Australian Government
Australian Taxation Office

# OECD Tax Academy for Tax and Financial Crime Investigation

## Managing Financial Investigations (Intermediate)

27 November to 29 November 2023

Presentation by Carla Grist, Australian Taxation Office

# Overview

## Day 1

- The Role of Professional Enablers in Financial Crime

## Day 2

- Money Laundering Examples and Case Studies

## Day 3

- Guest Presentation from AUSTRAC
- Interagency Co-operation
- Questions

| Monday<br>27-Nov-23 | Tuesday<br>28-Nov-23 | Wednesday<br>29-Nov-22 |
|---|---|---|
| **Starting Time 13:00 pm (Tokyo Time GMT+9)** | | |
| Opening Remarks and Welcome | Participant Presentation<br>(13:00 - 13:30) | Participant Presentation<br>(13:00 - 13:30) |
| Administration, Introductions and Expectations | Money Laundering Case Studies | AUSTRAC Presentation<br>Toby Wiseman |
| **Virtual Break** | | |
| The Role of Professional Enablers | Money Laundering Case Studies | Money Laundering Case Studies |
| **Lunch Break at 16:00 pm, Return to Class 17:00 PM (Tokyo Time GMT+9)** | | |
| The Role of Professional Enablers | Criminal Tax Investigations in Japan | |
| The Role of Professional Enablers | Money Laundering Case Studies | |
| **Virtual Break** | | |
| The Role of Professional Enablers | Money Laundering Case Studies | |
| Extra Time as Needed | Extra Time as Needed | |
| **Wrap up** | | |
| **End Time 19:00** | | |

Australian Government
Australian Taxation Office

# The Australian Taxation Office (ATO) is the principal revenue collection agency of the Australian Government

Our role is to effectively manage and shape the tax and superannuation systems that support and fund services for Australians, including:

- Collecting revenue
- Administering the goods and services tax (GST) on behalf of the Australian states and territories
- Administering a range of programs that provide transfers and benefits to the community
- Administering the major aspects of Australia's superannuation system
- Being custodian of the Australian Business Register.

# Day 1

# The Role of Professional Enablers in Financial Crime

# Day 1 – Outline

- **Overview of Money Laundering**
- **Professional Enablers**

**Please give freely of your knowledge and ask questions, there will also be time allocated at the end for questions.**

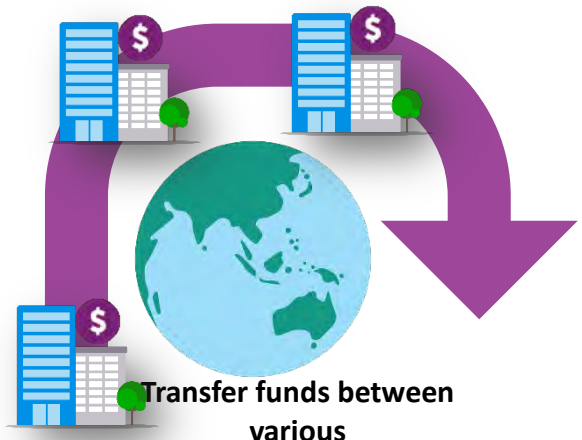
# Money Laundering

Money laundering has been addressed in the UN Vienna 1988 Convention Article 3.1 describing Money Laundering as:

***"the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions".***

The UN estimates the amount of money laundered globally in one year is 2 - 5% of global GDP, or $800 billion - $2 trillion in current US dollars. Due to the clandestine nature of money-laundering, it is however difficult to estimate the total amount of money that goes through the laundering cycle.

# Three stages of money laundering



Transfer funds between various offshore/onshore banks

Collection of illicit funds

1 Placement

2 Layering

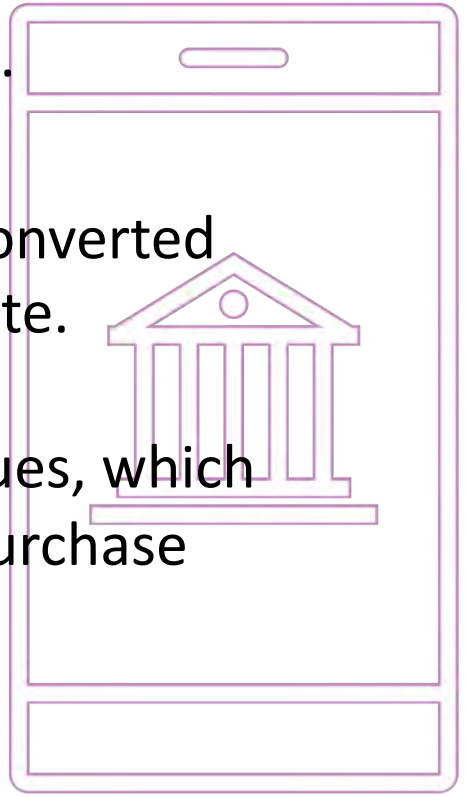
3 Integration

Dirty Money Integrates into the financial system


Purchase of Luxury Assets, Financial Investments, Commercial / Industrial Investments

# Stage 1: Placement

- $ Illegal funds or assets are first brought into the financial system.
- $ This 'placement' creates fund liquidity. For example, if cash is converted into a bank deposit, it becomes easier to transfer and manipulate.
- $ Money launderers place illegal funds using a variety of techniques, which include depositing cash into bank accounts and using cash to purchase assets.



# Stage 2: Layering

- To conceal the illegal origin of the placed funds, the funds are moved, dispersed or disguised. The process of distancing the placed funds from their illegal origins is known as 'layering‘.

- Money launderers use many different techniques to layer the funds. This includes transferring the funds domestically and internationally using multiple banks and accounts, having professionals act as intermediaries and transacting through corporations and trusts.

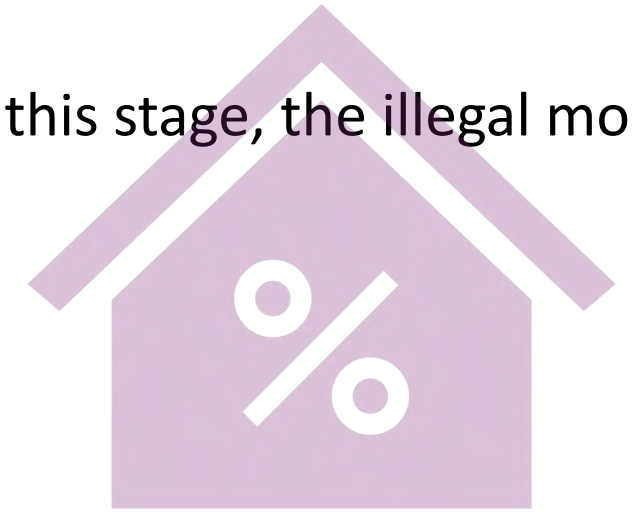
- Funds may be shuttled through a web of many accounts, companies and countries in order to disguise their origins.

# Stage 3: Integration

- $ Once the funds are layered and distanced from their origins, they are made available to criminals to use and control as perceivably legitimate funds. This final stage in the money laundering process is called 'integration‘.

- $ The laundered funds are made available for activities such as investment in legitimate or illegitimate businesses, or spent to promote the criminal's lifestyle.

- $ At this stage, the illegal money has achieved the appearance of legitimacy.



# Increased Money Laundering Threats: by region

**Africa:** Rapid digitisation of the financial sector has allowed new opportunities for criminals to increase their cyber based fraud avenues: phishing, ID theft, online banking, scams involving online assets. The profits are then laundered.

**Americas:** As Cyber enabled fraud continues to rise year after year so does the linked need to launder the proceeds of crime. Virtual assets have featured in recent years as a popular way to launder.

**Asia-Pacific:** Covid rapidly accelerated the integration of digital services with Illegal investment app fraud following.

**Caribbean:** Rapid increase in uptake of virtual based services: crypto, assets, mixers to clean money etc.

**Europe:** Increase in use of virtual assets to launder money, NFT's, initial crypto offerings.

**Middle East and North Africa:** Propelled forward by Covid identify based fraud has rapidly increased (impersonation, online banking, phishing, other online scams).

# Crypto Mixer

A crypto mixing service is an online service that makes it possible to conceal the origin or destination of cryptocurrencies. This service is used to split up cryptocurrencies, of both potentially illegal and legally obtained funds and mix them all together before transferring back to a chosen destination address.

There are two primary types of crypto mixers Centralised and Decentralised.

**Centralised**
A service where a fee is paid for use.

**Decentralised**
Peer to peer mixing with and agreed open-source protocol.

# Case example: Crypto Mixers

In June 2018 the Financial Advanced Cyber Team (FACT) of the Dutch FIOD started the investigation under the supervision of the National Public Prosecutor's Office for Serious Fraud and Environmental Crime and Asset Confiscation. The reason for the investigation was a report from cyber security company McAfee.

In 2020, the FIOD and the Public Prosecution Service took one of the largest online mixers for cryptocurrencies offline, named *Bestmixer.io*. The investigation was conducted in close co-operation with the Dutch Digital Intrusion Team (DIGIT), Europol and the authorities in Luxembourg, France and Latvia.

*Bestmixer.io* is one of the three largest mixing services for cryptocurrencies and offered services for mixing the cryptocurrencies bitcoins, bitcoin cash and litecoins. The service started in May 2018 and achieved a turnover of at least USD 200 million (approx. 25 000 bitcoins) in a year's time and guaranteed that the customers would remain anonymous.

The operation against *Bestmixer.io* is a significant and important step in the fight against criminal flows of money in general and virtual criminal flows of money in particular.

# What sectors are vulnerable to money laundering?

**Banks and credit unions**

**Remittance businesses (money transfer)**

**Casinos and other poker machine venues**

**TAB and Bookmakers**

**Stockbrokers and financial planners**

**Firms who deal in travellers cheques, money orders and stored value cards**

**Foreign exchange houses**

**Gold and silver bullion dealers**

**Cash Carriers**

# Recent and Emerging Trends in Money Laundering

- The number one focus for many countries is sanctions, especially for geo-political or conflict issues
- There is a renewed focus (in Australia) on casinos as ML 'tools'
- Decentralised Finance (DeFi) – virtual assets-based ML, Non-fungible tokens (NFTs), gaming and Metaverse.
- Cryptocurrency and the use of mixers are an important issue. This is a service that is provided to further anonymise transactions in cryptocurrency.
- Social Media has enabled the rapid sharing of information on how to take advantage of tax systems
- Use of Electronic Sales Suppression Tools (ESST)
- Daigou remains a point of interest as a way of moving illicit funds offshore
- Trade based money laundering is increasing in importance as there is more awareness of the issue
- As with everything in this space, the old classics of money remitters (informal value transfer systems such as Hawala banking), cash smuggling, co-mingling (with legitimate funds) etc are still prevalent
- There is increasing awareness of tax crime as a predicate offence for money laundering, as part of FATF Recommendation 3

# BREAK

# Professional Enablers

## Who are enablers, and how can they help Money Laundering activities?

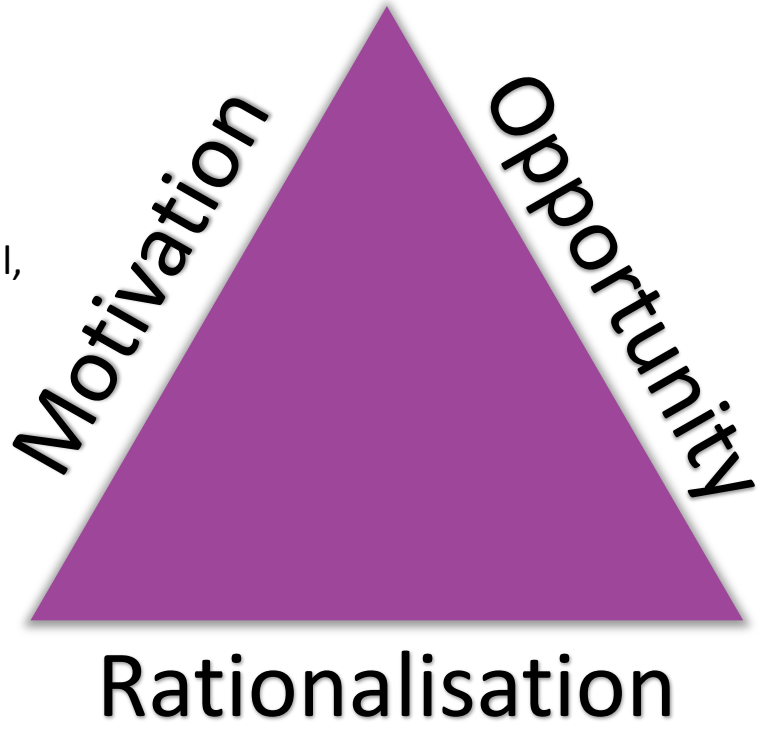
# Financial Crime Roles

**Behind every serious financial crime is a group of people who play different roles. These range from hardcore criminals who might be connected to international crime syndicates through to professional enablers who use their skills to steal information, set up fraudulent companies, hide money and leave victims in their wake. The 'personas' below have been developed to describe the kinds of criminals that are typically involved, and how to spot them based on their behaviours and what to do if you notice suspicious behaviour.**

# Why do people commit fraud?

## The Fraud Triangle

**Pressure/Motive:**
- The driver: financial, emotional, medical




**Opportunity:**
- Knowledge of a vulnerability
- Ability to commit the fraud

**Rationalisation:**
- The justification for committing fraud
- Convincing environmental factors

# The Hardcore Criminal

**Work by the SFCT reveals that most serious financial crime schemes are overseen by a 'controlling mind' who is the key instigator and beneficiary of the financial crime. Often, these individuals are members of or linked to organised (international) crime syndicates or groups.**

**Behaviours:**
• Hardcore criminals (blithely, deliberately and consistently) offend whenever opportunities arise.
• Organised criminals often use loosely connected networks that can quickly react to shifting market conditions.
• An individual can climb the ranks in their organisation rapidly. Success can be short lived, although some grow through the ranks to develop long criminal "careers".
• Often uses violence and coercion.
• Works with professional 'enablers' to conduct and conceal their crimes.
• Compartmentalise facets of their operations so no individual below them has full oversight.

**Warning signs**:
• Makes large payments in cash.
• Aggressive or intimidating behaviour.
• Uses blackmail to coerce others to conceal their financial crimes.


**Trends**:
• Proceeds of serious financial crime may be used to fund other crimes that cause considerable harms to the community – such as drug and human trafficking, sexual exploitation and terrorism.

# The Lieutenant

**The Lieutenant is the person on the ground who works for the Hardcore Criminal to source and manage the different resources and enablers they need. They will typically not be aware of the full extent of the crimes that 'their employer' is involved in. They will only know about their piece of the puzzle.**

**Behaviour:**

• Their role might include sourcing and/or managing: cash, accounts, dodgy businesses, co-conspirators, stolen data or IDs, straw directors, professional enablers and other labour.

**Warnings signs:**

• Provides limited details to recruits as to why their services are required.
• Offers to pay for services in cash.
• Heavy gambling.
• Offers to take professionals (e.g. enablers) out for lavish lunches.
• Engages professional services with the lure of large fees.
• Uses encrypted communication devices.

**Trends:**

• Increasingly uses technology and the dark web to conduct their crimes.

# The Launderer

**The Launderer sets up companies and money flow structures that make illegally gained proceeds (dirty money) appear legal (clean).**

**Behaviours:**

- Often takes money offshore and hides it to avoid paying tax.
- Uses nominee or straw directors.
- Conceals the source of money received.
- Inflates deductions they aren't entitled to or didn't accrue.
- Works with professional 'enablers' to conduct and conceal their crimes.


**Warning signs:**

- Purchases extravagant properties (often in the names of family members).
- A lavish lifestyle that doesn't seem to align with their income.
- Makes large payments in cash.
- Offers to take professionals (e.g. enablers) out for lavish lunches.
- Engages professional services with the lure of large future fees.

**Trends:**

- On the whole, organised criminals are involved in money laundering and funds obtained are used for other serious crimes such as drug and human trafficking, sexual exploitation and terrorism.
- Products and services known to be at risk of being exploited by money launderers include remittance services, gambling/wagering accounts, superannuation accounts, digital currency exchanges and banking products.

# The Straw Director

**This is a director of a company/companies destined to be liquidated within a short period of time, or a shell company that has been set up with the intention of avoiding tax and other liabilities.**
In some cases straw directors are not complicit in serious financial crimes, instead they are best described as ‘victims’. One tactic criminals use is to pay vulnerable people such as people with mental illness, backpackers or people who are in desperate need of money to list them on company documents as directors. In some cases criminals use people’s names without them even knowing.

**The behaviours and warning signs below are most relevant to ‘complicit’ straw directors.**
**Behaviours:**
- Distorts or ‘hides’ revenue for the purposes of avoiding paying tax.
- Fails to pay creditors, employees or subcontractors, or underpays them.
- May be coerced or bribed by a ‘lieutenant’.
- Helps to launder money.


**Warning signs:**
- A ‘serial’ director who is associated with more than one company that has become insolvent.
- Employees, suppliers and contractors are paid late, short-changed or not paid at all.

**Trends:**
- Sometimes these straw directors end up becoming expendable ‘fall guys’ for organised criminals. They are lured into playing what is presented as a signatory role, but then they are identified, bankrupted and prosecuted.
- They may not be aware of the full extent of the crimes they are involved in, only their piece of the puzzle.

# The Phoenix Operator

**The Phoenix Operator deliberately winds up or abandons a company (typically within a year) leaving its debts behind and no one to chase. Victims can include employees, investors and contractors.**

**Behaviours:**
- Starts another company up immediately to take over where the 'failed' company left off.
- Assets or employees are shifted to the controllers or to a new entity that begins trading, often under a similar name.
- Pays bribes to encourage people to turn a blind eye and keep quiet.

**Warnings signs:**
- Often flees the country.
- Labour exploitation: for example, provides third party assurance that work was completed when it wasn't, and in some cases by people who do not exist.
- Underpays workers and 'skims' monies received.
- Fails to pay subcontractors.
- The same individual is involved in several business 'failures'.

**Trends:**
- The property and construction industries have been targeted by phoenix operators.
- Other 'at risk' industries include food services, transport, agriculture and payroll services.

# The Enabler

**Enablers are professionals who use their skills, structures and networks to help facilitate serious financial crime. As enablers require advanced professional skills, as well as a network that facilitates interaction with other criminals, many enablers of serious financial crime may be older or more advanced in their careers.**

Like many businesses, professional intermediaries may also be targeted by criminals with an interest in the personal and/or commercially sensitive information they have access to.

**Behaviours:** Professional enablers advise criminals on how to structure their affairs and help facilitate financial crimes. This includes how best to store, launder and remit illicitly obtained funds, and how to structure local and offshore entities to hold and move assets while hiding their ownership and value. Behaviours will depend on the role they play in enabling the serious financial crime.
For example:

- A lawyer who sets up companies and tax structures to defeat tax obligations.
- An accountant who runs two sets of books / provides illegal advice to clients to help them evade tax.
- A liquidator who is in cahoots with a 'phoenix operator' and repeatedly liquidates dodgy companies.
- A banker who facilitates offshore payments or payments of false invoices.
- An immigration agent who provides false or underpaid labour.
- A service provider who:

generates false invoices | provides third party assurance that work was completed when it wasn't, and in som


ot exist | underpays workers and 'skims' monies received | uses fictitious names.

# Enablers Continued

**Warning signs:**

• Professional enablers can play an influential role in the decision making of criminals, including in the structuring of criminal or tax avoidance schemes and in introducing criminals to other ‘legitimate’ players.
• A lavish lifestyle that doesn’t seem to align with their income.
• Large quantities of cash.
• Businesses or professionals that appear to be ‘compromised’.

**Trends:**

• Organised crime groups operate throughout Australia and frequently engage in businesses or activities that appear to be operating legitimately, but when you peel back the layers of the illicit activities the links to more serious crime figures are exposed.
• Hawala-type informal money transfer systems are being used by organised crime entities to remit illicitly obtained funds offshore in secrecy. People who facilitate informal money transfers often do not appreciate the illegality of these systems in Australia or recognise how these systems are exploited by criminals

# BREAK

# Cyber Criminal

**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.**

**Behaviours:**

• Often uses 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.
• Stolen identities, information and phishing schemes can be used to steal from superannuation and share trading accounts, and purchase goods and services or loans using the victim's funds and ID.
• Other cyber criminals specialise in writing code and coordinating phishing exercises. Meanwhile, others provide hacking services, or 'testing services' that seek to compromise the security and information of government agencies, banks, businesses and other organisations.

**Warning signs:**

• Be aware of what you share – don't click on suspicious links or provide details for requests for personal information.
• Take notice of unusual activity in your accounts and report it straight away.
• Take notice of unusual emails such as password changes or verification links – delete suspicious emails and confirm your details through your own account.

**Trends:**

• Financial crime has evolved, and technology now plays a significant role.
• Some sectors known to be at risk of exploitation by data thieves include tax agents/accountants, real estate, migration services, employment services and HR/payroll.
• The impacts are long term – people may see the impacts for years afterwards if their identity is stolen.
• Cryptocurrencies can be used to launder money and transfer money overseas or back to Australia. In some cases this includes avoiding tax and laundering money by trading across currencies or in ways that make ownership anonymous.

# The Tax Fraud

**The Tax Fraud intentionally avoids paying tax in Australia.**

**Behaviours:**
• Is often an opportunist who take advantage of situations as they arise, works with professional 'enablers' to conduct and conceal their crimes and tries to bluff their way around the system.
• Intermediaries (such as tax and investor advisors) can play an influential role in their decision making, but this is one input into a broader decision making process.
• Provides false or misleading statements, for example:
- mischaracterises the true nature of transactions | understates income | inflates or claims deductions to which they aren't entitled | fails to maintain or intentionally destroys financial records | fails to lodge income tax returns or business activity statements (BAS) | withholds information from tax professionals or the ATO.

**Warning signs:**
• Keeps two sets of books or financial statements.
• Accepts large payments in cash, or doesn't declare income received in cash.
• Ignores legal advice or guidance from the ATO.
• Seems to live above their means or to have had a sudden increase in wealth (boats, cars, homes, jewellery, holidays).

**Trends:**
• This group typically has higher income and are often self-employed, company owners/directors or senior executives. They may use a tax professional/ intermediary to prepare tax returns and are more likely to be in a position to consider tax minimisation strategies.
• Research shows that some may consider evading their taxes as a result of financial or relationship difficulties (e.g. a separation or divorce).

# Other Roles

**The Responsible Citizen**
**Keeps an eye out for the warning signs of serious financial crime (such as a sudden increase in wealth – boats, cars, homes, jewellery, holidays) in relation to someone they know.**

**Behaviours:**
• Reports suspicious behaviour.

**The Victims**
• Direct victims of serious financial crime include:
- people who have their lifesavings targeted or their identities stolen by cyber criminals.
- businesses not paid for the goods or services they provided to a company they thought was legitimate.
- employers, where an employee has used their place of work to facilitate their crimes.
• All Australians are victims of serious financial crimes because they reduce the money available for essential community services, such as health and education, by millions of dollars every year.

# Warning Signs of Serious Financial Crime

## In a business and financial context

- ❑ Use of nominees or straw directors
- ❑ Keeping two sets of books or financial statements
- ❑ Understating income
- ❑ Failing to lodge income tax returns or business activity statements (BAS)
- ❑ Mischaracterising the true nature of transactions
- ❑ Inflating or claiming deductions to which they aren't entitled
- ❑ Withholding information from a tax professional or the ATO
- ❑ Ignoring legal advice or guidance from the ATO

## Personal and Purchasing behaviour

- ❑ Concealing money or the source of money
- ❑ Unexplained wealth or wealth not commensurate with income
- ❑ Suddenly spending more, such as on luxury items or collectibles (e.g. cars, boats and jewellery)
- ❑ Using fake names
- ❑ Providing false or misleading statements
- ❑ Making large purchases with cash
- ❑ Large cash withdrawals from ATMs
- ❑ Heavy gambling
- ❑ Aggressive or out of character behaviour may be a sign of stress related to financial crime

## Cybercrime and identity theft

- ❑ Unsolicited or suspicious requests for your personal information
- ❑ Unusual emails such as password changes or verification links (delete suspicious emails and
- ❑ confirm your details through your own account)
- ❑ Suspicious links or downloadable files in emails, text messages or social media posts from
- ❑ sources that don’t appear to be genuine (do not click or download)
- ❑ Unusual activity in your accounts (report it straight away)

# QUIZ

# QUESTIONS?

# Close of Day One

**Thank you!**

**Tomorrow we will provide an opportunity to answer any questions you've thought of overnight.**

**See you tomorrow.**

# Day 2

# Money Laundering Case Studies

# Overview

## Recap of Day One

## Money Laundering Typologies and Case Studies

## Breakout session

- How would you launder one million dollars?
- What types of Money Laundering do you see?

# Recap from Day One

## Money Laundering Overview

## Professional Enablers:

# 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

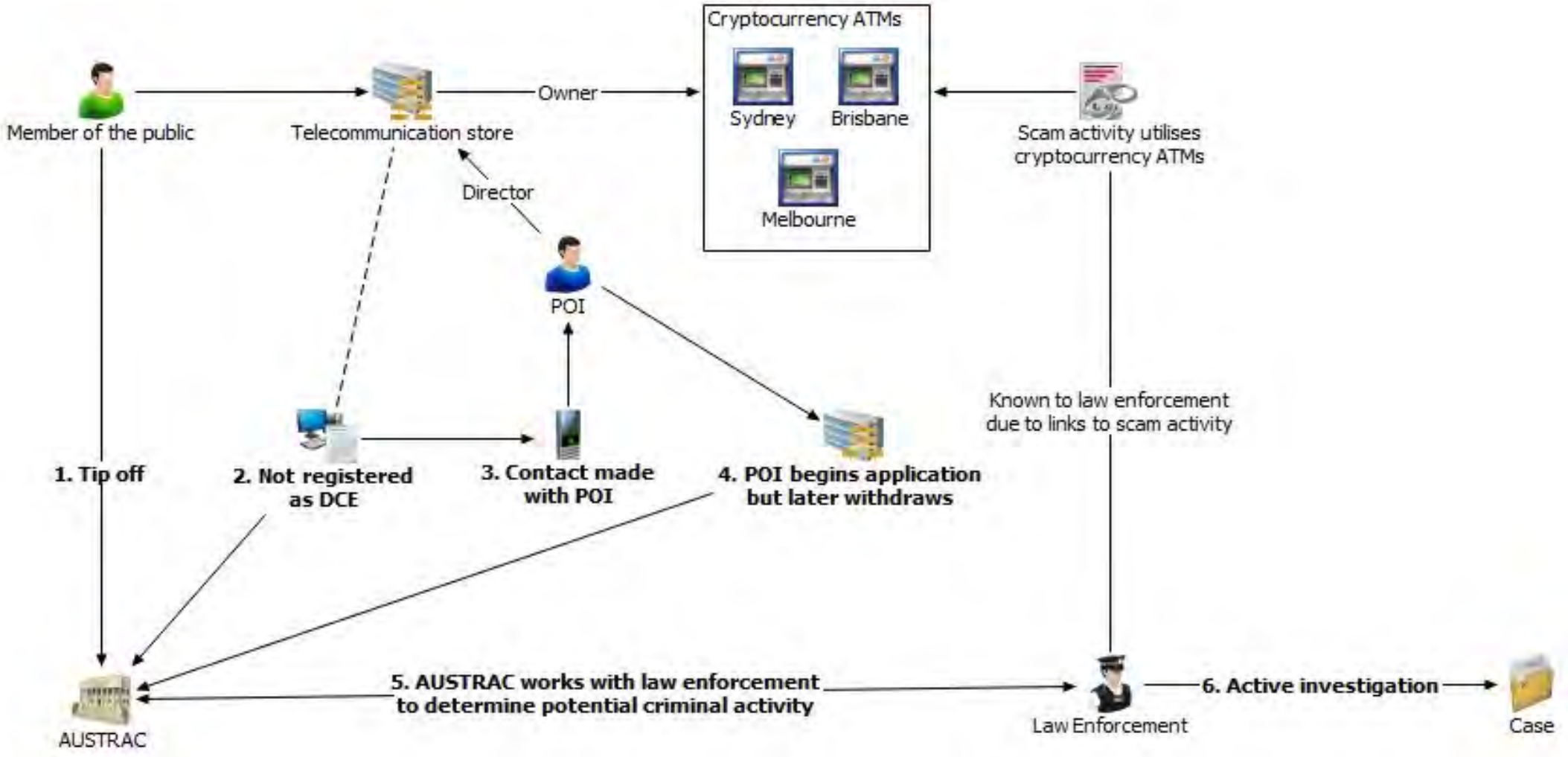
# Money Laundering Using Digital Currency: Layering

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.

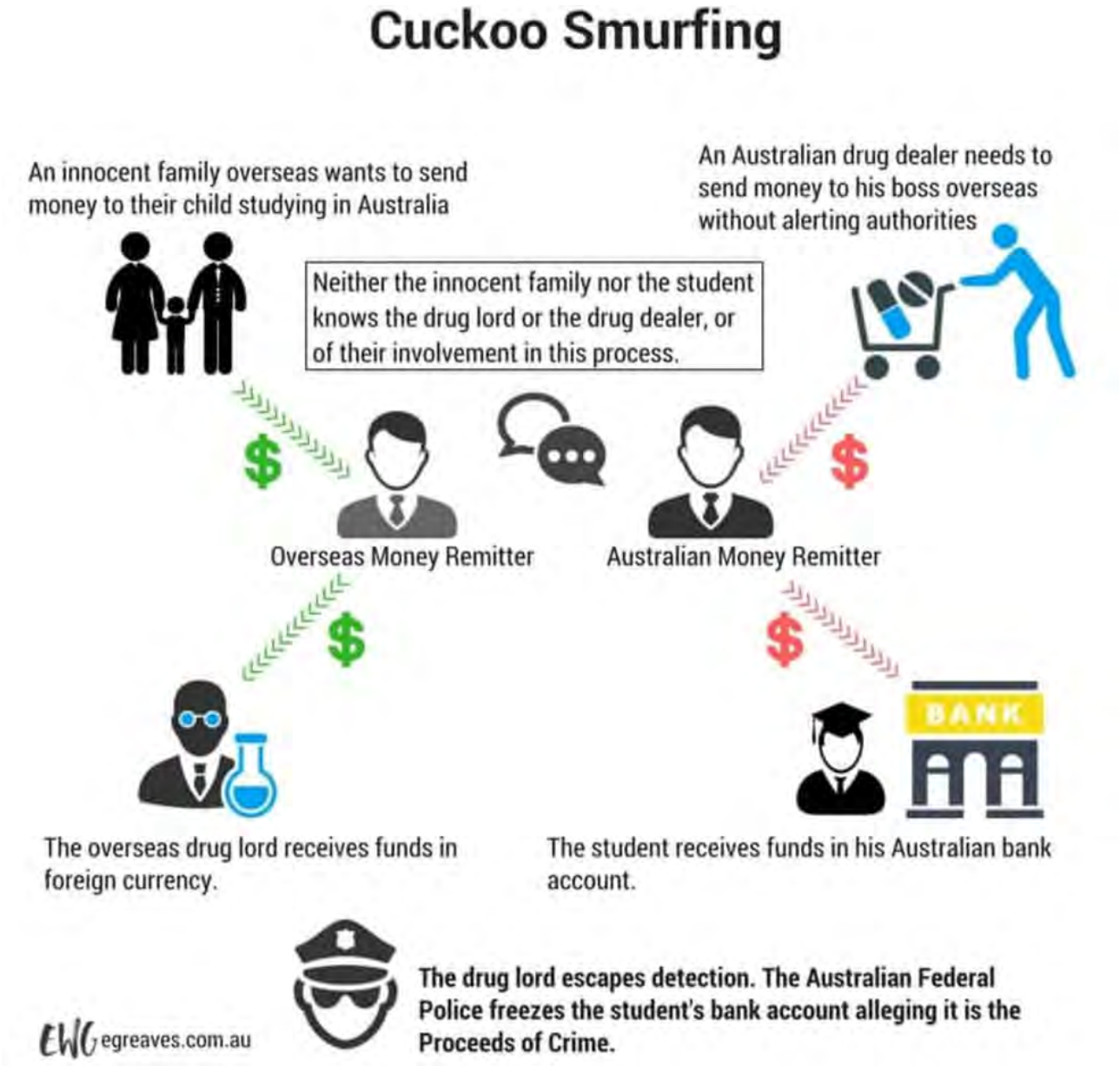
# Case Study: Unregulated Crypto ATMs



# Cuckoo Smurfing

A distinct breed of money laundering

Cuckoo smurfing differs from other money laundering typologies involving structuring and smurfing due to the use of a party not aware of the criminal process involving funds arriving into their account.



# Daigous

Cambridge Dictionary definition: “someone who is outside China who buys goods for someone who lives in China”

Example of Money Laundering incorporating Daigous:

1. An overseas organised crime syndicate sells their drugs through a third party in Australia.

2.The Australian distributer needs to get the profit back overseas to the syndicate without scrutiny.

3. To do this they use a ML organisation (can be on or offshore), where they will have the cash collected and cleaned on their behalf, for a commission.

4. The Australian distributor will hand over the cash to the collector working for the ML company.

5.The ML company will use their large reserves of cash to provide funds to the offshore syndicate, while their collector in Australia starts turning the illicit funds into legitimate goods or cash. This is where Daigous come in, translated as “surrogate shopper”.

6. The collector engages with the daigous who hire other community members to buy things such as large amounts of baby formula, pharmacy items, designer goods etc.

7. They hand over the goods to the collector who then ships them overseas to be resold with the profits going back into the ML company.

# Example: Alleged industrial-scale daigou operation

The Australian Federal Police dismantled an alleged industrial-scale daigou operation where, on a daily basis, cash hidden in boxes labelled baby formula would arrive at a commercial warehouse, the cash would be deposited at ATMs and the money would be used to purchase actual baby formula to be sold for a high price in China.


The organiser in China would monitor the cash counting live through CCTV cameras stationed in the office of the warehouse.

The controller in Sydney would allegedly open each box and count the cash with the CCTV camera positioned over his shoulder.

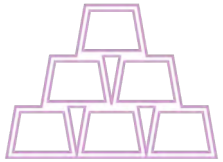
The AFP executed a search warrant in April 2022 at the warehouse and seized about $300,000 cash. Investigators suspect the money laundering organisation moved about $14.5 million in a one year period.

# Trade Based Money Laundering

- The process of disguising the proceeds of crime and moving value through the use of trade transactions, in an attempt to legitimise illicitly obtained funds.
- Any commodity can be used, however common commodities used in TBML include gold/precious metals, precious stones/jewellery, scrap metals, vehicles and small high value items such as electronics.

Attraction of trade for laundering:

- Networks, logistics and facilitators already in place.
- Limited capacity/resources for border agencies to detect illicit trade transactions.
- Few trade data exchange/sharing programs
- Scope to co-mingle illicit trade with legitimate business.
- Volume of trade.



# TBML Methodologies

**Over and under invoicing of goods and services**
Invoicing at a price that is a misrepresentation of a good or services value for the financial benefit of the exporter or importer.

**Over and under shipment of goods and services**
Manipulation of the quantity of what is being shipped or what services are being provided.

**Falsely described goods or services**
Misrepresenting the type or quality of a product.

**Multiple Invoices**
The goods and services will be valued correctly but there will be multiple payments made through various financial institutions all relating to the same purchase.

# TBML Red Flags

- The payment for goods is in excess of known market value.
- The payment for goods is below known market value.
- Discrepancies on shipping documents.
- Products do not correspond with line of business.
- Shipment is purchased by firms or individuals from foreign countries other than the country of the stated end-user.
- Difficult to determine the ultimate consignee of the commodity.
- Shipping route does not make economic sense.
- International fund transfers inconsistent with the business.
- Shipment going to/from a known or suspected transhipment country.
- No obvious use for commodity.
- Shipping weight inconsistent with commodity type and quantity.

# Strategies to address TBML

- Strengthen bilateral arrangements with foreign jurisdictions.
- Construct multilateral mechanisms for international cooperation and joint operations.
- Increase public-private collaboration.

# Targeting and Detection

**Data Analytics**
Examining import data with an automated technique such as Unit Price Analysis.

**Statistical Analysis**
Use of linear regression models on trade data concerning individual, non-aggregated imports and exports.

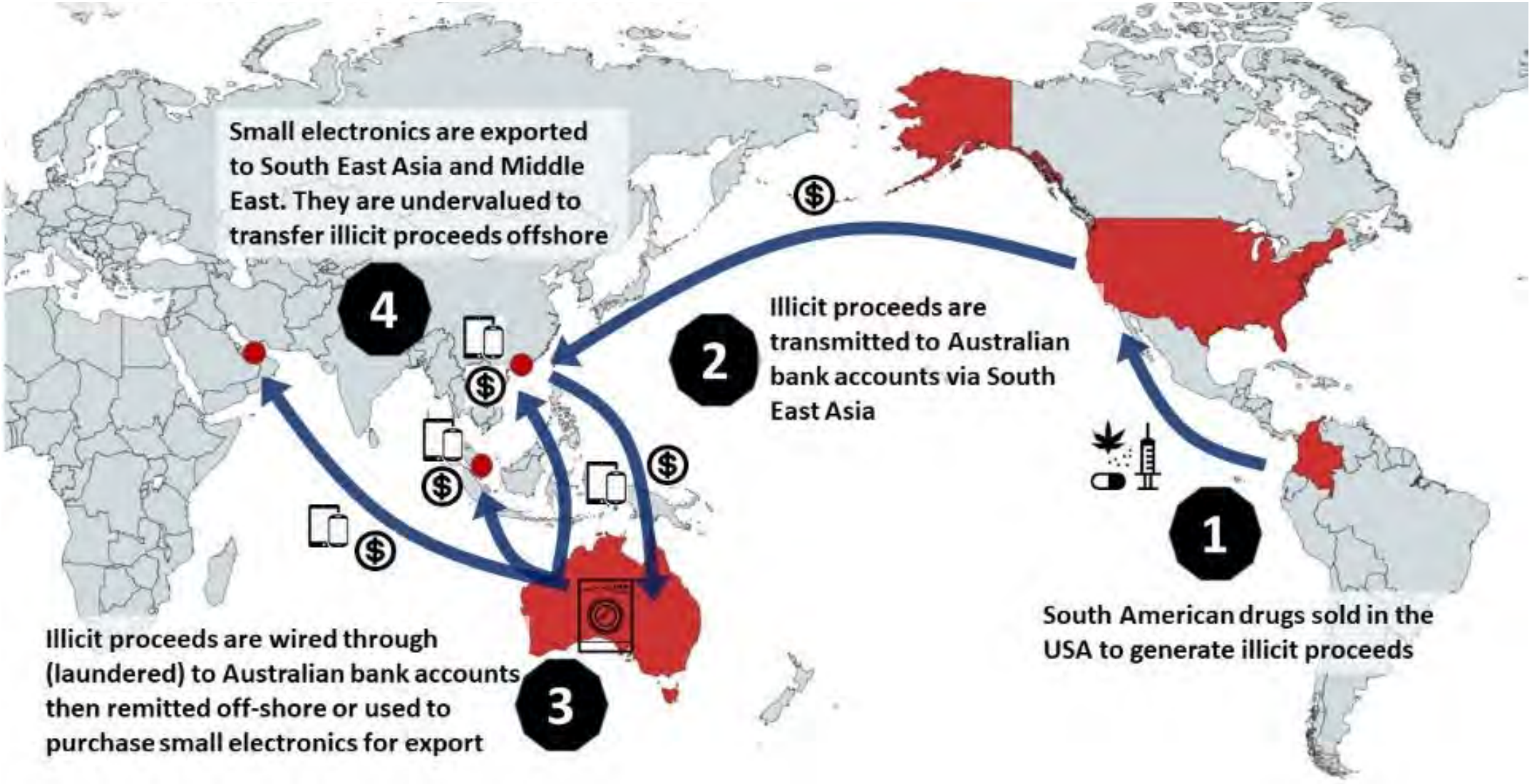
**Trend Analysis**
Comparing information such as origin, description, value route of shipment to detect irregularities.

**Typology Analysis**
Cross-comparing known typologies of risk with trade data, cross-border financial movements and intelligence.

**Trade Transparency**
Compare cargo movements between two countries to verify the data reported to each authority.

# BREAK

# Example – Trade based money laundering: Mobile Phones



# Example –Trade based money laundering: Gold

TBML under the guise of wholesale gold bullion trading.

**Placement** – The fraud actor made regular cash deposits, never going over the $10,000 reportable limit into their business account.

**Layering** – They then transferred money overseas via remitters to purchase gold.

**Integration** – The fraud actor then used the gold bullion it had imported into Australia to commercially trade, making the funds legitimate and completing the money laundering cycle.

# Breakout Session

## What types of Money Laundering do you see?

You will be divided into groups and assigned an element to discuss on ML.

Someone will need to be a spokesperson.

Please have one person in your group make notes.

You will have 10 Minutes to discuss with your group

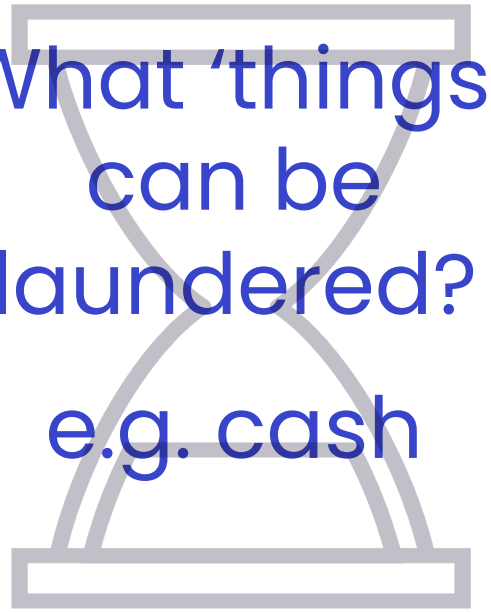
When we return we will be populating a virtual whiteboard and looking at each groups answers.

# Break out – group discussion

## Group One

What ‘things’ can be laundered?

e.g. cash



## Group Two

Why do people launder these ‘things?’

## Group Three

What ways can you launder these ‘things?’

## Group Four

Who helps or assists in laundering these ‘things?’

# What types of Money Laundering did you see?

# Examples of Money Laundering linked to Tax Crimes

# Entry level forms of Money Laundering / Tax crime

**Historically, when you thought of entry level money laundering it would be along the lines of:**

- **Small businesses/self employed contractors using their kids bank accounts to deposit cash**
- **Small time criminals “clean” their money through Casino’s or smaller gambling centres.**

The modern day version takes into account how most business now use a digital Point of Sale (POS) systems.

This has resulted internationally in the growing use of Electronic Sales Suppression Tools (ESST).

ESSTs are programs designed to interfere with electronic sales records. They can falsify, manipulate, hide, destroy, or prevent the creation of electronic sales records, often without an audit trail showing the interference. ESSTs can be physical and located on-site, Virtual or Cloud based and accessed through a mobile applications, or offered as a service by a third party.

Example: One small business has a high percentage of the eftpos transactions automatically diverted into third party accounts to avoid tax or sends the money straight to an offshore account. They then use it to buy themselves a new car via direct transfer to the dealer.

# Mid level forms of Money Laundering / Tax Crime

**Multiple small businesses all using ESST's.**

Example: A chain of convenience stores, all owned by the same person, use ESST's to inflate their activities and trades to add in more cash money trails and integrate money they are making from the sale of illegal tobacco under the counter into "legitimate" business takings.

They pay tax and GST however may also claim inflated deductions to minimise. They are using this interaction with the tax office to legitimises their money, through falsification of documents and false declarations.

Staff working for the convenience store have no idea as this is occurring as the owner does this outside of business hours.

The Accountant he uses also has no idea he has falsified his incomings and outgoings.

# High level forms of Money Laundering / Tax Crime

Enablers set up businesses with ESST built in, offer a service of ESST or teach businesses how to instal, use and avoid detection of ESSTs.

Serious Organised Crime Groups (SOCG) could make (or bribe) legitimate businesses to instal a ESSTs. Mainly in high cash areas such as restaurants, cafes, markets etc. to integrate their criminally obtained money into inflated takings, and then inflate expenses to offset. Using the tax system to “clean” and legitimise their money.

SOCG will also set up their own ML syndicates to conceal the illicit funds sources from activities such as trafficking, cyber crime, fraud offences and other financial crime. Any legitimate income the businesses make from being set up is not the priority, just an added bonus.

Some ESST’s can send money from deleted EFTPOS transactions to offshore to tax havens and then return the funds via payment platforms making those funds now “clean”.

When a person launders money, by definition, they are dealing in money that is reasonably believed to be the proceeds of crime.

# Common Defences for Money Laundering

Defences commonly encountered:

Gambling

Inheritance

Gifts or loans from friends

Savings or cash hoard

Sale of an asset

Any others?

# BREAK

# Breakout Session

## Let's Play!

## How would you launder 1 million dollars?

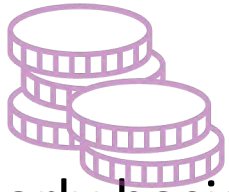
Your syndicate is an organised crime group based in South East Asia. Your group, amongst other activities, is involved in importing prefabricated concrete panels used in the construction of commercial buildings such as warehouses and large-scale accommodation buildings.

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.

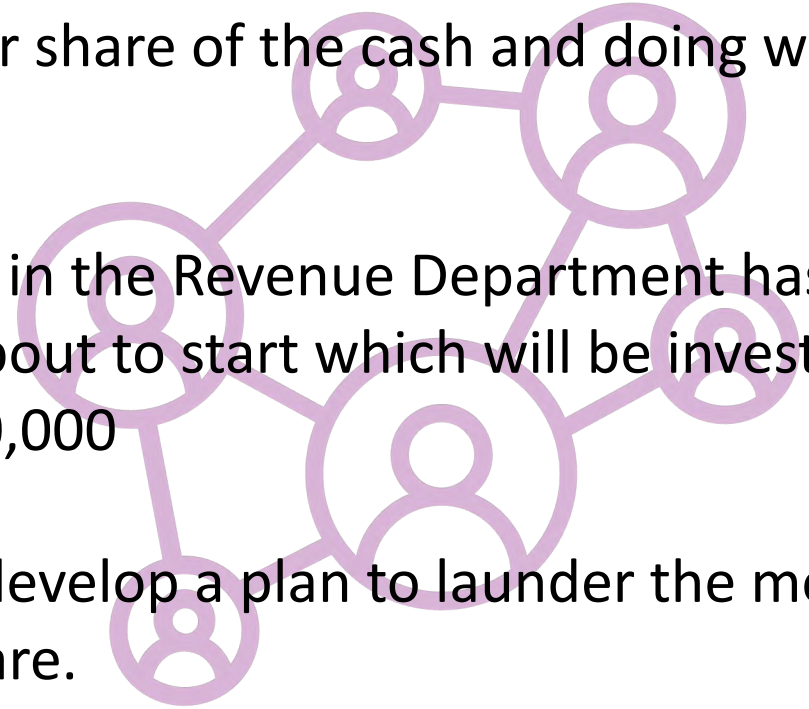
Each month, the construction companies pay the amounts owing into bank accounts operated by Dragon Panels with a Commercial Bank.

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 Tasks

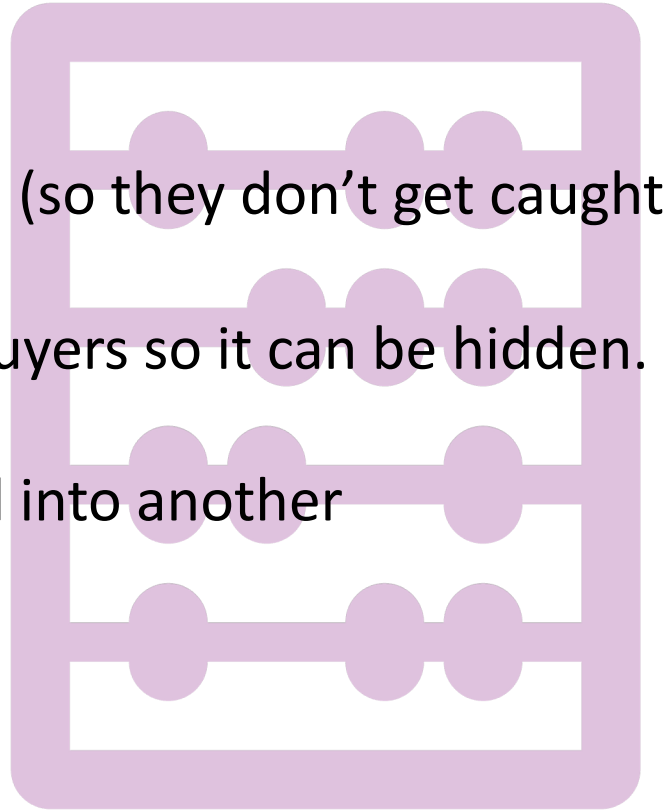
Your syndicate is to design a money laundering plan that addresses the following issues:

**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).

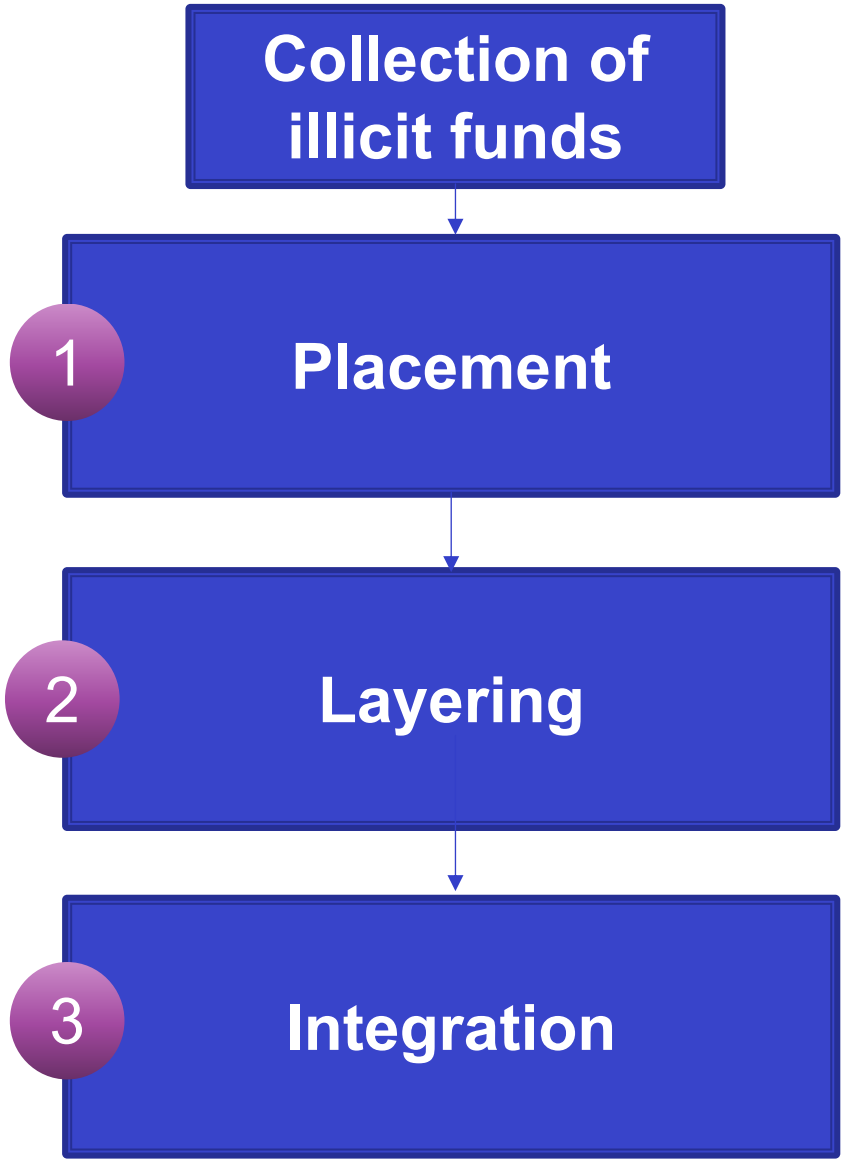
**Group 3**. Setting up new ways to receive money from buyers so it can be hidden.

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

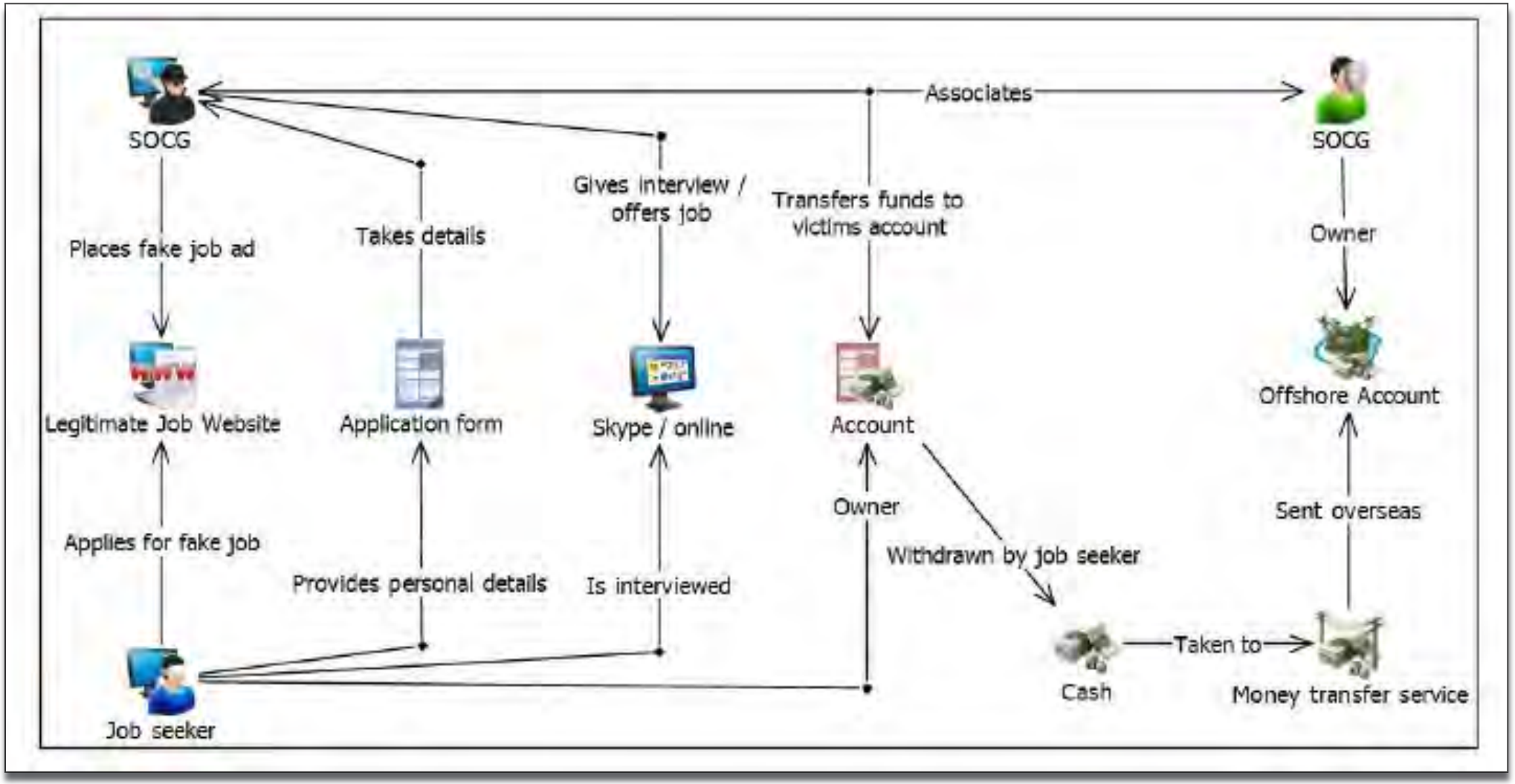


In relation to your plan, don't just mention what you would do but **explain how each money laundering typology would operate**.

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



# Job Scam Money Mules



# Black Market Peso Exchange

# Music Streaming

Studies indicate that up to 3% of music streams could be fraudulent in nature, manipulated to result in the payout of laundered funds.

How?

- Illicitly obtained funds are converted into Bitcoin
- This digital asset is used to pay for fake streams for artists that are linked to criminal networks.
- Those “artists” are then paid out by the streaming service.
- The illegal funds are now clean.

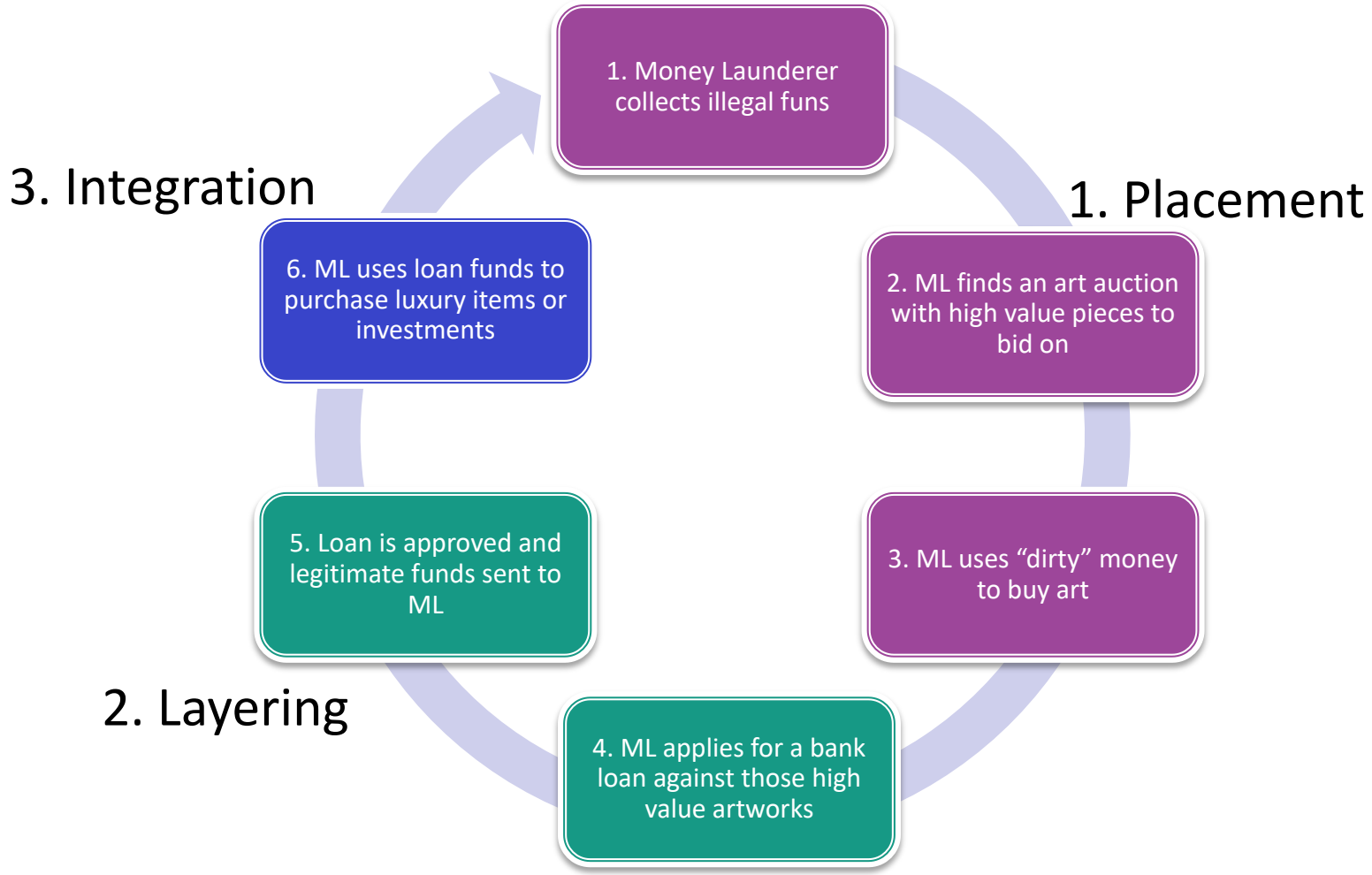
# Social Media

Social platforms such as TikTok and Twitch offer the option to donate to users while they share content.

How?

- Fraud actors gain access to stolen credit card details
- Those details are then used to buy the currency of the platform, for TikTok this is “Coins”
- Those content creators are then paid donations while sharing content
- The Coins can be redeemed for dollars
- The content creator then keeps a percentage and sends the remainder on the original fraud actor.

# The Art Market



# Case Study – Operation Beaufighter

## 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

**$68M**
actually received

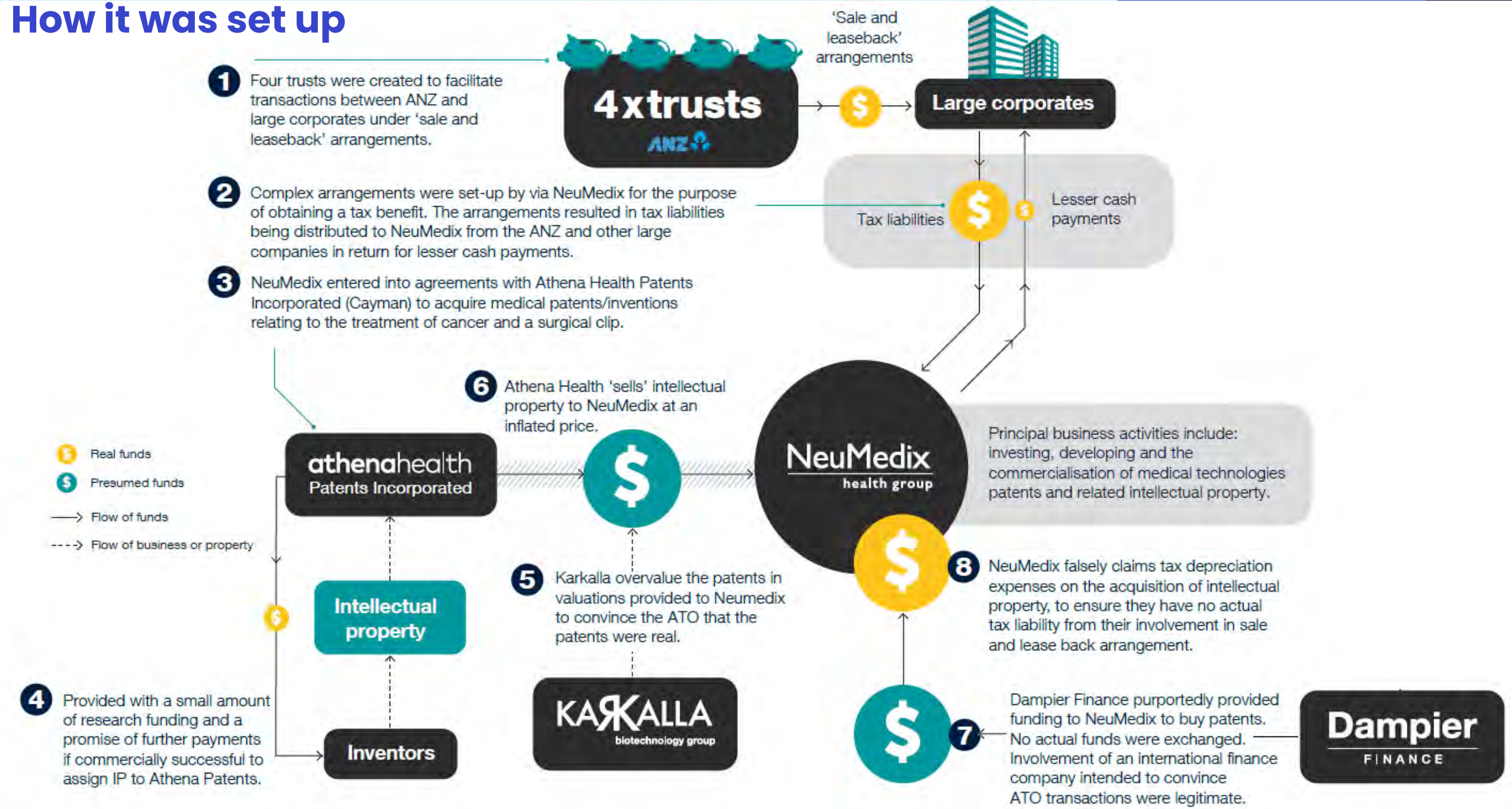
## The loss

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



# Company Information

athenahealth Patents Incorporated

Nominee Directors & shareholders.

Incorporated Cayman Islands

KARKALLA biotechnology group

Nominee Directors & shareholders.

Incorporated in Hong Kong

NeuMedix health group

Controlled by DICKSON and ISSAKIDIS

Incorporated in Australia

Dampier FINANCE

Controlled by DICKSON and ISSAKIDIS.

Incorporated in Samoa.

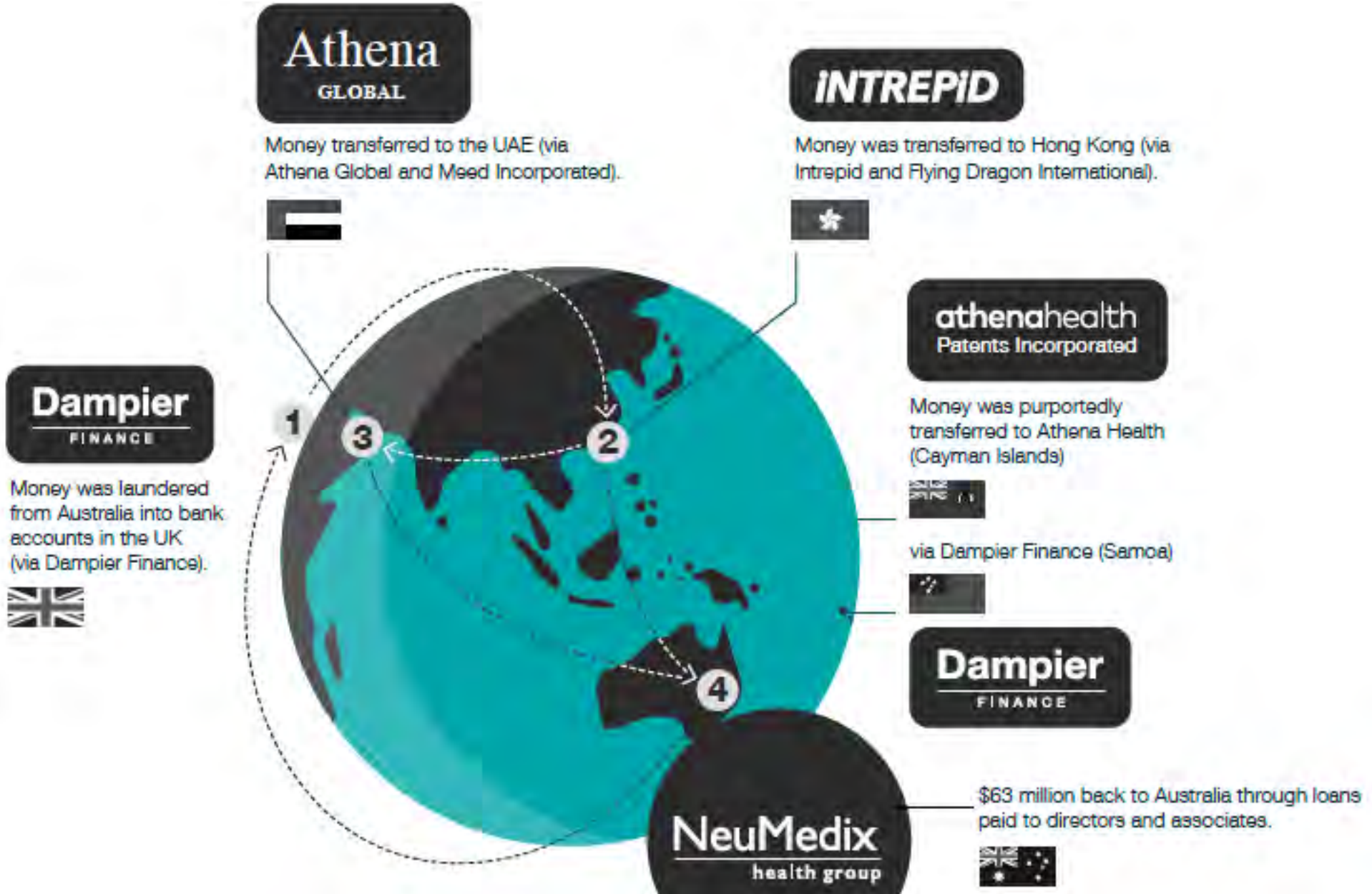
Over 3 years the tax obligations of the partnership totalled $387,000,000

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

# Where the funds moved



# Execution of Warrants

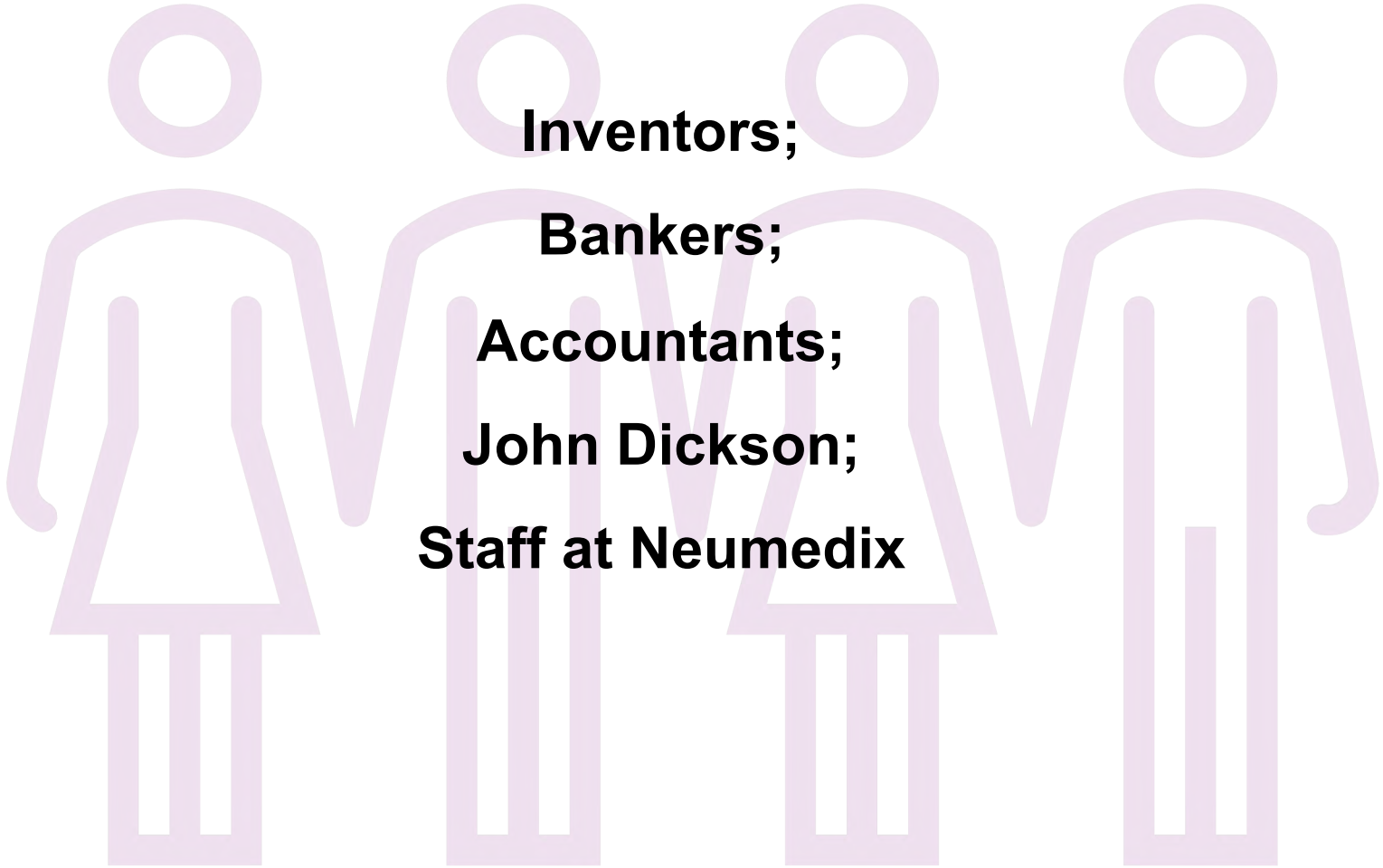
Multiple search warrants in multiple cities;
X-Agency teams

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)


FEDERAL POLICE
SOLD

# Witnesses



**Inventors;**

**Bankers;**

**Accountants;**

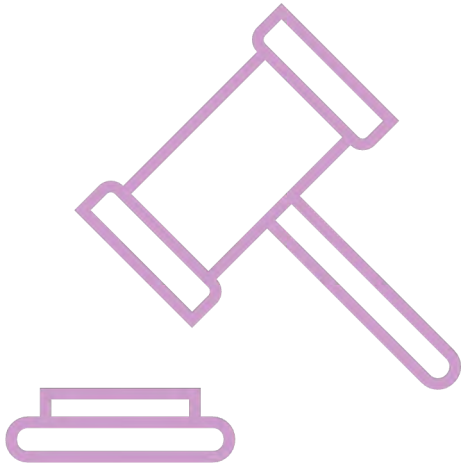
**John Dickson;**

**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.



# QUIZ

# QUESTIONS?

# Close of Day Two

**Thank you!**

**I hope you learned some new or interesting information about Money Laundering.**

**See you tomorrow.**

# Day 3

**Guest Presentation from AUSTRAC**

**Money Laundering**

**Interagency Cooperation**

**Questions**

# Interagency Cooperation

- Federal Agencies
- State Agencies
- Public and Private partnerships
- Taskforces and working groups
    - Serious Financial Crime Taskforce

# Real Estate

Method 1 – Use of third parties

Method 2 – Use of loans and mortgages

Method 3 – Manipulation of property values

Method 4 – Structuring of cash deposits to buy real estate

Method 5 – Rental income to legitimise illicit funds

Method 6 – Purchase of real estate to facilitate other criminal activity

Method 7 – Renovations and improvements to property

Method 8 – Use of front companies, shell companies, trust and company structures

Method 9 – Use of professional facilitators or 'gatekeepers'

Method 10 – Overseas-based criminals investing in Australian real estate

# QUESTIONS?

# 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)

2022 INTERPOL Global Crime Trend Summary Report https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

FATF – Interpol - Egmont Group (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, FATF, Paris, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illlicit-financial-flows-cyber-enabled-fraud.html

# Close of Day Three

## Thank you!