Serious Financial Crime

Identikit

Australian Government
Serious Financial Crime Taskforce

Help us fight serious financial crime which impacts all Australians.

Serious financial criminals deceive, cheat and steal from everyday Australians. Australia's Serious Financial Crime Taskforce (SFCT) wants your help to make sure these criminals pay.

Serious financial crimes have a serious impact on our community. Direct victims include people who have their lifesavings targeted or their identities stolen by cyber criminals, and small businesses that are not paid for the time, goods and services they provided to a company they thought was legitimate. More broadly, serious financial criminals decrease by many millions of dollars the money available for essential services we all rely on such as health and education.

Meanwhile, funds that are illegally obtained through tax evasion, tax fraud and other offences like money laundering or identity theft are often used to facilitate other crimes such as drug trafficking, for example, that cause significant harm to people and our communities.

Well-resourced and committed to making criminals pay

Led by the ATO, the SFCT is a joint-agency taskforce made up of experts from a range of federal law enforcement and regulatory agencies. Its combined knowledge, resources and experience has made the SFCT a formidable force with a strong track record in preventing, detecting and disrupting the most serious and complex forms of financial crime.

The SFCT also works with governments and organisations around the world to fight tax evasion on a global scale and is part of a globally connected network of investigative experts including the Joint Chiefs of Global Tax Enforcement alliance (the J5). The J5 aims to share intelligence and data in near real time and is focused on shared areas of concern and cross-national tax crime threats including cybercrime and cryptocurrency, and enablers of global tax evasion.

> *"Through our international and domestic partnerships, we are now better equipped than ever before to catch enablers and facilitators of financial crimes. Never before have criminals been at such risk of being detected as they now are. Our message for those who evade or cheat the tax system is that they have no place to hide."*

Will Day, Chief of the Serious Financial Crime Taskforce

Australian Government
Serious Financial Crime Taskforce

1800 060 062 | www.ato.gov.au/SFCT

You can help us stop serious financial criminals

This Serious Financial Crime Identikit has been developed to help Australians better understand how serious financial crime affects the community, the kinds of criminals involved and the warning signs to look out for. The kit features a series of 'personas' to describe the different roles that criminals who are involved in serious financial crime play, how they can be spotted and what to do if you see something suspicious. It also includes a checklist of the main warning signs to look out for as well as tips for protecting yourself from cybercrime.

There are two ways you can help:

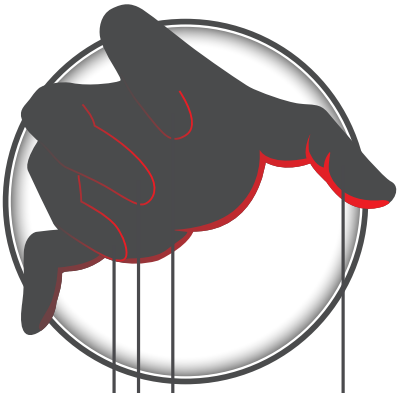
1. Keep an eye out for suspicious activity. If you have a tip-off or any concerns, please call the ATO tip-off hotline on **1800 060 062** or go to **www.ato.gov.au/SFCT** for further information.
2. Share this information with your network and encourage others to keep an eye out for anything suspicious.

The key personas involved

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.

Click on any of the personas below to read more.



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.

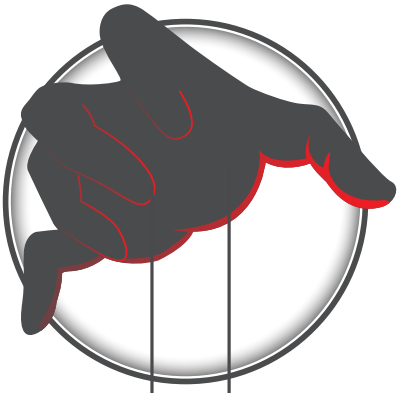
Warning signs:

- 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.

Australian Government
Serious Financial Crime Taskforce



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.

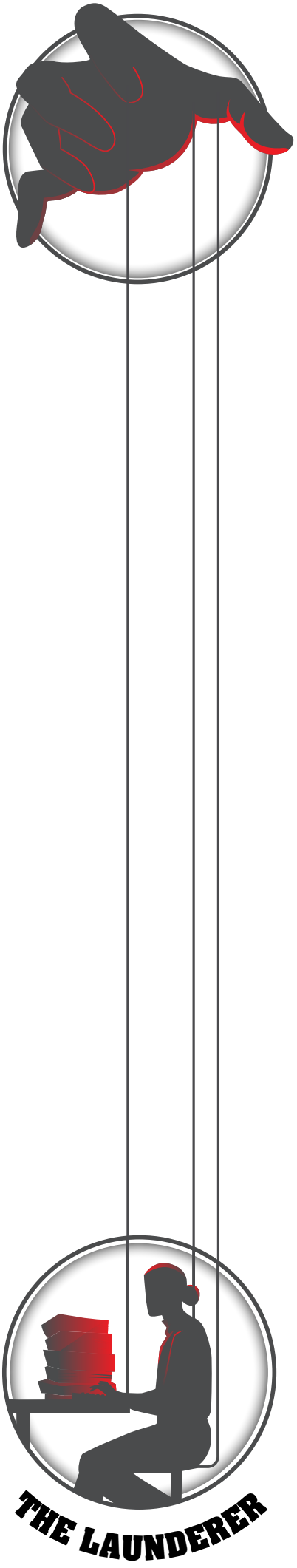
Warnings signs:

- 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.

Australian Government
Serious Financial Crime Taskforce



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:

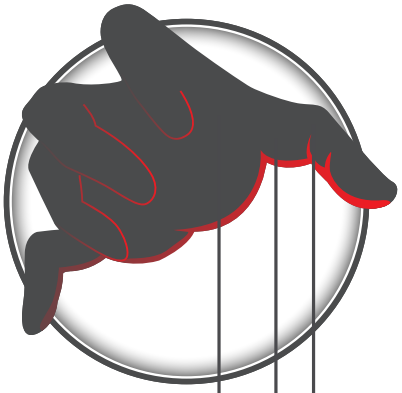
- Purchases extravagant properties (often in the names of family members).
- A lavish lifestyle that doesn't seem to align with their income.
- Makes large payments in cash.
- Offers to take professionals (e.g. enablers) out for lavish lunches.
- Engages professional services with the lure of large future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

Australian Government
Serious Financial Crime Taskforce

The Straw Director



Complicit Victim

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:

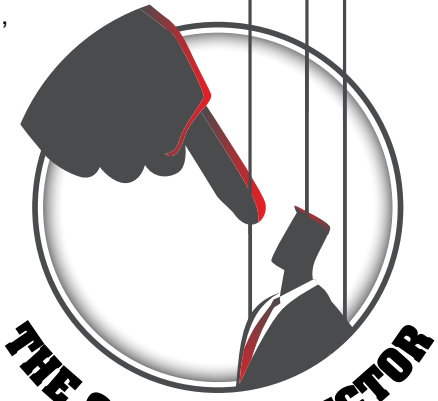
- Distorts or 'hides' revenue for the purposes of avoiding paying tax.
- Fails to pay creditors, employees or subcontractors, or underpays them.
- May be coerced or bribed by a 'lieutenant'.
- Helps to launder money.

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.

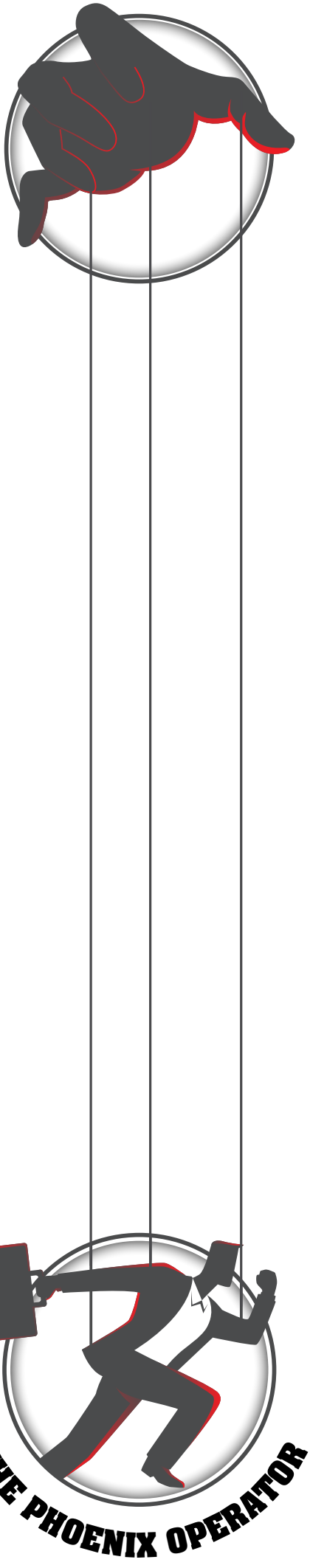
Trends:

- 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.



Australian Government
Serious Financial Crime Taskforce

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.

Australian Government
Serious Financial Crime Taskforce

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.

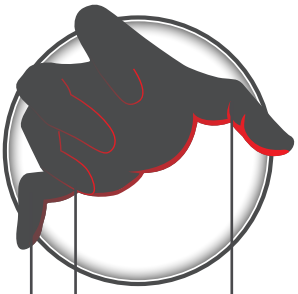
Like many businesses, professional intermediaries may also be targeted by criminals with an interest in the personal and/or commercially sensitive information they have access to.

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.

Continued over the page



Lawyers Accountants Tax advisers Labour providers Service providers Bankers

Australian Government
Serious Financial Crime Taskforce

The Enabler (cont'd)

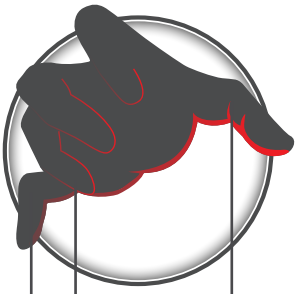
Warning signs:

- 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.

Professional associations can provide advice if you are concerned about what you are being asked to do.



Lawyers Accountants Tax advisers Labour providers Service providers Bankers

Australian Government
Serious Financial Crime Taskforce

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. Other criminals buy and then use these identities and information to carry out serious financials crimes that harm people, businesses, banks and the ATO (and therefore the Australian public).
- Stolen identities and information, and phishing schemes can be used to steal from superannuation and share trading accounts, and purchase goods and services using the victim's funds and ID.
- 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.
- Could be anyone from a teenage hacker living next door to a member of an offshore crime syndicate.

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:

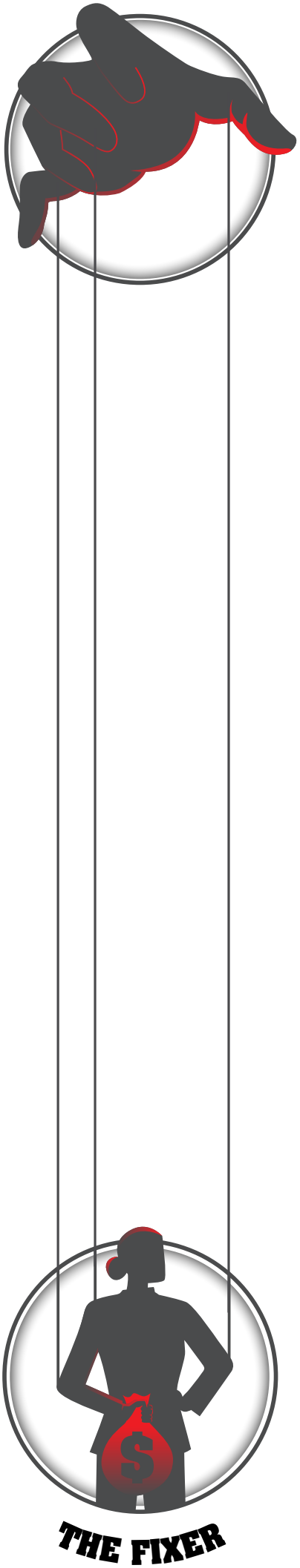
- Financial crime has evolved, and technology now plays a significant role.
- Some sectors known to be at risk of exploitation by data thieves include real estate, migration services, employment services and HR/payroll.
- The impacts are long term – people may see the impacts for years afterwards if 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.

Data thief Hacker Phisher Code writer Data buyer

THE CYBER CRIMINAL

Australian Government
Serious Financial Crime Taskforce

The Fixer



The Fixer profits by facilitating offshore tax evasion. More specifically, they help individuals, dodgy companies and criminal syndicates conceal the source of money and how much money they have.

Behaviours:

- Provides a 'service' out of a tax haven (e.g. citizenship, ID, a set of nominal directors, bank accounts and a company creation agent).
- Hides a shareholder's identity via offshore entities.
- Assists organised crime groups to establish offshore entities to hold assets, and hide their ownership, value and movement.

Warnings signs:

- Offers services via the dark web.

Trends:

- People used to have to be well off and have the right connections to engage in this activity. This offering has been made more widely available in recent years so that services can be acquired for a fixed fee by anyone with access to the dark web.
- Offshore secrecy arrangements are increasingly being exploited to facilitate tax evasion and money laundering.

Australian Government
Serious Financial Crime Taskforce

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).

If you think you're involved in an offshore tax arrangement, come forward and make a voluntary disclosure. This may lead to reduced penalties and interest, particularly if an audit is conducted.

Australian Government
Serious Financial Crime Taskforce

The Rorter

The majority of people do the right thing and only access the benefits they are entitled to. The Rorter lies or withholds information to fraudulently access a range of government subsidies (including COVID-19 stimulus measures).

Warning signs:

- Makes false claims for a stimulus measure (e.g. where there is no history of previous employment).
- Makes claims as both an employee and an eligible business.
- Makes multiple claims or amends paperwork in order to claim for a stimulus measure.
- Obtains access to a payment, makes claims for amounts not entitled to or increases the amount entitled to for stimulus payments.

Trends:

- The impact of COVID-19 has led some people to consider new or risky opportunities in an effort to regain share market losses or supplement their income.
- Measures designed to protect the integrity of the government's stimulus measures have ensured only a small number have attempted to gain benefits fraudulently.

Australian Government
Serious Financial Crime Taskforce

Other players

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.
- Can confidentially report any concerns via **www.ato.gov.au/tipoff** or by calling **1800 060 062.**

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.

You can help us stop serious financial crime by being on the lookout for suspicious activity.

Some of the warning signs are in the checklist below.

1. 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

2. 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

Australian Government
Serious Financial Crime Taskforce

If you have a tip-off or any concerns, please call the ATO tip-off hotline on **1800 060 062** or go to **www.ato.gov.au/SFCT** for further information.

Cybercrime and identify theft are growing areas of concern.

Rapidly evolving technology provides a platform for cyber criminals to gain online access to information and sensitive data, facilitating opportunities for criminals to commit crimes, including tax crime and identity theft. Below are some potential warnings signs of cybercrime and tips for protecting yourself and your information.

✓ 3. 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)

Click on any of the personas below to read more.

Australian Government
Serious Financial Crime Taskforce

If you have a tip-off or any concerns, please call the ATO tip-off hotline on **1800 060 062** or go to **www.ato.gov.au/SFCT** for further information.

About the Serious Financial Crime Taskforce (SFCT)

The SFCT is focused on offshore tax evasion, illegal phoenix activity, cybercrime affecting the tax and superannuation systems and crime related to the Commonwealth Coronavirus Economic Response Package.

Our work is strengthened by:

- **Sophisticated analytics:** The sheer size of information available to us for analysis and our information sharing capabilities sends a clear message to those tax cheats who believe that their activities are hidden and beyond our reach – they're not.
- **Significant funding:** On 1 July 2019 a further $182.2 million was allocated across four years to extend the SFCT and further strengthen our powers to fight serious financial and organised crime activities that present the highest risk to Australia's tax and superannuation systems.
- **The community's trust and help:** We receive valuable information from members of the community who suspect something suspicious and contact us on **1800 060 062** or via **www.ato.gov.au/tipoff**.
- **Global reach:** Our international and domestic intelligence-sharing relationships help uncover even the most intricately-planned tax evasion schemes. Australia now has international treaties and information exchange agreements with over 100 jurisdictions.
- **Highly skilled people, who are world-renowned:** The SFCT is supported by world-class investigative experts, researchers, forensic accountants, lawyers, cyber-experts and other specialists. In fact, the SFCT provides training to other countries that share an interest in bolstering their ability to deter and respond to serious financial crime.
- **The law on our side:** We investigate all serious tax-related fraud offences and share information with our Commonwealth partners. Where the evidence warrants it, we refer cases to the Commonwealth Director of Public Prosecutions (CDPP) for prosecution.

Current SFCT members include:

Australian Taxation Office (ATO)	Australian Federal Police (AFP)
Australian Criminal Intelligence Commission (ACIC)	Attorney-General's Department (AGD)
Australian Transaction Reports and Analysis Centre (AUSTRAC)	Australian Securities and Investments Commission (ASIC)
Commonwealth Director of Public Prosecutions (CDPP)	Services Australia
Department of Home Affairs (Home Affairs), incorporating its operational arm, the Australian Border Force (ABF)	

Serious Financial Crime
Identikit

1800 060 062 | www.ato.gov.au/SFCT

Australian Government
Serious Financial Crime Taskforce