Complex Money Laundering and the Role of Tax Investigators

Australian Government
Australian Taxation Office

Delivered by Carla Grist and Mark Robinson

On Behalf of the ATO for the OECD Asia-Pacific Academy for Tax and Financial Crime Investigation - 23 May to 1 June 2022

With a supporting session on day two from Austrac representative Sam Lamour

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.

Introductions

- We are….
- You are….
- Timings
- Learning outcomes
- Expectations

Introductions and Admin

We have about 50 - 60 minutes per session, but **please be flexible** if discussions are flowing.

Breaks may occur sooner or later depending on topic and conversation. Please try to be back on time.

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

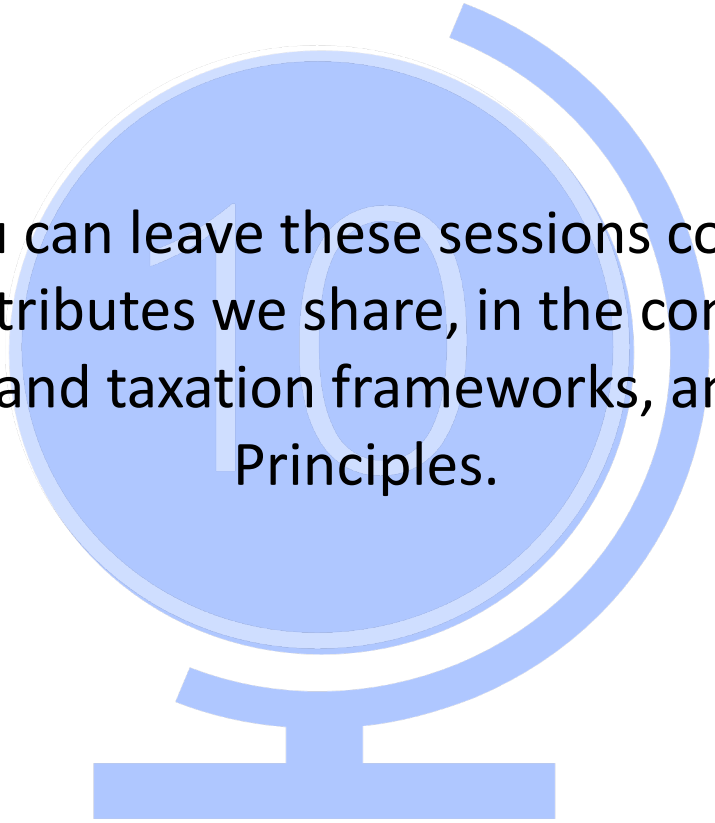
Break out rooms – we will ask you to move into break out rooms to discuss and work together on a topic or question.

The sessions are to bring awareness/knowledge around:

- Types of money laundering (ML)
- Means of ML
- Tax crimes and ML
- Tips and tricks to identify ML methods and actors
- New and emerging risks in ML
- The value of strong cross agency collaboration

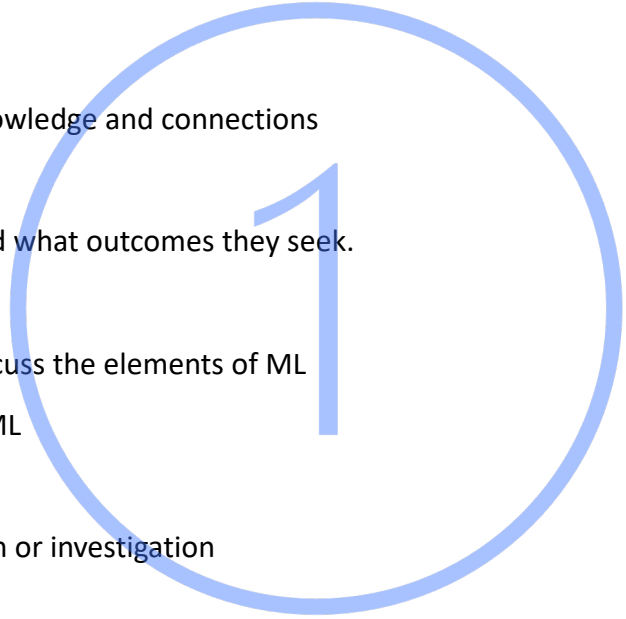
Tuesday	Wednesday
24-May-22	25-May-22
Starting Time 13:00 pm (Tokyo Time GMT+9)	
Participant Presentation (13:00 - 13:30)	Participant Presentation (13:00 - 13:30)
Fighting Tax Crime:The 10 Global Principles What is Money Laundering? *Breakout session	Austrac
Virtual Break	
Entry/mid/high level examples. Enablers	Money laundering legal framework - Practical Exercise ("Catch me if you can") 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	

We hope you can leave these sessions considering the common attributes we share, in the context of your countries legal and taxation frameworks, and the 10 Global Principles.



Day One

- Participant Presentation
    - A selected case study or insight from a participant is shared to build knowledge and connections
- Fighting Tax Crime – The ten Global Tax Principles
    - We unpack the key principles for collaboration, what they consist of and what outcomes they seek.
- What is Money Laundering?
    - Participants split into groups and go to a virtual ‘Break out’ room to discuss the elements of ML
- Entry, Middle and High Level Types of ML and Types of enablers who support ML
- Emerging Threats
    - new and emerging risks/methods to circumvent ML, tax crime detection or investigation
- Role of tax investigations in detecting and combatting ML
- Case studies of ML
    - Unpacking methods used by various enablers and investigation strategies



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

- A selected case study or insight from a participant is shared to build knowledge and connections

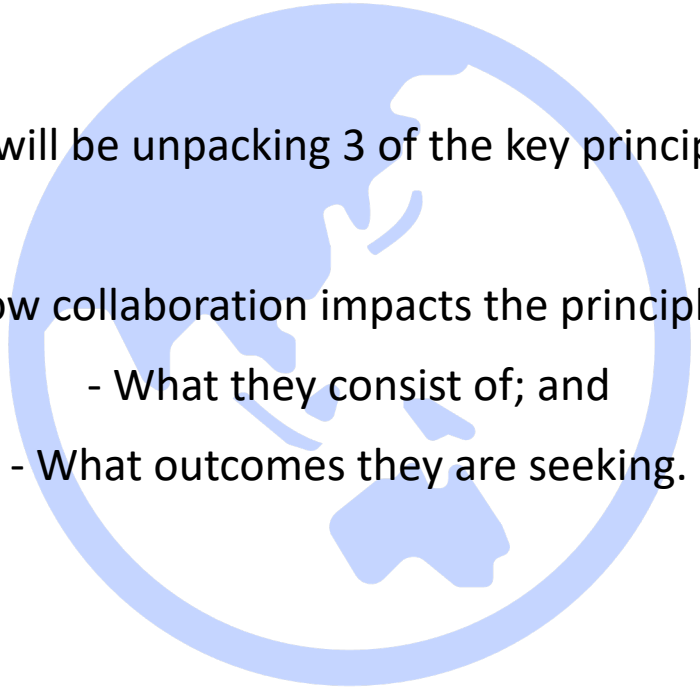
- Case Study - how tax crime fits in to predicate offences to money laundering.

- Case Study - future focus

Participant Presentation

We are very pleased to hear from…

The Ten Global Principles



We will be unpacking 3 of the key principles.

-How collaboration impacts the principles;

- What they consist of; and

- What outcomes they are seeking.

Fighting Tax Crime: The 10 Global Principles

1	Ensure tax offences are criminalised	Jurisdictions should have the legal framework in place to ensure that violations of tax law are included as a criminal offence, and that effective sanctions apply in practice.
2	Devise an effective strategy for addressing tax crimes	In order to ensure the effectiveness of the law on tax crimes, jurisdictions should have a strategy for addressing tax crimes. The strategy should be regularly reviewed and monitored.
3	Have adequate investigative powers	Jurisdictions must have appropriate investigative powers to successfully investigate tax crimes.
4	Have effective powers to freeze, seize and confiscate assets	Jurisdictions should have the ability to freeze / seize assets in the course of a tax crime investigation, and the ability to confiscate assets.
5	Put in place an organisational structure with defined responsibilities	A Jurisdiction should have an organisational model with defined responsibilities for fighting tax crime and other financial crime.
6	Provide adequate resources for tax crime investigation	Tax crime investigation agencies should have adequate resources.
7	Make tax crimes a predicate offence for money laundering	Jurisdictions should designate tax crimes as one of the predicate offences for money laundering.
8	Have an effective framework for domestic inter-agency co-operation	Jurisdictions should have an effective legal and administrative framework to facilitate collaboration between tax authorities and other domestic law enforcement and intelligence agencies.
9	Ensure international co-operation mechanisms are available	Tax crime investigation agencies must have access to criminal legal instruments and an adequate operational framework for effective international co-operation in the investigation and prosecution of tax crimes.
10	Protect suspects' rights	Taxpayers suspected or accused of committing a tax crime must be able to rely on basic procedural and fundamental rights.

Principle 7. Make tax crimes a predicate offence for money laundering

Jurisdictions should designate tax crimes as one of the predicate offences for money laundering.

A predicate offence is a crime that is a component of a more serious crime. In regards to money laundering, predicate offences may give rise to funds or assets that may then be laundered to obscure the illegal source.

Ways for jurisdictions to designate tax crimes as predicate offences for money laundering:

- Use an **inclusive approach** and identify all criminal offences as predicate offences;
- Use a **threshold approach** and designate as a predicate offence all offences meeting a certain threshold, such as being punishable by one year imprisonment or more, or offences designated in a category of “serious offences;” or
- Use a **list approach** and create an explicit list of offences that are predicate offences.

The FATF Recommendations provide that: “…Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences”

Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog.

Principle 8. Have an effective framework for domestic inter-agency co-operation

Jurisdictions should have an effective legal and administrative framework to facilitate collaboration between tax authorities and other domestic law enforcement and intelligence agencies.

Combating financial crimes comprises a number of key stages, including the prevention, detection, investigation and prosecution of offences, as well as the recovery of the proceeds of crime. Depending upon the circumstances, this can involve a number of government agencies, including the tax administration, the customs administration, financial regulators, AML authorities including the FIU, the police and specialised law enforcement agencies, anti-corruption authorities and the public prosecutor's office.

Models of information sharing:

Generally, there are four different types of co-operation with respect to sharing information among different agencies:

- direct access to information contained in agency records or databases.
- an obligation to provide information automatically (i.e. at regular intervals) or spontaneously (i.e. on the occasions when relevant information is identified)
- an ability, but not an obligation, to provide information spontaneously; and
- an obligation or ability to provide information in response to a specific request

Other forms of co-operation

Example: Australia's Serious Financial Crime Taskforce

The Serious Financial Crime Taskforce (SFCT), led by the Australian Taxation Office, is a joint-agency taskforce established on 1 July 2015. It brings together the knowledge, resources and experience of relevant law enforcement and regulatory agencies to identify and address the most serious and complex forms of financial crime. As such the SFCT is the primary mechanism utilised by the ATO to respond to serious financial crime. It also supports Australia's involvement as a member the Joint Chiefs of Global Tax Enforcement (J5).

The SFCT's goal is to target serious financial crimes of the highest priority, with a specific focus on 4 key areas:
- Cybercrime (technology-enabled crime) affecting the tax and superannuation systems
- Offshore tax evasion
- Illegal phoenix activity
- Serious financial crime affecting the ATO-administered measures of the Commonwealth Coronavirus Economic Response Package.

Australian Government Serious Financial Crime Taskforce | AFP Australian Federal Police | Australian Criminal Intelligence Commission | Australian Border Force | ASIC | Australian Government Australian Taxation Office | Australian Government Attorney-General's Department | Australian Government AUSTRAC | CDPP

The above icons are hyperlinked if you would like to take a closer look at any of the agencies

Principle 9. Ensure international co-operation mechanisms are available

Tax crime investigation agencies must have access to criminal legal instruments and an adequate operational framework for effective international co-operation in the investigation and prosecution of tax crimes.

Tax crimes very frequently have an international dimension, for instance because a foreign jurisdiction was used to hide assets or income, or because the proceeds from illicit transactions are kept abroad, without being declared to tax authorities. Since criminal activity can cross international borders while investigation agencies have powers which are limited by jurisdictional boundaries, co-operation amongst investigation agencies is extremely important.

Principle 9. (Continued)

Ensure international co-operation mechanisms are available

In seeking a successful holistic approach to fighting tax crime, it is important that jurisdictions have a far-reaching and functioning international co-operation network. This network should be characterised by the following features:

- be in place with a wide geographical coverage of other jurisdictions;
- cover a wide range of types of assistance, including exchange of information and other forms of assistance in investigation and enforcement; (OECD, 2012[1])
- be supported by a domestic legal framework that allows the sharing of information both sent and received under international legal instruments with all relevant domestic criminal investigation, intelligence and enforcement agencies, where appropriate (i.e. tax authorities, criminal investigation authorities, FIUs, AML authorities); and
- be given effect in practice, including having a clear operational framework for international co-operation. This should include having dedicated and identified contact points that foreign agencies can contact in case of a request for assistance, sufficient resources to fulfil requests for assistance, as well as training and awareness for domestic investigation agencies as to the availability of international co-operation and how to make effective requests.

ATO Tax Audits or Investigation

Civil vs Criminal Law Treatment

Tax Audit	Investigation
Gather information	Gather evidence
Use Notice Powers to obtain documents	Use search warrant or voluntary requests to obtain documents
Use Notice Powers to interview taxpayers	No compulsory powers
Balance of probabilities Onus on Taxpayer	Criminal standard Onus on Prosecution
Prepare documentation for stakeholders	Prepare documentation for court (via CDPP)
Focus on transaction	Focus on person / persons.

Examples of measures that can be taken to enhance compliance:

Tax fraud (serious organised crime)	Combatting and preventing fraud	Anti-fraud measures	•Tax investigation and audits •Prosecution and penalties •Elimination from legal financial circles •Cooperation with the judicial system/police
Tax evasion (shadow economy, income underreporting, illegal employment)	Controls and sanctions		•Controls, investigations •Tax audits (risk analysis) •Prosecution and penalties •Tax collection
Tax avoidance (aggressive tax planning, avoidance models)	Monitoring and cooperation		•Risk management •Office and field staff controls •Official first visits •Tax collection
Tax compliance (voluntary disclosure, fulfilment of tax obligations)	Support and simplification		•Information and forms •Cooperation with interest groups •Horizontal monitoring •Advance rulings

Money Laundering

Discussions and group work.

What is it?

Why does it happen?

What can be ‘laundered’?

What types of Money Laundering do you see?

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 do you see?

What did we learn?

Three stages of money laundering

Collection of illicit funds

1 **Placement**

2 **Layering**

3 **Integration**

Dirty Money Integrates into the financial System

Transfer funds between various Offshore / Onshore Banks

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.

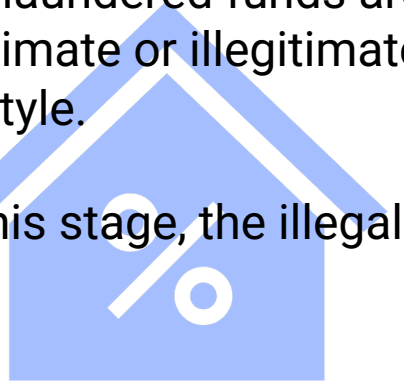
$ Funds may be shuttled through a web of many accounts, companies and countries in order to disguise their origins.

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.



How much money is laundered?

- According to the UNODC, money laundered globally is estimated at 2-5% of global GDP, or US$800 billion to US$2 trillion annually.
- Less than 1% of global illicit financial flows are currently seized by authorities.
- An estimated AU$200 billion is laundered in the Asia-Pacific region.

What sectors are vulnerable?

- 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

Money Laundering Organisations (MLOs)

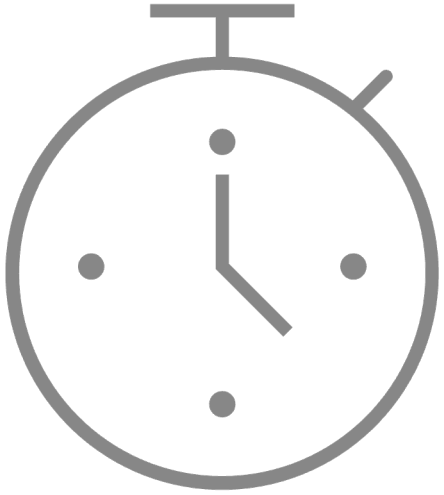
Key methodologies

- Money mules/third-party cash deposits
- Cuckoo smurfing
- Onshore and offshore company structures
- Trade-based money laundering (TBML)
- Emerging: Daigou Activity

Cuckoo smurfing: a distinct breed of money laundering

The term 'cuckoo smurfing' originated in Europe because of similarities between this typology and the activities of the cuckoo bird. Cuckoos lay their eggs in the nests of other species of birds, which then unknowingly take care of the eggs believing them to be their own. 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.

BREAK



Examples of Money Laundering linked to Tax Crimes

Entry level forms of Money Laundering / Tax crime

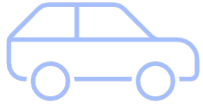
Historically, when you thought of entry level money laundering it would be along the lines of:
- **Small businesses/self employed contractors using their kids bank accounts to deposit cash**
- **Small time criminals "clean" their money through Casino's or smaller gambling centres.**

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

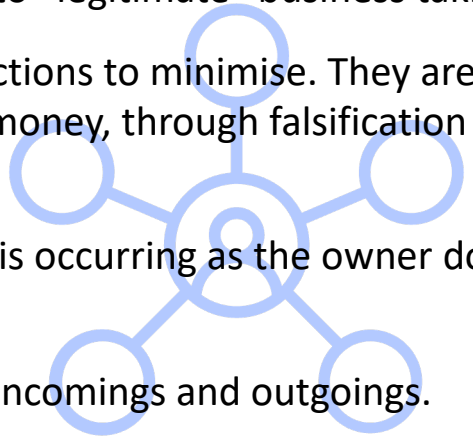
Multiple small businesses all using ESST's.

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.



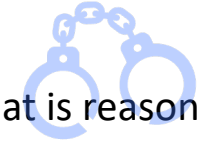
High level forms of Money Laundering / Tax Crime

Enablers could 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.

Enablers

Who are enablers, and how can they help ML activities?

Here we will look at some typologies, including Enablers

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 dodgy companies, hide money and rip people off. 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.

Serious Financial Crime Taskforce Identikit

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

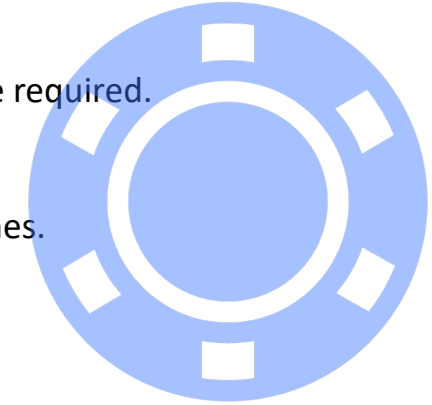
The Lieutenant is the person on the ground who works for the Hardcore Criminal to source and manage the different resources and enablers they need. They will typically not be aware of the full extent of the crimes that 'their employer' is involved in. They will only know about their piece of the puzzle.

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.



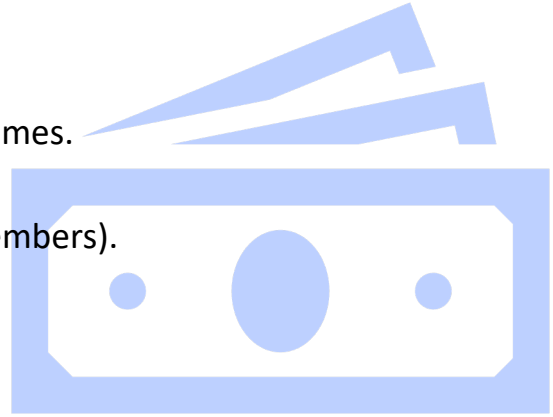
Trends:

• 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.

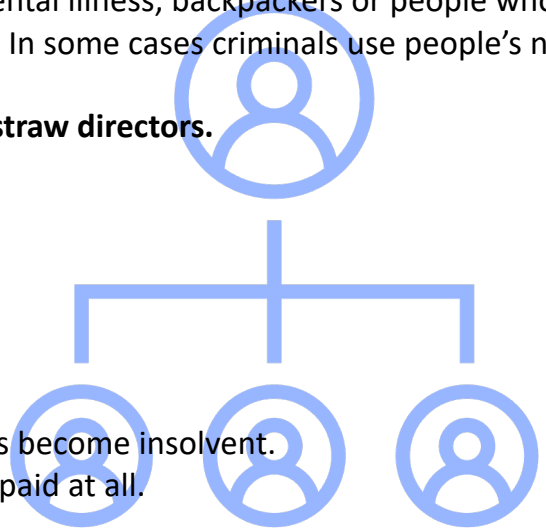
Trends:
- On the whole, organised criminals are involved in money laundering and funds obtained are used for other serious crimes such as drug and human trafficking, sexual exploitation and terrorism.
- Products and services known to be at risk of being exploited by money launderers include remittance 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 some cases by people who do not 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

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.

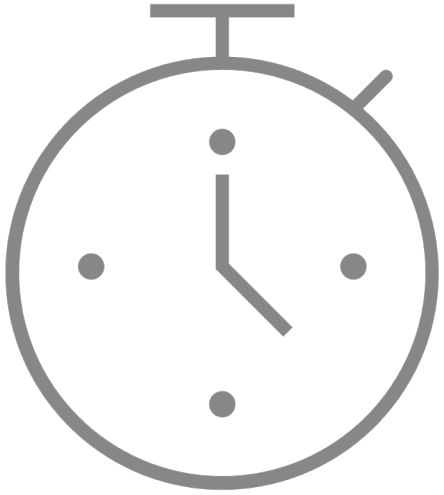
• Research shows that some may consider evading their taxes as a result of financial or relationship difficulties (e.g. a separation or divorce).

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.

BREAK



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

Trade Based Money Laundering

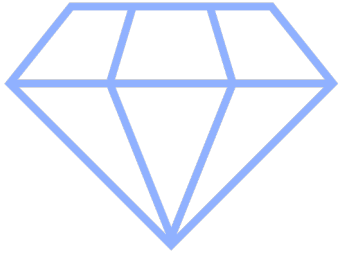
- The process of disguising the proceeds of crime and moving value through the use of trade transactions, in an attempt to legitimise illicitly obtained funds.
- Any commodity can be used, however common commodities used in TBML include gold/precious metals, precious stones/jewellery, scrap metals, vehicles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

- False Invoicing
- Double Invoicing
- Over & Under-Valuation
- Over & Under-Shipment



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.

Example of successful implementation of tax crime strategy in the Netherlands: Crypto mixers

In 2020, the FIOD and the Public Prosecution Service took one of the largest online mixers for cryptocurrencies offline, named *Bestmixer.io*. This operation dealt a severe blow to the concealment of criminal flows of money by mixing cryptocurrencies. Six operational servers have been dismantled and seized in the Netherlands and Luxembourg. The investigation was conducted in close co-operation with the Dutch Digital Intrusion Team (DIGIT), Europol and the authorities in Luxembourg, France and Latvia. In June 2018 the Financial Advanced Cyber Team (FACT) of the 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.

The investigation gathered information regarding transactions between customers and *Bestmixer.io*. The customers are located all over the world. The FIOD and EUROPOL analysed the information together and the data was shared with other countries. On the 'darknet', cryptocurrencies are a regular means of payment and are often used in the criminal world. 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 against payment of a commission, after which they are mixed together in a different combination.

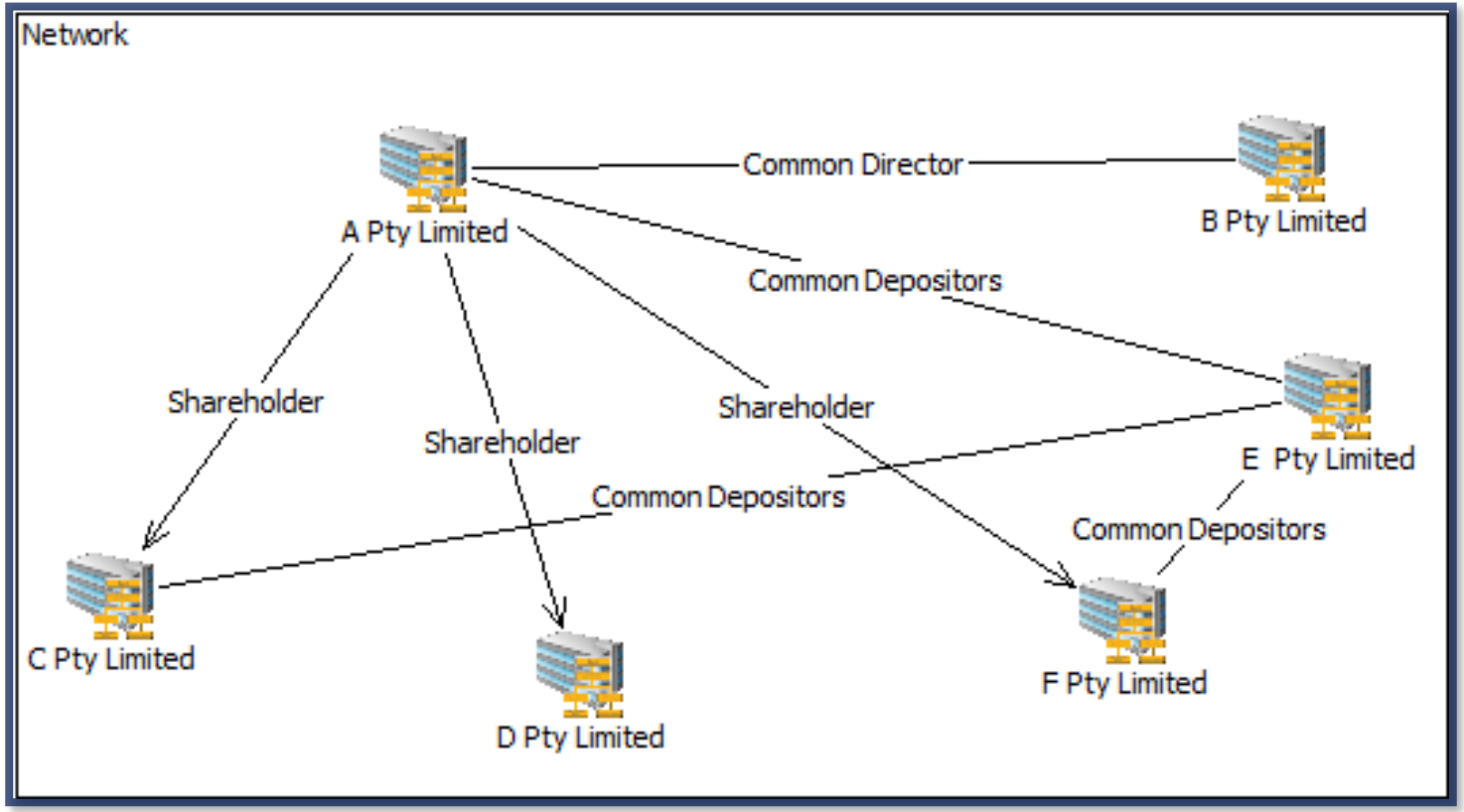
People who use a mixing service probably do so to increase their anonymity. The investigation so far shows that many of the mixed cryptocurrencies have a criminal origin or destination and probably used to conceal and launder criminal flows of money. The total turnover of darknet markets amounts to approx. USD $800 million per year.

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 one year and guaranteed that customers would remain anonymous.

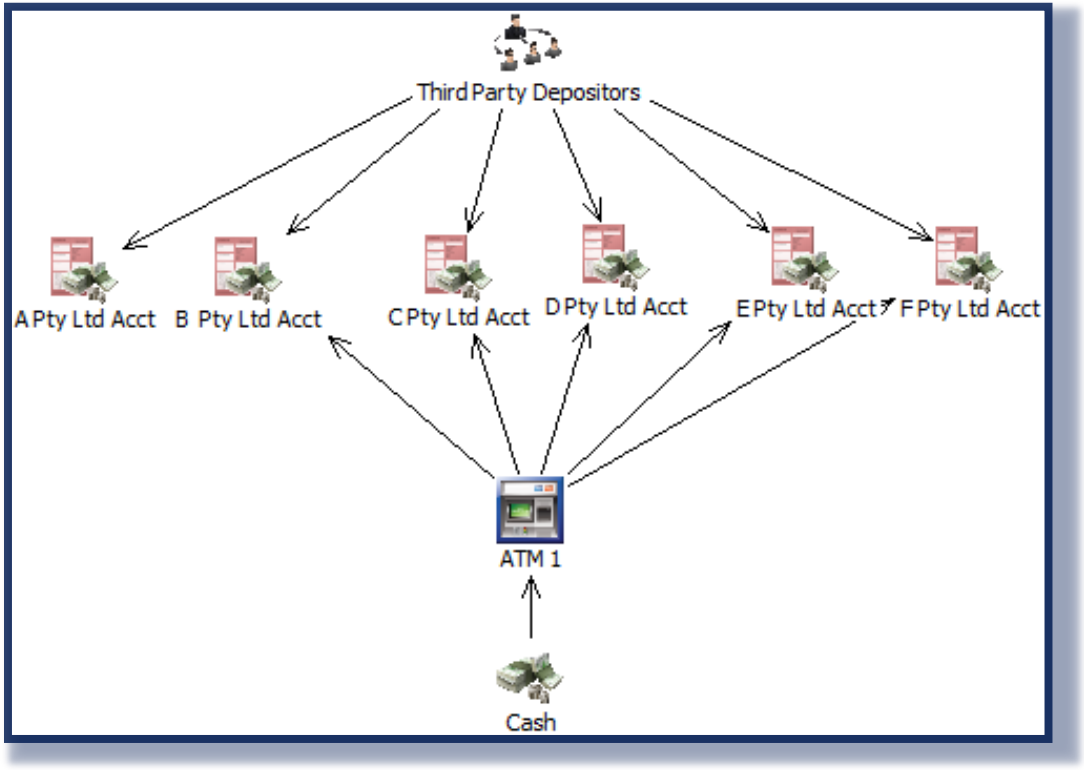
The role of Tax Investigators in the fight against Money Laundering

We **will be looking at two case studies where tax Investigators detected or identified ML typologies.**

Case Study 1: Professional Money Laundering Syndicate

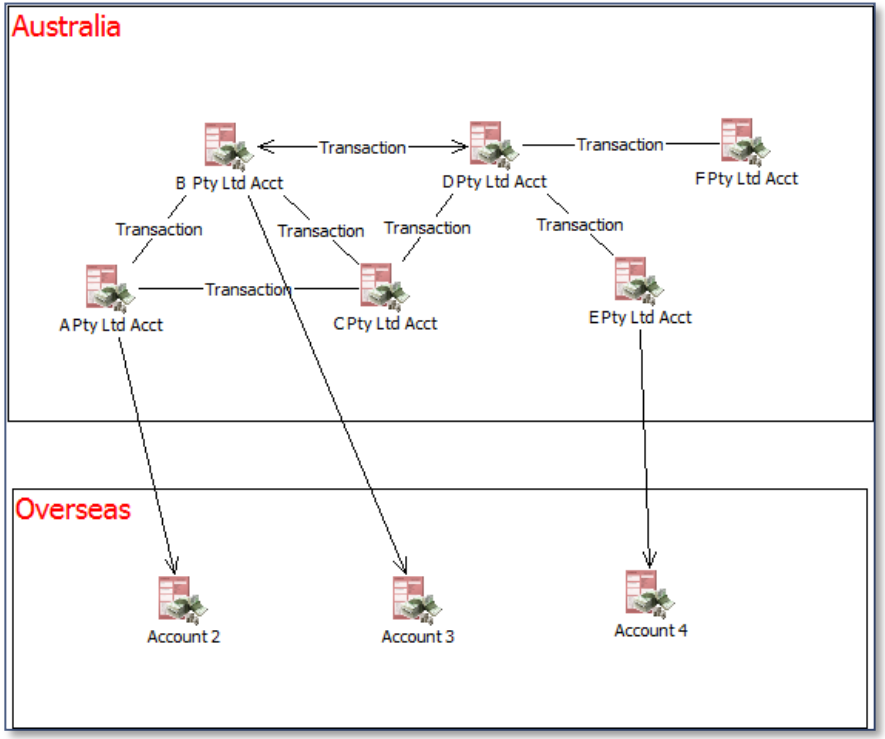


Case Study 1: Professional Money Laundering Syndicate



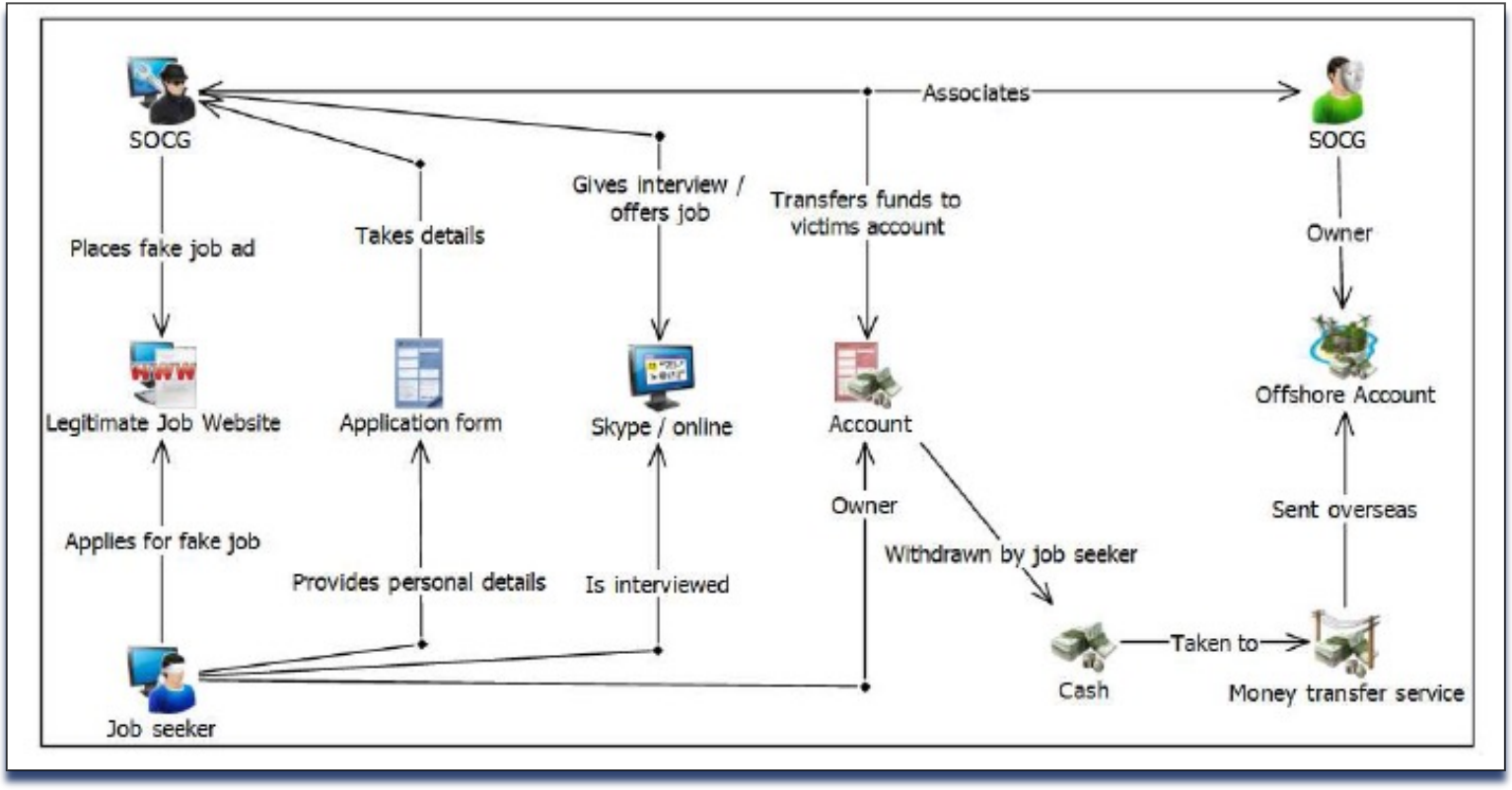
Placement

Case Study 1: Professional Money Laundering Syndicate



Layering

Case Study 2: Job Scam Money Mules



End of Day One

So, what did we learn today?

Kahoot quiz

Please go to Kahoot.it

Kahoot