Print whole section

Our focus

Outlines the key areas presenting a higher risk that we pay particular attention to.

Offshore tax evasion

Most offshore dealings are legitimate, but some people evade paying tax.

Global cooperation

Our domestic and international relationships help us to reduce opportunities for tax crime and tackle tax evaders.

Joint Chiefs of Global Tax Enforcement

How the Joint Chiefs of Global Tax Enforcement (J5) combat transnational tax crime through enforcement collaboration.

Serious Financial Crime Taskforce

The ATO-led Serious Financial Crime Taskforce tackles the most serious forms of financial crime.

Financial crime

Financial criminals deliberately abuse the tax and superannuation

Illicit tobacco

Why it's a serious offence to grow, manufacture or produce illicit tobacco and what penalties may apply.

Refund fraud

Refund fraud occurs when people dishonestly claim refunds, rebates or offsets they aren't entitled to.

Organised crime

What is organised crime, it’s impacts and how the ATO takes action to tackle criminal activities.

Illegal phoenix activity

Find out what illegal phoenix activity is, the warning signs, how to protect yourself and how to report a company.

Data leaks

We are constantly receiving information that helps us detect and investigate tax evasion and other illegal activities.

QC 33621

Offshore tax evasion

Most offshore dealings are legitimate, but some people evade paying tax.

Last updated 11 February 2025

Offshore tax evasion

Australian residents (for tax purposes) are taxed on their worldwide income. Most offshore dealings are legitimate and comply with Australian tax laws. But some people try to exploit secrecy provisions in other countries to evade paying tax in Australia. Offshore tax evasion occurs when a person evades paying tax by either holding their money and assets offshore or by not declaring their offshore income.

Offshore tax evasion is a form of financial crime, and like all financial crimes, is diverse in nature, scale and the amount of harm it causes. It is often structured in ways that combine legal and illegal transactions.

Those involved often combine both types of payments in the hope of making it more difficult for us to unravel the full extent of their activities.

We are equipped with the resources, sophisticated data matching and analytics capability, and intelligence sharing relationships to uncover even the most elaborate offshore dealings.

Offshore tax evasion results in less tax revenue which means less funding for essential community services like health and education.

How we tackle offshore tax evasion

In Australia, we work with the ATO-led Serious Financial Crime Taskforce (SFCT) to tackle offshore tax evasion.

We also work with governments and organisations around the world to fight tax crime on a global scale. One example of our global cooperation is through the Joint Chiefs of Global Tax Enforcement.

Australia has a network of international treaties and information exchange agreements with over 100 jurisdictions, allowing us to obtain information about suspected tax evasion. We also regularly receive information from informants and third parties.

Not only does this information help us identify those who are involved in offshore tax evasion, but it also helps us to identify enablers including tax professionals, lawyers and financial advisors who promote or facilitate offshore tax evasion arrangements. Where

appropriate, we use the Commissioner of Taxation's formal access and information gathering powers to obtain information about their clients.

The sheer volume of information we have available and will continue to build on through our relationships with key partners, should send a clear message to those who believe their offshore evasion activities are secure and beyond our reach – they are not.

Consequences of offshore tax evasion

Those who take part in offshore tax evasion do so to the detriment of the Australian community. This is something we will not tolerate. We will catch offshore tax evaders and hold them to account.

Our national and global cooperation is reducing tax evasion in the Australian tax system. Our international partners are also reporting similar results.

Offshore tax evasion is a global problem that we are addressing through global solutions. It's clear that our efforts to tackle offshore tax evasion are paying off and that our strong partnerships will enable us to uncover even the most elaborate offshore tax evasion schemes.

In recent years over 2,500 exchanges of information have occurred which have enabled us to raise tax liabilities of $1 billion.

If you think you might be involved in offshore tax evasion, we encourage you to come forward. Making a voluntary disclosure can lead to reductions in penalties and interest, particularly if it is made before we notify you of an audit.

Find out how we're closing the net on offshore tax evasion.

Media releases

- ATO welcomes decision in Commissioner of Taxation v Rawson Finances
- 19-year tax fraud probe ends in jail time for scheme promoter

Offshore Tax Evasion case studies

Case studies that show how we detect and disrupt illegal offshore tax arrangements.

How we're closing the net on offshore tax evasion

Explains offshore tax evasion and the global approach the ATO takes to uncover illegal offshore dealings.

QC 41324

Offshore Tax Evasion case studies

Case studies that show how we detect and disrupt illegal offshore tax arrangements.

Last updated 11 February 2025

About offshore tax evasion

While most Australian's do the right thing, there are a small percentage who try to use offshore arrangements to avoid paying millions of dollars in tax.

These individuals create offshore structures to try to disguise beneficial ownership to evade their domestic tax obligations by using a combination of foreign entities, nominee arrangements and offshore service providers (OSP). These arrangements can be highly sophisticated and involve the creation of multiple entities across several jurisdictions.

If you know or suspect that someone may be committing tax crime you can report it by either:

- completing the tip-off form
- phoning us on **1800 060 062**.

Case studies

Mr Smith's avoidance of his offshore tax obligations

Mr Smith is an Australian resident, a qualified orthodontist and is the beneficial owner of two offshore companies. Both companies are registered in the British Virgin Islands and are administered by an offshore services provider (OSP) based in Hong Kong.

For 2 years, both offshore companies traded in Australian Stock Exchange (ASX) listed entity shares and derived a net profit of $2 million and $5 million.

Mr Smith used arrangements with third-parties to return some of the profits of the offshore companies to Australia for his own benefit.

Mr Smith provided information to the ATO in an attempt to explain the arrangements. As part of his explanation, he contended that the companies were established by his deceased father and that he had limited knowledge about the entities.

Some of the information provided didn't make sense and the ATO's enquiries continued. Though there was no information to suggest that Mr Smith was the legal owner of the share capital of the offshore entities, it was evident that nominee directors and shareholders were used and Mr Smith in fact held the right to receive the capital or profits of the offshore entities.

It was concluded by the ATO that Mr Smith failed to comply with his income tax reporting obligations and as a result the ATO raised assessments for outstanding tax liabilities on the basis that he was an attributable taxpayer of the controlled foreign companies (CFCs). Penalties and interest were also payable on the tax shortfalls. A referral for investigation for potential criminal behaviour was also made.

Ms Thompson's undeclared offshore income

Ms Thompson is an accountant with many years' experience in the industry and is the founding director of her own accounting firm.

Several external companies engage the services of Ms Thompson's accounting firm as external auditors. The Annual Reports for these companies list entities linked to a known offshore service provider (OSP) in their top 20 shareholders.

Ms Thompson has also been personally linked with a foreign registered company administered through the same OSP. Information indicates

that this foreign company has been trading in shares. Over a period of nearly 6 years this foreign company made payments directly to third parties for the benefit of Ms Thompson. For example, payments were made for the purchase of a luxury vehicle for Ms Thompson, for home renovations and for the payment of school fees for her children.

After analysing all available information, ATO compliance officers confirmed that the foreign company had derived active income and that the payments to third parties for the benefit of Ms Thompson were made from profits. No other parties were found to have benefited from the foreign company's profits.

It was found that Ms Thompson had not declared this income in relevant income tax returns and amended assessments were raised to include the additional tax liabilities. Penalties and interest were also payable.

As Ms Thompson is a registered Tax Agent a referral to the Tax Practitioners Board was also made for potential breaches of the Code of Professional Conduct which could result in her tax agent's registration being terminated.

QC 73802

How we're closing the net on offshore tax evasion

Explains offshore tax evasion and the global approach the ATO takes to uncover illegal offshore dealings.

Last updated 11 February 2025

This infographic provides more information on how we're closing the net on offshore tax evasion (PDF, 888KB).

What is offshore tax evasion?

Offshore tax evasion is a crime where a person deliberately evades paying tax by holding money and assets offshore.

Our role at the ATO is to identify and catch these individuals.

A global approach that gets results

We use sophisticated tools and a highly collaborative approach to information sharing to get results. We work with our domestic and international partners to manage offshore tax evasion risks and deter those considering getting involved in offshore tax evasion schemes.

Our international partners:

- The Joint Chiefs of Global Tax Enforcement (J5) – Australia, Netherlands, UK, US, Canada.
- The Organisation for Economic Co-operation and Development (OECD).
- Joint International Taskforce on Shared Intelligence and Collaboration (JITSIC).

These global partnerships have resulted in:

- the establishment of the Common Reporting Standard for collecting, reporting and exchanging financial information on foreign tax residents
- more than 2,500 exchanges of information, enabling us to raise tax liabilities of $1 billion
- 100 jurisdictions linked by international treaties and exchange agreements
- more effective disruption of offshore tax evasion activities by Australian authorities.

Offshore tax evasion comes at a cost

Offshore tax evasion results in less tax revenue, which means less funding for essential community services like health and education.

We're committed to protecting the community from offshore tax evasion.

A partnership closer to home

The Serious Financial Crime Taskforce (SFCT): ATO-led, joint-agency taskforce with formidable resources and data-matching capability.

$556 million collected by the SFCT from serious financial crime activities, including offshore tax evasion. (As at 31 December, 2021)

Think you've been involved in offshore tax evasion?

Find out more about offshore tax evasion – including how to make a voluntary disclosure or a confidential tip-off – at ato.gov.au/offshoretaxevasion.

Remember: If you come forward early with information, it could mean reduced penalties and interest.

QC 61569

Global cooperation

Our domestic and international relationships help us to reduce opportunities for tax crime and tackle tax evaders.

Last updated 11 February 2025

Our cross-agency and international relationships help us keep up to date with the changing nature of tax evasion and crime. This includes putting in place best-practice tax laws to reduce opportunities for tax evasion and crime and increase the chances of catching tax evaders.

Legitimate cross border financial transactions are a feature of the global economy. However, income concealed offshore, poor transparency of offshore activities, and practical difficulties associated with getting information about a taxpayer's offshore activities all present risks for the international tax system.

In response, we work with governments and organisations around the world to fight tax evasion and crime on a global scale. Our strategies include:

- working with revenue collection agencies around the world, who are increasingly sharing intelligence and expertise in financial investigations to fight tax evasion and organised tax crime
- collaborating with a range of stakeholders, including private sector partners
- participating in information sharing, automated data matching, intelligence gathering, analytics, investigations and audits with

international tax administrations using Australia's bilateral tax treaties and the Multilateral Convention on mutual administrative assistance in tax matters

- working with our partner agencies through the Serious Financial Crime Taskforce (SFCT) to address the most serious forms of financial and organised crime
- working with Australian Transaction Reports and Analysis Centre (AUSTRAC), with its enhanced capability to detect, monitor and report international transactions
- working internationally with the Joint Chiefs of Global Tax Enforcement (J5) to gather information, share intelligence and conduct joint operations in relation to cybercrime, cryptocurrency fraud and enablers and facilitators of offshore tax crime
- working with other OECD networks like the Joint International Taskforce on Sharing Intelligence and Collaboration (JITSIC) to share information relating to tax avoidance and evasion.

In addition to these strategies, Australian courts have endorsed our use of information from overseas informants as part of tax assessment and audit processes.

This engagement at the international level allows us to share intelligence, improve our ability to influence international policy, and cooperate with other jurisdictions.

We collaborate with international revenue agencies bilaterally, and through groups and forums such as the OECD, Global Forum and the Commonwealth Association of Tax Administrators

OECD

We contribute to a number of forums on tax administration supported by the Organisation for Economic Co-operation and Development (OECD), which brings together more than 30 governments from across the globe. This collaborative work provides valuable support and the opportunity to share best-practice processes with our international counterparts. The Australian Taxation Office (ATO) participates in the:

- Taskforce on Tax Crimes and Other Crimes, which is mandated to improve the ability of tax administrations to identify, audit, investigate and disrupt tax crime and other serious crimes, including

money laundering and bribery, by sharing experiences and examining specific tax and crime risks.

- Tax Crime Enforcement Network, a pilot program within the framework of the TFCT, which focuses on improving international cooperation among law enforcement agencies to combat tax crimes effectively.

Global Forum

The Global Forum was originally established in 2001 by both OECD and non-OECD countries to tackle the use of secrecy jurisdictions. The forum's primary focus is to exchange information and to develop the international standard of transparency. The forum now includes 122 members, making it the largest tax group in the world. With the support of the G20, the forum was re-structured in 2009 to establish an in-depth peer-review process. The Peer Review Group (PRG) monitors and reviews the progress of its members towards the international standard of transparency and exchange of information.

QC 33612

Joint Chiefs of Global Tax Enforcement

How the Joint Chiefs of Global Tax Enforcement (J5) combat transnational tax crime through enforcement collaboration.

Last updated 1 May 2026

About the J5

Tax crime is a global problem that needs a global solution. The Joint Chiefs of Global Tax Enforcement (J5) lead the fight against transnational tax crime and money laundering. This includes

cryptocurrency threats and those who undertake, enable or facilitate global tax evasion.

The J5 group brings together leading tax, offshore tax evasion, cryptocurrency and cyber experts from:

- Australia – Australian Taxation Office
- Canada – Canada Revenue Agency
- Netherlands – Dutch Fiscal Intelligence and Investigation Service
- United Kingdom – His Majesty's Revenue and Customs
- United States – Internal Revenue Service Criminal Investigations.

These countries share intelligence to discover threats and conduct operations focused on disrupting enablers of tax crime. Meanwhile, they strengthen respective systems to maintain the integrity of tax administration and ensure compliance with tax laws.

The J5 mission

Media: J5 – Working together to tackle tax crime https://tv.ato.gov.au/ato-tv/media?v=bd1bdiunhsxowx (**Duration:** 3:18)

J5 results

The J5 was formed on 1 July 2018 in response to a call to action from the Organisation for Economic Co-operation and Development (OECD) for countries to do more to tackle the enablers of tax crime. All 5 countries face similar threats from organised crime groups and wealthy offshore tax evaders. These groups are resourced and have access to professional enablers to hide income and assets using the global financial system.

The J5 is a strong international alliance with a shared goal to target facilitators and enablers, cybercrime and cryptocurrency. It also builds capability around data platforms that will help the work of each country.

By working together, the J5 apply pressure to the global criminal community more effectively than working alone. The J5 alliance is

dedicated to ensuring that those that break tax laws face the consequences of their actions.

Serious Financial Crime Taskforce

The ATO continues to work with partner agencies in the ATO-led Serious Financial Crime Taskforce (SFCT) to support J5 operations. The partnership between the SFCT and J5 grows stronger while advancing investigations into transnational tax evasion and associated money laundering. The SFCT investigates the most serious and complex forms of financial crime that present the highest risk to Australia's tax and superannuation systems.

For more information, see Serious Financial Crime Taskforce.

Cyber Challenge events

Crypto assets (such as cryptocurrencies) are being increasingly used for criminal activities. This is due to their anonymous nature and the ease and speed with which they can be sent anywhere in the world. Reducing the growing threat that crypto assets pose to tax administrations and law enforcement agencies worldwide is a key focus for the J5.

The J5 hold annual Cyber Challenge events which bring together experts from each country. Together they identify leads into tax evasion and money laundering involving crypto assets.

In September 2025, investigators and analysts from J5 agencies met in Zwolle, Netherlands for the annual Cyber Challenge. The focus of 2025 Cyber Challenge included darknet markets and illicit cryptocurrency activity, transnational organised crime groups and identity-based fraud schemes. This Challenge also included a focus on joint operations with immediate real world impact.

Global Financial Institutions Partnership summit

The J5 have hosted the annual Global Financial Institutions Partnership summit since 2022. The summit brings together financial institutions, banking associations, Financial Intelligence Unit representatives and

other partners to discuss effective practices in combating tax and financial crime.

The most recent summit was held in Ottawa, Canada in October 2024. Discussions and projects focused on the threats of identity theft-based crimes, misuse of financial technology and trade-based money laundering.

Resources

Learn more about how the J5 work to tackle transnational tax crime:

- J5 video – Inside the J5
- J5 chiefs' podcast – London 2022
- J5 animation: J5 – Tackling tax crime together
- J5 video: J5 – Working together to tackle tax crime

Media releases

- J5 links suspicious activity to cryptocurrency platforms in new advisories 12 February 2026
- J5 'Cyber Challenge' unites global tax enforcers against criminals exploiting cryptocurrency and the dark web 17 September 2025
- J5 releases 3 reports on the misuse of fintech, ID-based crimes, and trade-based money laundering in plastic waste as part of the Global Financial Institutions Partnership 10 June 2025
- J5 countries host fourth Global Financial Institutions Partnership Summit (PDF, 221KB) 24 October 2024
- Film producer indicted for multi-decade tax conspiracy
  23 September 2024
- J5 reviews cryptocurrency risk factors during Cyber Challenge
  19 September 2024
- J5 publishes first report detailing the alliance's global impact
  26 July 2024
- Former defence contractor and his wife indicted for evading U.S. taxes on profits from selling jet fuel to the U.S. military (irs.gov) (PDF, 213KB) 3 July 2024

- J5 issues notice to financial institutions about risk indicators tied to cryptocurrency assets (irs.gov) 23 May 2024
- J5 countries host Cyber Challenge focused on data mining and financial reporting 3 November 2023
- International tax advisor arrested for helping to conceal over $100 million of income for high-net-worth U.S. taxpayers (PDF, 133KB) 14 July 2023

QC 61181

Financial crime

Financial criminals deliberately abuse the tax and superannuation systems to gain illegal financial benefits.

Last updated 11 February 2025

Unfortunately, a small percentage of Australians deliberately abuse the tax and superannuation systems for their financial benefit. We are committed to preventing, detecting, disrupting and bringing the perpetrators of tax and financial crime to account.

Financial crime explained

Financial crime is not victimless and has a serious economic impact on the community. It deprives the community of funding for essential services such as health, education and infrastructure.

Financial crime also has significant direct impacts on individuals and businesses. Examples can include:

- cyber criminals who steal people's life savings or identities
- companies which are deliberately liquidated, wound up or abandoned (referred to as illegal phoenix activity) before they can pay creditors such as the ATO, honest businesses or subcontractors
- organised criminals who orchestrate illicit tobacco growing operations, robbing our community of millions in revenue and taking business from legitimate retailers.

In most cases there is a toll on victims' emotional wellbeing, physical health and relationships as well.

Thankfully, only a small percentage of people deliberately abuse the tax and superannuation systems to reap illegal financial benefits. Such activities can include:

- tax evasion (blameworthy act or omission by the taxpayer)
- tax fraud (taxpayer making a false statement to the ATO about their tax or being recklessly careless about whether what they state is true or false)
- other offences like money laundering or identity theft.

Illegally obtained proceeds from financial crime are often used to facilitate organised crime, costing Australia up to $68.7 billion each year. Organised crime harms real people and our communities, which is why we are committed to disrupting and dismantling organised crime syndicates. Under the Commonwealth Organised Crime Strategic Framework, we have a shared responsibility to tackle the financial aspects of serious organised crime.

Like any crimes, financial crimes are diverse in nature, scale and the amount of harm they cause. They are often structured in ways that combine legal and illegal transactions and payments, trying to make it difficult to unravel the full extent of the illegal activities.

Whether financial crime threats originate in Australia or offshore they are usually enabled by facilitators and technology. For example, rapidly evolving technology and platforms help cyber criminals access information and sensitive data, making it easier for them to commit crimes against:

- individuals
- businesses
- the government.

Indications of financial crime

When people commit financial crimes they typically misrepresent or conceal the true nature of their transactions, assets or ownership of entities. Some of the indicators we look for include:

- use of nominees or straw directors

- unexplained wealth or wealth that is at odds with their reported income
- giving false or misleading statements to the ATO
- mischaracterising the true nature of transactions
- understating income
- inflating or claiming deductions to which they aren't entitled
- keeping two sets of books or financial statements
- failing to keep records or intentionally destroying financial records
- concealing money or the source of money
- making payments in cash
- using fictitious names or names of unauthorised third parties
- failing to lodge income tax returns or business activity statements (BAS)
- failing to pay tax debts when they are due
- withholding information from a tax professional or the ATO
- ignoring legal advice or guidance from the ATO.

Tax evasion or fraud

Tax evasion involves some blameworthy act or omission by the taxpayer.

Tax fraud is more serious and involves the taxpayer making a false statement to the ATO about their tax or being recklessly careless about whether what they state is true or false.

Examples of fraud or evasion include:

- recklessly claiming deductions that the taxpayer was not entitled to
- withholding information from the Commissioner or failing to keep records
- submitting false, backdated or altered documents
- paying wages in cash and not reporting the wages paid to the ATO

- not remitting GST, Pay As You Go Withholding (PAYGW) tax or Superannuation Guarantee charges to the ATO
- making false statements
- disguising expenses intended for personal benefit as business expenses.

Where there is enough evidence to suggest that a person has acted knowingly or recklessly to dishonestly get a payment or refund from the ATO, we consider making a referral for criminal investigation and prosecution.

How we tackle financial crime

We are a key participant in many taskforces and coordination groups. Our shared goal is to identify and dismantle financial crime in Australia. Some of our key partnerships include:

- Criminal Assets Confiscation Taskforce (CACT)
- National Anti-Gangs Squad (NAGS)
- ATO-led joint agency Serious Financial Crime Taskforce (SFCT).

Internationally, we work through alliances such as the Joint Chiefs of Global Tax Enforcement (J5), to crack these criminal enterprises wide open.

Our partnerships allow us to share intelligence and information, bringing the most serious offenders of financial crime to account.

Fact sheet

Find out about one of our complex tax fraud investigations known as Operation 4 and how the scheme was set up. You can also download this information as a fact sheet (PDF, 313KB).

Case studies

Our financial crime case studies reinforce that those who deliberately abuse the tax and superannuation systems for financial benefit will be caught.

Boiler room schemes

Boiler room or cold-call investment fraud often involves technology and identity fraud to rob victims of their savings.

Ponzi schemes

The Ponzi scheme warning signs, and how to protect yourself and others.

QC 64530

The scheme - how it was set up

Operation 4 – how the scheme was set up.

Last updated 12 February 2024

Stage 1

The Tier 1 developers contracted the Tier 2 building companies to construct a development, such as a hotel and golf course.

Stage 2

The Tier 2 building companies obtained supplies or labour from the small (shell) Tier 3 suppliers, such as a bricklayer.

Stage 3

The developer claimed they paid GST to the building companies and the building companies claimed they paid GST to the sacrificial suppliers – GST skimming. Grossly inflated construction costs and purchases of goods between the companies that never actually occurred were also recorded to claim additional GST.

Stage 4

Mr Li Zhang conspired with the intention to cause loss to the Commonwealth of $15 million by fraudulently obtaining GST refunds.

He was sentenced to 10 years in jail with a non-parole period of 6 years and 8 months.

You can also download this information as an infographic.

QC 101192

Boiler room schemes

Boiler room or cold-call investment fraud often involves technology and identity fraud to rob victims of their savings.

Last updated 11 February 2025

Boiler room schemes

In a typical boiler room scheme, a salesperson cold-calls and offers investment opportunities to people they have targeted through identity fraud or technology. These opportunities can include:

- sports trading
- foreign exchange currency trading
- lay trading (gambling related methodology)
- cryptocurrency
- other financial investment or gambling related products.

The targets come from lists provided by lead generation agencies; some of which are controlled by other boiler rooms.

Victims are persuaded to pay a significant ‘subscription fee’ for expert trading advice, or a ‘software licence fee’ for in-house designed trading prediction software, in return for a promise of high returns. Often, fees aren't set until after establishing what the victims can afford to pay.

On investment, victims receive fabricated examples of significant investment returns. A 'critical incident' then occurs, causing the company to fail and the victims' investments to be lost.

The organised criminals behind these schemes never intend to honour the investment. The sole purpose of boiler rooms is to embezzle victims' funds to benefit the organised crime syndicate, at the cost of those who need it most.

Example: Mr Smith's devastating loss

A telemarketing salesperson operating out of a boiler room cold-calls Mr Smith, a self-funded retiree, offering a too good to be true opportunity to invest in sports trading. Mr Smith was targeted as he appeared on a list identifying those who have a high income and an interest in investing. What Mr Smith didn't know was that the investment was incapable of producing the high profits it promised.

Mr Smith investigates the legitimacy of the company, checking out their professional looking website and glossy brochures, and confirming their office was located in a major Australian city. He also searches for any negative reviews online. The boiler room anticipates Mr Smith's due diligence; their office is virtual, any complaints about the company are quickly removed and people involved in the scheme post false positive testimonials regularly.

As Mr Smith sees no cause for concern, he agrees to proceed with the investment opportunity, providing the principal funds. He is then offered another opportunity to purchase expert trading advice for a significant 'subscription fee' which he gladly accepts to increase his earning potential.

After watching his online 'trading account' tick over, Mr Smith continues to add more funds to the investment. One day, he tries to withdraw some of his earnings and he is suddenly locked out of his account. He later learns the company has gone into voluntary administration.

The boiler room never traded on Mr Smith's behalf; the information he saw in his online account was completely false. Mr Smith's investments were laundered by an organised crime

syndicate to fund their lavish lifestyles and allow them to engage in even more serious crimes.

The personal impact on Mr Smith's life was devastating; not only did he suffer a significant financial loss which he'll never get back, his wife no longer trusts him to make financial decisions, he has trouble sleeping and he takes antidepressants to ease his anxiety, stress and depression.

Tackling boiler room activity

We partner with intelligence, regulatory and law enforcement agencies to detect, prevent and bring the perpetrators of financial crime to account. We make no apologies for pursuing those who break the law. This behaviour is deliberate, calculated and cheats everyday Australians out of their hard-earned savings.

How to protect yourself

Boiler room syndicates rob victims of their savings and unfortunately most do not get their money back. Victims also often need support to move forward and rebuild their lives, both financially and non-financially.

If any of the following have occurred to you, you may be at risk of becoming a victim:

- You have completed an online survey and included details such as your salary and/or your interest in self-managed superannuation. Or, you have searched for investments online or attended an investment seminar. Your details may then be sold onwards.
- A salesperson approaches you with a slick and sophisticated sales pitch involving either financial management schemes or computer software. They will claim that the opportunity you are offered is low-risk and high-reward.

You can protect yourself from boiler room activity by:

- not being pressured into making decisions over the phone. Always take the time to conduct your own research and seek a second opinion from a trusted adviser

- being suspicious of anyone that offers you easy money. You may investigate the legitimacy of the salesperson before signing up for the 'investment'. Remember, boiler rooms often have virtual offices, false identities, fake receptionists and fake testimonials
- using the ASIC MoneySmart website to stay informed on how to identify an investment scam and how to check if an investment is real
- confidentially reporting fraudulent activity to the ATO by making a tip-off or phoning **1800 060 062**.

QC 67250

Ponzi schemes

The Ponzi scheme warning signs, and how to protect yourself and others.

Last updated 11 February 2025

What is a Ponzi scheme?

A Ponzi scheme is a form of fraud that attracts investors by promising high returns with little to no risk. New investors bring in money which pays dividends, or other types of payments, to existing investors. There is no actual investment offered by scheme operators.

Some warning signs of Ponzi schemes include:

- the rate of return looks too good to be true
- a promise of consistent returns regardless of market conditions and other external factors
- the logistics of the investment are too complicated to explain
- someone you know tries to recruit you
- the recruiter encourages you to make a quick decision

- the recruiter has already invested in the scheme.

Existing investors in a Ponzi scheme receive dividends funded by new investors and are unlikely to suspect that it is not a genuine investment. This encourages these investors to target friends, family and other acquaintances into the scheme, often attracting more vulnerable groups and individuals with the promise of quick returns on their investment.

In some cases, recruiters attract new investors by saying their investment in the scheme is a way to avoid tax.

Ponzi schemes need new investors and their money to survive. When scheme promoters fail to attract new investors, the scheme will collapse, leaving most new investors out of pocket and with little to no recourse to recoup their losses.

Example: Ms Jones loses her nest egg

Ms Jones makes a comfortable living as an office manager. She's already saved $200,000 for her retirement but is on the lookout for more investment opportunities.

While talking to a friend in the office, a colleague overhears. Her colleague says that her financial adviser has been able to get her a great return on her investment, far higher than the market average. Intrigued by her colleague's claim, Ms Jones asks for the financial adviser's contact details.

When Ms Jones calls the financial adviser, he promises a risk-free investment with a high rate of return, regardless of market conditions. He convinces Ms Jones that he has cracked the code on investments, using a lot of complicated financial jargon in the process. However, he says that he unfortunately cannot take her as a client because he only takes 10 clients at a time. She is disappointed and asks him to let her know when a spot is available. A few days later, he calls back to tell her he can now take her as a client and rushes to sign her up before other potential clients take that spot. In the rush to sign up, Ms Jones forgoes the usual checks she would normally do to make sure the investment is legitimate, such as checking the financial adviser's Australian Financial Services Licence or getting a second opinion from another trusted adviser.

Ms Jones believed her retirement fund was being invested in ways that would see her double her nest egg. However, her fund was being used to pay dividends to investors like Ms Jones' colleague, who had previously signed up, so they didn't suspect anything was wrong.

A few months go by and Ms Jones has not seen any returns on her investment. Meanwhile, the financial adviser has spent Ms Jones' money on himself. The scheme comes undone when the adviser cannot find new investors, and therefore cannot pay dividends to his existing ones. Upon further investigation into the financial adviser, Ms Jones finds that he was operating a Ponzi scheme, and reports him to ASIC.

Unfortunately for Ms Jones and the rest of the investors, there is little recourse for their losses. Their money has been lost to the financial adviser's scheme and has been used to fund his lavish lifestyle. Ms Jones now must start building her retirement fund from scratch.

Reporting Ponzi schemes

We are committed to disrupting all forms of financial fraud in the community that causes harm and undermines the integrity of the tax system, including Ponzi schemes.

You can protect yourself and others from investing in Ponzi schemes by being aware of the red flags and checking online resources about schemes from the ATO and ASIC. If you are unsure if a scheme is a Ponzi scheme, you can get a second opinion from a trusted financial or legal adviser.

If you suspect you or someone you know is involved in a Ponzi scheme, refer to the ASIC MoneySmart website for how to report the scheme. You can also confidentially report fraudulent activity to us by making a tip-off or phoning **1800 060 062**.

QC 71279

Illicit tobacco

Why it's a serious offence to grow, manufacture or produce illicit tobacco and what penalties may apply.

Last updated 6 March 2026

The illicit tobacco trade

Engaging in the illicit tobacco trade is a serious offence. It significantly deprives the Australian community of vital funding which could be used to fund essential community services such as health, education, transport and infrastructure.

Tobacco is illicit when it is grown, manufactured and/or produced in Australia or imported into the domestic market without customs duty being paid.

Illicit tobacco products may include:

- cigarettes
- cigars
- loose tobacco (also known as 'chop-chop')
- tobacco leaf and plant matter.

The illicit tobacco trade includes but is not limited to the unlicensed:

- production of tobacco plant or leaf
- manufacture of tobacco products
- tobacco sold without payment of taxes.

Tackling illicit tobacco

We use a range of investigative and legislative approaches to disrupt illicit tobacco activity. These include:

- gathering intelligence
- conducting investigations

- conducting audits and using proceeds of crime action to target wealth created by those participating in the growing, manufacture, distribution or sale of illicit tobacco
- working with federal and state government and law enforcement agencies as part of investigations and intelligence sharing (see Illicit Tobacco Taskforce)
- identifying, seizing and destroying identified crops
- collecting evidence as part of prosecution activity
- using the *Taxation Administration Act 1953, Excise Act 1901* and the *Criminal Code Act 1995* to prosecute offenders.

Every crop we seize and destroy, burns another hole in the illicit tobacco trade. We continue to disrupt the illicit tobacco trade by prosecuting those who are found to be domestically growing and manufacturing illicit tobacco.

See examples in our illicit tobacco case studies.

Table 1: Illicit tobacco enforcement – results as at 31 March

Financial year	Number of seizures	Amount seized and destroyed (kilograms)	Cigarettes (sticks)	Estima ex ($mill
2018–19	8	41,400	Nil	
2019–20	22	130,656	11,480	
2020–21	23	109,186	5,496,379	
2021–22	21	110,349	1,661,520	
2022–23	16	66,711	1,207,516	

2023–24	81	16,687	13,382,445	
2024–25	9	23,311	6,789,411	
2025–26	11	527	28,210,960	
Total	**191**	**498,827**	**56,759,711**	

Illicit Tobacco Taskforce

On 1 July 2018, the Illicit Tobacco Taskforce (ITTF) was established as part of new reforms. The ITTF enhances the ability of the ATO and our partner agencies to protect Commonwealth revenue, by proactively detecting, disrupting and dismantling serious organised crime syndicates that deal in illicit tobacco.

The taskforce draws on the expertise and advanced capabilities of the:

- ATO
- Australian Border Force (lead)
- Department of Home Affairs
- Australian Criminal Intelligence Commission
- Australian Transaction Reports and Analysis Centre
- Commonwealth Director of Public Prosecutions and law enforcement partners.

Using the consolidated power of these government agencies, the taskforce fights back against organised international and local criminals that operate multimillion dollar crime syndicates.

Domestically grown tobacco

The ATO is responsible for domestically grown or manufactured tobacco. It's illegal to grow tobacco in Australia without the

appropriate excise licence. Currently, no one is licensed to grow or manufacture tobacco seed, plant or leaf for commercial sale or personal use.

We receive referrals from the ITTF, state law enforcement partners and tip-offs from industry and the community. We use the referrals to produce actionable intelligence to bring both civil and criminal consequences against those who engage in illicit tobacco.

However, organised crime syndicates continue to set up and run these growing operations, sometimes by targeting unsuspecting landowners, attempting to lease land to grow illicit tobacco. These operations are not run by genuine farmers or landowners, but by criminals living and operating in local communities.

Organised criminals who deal in illicit tobacco rob the Australian community of valuable revenue, instead:

- using their profits to fund their lavish lifestyles
- allowing them to continue to engage in criminal behaviour well beyond the sale of illegal tobacco.

Signs that someone is growing tobacco

Some of the signs that land is being used to grow, manufacture or produce illicit tobacco are:

- intense labour production between November and May
- people approaching real estate agents, landowners or farmers to lease land within or outside of the state they live in
- suspicious responses to online and print ads where land is being advertised for sale or lease
- unusual earthworks along creeks and rivers on private and public land
- an unusual source of loose tobacco
- unexplained and potentially unlawful use of water resources
- a strong tobacco odour
- large, leafy plants that, depending on the size, may resemble kale, cabbage or corn and may have a pink flower growing on top

- other suspicious activity.

'Under the counter' tobacco

Organised crime syndicates also target tobacco retailers across Australia to buy and sell illegally grown tobacco, also known as 'under the counter' or 'black market' tobacco.

Buying and selling illicit tobacco is a serious tax crime. Retailers choosing to become involved in the illicit tobacco trade not only contribute to the loss of funding for essential community services, but they also gain an unfair advantage over honest businesses who are doing the right thing. There are penalties for selling illicit tobacco.

Removing illicit tobacco from our streets creates a level playing field for all retailers.

Signs that someone is selling illicit tobacco

Some of the signs that tobacco retailers are selling 'under the counter' tobacco are:

- cigarettes, cigars or loose-leaf tobacco (sometimes referred to as 'chop-chop' or 'roll your own') are missing health warning labels
- strong tobacco odour despite the shop containing strongly scented items like candles and incense
- customers asking for 'cheap cigarettes' or 'under the counter cigarettes'
- customers leaving a retailer with small plastic bags, often black in colour.

Penalties

The government passed the Treasury Laws Amendment (Illicit Tobacco Offences) Bill which outlines a tobacco offence regime. The tax laws increased the set penalties to a level that provides greater deterrence to illegal activity. The penalty amount is calculated in multiples of a penalty unit. If the infringement occurred on or after 7 November 2024, the penalty unit amount is $330.

Table 2: Penalties by activity for illicit tobacco

Activity	Penalty
Possessing more than 2 and less than 5 kilograms	Civil penalty – a fine of up to $33,300
Possessing 5 kilograms or more	Criminal penalty – a criminal conviction with a prison sentence of up to 5 years or a fine between $66,000 and $330,000, or both
Selling illicit tobacco products	Criminal penalty – a criminal conviction with a prison sentence of up to 5 years or a fine between $66,000 and $330,000, or both
Buying illicit tobacco products	Criminal penalty – a criminal conviction with a prison sentence of up to 5 years or a fine between $66,000 and $330,000, or both
Manufacturing or producing illicit tobacco	Criminal penalty – a criminal conviction with a prison sentence of up to 10 years or a fine between $165,000 and $495,000, or both

Tobacco tax gap

The tobacco tax gap is the difference between the estimated value of excise or customs duty raised from tobacco according to the law ('tobacco duty') and the value actually raised for a financial year. The tobacco tax gap estimate includes illicit tobacco importation and 'chop-chop'.

For 2022–23, we estimate the net tobacco tax gap to be 14.3%. This equates to approximately $2.7 billion in lost excise revenue, meaning that $2.7 billion was channelled into organised criminal activities, instead of funding essential community services.

How to report it

If you suspect that illicit tobacco is being grown, manufactured or sold in your community you can report it anonymously to us by:

- making a tip-off
- phoning **1800 060 062**.

Keep up to date

Learn more about what illicit tobacco is and how we are fighting back. Discover and share our content.

- Illicit tobacco infographic (PDF, 469KB)
- Retail illicit tobacco infographic (PDF, 310KB)
- Illicit tobacco case studies

Media releases

- Targeted strike to illicit tobacco trade
- Criminal syndicate left reeling after massive illicit tobacco bust
- From whisper to warrant: $4.4 million of illicit tobacco seized
- Viper arrest 14 and seize $4.8m worth of illicit tobacco
- Putting the chop on illicit tobacco crops
- Crop goes up in smoke thanks to tobacco tip-off
- VIPER Taskforce execute 27 warrants and lay Commonwealth charge of directing a criminal organisation
- Lunar seize 11 firearms, cash and a further 3 tonnes of illicit tobacco worth over $6m
- Lunar seize almost seven tonnes of illicit tobacco worth over $12 million
- Tackling the root of the problem: $5.2 million of illicit tobacco destroyed
- Lunar and VIPER seize over $2 million of illicit tobacco products
- Multi-million dollar money laundering investigation smashes illicit tobacco and vape supply
- Third major illicit tobacco bust for Operation Junglevine2

- Operation Junglevine2 slashes second tobacco crop
- Investigation into illicit tobacco syndicate
- Tip-off pays off as illicit tobacco uprooted in joint raids
- ATO takes the shine out of Sunshine Coast illicit tobacco trade
- Transnational illicit tobacco crime groups disrupted as part of global action on illicit tobacco trade
- ATO burns a $52 million hole in illicit tobacco trade
- $5.1 million in illicit tobacco smoked out
- Operation Greyhound sniffs out $42 million in illicit tobacco

QC 54675

Refund fraud

Refund fraud occurs when people dishonestly claim refunds, rebates or offsets they aren't entitled to.

Last updated 11 February 2025

While most people do the right thing, the small number of people who engage in refund fraud will be held to account.

Examples of refund fraud

Refund fraud is claiming a tax refund or other benefit by giving us false information. It is more than a careless or accidental mistake because it is undertaken in a deliberate and deceitful way.

Refund fraud can also involve identity crime. This is where personal identity information is stolen and used to lodge fake refund claims in someone else's name.

Refund fraud can include:

- making false work-related expense claims

- providing fake information and documents, such as invoices and receipts
- lodging fraudulent returns using false or stolen identities
- claiming GST refunds through fraudulent business registrations.

If you've made an honest mistake or are falling behind on your obligations, we'll work with you to find a solution. But we'll hold people who deliberately set out to cheat the system to account. This could include administrative penalties, or even criminal prosecution.

Example: criminal conviction for fake donation deductions case study

A public servant falsely claimed to have spent more than $100,000 on gifts and donations. She was convicted and fined $10,000.

Over the course of 5 years, she claimed to make regular donations to an entity. The refunds were never paid out, as she was unable to support her claims. But in one instance, she tried to mislead our auditors by providing a false letter.

When we got in touch with the 'author', she had never seen the letter before. The ABN and signature were also incorrect.

During sentencing, the Magistrate noted that the defendant had continued to make false claims despite being audited several times, which was an escalation of criminal behaviour.

Example: fake invoices lead to prosecution case study

A man working in aged care claimed deductions for a different degree to the one he had undertaken. He received a criminal conviction, a $5,000 fine and was ordered to pay $3,000.

Over 3 years, he claimed almost $75,000 worth of work-related self-education expenses.

He gave his tax agent invoices that said he was studying a course. They even included a break-down of the subjects he was taking that semester.

But when we reached out to the university, it was clear the invoices had been changed. He was studying a different course, which did not relate to his employment. He wasn't entitled to claim the expenses.

Example: teacher convicted after producing 36 false documents case study

A teacher made an elaborate attempt to mislead our auditors. She received a criminal conviction, a $3,500 fine and was ordered to pay $10,000.

When we audited her tax returns, they included unusually high work-related travel, clothing and self-education expenses. We gave her the opportunity to amend her tax returns to reduce potential penalties. But instead of withdrawing the false claims, she produced 36 false documents to back them up.

The auditors quickly identified inconsistencies in the documents, including spelling mistakes and invalid phone numbers and ABNs. Checks with the companies in question confirmed the documents were fake.

Our approach to refund fraud

Refund fraud steals revenue that is used for the whole community and disadvantages Australians who do the right thing. We take it very seriously, and we have a range of controls and systems in place to detect potential refund fraud, including:

- analytical models that use behavioural and statistical algorithms to analyse information on tax returns, business activity statements and other tax forms

- strong data- and intelligence-sharing capabilities with our partners in Australia and overseas.

If you have information about suspected refund fraud, you can confidentially report it to us.

Learn more about how we keep the tax system fair for everyone by accessing our latest tax crime prosecution results and case studies.

GST refund fraud attempts

Learn about GST refund fraud and what to do if you become involved.

QC 33610

GST refund fraud attempts

Learn about GST refund fraud and what to do if you become involved.

Last updated 2 October 2025

GST refund fraud

We have identified a significant number of GST refund fraud attempts.

The attempted fraud involves an individual:

- inventing a fake business
- lodging a fraudulent Australian business number (ABN) application, and
- submitting fictitious business activity statements (BAS) to attempt to gain a false GST refund.

The fraudulent activity has been circulating as online advertising and content, particularly on social media. We are working with digital platforms to shut down this advertising.

Reminders for the community

Registering for an ABN and applying for GST refunds when you don't own or operate a business or are not eligible is fraud. Remember:

- The ATO does not offer loans. If you see someone advertising a way to get a loan from the ATO, it's not legitimate.
- The ATO does not administer COVID disaster payments.
- If you are **not** operating a business, you do not need an ABN, and you don’t need to lodge a BAS.
- Backdating your business registration so you can apply for a refund will flag you as high risk in our systems.
- False declarations may impact eligibility for other government payments.
- We have the data matching ability to detect these patterns and stop the fraud.
- You are liable to repay the entire amount of any fraudulently obtained GST refund, regardless of what you paid someone to lodge a BAS on your behalf.
- Selling or sharing your myGov credentials may result in other people accessing your personal information and using it for their financial gain.

If something seems too good to be true, seek independent advice from an adviser who has no connection to the arrangement before taking any action, or phone us.

What to do if you are involved

If you become involved in this arrangement, talk to us now. We'll be able to support you with a range of self-help options. You may be able to correct it yourself, we may be able to assist you, or we may refer you to a trusted advisor like a tax agent to help you.

We are urging anyone already involved to come forward now on a voluntary basis rather than face tougher consequences later. We will be recouping the funds, and there will be a better outcome for you if you come to us first.

Correct it yourself

You may be able to correct this yourself. You will need to follow the steps in this order:

1. Revise your activity statement
2. Cancel your ABN
3. Cancel your GST registration
4. Set up a payment arrangement

If you think your identity has been compromised

If you think you've become involved in this arrangement because your identity was compromised, phone us on **1800 467 033** to put additional controls on your account.

Tax fraud, evasion and crime is not victimless. It's a serious offence that takes money away from the community and essential services like health and education.

We take all reports of tax crime seriously. If you have any information to share, you can make a tip-off. You can make a report anonymously.

GST refund fraudsters are held to account

Refund fraud is claiming a tax refund or other benefit by providing false information to the ATO. It is more than a careless or accidental mistake because it is undertaken in a deliberate and deceitful way. We view GST refund fraud seriously. For some, this has resulted in prosecution or criminal charges as these dishonest individuals have found out.

GST fraud media releases

- False claims, real consequences for GST fraud
- ATO holds more GST fraudsters to account
- Concrete consequences for GST crooks
- From fake nails to fake GST claims
- Correcting the record on Operation Protego

- ATO and AFP crackdown on Op Protego promoters
- Taskforce takes further action on GST fraud
- GST fraud crackdown: ATO-led taskforce executes raids across the country
- ATO warns community: do not engage in GST fraud

Operation Protego

Sentencing details for Operation Protego, an ATO-led investigation into large-scale GST fraud.

QC 69474

Operation Protego

Sentencing details for Operation Protego, an ATO-led investigation into large-scale GST fraud.

Last updated 7 April 2026

About Operation Protego

Operation Protego is an ATO-led investigation into large-scale GST fraud that was promoted particularly on social media. The attempted fraud involves an individual:

- inventing a fake business
- lodging a fraudulent Australian business number (ABN) application, and
- submitting fictitious business activity statements (BAS) to attempt to gain a false GST refund.

In May 2022 we issued warnings to the community to be on the lookout for fraud schemes being promoted through social media and other channels. We advised those who were involved to come forward.

The most serious offenders of financial crime are referred to the ATO-led Serious Financial Crime Taskforce (SFCT), including individuals involved in Operation Protego. The SFCT is taking firm action against individuals, facilitators and promoters suspected of defrauding the community by inventing fake businesses to claim false GST refunds.

You need to check the facts – nobody is giving money away for free or offering loans that don't need to be paid back. Simply speaking, if you don't operate a business, you don't need an ABN, and you shouldn't lodge a BAS. This is fraud.

Individuals sentenced under Operation Protego will now have a criminal record which may impact their career prospects, ability to travel overseas and ability to obtain loans and insurances. The debt from the fraudulent GST refunds remains on their records and the ATO will continue to chase it down, which includes seizing any future refunds.

For those who may be tempted by the promise of big gains, the ATO has sophisticated risk models. We work with banks, law enforcement agencies and other organisations to share information and detect fraud. We also have access to intelligence through community tip offs, and other information sources. The SFCT 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.

Latest news

1 April 2026 – Zoe Ward sentenced to 2 years jail

Zoe Ward was sentenced in the Southport District Court to 2 years imprisonment after fraudulently obtaining over $50,000 in GST refunds, contrary to subsection 135.1(1) of the Criminal Code (Cth).

Ms Ward obtained an Australian business number (ABN), claiming that she was a sole trader conducting a business that offered beauty services or salon operations.

Between January to April 2022, Ms Ward facilitated the lodgment of 5 false business activity statements (BAS). She received $54,821 in fraudulent GST refunds and attempted to obtain a further $14,239 but these payments were stopped by the ATO.

A search warrant and audit concluded she was not carrying out a legitimate business, therefore she was not entitled to receive the GST refunds.

Ms Ward was released on $1000 recognisance, to be of good behaviour for 3 years and ordered to repay $52,409.15.

13 March 2026 – Aaron Hennig sentenced to 1 year and 2 months jail

Aaron Hennig was sentenced to 1 year and 2 months in jail for fraudulently obtaining more than $72,068 and attempting to obtain a further $48,035 in fraudulent GST refunds.

Mr Hennig was charged with:

- one count of obtaining a financial advantage by deception contrary to section 134.2(1) of the Criminal Code (Cth), and
- one charge of attempting to obtain a financial advantage by deception contrary to sections 134.2(1) and 11.1 of the Criminal Code (Cth).

Mr Hennig reactivated his ABN and registered for GST, claiming to run an antique furniture restoration business. He then lodged 9 false business activity statements (BAS), allowing him to obtain the fraudulent GST refunds into his personal bank accounts.

Thanks to strong partnerships between the ATO and financial institutions, Mr Hennig's bank identified the unusual deposits and referred the matter to the ATO. This prompted an ATO audit and search warrant later executed as his residence.

During the search, the records, documents, and items found showed that Mr Hennig was not running a legitimate business.

Mr Hennig is to be released after having served three months' imprisonment on a recognisance release order, to be of good behaviour for 2 years with 12 months supervision, a security of $500 with a non-parole period of 3 months and a 1-year post release supervised good behaviour bond.

Mr Hennig has been ordered to repay the amount of $52,817.

24 October 2025 – Michael Neal Mitchell sentenced to 1 year and 11 months jail

Michael Neal Mitchell was sentenced to 1 year and 11 months jail in the Penrith District Court for dealing with the proceeds of indictable crime contrary to subsection 400.4(1) of the Criminal Code (Cth). He will be released on a recognisance release order on 11 September 2026.

Mr Mitchell had an Australian business number (ABN) registered to him for a goods transportation business. The ABN was also registered for GST and fuel tax credits. His registration indicated that he used both diesel and petrol fuel in a vehicle with a gross vehicle mass (GVM) greater than 4.5 tonnes.

Twenty-two false business activity statements (BAS) were lodged under his name. GST refunds were paid for 9 of these lodgments with Mr Mitchell receiving over $108,289 before the other lodgments were stopped by the ATO.

During the investigation process, it was discovered that Mr Mitchell spent the money on personal expenses, transferred to other bank accounts in his name or withdrawn as cash. No funds were spent on business related activities. It was also found that he did not have a licence that would permit him to drive vehicles with a GVM of more than 4.5 tonnes. Nor did he have a vehicle registered in his name with a GVM greater than 4.5 tonnes.

The ATO determined that Mr Mitchell was not operating a business and therefore was not entitled to the GST refunds.

7 October 2025 – Kaleisha Henrick sentenced to 6 months jail

Kaleisha Henrick was sentenced to 6 months jail in the Launceston Magistrates Court after being charged with 2 counts of obtaining a financial advantage by deception contrary to subsection 134.2(1) of the Criminal Code (Cth).

In 2021, an Australian business number (ABN) for a fictitious plastering business was set up in Ms Henrick's name. Shortly after, 2 business activity statements (BAS) were lodged, resulting in over $38,000 in GST refunds being paid to her bank account. During an ATO audit, Ms Henrick claimed that a third party had set up the ABN on behalf and she had agreed to transfer portions of the refunds to this person. It was determined that she was not running a legitimate business and therefore she was not entitled to the refunds.

The presiding judge noted that Ms Henrick displayed a lack of insight into the seriousness of the offence. The judge also observed that the fraud was deliberate but didn't occur over a long period of time, it was more opportunistic than planned.

Ms Henrick has been ordered to repay the full amount of $38,901.

7 August 2025 – Sharni Lipscombe sentenced to 3 and a half years jail

Sharni Lipscombe was sentenced in the Beenleigh Magistrates Court to 3-and-a-half years imprisonment for 14 counts of obtaining a financial advantage by deception contrary to section 134.2(1) of the Criminal Code (Cth) and a further 2 years imprisonment for 3 counts of attempting to obtain a financial advantage by deception contrary to sections 134.2(1) and 11.1(1) of the Criminal Code (Cth). All sentences were to be served concurrently, and a non-parole period of 12 months was fixed.

Ms Lipscombe obtained an Australian business number (ABN), claiming she was providing beauty services or a salon operation business. Between October 2021 and May 2022, she lodged 17 fictitious business activity statements (BAS), dishonestly receiving over $269,000 in GST refunds and attempting to obtain a further $86,331.

An ATO audit found that Ms Lipscombe claimed over $4.4 million in purchases and over $448,544.50 in sales during the lodgment period. Internet searches returned no evidence of an online presence or advertising for her business.

Ms Lipscombe has been ordered to repay $269,393.

For more information, see False claims, real consequences for GST fraud.

4 August 2025 – Jade Parviainen sentenced to 22 months jail

Jade Parviainen was sentenced to 22 months jail in the Melbourne County Court. She was charged with 8 counts of obtaining a financial advantage by deception contrary to section 134.2(1) of the Criminal Code (Cth) and one count of attempting to obtain a financial advantage by deception contrary to sections 11.1 and 134.2(1) of the Criminal Code (Cth).

She is to be released immediately on a recognisance release order to be of good behaviour for 2 years.

Ms Parviainen has been ordered to repay $230,720.

In August 2021, Ms Parviainen registered for an Australian business number (ABN) for a Dental Laboratory. Over the following months, she lodged 9 business activity statements (BAS) and dishonestly obtained over $230,000 in GST refunds and attempted to obtain a further $49,947.

For more information see, False claims, real consequences for GST fraud.

1 August 2025 – Samantha Olson sentenced to 18 months jail

Samantha Olson was sentenced to 18 months jail in the Southport District Court. Ms Olson was charged with one count of obtaining a financial advantage by deception contrary to section 134.2(1) of the Criminal Code (Cth) and one charge of attempting to obtain a financial advantage by deception contrary to sections 11.1 and 134.2(1) of the Criminal Code (Cth).

She will be released after serving 6 months in custody, on the condition that she be of good behaviour for 2 years and has been ordered to repay $20,000 to the ATO within one week of the sentencing date.

Ms Olson was also ordered to repay the remaining $119,834.

Ms Olson registered an Australian business number (ABN) for a party planning business that was direct selling beauty products. From October 2021, and over the following 8 months, Ms Olson submitted 15 fictitious business activity statements (BAS). She claimed $139,834 in GST refunds that she was not entitled to and attempted to obtain a further $17,336 which was stopped by the ATO.

The ATO conducted an audit and discovered that Ms Olson claimed she made purchases in excess of $1.8 million with little to no income reported. After analysing her bank accounts, it was discovered that the refunds were swiftly withdrawn, transferred to friends, or spent on items such as furniture or for food and general shopping expenses.

An ATO audit found no evidence suggesting Ms Olson was running a business, and therefore was not entitled to the GST refunds she had

claimed.

For more information see, False claims, real consequences for GST fraud.

29 July 2025 – Bryce Nutley sentenced to 18 months jail

Mr Bryce Nutley was sentenced to 18 months jail after being charged with 3 counts of dishonestly obtaining a gain from the Commissioner of Taxation between 15 February 2022 to 27 May 2022, contrary to section 135.1(1) of the Criminal Code (Cth). He will be released immediately on the condition that he be of good behaviour for 2 years.

He received reparation orders for the total amount he stole. He was required to pay $2,000 prior to leaving the courthouse with the monies being forwarded to the ATO, pay a further $8,000 within 15 months of the sentencing date, and must pay back the remaining $39,600.

In February 2022, Mr Nutley registered for an Australian business number (ABN), claiming to be a sole trader providing 'lawn mowing or care' services.

Over the next 4 months, a total of 6 false BAS were lodged in his name.

An ATO audit found no evidence of genuine business activity records, or operational assets. Instead, funds were misused on sports betting, retail purchases, food delivery services, and transfers to family members and friends, including others who have also been sentenced for their involvement in the scheme. Ms Nutley (the accused's sister), Ms Pakatyilla, and Ms Hoek have previously been sentenced under Operation Protego for their roles in the broader fraud scheme.

For more information see, False claims, real consequences for GST fraud.

7 July 2025 – Kim Orense sentenced to 18 months jail

MrKim Orense was sentenced to 18 months in jail in the Penrith Local Court for dealing with the proceeds of indictable crime contrary to subsection 400.4(1) of the Criminal Code (Cth). He is to be released after serving 10 months upon entering into a recognisance release order of $1 to be of good behaviour for 2 years.

Mr Orense obtained an Australian business number (ABN), claiming that he was conducting a business that offered household repair services.

Between October 2021 and April 2022, Mr Orense lodged 14 false business activity statements (BAS). He received $214,011 in fraudulent GST refunds and transferred these funds to other bank accounts or associates, including Abigail Ussher, his former partner, who has also been sentenced under Operation Protego.

A search warrant was executed at Mr Orense's residence. No business records, invoices, tools or equipment were found. The search concluded that he was not carrying out a legitimate business.

For more information, see ATO holds more GST fraudsters to account.

7 July 2025 – Abigail Ussher sentenced to 12 months jail

Ms Abigail Ussher was sentenced to 12 months in jail in the Penrith Local Court for dealing with the proceeds of indictable crime contrary to subsection 400.4(1) of the Criminal Code (Cth). She is to be released after serving 5 months upon entering into a recognisance release order of $1 to be of good behaviour for 2 years.

Ms Ussher obtained an Australian business number (ABN) for a business that provided crime scene cleaning services. She subsequently lodged 3 original and 4 revised business activity statements (BAS) claiming GST refunds.

Upon receiving the funds, Ms Ussher transferred them to personal accounts, or other third parties. She transferred funds to Kim Orense, her former partner, who has also been sentenced under Operation Protego.

A search warrant concluded she was not carrying out a business as no business records, invoices or specialist cleaning equipment was found in her residential premises.

For more information see, ATO holds more GST fraudsters to account.

16 June 2025 – Tewhanaupani Nukunuku sentenced to 2 years and 3 months jail

Mr Tewhanaupani Nukunuku was sentenced in the Melbourne County Court to 2 years and 3 months in jail with a non-parole period of

9 months after obtaining $168,000 in GST refunds and attempting to obtain a further $100,000 which was stopped by the ATO.

Mr Nukunuku claimed to operate a concreting business and lodged 8 false business activity statements (BAS) over a 6-month period.

An initial ATO audit, concluded Mr Nukunuku was not running a legitimate business, it was also discovered that Mr Nukunuku did not hold a registration or license to do the work he claimed he was doing.

A second audit found that he had spent the funds on luxury items including accommodation at hotels and serviced apartments, travel, retail shopping, and entertainment.

Mr Nukunuku will be released after serving 9 months on recognisance release order requiring him to give security in the sum of $1,000 on condition he be of good behaviour for 2 years.

For more information, see Concrete consequences for GST crooks.

12 June 2025 – Daniel Copeland sentenced to 3 years jail

Mr Daniel Copeland was sentenced to 3 years in jail in the Newcastle District Court contrary to section 134.2(1) of the Criminal Code (Cth) for fraudulently obtaining over $1.1 million in GST refunds.

Mr Copeland obtained an Australian business number (ABN) and claimed he provided plastering services. He then submitted 23 false business activity statements (BAS) which allowed him to receive fraudulent GST refunds totalling $1,134,163.37.

Mr Copeland used the funds for gambling, personal living expenses, accommodation, purchases at a car dealership and cash withdrawals.

An ATO audit was unable to identify any evidence of a legitimate business during the offending period, therefore Mr Copeland was not entitled to any of the GST refunds he claimed.

He was released on $100 recognisance, to be of good behaviour for 5 years and ordered to repay the full $1.1 million.

For more information, see Concrete consequences for GST crooks.

5 June 2025 – Darnelle Te Kiri sentenced to 17 months jail

Ms Darnelle Te Kiri was sentenced to 17 months imprisonment in the Melbourne County Court contrary to section 134.2(1) of the Criminal Code (Cth) for fraudulently obtaining $202,936 through false business activity statements (BAS).

In 2021, Ms Te Kiri registered an Australian business number (ABN) for hospitality and bar work services and lodged 8 false BAS over 7 months, claiming to have spent over $2 million in purchases despite reporting little to no income. An ATO audit found no evidence of a legitimate business.

The funds were spent on rent, groceries, pubs and gaming, ATM withdrawals, and transfers to third parties and international money services. She was released immediately on $1,000 recognisance, to be of good behaviour for 2 years and ordered to repay the full $202,936.

For more information, see Concrete consequences for GST crooks.

20 May 2025 – Gregory Pimm sentenced to 2 years 6 months jail

Gregory Pimm was sentenced to 2 years and 6 months jail for obtaining a financial advantage by deception, and 2 years for attempting to obtain a financial advantage by deception. These sentences are to be served concurrently. He is to be released on a recognisance order of $500 after serving 6 months imprisonment. As a conditions of the recognisance, he is also required to be of good behaviour for 3 years and subject to the supervision of a probation officer for 2 years.

Mr Pimm reactivated an Australian business number (ABN) for a road freight transport operation. Between February and October 2022, he lodged 37 false business activity statements (BAS). He obtained $167,690 in GST refunds and attempted to obtain a further $302,825 in fraudulent GST refunds which was stopped by the ATO.

He falsely reported his total sales, the GST collected on the sales, GST on purchases made and GST credits the ATO owed him. The ATO noticed the inconsistencies in his reporting and initiated an investigation which found he wasn't running a business and wasn't entitled to any GST refunds.

Mr Pimm has been ordered to repay the amount of $167,690.

For more information, see From fake nails to fake GST claims.

20 May 2025 – Skye Hoek sentenced to 3 months jail

Skye Anne Hoek was sentenced to 3 months jail after fraudulently obtaining $25,147 in GST refunds. She was charged with one count of obtaining a financial advantage by deception. Her friend, Ms Nutley, was sentenced earlier this month on similar charges.

Ms Hoek obtained an Australian business number (ABN), claiming to be running a retail business. She provided her myGov sign in details to another individual and gave them permission to lodge the business activity statements (BAS). Two false BAS were lodged in her name, allowing her to obtain the funds.

An ATO search warrant was executed at Ms Hoek's residence, where investigators found no evidence she was running a legitimate retail business. An ATO audit and internet search later concluded she was not operating a business and not entitled to any GST refunds.

The ATO has begun reclaiming the funds Hoek obtained. Initially, the bank froze $23,666 as they suspected it was fraud. Those funds were recovered by the ATO through garnishee action. Further funds were recovered through her income tax returns. She has received reparation orders for the remaining debt of $780.

For more information, see From fake nails to fake GST claims.

2 May 2025 – Tiarn Nutley sentenced to 9 months jail

Tiarn Nutley was sentenced to 9 months jail after being charged with one count of dishonestly obtaining a financial gain. She will be released immediately on a recognisance release order of $2,000 and is required to be of good behaviour for 12 months.

Ms Nutley obtained an Australian business number (ABN) for a business she claimed provided beauty and salon services.

An existing ABN was used to claim GST refunds. Ms Nutley provided her myGov sign in details to Skye Hoek and another friend. The 2 friends then arranged to lodge 6 false business activity statements in Ms Nutley's name, allowing her to dishonestly obtain $49,700 in GST refunds. There was an attempt to claim a further $25,000, but this was stopped by the ATO.

Following a search warrant and an ATO audit, it was concluded Ms Nutley was not running a legitimate business and therefore not entitled to any GST refunds. During additional warrant activity, Ms Nutley said she paid $9,000 from each refund to Ms Hoek as payment for organising the lodgments.

Ms Nutley has been ordered to repay the amount of $49,700.

For more information, see From fake nails to fake GST claims.

15 April 2025 – Joshua Merrett sentenced to 2 years 11 months jail

Joshua Merrett was sentenced to 2 years and 11 months jail. He is to be released after serving one year and 8 months, upon entering into a recognisance release order of $1,000, and to be of good behaviour for 2 years. He was charged with one count of obtaining a financial advantage by deception and one count of attempting to obtain a financial advantage.

He was also charged with one count of failing to comply with an order, as he did not provide his iPhone passcodes within 7 days to the Australian Federal Police after they seized his phone.

In June 2019, Mr Merrett registered for an Australian business number (ABN) for a business specialising in staircase manufacturing and repairs and antique furniture repairs. Between June 2021 and June 2022, he lodged 31 business activity statements (BAS). This resulted in $394,801 in refunds within a 3-month period, which triggered an audit and account lockdown. He attempted to obtain a further $336,193.

Mr Merrett tried to avoid ATO auditors but could not escape the consequences of his deceptive actions, as 2 months after the last GST refund was paid ATO investigators and Australian Federal Police conducted a search warrant at his residence.

The search found no evidence of any commercial activity, or sales or purchases consistent with running a business. However, they did discover evidence that identified another offender, who now finds themselves in court facing similar charges.

Mr Merrett will now have a criminal record and received reparation orders leaving him with a debt of $392,917. It may also impact his career prospects, ability to travel overseas and ability to obtain loans and insurances.

For more information, see Stairway to jail over GST fraud.

2 April 2025 – Kristopher Andree-Jansz sentenced to 4 years 7 months jail

Kristopher Andree-Jansz was sentenced to 4 years 7 months jail after he claimed $2,402,258 in GST refunds which he was not entitled to and attempted to claim a further $323,694.

He was charged with 24 counts of obtaining a financial advantage by deception and 3 counts of attempting to dishonestly obtain a financial advantage by deception. He has a non-parole period of 2 years 7 months and has been ordered to repay $2,402,258 million.

This debt is inescapable, the individual will now have a debt against their account and interest will continue to apply. Any refunds will be offset immediately to repay the debt.

Mr Andree-Jansz applied for an Australian business number (ABN) claiming he was a sole trader providing plumbing services. Between March 2021 and February 2022, Mr Andree-Jansz lodged a total of 35 business activity statements (BAS), claiming his business had made nearly $30 million worth of purchases.

An ATO audit found no evidence to suggest Mr Andree-Jansz was running a real business. Instead, he was found spending the fraudulently claimed refunds on personal luxury purchases.

For more information, see Victorian man slips up over $2.4 million fraud.

18 March 2025 – Jessica Pakatyilla sentenced to 2 years jail

Jessica Pakatyilla was sentenced to 2 years jail after being charged with 2 counts of obtaining a financial advantage by deception, and one count of attempting to dishonestly obtain a financial advantage by deception. She is to be released immediately on a recognisance order of $500, and to be of good behaviour for 2 years.

In 2022, Ms Pakatyilla lodged 6 business activity statements (BAS) for a fake business that claimed to be providing babysitting services. She claimed $49,700 in GST refunds that she was not entitled to and attempted to obtain a further $24,600 which was stopped by the ATO.

An ATO audit concluded Ms Pakatyilla was not operating a legitimate business, and instead used the fraudulently obtained funds for clothing, travel, and food purchases.

Ms Pakatyilla was also ordered to pay reparation of $49,700.

25 February 2025 – Benjamin West sentenced to 2 years jail

Benjamin West has been sentenced to 2 years jail. He is to be released after serving 6 months in custody, on a recognisance release order of $500, and to be of good behaviour for 2 years. Mr West was also ordered to pay reparation of $49,226.

In February 2022, Mr West applied for an Australian business number claiming he was providing garden and lawn maintenance services. He then knowingly provided his myGov sign in details to a third party who lodged 6 business activity statements, allowing Mr West to fraudulently obtain $49,226 in GST refunds before attempting to obtain a further $25,060 which was stopped by the ATO.

An audit by the ATO determined that he was not operating a legitimate business, and therefore not entitled to the GST refunds he had claimed.

17 February 2025 – Adam Hohenberger sentenced to 2 years and 3 months jail

Adam Hohenberger was sentenced to 2 years and 3 months in jail for committing GST fraud. He is to be released after serving 8 months in custody, on a recognisance release order. He must be of good behaviour and be supervised by a probation officer for 19 months.

Mr Hohenberger was charged with 22 counts of obtaining a financial advantage by deception and 16 counts of attempting to obtain a financial advantage by deception.

In May 2020, an Australian business number (ABN) was created for a construction repair business in Mr Hohenberger's name. In 2022, he lodged 98 business activity statements (BAS) receiving over $108,000 he was not entitled to.

During the audit process it was discovered that Mr Hohenberger did not have the skills required to repair construction machinery and therefore he was not operating a legitimate business.

Mr Hohenberger was also ordered to repay $108,451 to the ATO.

QC 73209

Organised crime

What is organised crime, it's impacts and how the ATO takes action to tackle criminal activities.

Last updated 11 February 2025

Organised crime impacts the lives of Australians in many ways. It is a national security threat that is destructive, pervasive and sinister, costing Australia up to $68.7 billion each year.

Organised crime explained

Organised crime can involve a range of criminal activities such as:

- illicit drug activity and illicit tobacco
- tax or other financial crime
- identity or cybercrime
- money laundering
- crimes against people (such as human trafficking).

Organised crime is transnational in nature, technology-enabled and increasingly functions as a business relying on professionals to help launder ill-gotten gains by setting up structures to place, layer and integrate funds.

Serious and organised crime harms our community, economy, government and way of life. Defrauding the tax and superannuation systems is not victimless and deprives the community of funding for essential services such as hospitals, schools and roads.

Tackling organised crime

The ATO contributes to Australia's Commonwealth Organised Crime Strategic Framework tackling organised crime and reducing harm to the community. The Framework sets out a coordinated and cohesive whole-of-government approach to address the significant threats from organised crime.

As part of our shared responsibility under the Framework, we take action to counter the impact of serious and organised crime on the tax and super systems.

We do this by:

- targeting known business models used to facilitate tax crime such as:
  - complex financial structures to conceal wealth
  - infiltration of legitimate industries by organised criminals
  - phoenix activity
  - refund fraud
  - abuse of offshore secrecy havens
  - concealment of income or assets offshore
  - intermediaries facilitating the use and abuse of offshore structures and accounts
- working with state, Commonwealth and international law enforcement partners to share intelligence and coordinate strategies targeted at disrupting serious criminal behaviour
- applying differentiated enforcement approaches to those who facilitate serious and organised crime, focusing on ensuring the correct amount of tax is reported and paid on all income, including profits derived from illegal activity.

We have the resources, data-matching capability and intelligence-sharing relationships, under the Commonwealth Organised Crime Strategic Framework, to bring even the most serious organised criminals to account.

Where we identify concerns about suspected tax fraud or evasion, we undertake audits, raise assessments, apply penalties and take firm debt recovery action. Our data holdings include:

- property, other asset sales and purchases

- Australian Securities and Investments Commission (ASIC) and Australian Business Register (ABR) information
- motor vehicle data
- share transactions
- bank interest, dividend and Australian Transaction Reports and Analysis Centre (AUSTRAC) data
- migration data
- foreign income data.

Our approaches under the Framework include:

- coordinated targeting of organised crime in conjunction with other state and Commonwealth law enforcement agencies
- demanding lodgment of outstanding income tax returns and business activity statements
- pursuing civil debt recovery action against outstanding debt of key individuals, their business entities and family associates
- undertaking audit activities in relation to income tax, GST, superannuation and Pay As You Go Withholding (PAYGW) obligations
- supporting criminal investigations against those involved in tax crime
- asset restraint and forfeiture using proceeds of crime actions through the joint agency Criminal Asset Confiscation Taskforce (CACT).

We also have an increased focus on:

- working with our international partners including the Joint Chiefs of Global Tax Enforcement (J5) to disrupt those who enable international tax evasion, tax crime and money laundering
- targeting those who use technology to commit tax crime such as cybercrime
- coordinating action through the many taskforces in which we are a key participant such as the Serious Financial Crime Taskforce (SFCT), the CACT and the National Anti-Gangs Squad (NAGS)

- supporting Commonwealth programs such as the Trusted Digital Identity Framework.

Case studies

Our organised crime case studies reinforce that we are committed to disrupting, investigating and penalising the perpetrators of organised crime – there is no place to hide.

QC 33618

Villain Academy

A video game about unscrupulous infiltration.

Last updated 7 November 2025

We all know that integrity is central to building a high-performing and trusted Australian Public Service (APS). To embed integrity well, it is essential to not only apply the 'rules', but to know how to make ethical and defensible decisions in a range of situations.

To help APS employees build awareness about the subtleties of grooming, the ATO is pleased to share our Villain Academy interactive video game. The game is an exciting initiative that challenges ATO staff to 'choose their own adventure' by stepping into the shoes of a villain and attempt to infiltrate the ATO.

The game is designed to test skills and judgment, show you the darker side of human nature, and the consequences of your choices. In 15 minutes, players gain insights about how to stay alert to the risks and vulnerabilities of grooming and how to protect themselves and others from fraud and corruption risks. The Villain Academy game comes with a support guide (PDF, 185KB), which is designed to work together with the game, and provide more detailed information on the themes covered. A manager guide (PDF, 185KB) is also available to help you lead discussions and generate conversations with your team.

Test yourself or your team by playing Villain Academy now or if you use screen reading software, you can download the Villain Academy

accessible version (DOCX 96.7KB)

Note: Villain Academy is an ATO learning resource. Scenarios are fictional and developed to raise awareness of fraud and corruption risks. ATO specific hyperlinks referred to in the game and guides will not open for users outside the ATO.

For further information about these resources contact the ATO's Fraud Prevention and Internal Investigations team.

QC 73790

DAISIE

Play 'DAISIE', an interactive game of ethics and flawed logic.

Published 18 February 2026

About DAISIE

Integrity is the foundation of a high-performing and trusted Australian Public Service (APS). But integrity isn't just about following the rules, it's about making sound, ethical decisions in complex and sometimes ambiguous situations.

To support APS employees in building their integrity capability, the ATO is excited to introduce DAISIE: the Developmental Artificial Intelligence for Situational Integrity and Ethics, our interactive game that puts your ethical reflexes to the test.

DAISIE isn't just another training module. She's a slightly glitchy AI with a sarcasm chip and a mission: to observe your human decision-making and judge it. Harshly.

Why play DAISIE

Because integrity starts with each of us. In this interactive game, you'll face dilemmas that are just a little too relatable as you help DAISIE

calibrate her decision-making matrix.

DAISIE will challenge your thinking and through her attempts at humour might even teach you something about the importance of integrity and human oversight along the way.

Expect glitchy sarcasm, unexpected twists, and a few uncomfortable truths. Prepare to face the consequences, because DAISIE doesn't hold back.

Plus, it's fun. Let's be honest, when was the last time training made you laugh?

Take just 15 minutes and dive in today, explore the scenarios, and see how your decisions stack up.

Together, we can fight fraud with integrity.

Play DAISIE

DAISIE is paired with a DAISIE Support guide (PDF, 227KB) to help you navigate ethical dilemmas. The game and guide are designed to work together. There's also a DAISIE Manager discussion guide (PDF, 229KB) to spark team conversations about integrity in everyday work.

Play DAISIE now

If you use screen-reading software or need a transcript, download the DAISIE accessible version (PDF, 120KB).

DAISIE logo.**Note:** DAISIE is an ATO learning resource. ATO-specific hyperlinks referred to in the game and guides will not open for users outside the ATO.

For further information, contact the Fraud Prevention and Internal Investigations team.

QC 106153

Illegal phoenix activity

Find out what illegal phoenix activity is, the warning signs, how to protect yourself and how to report a company.

Last updated 13 October 2025

About illegal phoenix activity

Watch:

Media: Protect yourself from illegal phoenix activity (ato.gov.au) https://tv.ato.gov.au/media/bd1bdiuba5ynip (**Duration:** 00:33)

Illegal phoenix activity is when a company is liquidated, wound up or abandoned to avoid paying its debts. A new company is then started to continue the same business activities without the debt.

Illegal phoenix activity can occur in any industry or location. However, it is particularly prevalent in the following industries:

- property and construction
- labour hire
- security
- regional Australia – mining, agriculture, horticulture, and transport.

Phoenixing causes significant harm to the community because:

- Employees miss out on wages, superannuation and entitlements.
- Other businesses are put at a competitive disadvantage.
- Suppliers or sub-contractors are left unpaid.
- The community misses out on revenue that could have contributed to community services.

The economic impact of illegal phoenix activity on business, employees, and government is estimated to be $4.89 billion annually. This amount includes the:

- cost to business from unpaid creditors of $3,300 million
- cost to employees through unpaid entitlements of $155 million
- cost to government of $1,440 million.

Warning signs of illegal phoenix activity

Media: Protect your business from illegal phoenix activity https://tv.ato.gov.au/media/bd1bdiunjhxr4c (**Duration:** 00:33)

There are warning signs that indicate when a business may be involved in illegal phoenix activity. See our tips for:

- Employers – how to protect your business from phoenix companies
- Employees – how to check if the business you work for could be phoenix.

What to look for when running a business

When running your own business you can take steps to protect yourself from other businesses that may be wound up or closed. Look out for any of the following behaviours from a company you are working with:

- quotes that are lower than market value
- company directors who have been involved with liquidated entities before
- requests for payments to a new company
- changes to a company's directors and name, while the manager and staff remain the same.

Before you work with another business

Before you work with a business, check them out thoroughly by:

- confirming they are registered and their Australian business number (ABN) is valid at ABN Lookup
- searching the ASIC Connect registers to check they are
  - a registered entity
  - not in liquidation or external administration
- asking for references
- doing a credit check on them
- searching online to see if the company and its directors have any negative media reports

- reviewing your terms of trade, such as
  - asking for upfront payments, cash on delivery or payments in instalments
  - ensuring you're taking a large enough deposit.

Avoid illegal phoenix advice

If your business is insolvent or struggling to pay its debts, it's important to seek specialist advice from a qualified and registered insolvency practitioner.

Registered liquidators and trustees will provide you with sound legal advice that you can rely on. Be wary of other insolvency advisers who suggest actions designed to help directors avoid paying their creditors.

What to look for if you're an employee or contractor

If you're working for a company, look out for any warning signs that your employer may be involved in illegal phoenix activities, such as:

- You don't receive a payslip.
- The company ABN and name changes, but the phone number or address stays the same.
- Your super or other employment entitlements are not being paid.
- Your pay is late, less than what it should be or you are being paid under the minimum wage.
- Your payslip records a different employer name to whom you believe you work for.

You can protect yourself by:

- checking your super is being paid
- checking your payslip for changes to your employer's name or information
- if you are being paid irregularly, asking why and contacting the Fair Work Ombudsman for advice
- searching the company online to check for any negative coverage.

Visa holders

If you're working in Australia on a subclass 482 temporary skill shortage (TSS) visa or subclass 457 temporary work (skilled) visa, you must be working for your sponsor business.

If you are working for a different business, you may be missing out on employee entitlements or being paid less than the award rate.

See the Fair Work Ombudsman resources to help you check your workplace rights and entitlements.

Report illegal phoenix activity

We're working with other government agencies through the Phoenix Taskforce to stamp out illegal phoenix activity.

You can help us stop illegal phoenix activity by reporting it. If you know of or suspect phoenixing, report it to us by:

- completing a tip-off form
- phoning **1800 060 062**
- emailing phoenixreferrals@ato.gov.au.

We take all reports seriously.

Due to privacy laws, we can't give you any updates or tell you the outcome of the information you provide.

You can also:

- Report unpaid super contributions from my employer to the ATO.
- Phone the Department of Employment Workplace Relations Fair Entitlements Guarantee hotline on **1300 135 040** to get help claiming unpaid employment entitlements if you lose your job due to liquidation or bankruptcy of your employer.
- Contact the Fair Work Ombudsman on **13 13 94** for advice about minimum wages and conditions of employment.
- Make an online enquiry to the Australian Securities & Investment Commission to get advice on making a claim against your employer if they've been placed in liquidation.

Media releases

- Cycle ends in jail time for illegal phoenix operators – ATO media release, 9 September 2021.

Authorised by the Australian Government, Canberra.

Phoenix Taskforce

The Phoenix Taskforce brings federal, state and territory agencies together to combat illegal phoenix activity.

Insolvency advice and illegal phoenix activity

Some insolvency advisers promote illegal phoenix activity. Find out what kind of advice to look out for.

QC 33609

Phoenix Taskforce

The Phoenix Taskforce brings federal, state and territory agencies together to combat illegal phoenix activity.

Last updated 4 February 2026

Media: Protect yourself from illegal phoenix activity https://tv.ato.gov.au/ato-tv/media?v=bd1bdiuba5ynip (**Duration:** 0:33)

About the Phoenix Taskforce

The Phoenix Taskforce was established in 2014 to detect, deter and disrupt illegal phoenixing.

We provide education and advice on how businesses can protect themselves and not break the law. We also work with specific

industries and supply chains to close off opportunities.

Phoenix Taskforce agencies share information and use sophisticated data-matching tools to identify those promoting or engaging in illegal phoenix activity.

We take action against phoenix operators by:

- working together to disrupt their business model and make it financially unviable
- removing their ability to operate
- applying financial penalties
- prosecuting the worst offenders.

The most serious cases are referred to the Serious Financial Crime Taskforce.

There are civil and criminal offences for those who promote or engage in illegal phoenix activity. This includes penalties for removing assets to hide them from creditors when a company is wound up. ASIC and liquidators also have additional powers to recover assets for the benefit of employees and other creditors.

Where we suspect phoenix activity we can also:

- estimate liabilities for businesses that aren't meeting their lodgment obligations
- make directors personally liable under the director penalty regime for their company's liabilities
- retain refunds where a business has failed to provide an outstanding notification (that is, they don't lodge).

You can report suspected illegal phoenix activity by making an anonymous tip-off.

We're verifying the identity of directors through the director identification number (director ID) initiative. This initiative is:

- helping to prevent the use of false and fraudulent director identities
- making it easier for government regulators to trace directors' relationships with companies over time to help better identify and eliminate director involvement in unlawful activity.

Additional funding

Along with ASIC, we've received additional resources to help target facilitators and pre-insolvency advisers.

We're continuing to work with ASIC to establish better data sharing and improved analytics capability. This includes establishing the Phoenix Compliance Program, a key initiative within our compliance strategy, to target individuals who promote and facilitate illegal phoenix activity.

Phoenix Taskforce results

Up until 31 December 2025, our Phoenix Compliance Program has raised more than $3.12 billion in liabilities from audits and reviews of illegal phoenix activities. We've also returned more than $1.35 billion to the community.

Achievements for 2025–26

In 2025–26, we:

- Completed over 547 audits and reviews.
- Collected more than $108 million in cash, contributing to government spending on essential services.
- Received more than 1,843 referrals of suspected illegal phoenix activity through the Tax Integrity Centre.
- Shared 44 disclosures of information between agencies, helping identify those engaging in or promoting illegal phoenix activity.

Phoenix Taskforce members

The Phoenix Taskforce is made up of key federal, state and territory government agencies.

The current members are:

- ACT Revenue Office
- Attorney-General's Department South Australia, Consumer and Business Advice
- Australian Border Force

- Australian Criminal Intelligence Commission
- Australian Federal Police
- Australian Financial Security Authority
- Australian Securities & Investments Commission
- Australian Taxation Office
- Australian Transaction Reports and Analysis Centre
- Building Commission NSW
- Clean Energy Regulator
- Consumer Affairs Victoria
- Department of Climate Change, Energy, the Environment and Water
- Department of Employment and Workplace Relations
- Department of Local Government, Industry Regulation and Safety
- Department of Treasury and Finance WA
- Department of Treasury and Finance South Australia (Revenue SA)
- Department of Health, Disability and Ageing
- Environment Protection Authority SA
- Environment Protection Authority Tasmania
- Environment Protection Authority Victoria
- Fair Work Ombudsman
- Labour Hire Authority Victoria
- NSW Environment Protection Authority
- NSW Fair Trading
- NSW Long Service Corporation
- NSW Police Force
- NSW State Insurance Regulatory Authority

- Queensland Building and Construction Commission
- Queensland Department of Environment, Tourism, Science and Innovation
- Queensland Office of Industrial Relations
- Queensland Revenue Office
- Return to Work SA
- Revenue NSW
- State Revenue Office of Tasmania
- State Revenue Office VIC
- Territory Revenue Office NT
- Victorian Building and Plumbing Commission
- Victorian Legal Services Board and Commissioner
- Victoria Police
- Western Australia Police Force
- WorkCover Queensland
- WorkSafe ACT
- WorkSafe Victoria

QC 51054

Insolvency advice and illegal phoenix activity

Some insolvency advisers promote illegal phoenix activity. Find out what kind of advice to look out for.

Last updated 17 April 2023

If your business is insolvent or struggling to pay its debts, it's important to seek specialist advice from a qualified and registered

insolvency practitioner as soon as you can. Be wary of inappropriate insolvency advice that could lead to illegal phoenix activity.

Watch:

Media: Pre-insolvency phoenixings https://tv.ato.gov.au/ato-tv/media?v=bi9or7odigbjss (**Duration:** 01:07)

Insolvency advice to watch out for

Registered liquidators and trustees will provide you with sound insolvency advice that you can rely on. But some insolvency or pre-insolvency advisers suggest actions designed to help directors avoid paying their creditors and create new companies to continue on without debts.

This is illegal phoenix activity and can result in serious penalties. Following this advice could put you at risk of a fine, criminal conviction or even a jail term.

Be wary if an adviser:

- contacts you with advice, especially after your creditor has taken court action
- suggests you transfer your assets to a third party without payment
- offers advice on restructuring your business to avoid paying debts or other obligations
- offers you a fee based on a percentage of your debt or obligations
- tells you they know a liquidator who will protect your personal interests or assets
- tells you about a valuer who can under-value any assets
- asks you to provide incorrect information to authorities
- suggest you can withhold or destroy relevant records to prevent access by the liquidator or bankruptcy trustee
- suggests they deal with the liquidator or trustee on your behalf.
- encourages you to engage in any kind of illegal activity.

What to do

If your business is experiencing difficulties, it's important to take action and get advice straight away. The ASIC website has information:

- for directors whose companies are in financial difficulty or insolvent
- about illegal phoenix activity.

If you need to wind up your company or re-structure your business, a registered liquidator or registered trustee will be able to help you.

The Phoenix Taskforce is working to stop people promoting or engaging in illegal phoenix activity. If you're offered advice that you think is illegal, report it to us.

Authorised by the Australian Government, Canberra.

QC 64127

Data leaks

We are constantly receiving information that helps us detect and investigate tax evasion and other illegal activities.

Last updated 16 April 2026

We receive intelligence from a range of sources, including:

- concerned community members and advisers
- our domestic partner agencies
- our international alliances and tax treaty partners.

The nature of this intelligence can vary from a simple phone call to digital files, containing millions of electronic documents. The provision of digital files with the intent of exposing confidential information is referred to as a data leak.

We are dedicated to tackling tax crime committed by the small minority who attempt to evade their obligations at the expense of the rest of the community. We work with our domestic and international partners

to manage domestic and offshore tax evasion risks and deter those considering entering tax evasion schemes and arrangements.

Data leaks explained

A data leak occurs when confidential information is provided by an individual or a network, and is shared with government agencies, media outlets, or other organisations. Usually, the individual or network intends to expose individuals, groups, or businesses linked to potential criminal activity.

Data leaks normally attract public attention because of the controversial nature in which the information was obtained and the possible content of the data. They are just one of many sources that we use to detect and take action against offshore tax evasion.

Intelligence we have derived from data leaks such as the *Panama Papers, Paradise Papers*, and *Pandora Papers* has assisted us, and governments around the world, in identifying those involved in offshore tax evasion arrangements.

We work collaboratively with the Joint Chiefs of Global Tax Enforcement (J5) and the Joint International Taskforce on Shared Intelligence and Collaboration (JITSIC) to share, review and assess intelligence sourced from data leaks.

Offshore structures and accounts

It is not illegal to have an offshore business structure or bank account and there are many legitimate reasons for doing so. Appearing in a data leak does not imply wrongdoing. Taxpayers included in data leak information have reasonable explanations for structuring their assets the way they do.

However, we do take action against instances of offshore tax evasion.

Offshore service providers and professional enablers

Services offered by offshore service providers (OSPs) are not illegal. However, some professional enablers offer services that are attractive to individuals and entities that look for ways to:

- conceal their beneficial ownership of assets, or

- transfer untaxed income between jurisdictions.

Professional enablers of tax crime operate across international jurisdictions that have a lower perceived risk and a reputation for strict secrecy provisions. This enables additional levels of layering and anonymity for clients.

A small number of Australians are on the lookout for ways to evade paying tax.

We're also on the lookout for tax evasion signs. We have international and domestic intelligence-sharing relationships to uncover even the most intricately planned tax evasion schemes. Australia has international treaties and information exchange agreements with over 100 jurisdictions. The days of the secret tax haven are increasingly numbered.

Our partnerships

We are Australia's principal revenue collection agency. We administer the tax, excise and superannuation systems that support and fund services for Australians and deliver various social and economic benefits and incentive programs. We work with domestic and international partner agencies to tackle all forms of tax crime, including those from offshore tax evasion. Read more about the fight against tax crime.

Domestic partners

A large portion of the data files we obtain are provided to us as a result of the work we have done to develop information sharing policies and procedures under the legislation. We work in collaboration with government agencies, and domestic law enforcement agencies such as the:

- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Border Force (ABF)
- Australian Securities and Investments Commission (ASIC).

We lead the joint-agency Serious Financial Crime Taskforce (SFCT). The taskforce 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.

International partners

Transnational transactions are an unavoidable feature of a globalised economy that tax evaders use to conceal their income and assets. This does not just affect Australia; it is a problem for governments around the world.

Tax crime is a global problem that requires a global solution. We have developed international relationships with national revenue agencies to share intelligence and expertise in financial investigations to fight tax crime.

We have a range of tax treaties and agreements with dozens of countries to help facilitate the exchange of intelligence bilaterally and multilaterally. We are heavily involved in and support a number of international tax forums.

We collaborate with international tax administrations as a member of the Joint Chiefs of Global Tax Enforcement, also known as the J5. The group leads the fight against international tax crime and money laundering, including cryptocurrency threats and those who undertake or enable global tax evasion.

The other J5 members are:

- Her Majesty's Revenue and Customs (United Kingdom)
- Internal Revenue Service Criminal Investigation (United States)
- Canadian Revenue Agency (Canada)
- Dutch Fiscal Information and Investigation Service (Netherlands).

How we use data leaks

Some people are tempted to think that a data leak by itself is enough to commence investigations or legal action, but this is far from the truth. For example, the *Paradise Papers* leak that occurred in November 2017 contained over 13.4 million files.

Not every file contained in the leak was relevant to tax evasion or tax crime, so understanding what is in a data leak requires considerable logistical and analytical modelling. While we respond to a data leak the same way we respond to information received from informants or other jurisdictions, large data leaks require a significant amount of man-hours and technical sophistication to process.

As technology advances, we are further refining and developing skills and techniques to analyse information more rapidly. Not everyone who has offshore entities, structures or bank accounts is linked to criminal activities.

It is legal to enter into some of these arrangements. But we know many people opt to use the secrecy afforded by offshore jurisdictions to hide their income. After the data has been assessed, we identify and review names, entities, addresses, phone numbers and link other details to form a complete picture of the behaviour of the individuals and entities contained in the leaks.

Once this is done, we determine which entities identified in the data leak are:

- acting lawfully and meeting their tax obligations
- associated with existing investigations
- appearing on our radar for the first time.

Data leak activities

We often have multiple audits or investigations in progress, most of which are not known to the public. There are some investigations which capture the interest of the community. The following cases are good examples of our approach.

Find out about

- Panama Papers
- Swiss bank tax evasion involvement
- Paradise Papers

Panama Papers

What happened

In 2015 an anonymous source leaked 11.5 million financial and legal documents from Mossack Fonseca, the fourth largest offshore law firm operating globally with headquarters in Panama. The firm specialised in trusts, investment services, and international restructuring. The informant stated he had become disillusioned with what he considered to be the criminal complicity of the firm and provided the data to a German newspaper Süddeutsche Zeitung. The newspaper quickly realised it would not be able to review all 11.5 million documents and approached the International Consortium of Investigative Journalists (ICIJ) for assistance.

The database consisted of the names of 200,000 offshore entities and over 2.6 terabytes of data in the form of emails, bank accounts and trust documents. All this information was unstructured.

After the ICIJ conducted their own investigative work into the data, they published the first stories about the information contained in the data in April 2016. The stories revealed a number of linkages to high profile individuals from around the world.

At the same time, Joint International Taskforce on Shared Intelligence and Collaboration (JITSIC) member countries also obtained publicly available data, and incorporated the data with their own intelligence to identify risks.

What we did

As the chair of JITSIC, Commissioner Chris Jordan led members of the taskforce in developing a coordinated approach to investigating the *Panama Papers*. This collaboration clarified how resources would be combined and led to an agreed strategic approach on how to identify taxpayers using offshore institutions to evade tax.

The effect of JITSIC's information sharing agreements came into force. Overall, there were a total of 736 exchanges of information. This includes a number of unprompted exchanges, meaning a member country identified information relevant to a partner nation's investigations, and forwarded it on for their consideration. Individually, Australia delivered 52 outgoing exchanges in order to assist its partners with their own investigations.

Six months after the ICIJ published its first report about the *Panama Papers*, we made 15 unannounced access visits throughout Australia and informed the community that more than 100 taxpayers would be

contacted and advised they were subject to compliance action. We also advised we had detected taxpayers and advisers linked to:

- tax evasion
- illicit fund flows
- corruption.

Results

During our early investigations, we discovered approximately 1,400 Australians who were identified in the *Panama Papers*. Upon further analysis, we found that around 600 individuals had already come forward to advise us of their tax position and meet their tax obligations. We then identified approximately 570 taxpayers to undergo compliance assessments.

Our work with the *Panama Papers* has resulted in significant numbers of compliance actions against tax evaders and vast improvements in our understanding of how to approach these investigations.

For the Panama Papers, as at 31 March 2026 there has been:

- more than $256 million raised in liabilities
- more than $70 million collected in cash
- more than 540 audits and reviews finalised.

International Consortium of Investigative Journalists

The International Consortium of Investigative Journalists (ICIJ) is not associated with any tax agencies. They are an organisation of international journalists who collaborate on in-depth investigative stories in order to produce articles about issues that cross international boundaries.

Swiss bank tax evasion involvement

What happened

In 2017, the ATO and other domestic agencies were notified by our international partners that they had information relating to a group of managers working with a prominent Swiss Bank who appeared to be facilitating tax evasion for their clients. Our international partner

agencies had received information which indicated these managers were responsible for maintaining thousands of unnamed and numbered bank accounts.

In March 2017, authorities from the Netherlands and the United Kingdom executed arrest warrants on the facilitators of the secret bank accounts. After this, we notified the community that our partners had supplied us with intelligence connecting 346 Australians with the facilitators of these bank accounts.

What we did

As soon as we received the data leak from our European partners we commenced an investigation into the information contained in the data. The investigations team pursued multiple lines of enquiry using our existing intelligence resources to link individual taxpayers to the accounts provided to us.

Results

As a result of the investigation, we expanded the initial number of individual taxpayers suspected from 346 to 578.

During our investigation, we found the vast majority had complied with their tax obligations. However, we identified 106 taxpayers where a range of immediate compliance action was needed. Compliance action may include investigations of financial circumstances and audits to determine if they have used sophisticated systems of numbered accounts to conceal or transfer wealth to evade their tax obligations in Australia.

Working with our domestic partners, we have identified more than 5000 cross-border transactions worth more than $900 million in total. The transactions are undergoing further analysis to determine any potential offshore tax evasion risks.

Finally, the complex process of investigations occurred quickly and has resulted in further improving our investigative skills and capability. The success of our network of treaty partners, and our ability to share intelligence is a clear message to those who devise or participate in tax evasion schemes, you will be caught.

Paradise Papers

What happened

In 2017, media outlets around the world published stories about the largest data leak in history. The media attention concerned 13.4 million files downloaded from Bermudan law firm Appleby, Singapore based Asiaciti Trust, as well as corporate registries in 19 recognised tax havens around the world.

The leak came about as a result of a breach of Appleby's database by an anonymous actor. The data was provided to a German newspaper that provided it to the ICIJ. The files included emails, statements, and other financial records dating back as far as 1950.

The data contained personal details of high-profile individuals and corporations from around the world. Many of the media stories covered specific cases of the tax structures and the use by multinationals to divert profits away from their country of origin.

What we have done so far

Hours after learning of the leak we met with our partners in JITSIC to discuss the approach to the *Panama Papers*. Projects were allocated to individual member nations. We were assigned to lead a data working group and marshalled resources from member countries to assist. The methods and the lessons we learned during the *Panama Papers* were applied to the *Paradise Papers* and we have been able to identify individuals and entities more easily.

Results

A detailed analysis of the data is almost complete. From our vigorous processes, we have found there are a small number of cases with a potential tax risk that require ongoing inquiries.

We have used the *Paradise Papers* to develop a better understanding of the business models used by promoters of tax evasion. For example, firms like Appleby and Mossack Fonseca provide services focusing on registration and administration. They market the services to promoters and facilitators who design the tax evasion scheme, and task these firms with the mundane paperwork.

JITSIC plans to use information like this as well as its significant collective resources to disrupt the business model of the individuals who peddle these illegal schemes to their clients.

Make a tip-off

If you suspect that tax evasion or other illegal activities are being undertaken in your community, you can report it anonymously to us by:

- making a tip-off
- phoning **1800 060 062**.

You can also read about How we're closing the net on offshore tax evasion (includes a downloadable infographic).

Media releases

- ATO statement regarding the Pandora Papers

QC 57844

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.

Copyright notice