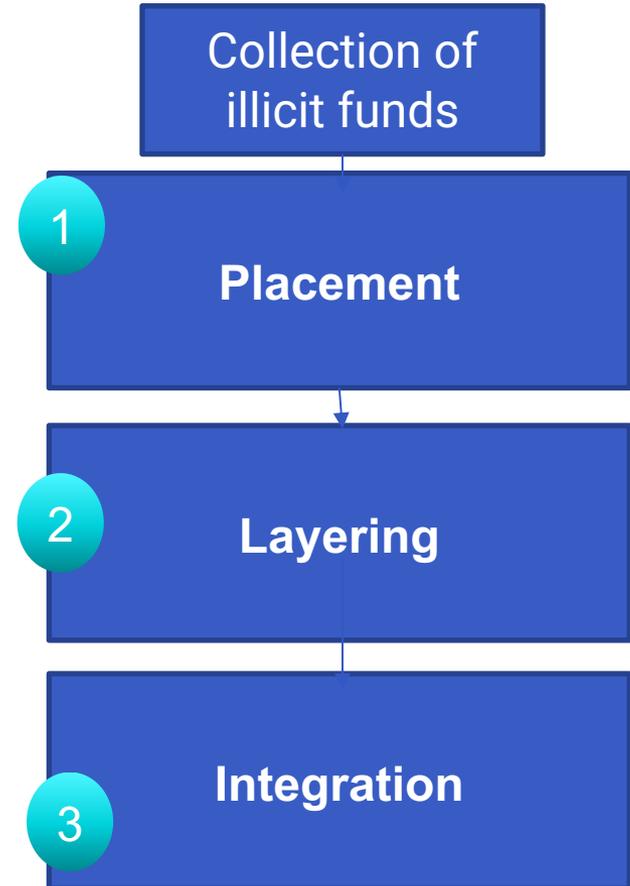
Group 3. Setting up new ways to receive money from buyers so it can be hidden.

Group 4. Ways to get the money out of the country and into another

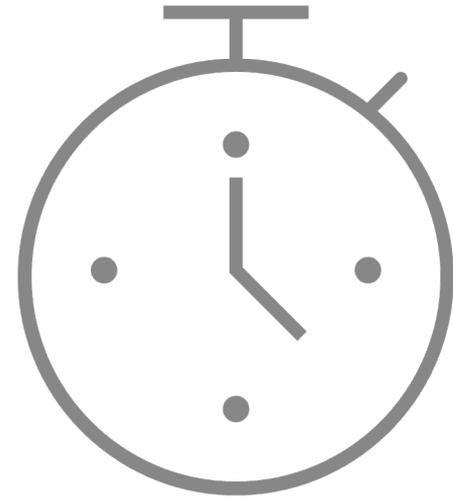


In relation to your plan, don't just mention what you would do but **explain how each money laundering typology would operate.**

The number of typologies used is a matter for your group however; please try at least 3-4 laundering methods.



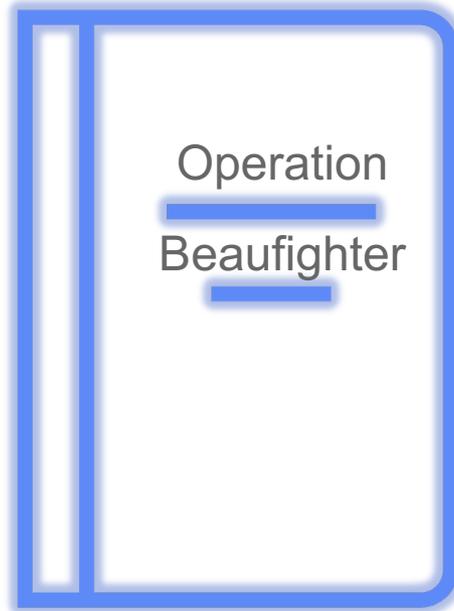
BREAK



Participant Presentation

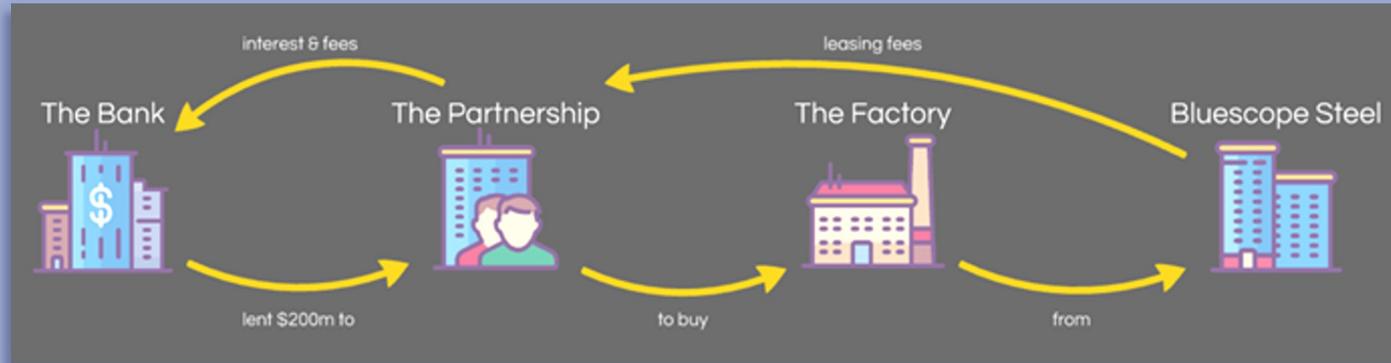
We are very
pleased to
hear from XXX

Case Study: Predicate offences to money laundering and how tax crime fits in.



Case Study One

Operation Beaufighter



Case Study Two

Directors

All companies are controlled by:



Anthony Dickson

Michael Issakidis

NeuMedix Health Australasia Pty Ltd
Athena Health (Cayman islands company)
Karkalla (fake Samoan company)
Dampier Finance (Samoan financier)
Athena Global (UAE)
Meed Inc (UAE)

Proceeds of a crime

All companies are controlled by:

\$ 63,715,000

received from 4 unit trusts

\$ 68 M

actually received



The loss

or risk of loss that was intended to be caused to the Commonwealth was

30% of approx
\$450 million

approx **\$135 million** in the relevant years.

The balance of

\$300 million

understated income had no tax paid on it in later years, with another **\$100 million** tax not paid.

How it was set up

1 Four trusts were created to facilitate transactions between ANZ and large corporates under 'sale and leaseback' arrangements.



2 Complex arrangements were set-up by via NeuMedix for the purpose of obtaining a tax benefit. The arrangements resulted in tax liabilities being distributed to NeuMedix from the ANZ and other large companies in return for lesser cash payments.



3 NeuMedix entered into agreements with Athena Health Patents Incorporated (Cayman) to acquire medical patents/inventions relating to the treatment of cancer and a surgical clip.

6 Athena Health 'sells' intellectual property to NeuMedix at an inflated price.



5 Karkalla overvalue the patents in valuations provided to Neumedix to convince the ATO that the patents were real.



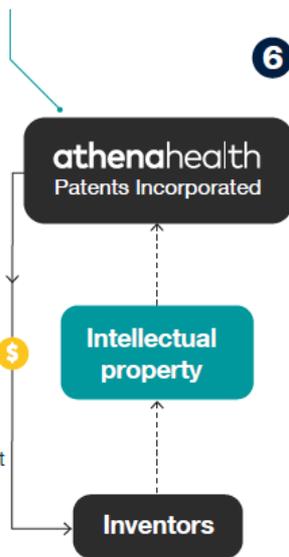
8 NeuMedix falsely claims tax depreciation expenses on the acquisition of intellectual property, to ensure they have no actual tax liability from their involvement in sale and lease back arrangement.



7 Dampier Finance purportedly provided funding to NeuMedix to buy patents. No actual funds were exchanged. Involvement of an international finance company intended to convince ATO transactions were legitimate.



4 Provided with a small amount of research funding and a promise of further payments if commercially successful to assign IP to Athena Patents.



\$ Real funds
\$ Presumed funds
 → Flow of funds
 ---> Flow of business or property

Company Information



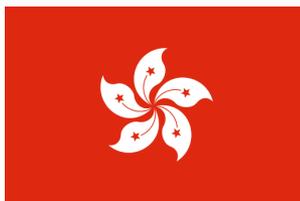
Nominee Directors
& shareholders.

Incorporated
Cayman Islands



Nominee Directors
& shareholders.

Incorporated in
Hong Kong



Controlled by
DICKSON and
ISSAKIDIS

Incorporated in
Australia



Controlled by
DICKSON and
ISSAKIDIS.

Incorporated in
Samoa.



Over 3 years the tax obligations of the partnership totalled \$387,000,000

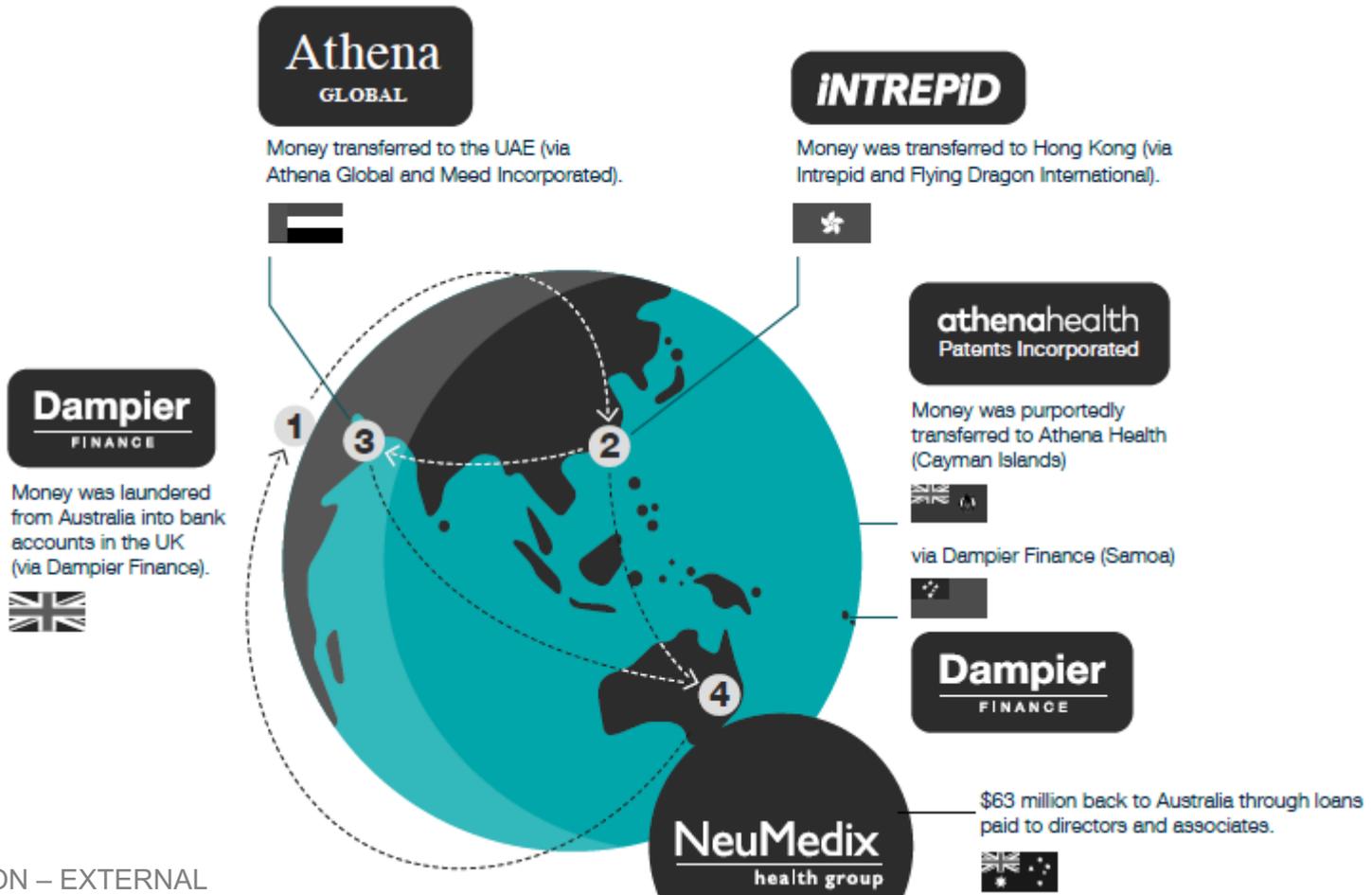
The tax obligations were *entirely offset* by the losses claimed by Neumedix for purchasing medical IP

The ATO missed out on \$135,000,000 in tax revenue

DICKSON and ISSAKIDIS, under the terms of the partnership, received approximately \$63,000,000



Money Laundering – where the funds moved

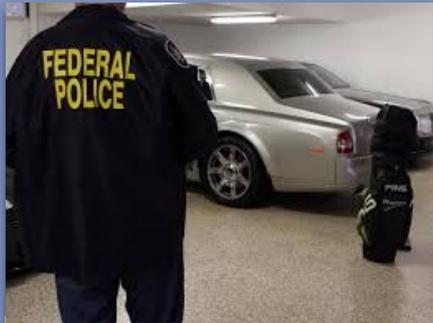


Execution of Warrants

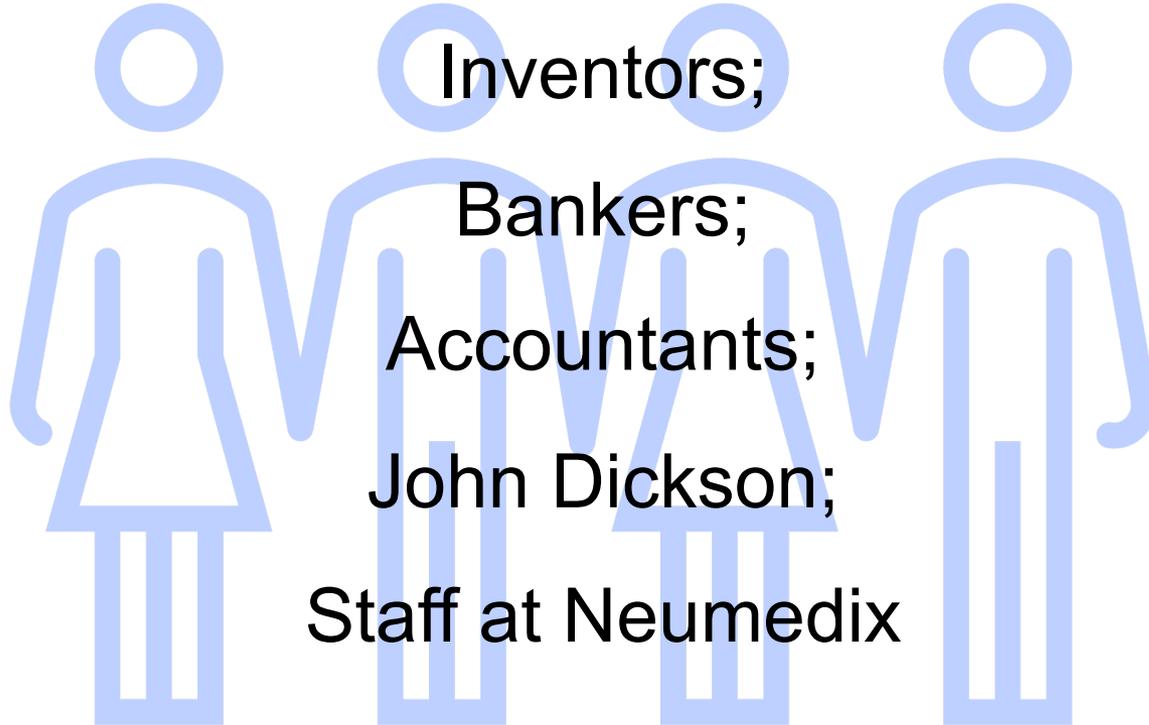
Multiple search warrants in multiple cities;
X-Agency teams

Most valuable results came from the Neumedix office and
DICKSON's house;

Law office – only records of trust accounts sought due to
Legal Professional Privilege (LPP)



Witnesses



Inventors;

Bankers;

Accountants;

John Dickson;

Staff at Neumedix

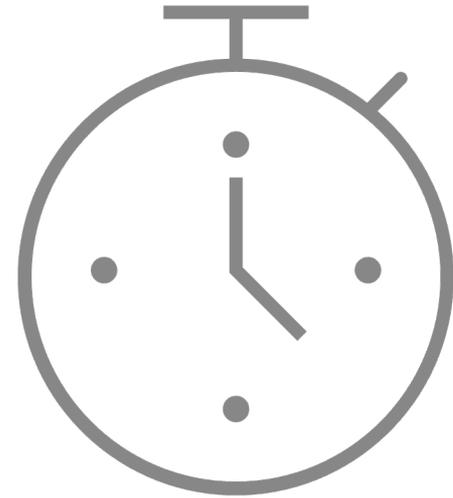
Outcomes

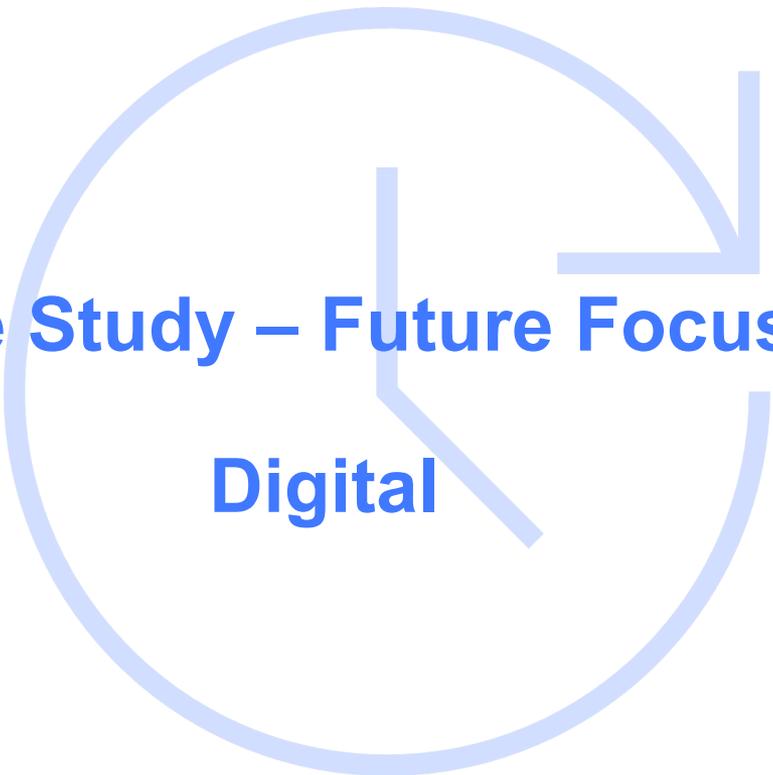
On 29 March 2018, Michael Issakidis faced the Supreme Court of NSW for his involvement in the largest prosecuted tax fraud case in Australia's history.

Issakidis was sentenced to 10 years and three months jail for his involvement in the operation. This followed the 2015 sentencing of Dickson, whose original 11-year sentence was increased to 14 years on appeal.



BREAK





**Case Study – Future Focus:
Digital**

Money Laundering Using Digital Currency: Placement

- Criminal converts their illicit proceeds into digital currency or vice versa
- A criminal is most exposed and identifiable during conversion process



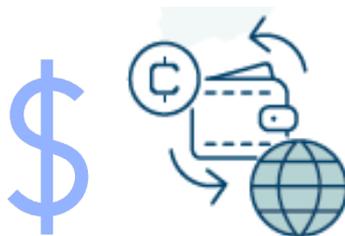
Money Laundering Using Digital Currency: Layering

Criminal moves or converts the illicit funds across different digital currencies, accounts or institutions to distance the funds from their source.

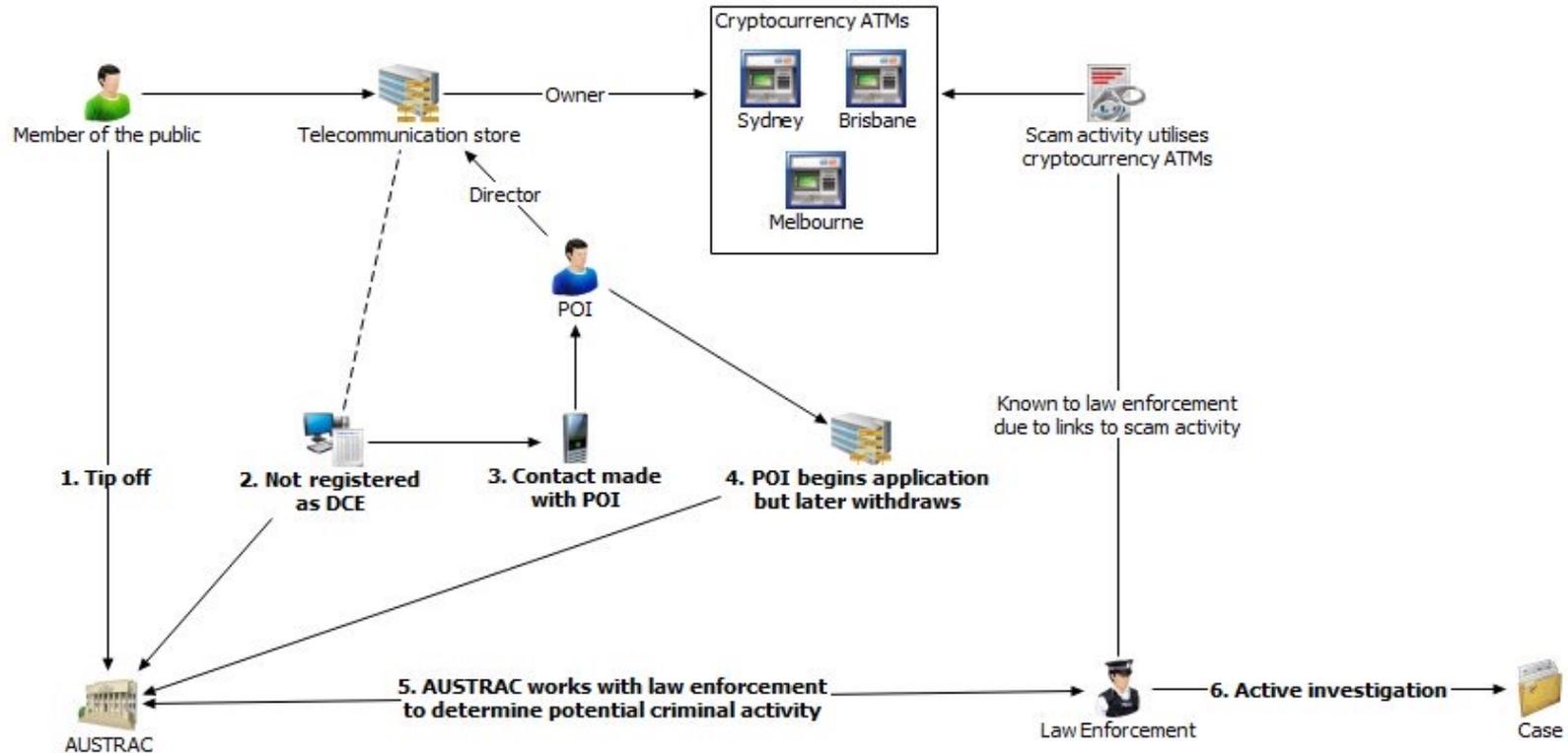


Money Laundering Using Digital Currency: Integration

Criminal spends the digital currency or reintroduces it back into the traditional financial system



Working with regulatory partners – Unregistered crypto ATMs



So, what did we learn?

How will we use this back in our workplaces?

Don't forget other resources available to you.



Thank you!





Australian Government
Australian Taxation Office

ato.gov.au

Mark.robinson@ato.gov.au

Carla.Grist@ato.gov.au

Resources

- [The fight against tax crime | Australian Taxation Office \(ato.gov.au\)](#)
- <https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Joint-Chiefs-of-Global-Tax-Enforcement/>
- <https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Serious-Financial-Crime-Taskforce/>
- <https://www.oecd.org/tax/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-and-other-financial-crimes.htm>
- <https://www.oecd.org/tax/crime/improving-cooperation-between-tax-and-anti-money-laundering-authorities.htm>
- [Combating virtual assets-based money laundering and crypto-enabled crime: Recommendations of the Tripartite Working Group on Criminal Finances and Cryptocurrencies | Basel Institute on Governance \(baselgovernance.org\)](#)