



Australian Government

AUSTRAC

FIGHTING
FINANCIAL
CRIME
TOGETHER

MONEY LAUNDERING IN AUSTRALIA

NATIONAL RISK ASSESSMENT

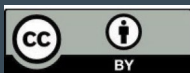
COPYRIGHT

© Commonwealth of Australia 2024

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).



Use of the Commonwealth Coat of Arms The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.pmc.gov.au/government/its-honour).

This risk assessment is intended to provide a summary and general overview; it does not assess every risk or product relevant to foreign subsidiary banks. It does not set out the comprehensive obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), the Anti Money Laundering and Counter Terrorism Financing (Prescribed Foreign Countries) Regulations 2018 (AML/CTF Regulations) or the Anti Money Laundering and Counter Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules). It does not constitute nor should it be treated as legal advice or opinion. The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication. AUSTRAC recommends that independent professional advice be sought.

CONTACT US

If you have questions about your AUSTRAC compliance obligations, or enquiries regarding the licence and any use of this report please email contact@austrac.gov.au or phone 1300 021 037 (within Australia).

AUSTRAC is committed to continual improvement and values your feedback on its products. We would appreciate notification of any outcomes associated with this report by contacting AUSTRAC at austrac.gov.au/contact-us/form.

CONTENTS

EXECUTIVE SUMMARY	4
KEY FINDINGS	5
INTRODUCTION	9
WHAT IS MONEY LAUNDERING?	10
AUSTRALIA'S AML/CTF REGIME	12
INTERNATIONAL CONTEXT	12
DOMESTIC CONTEXT	15
KEY FEATURES OF AUSTRALIA'S MONEY LAUNDERING ENVIRONMENT	20
THREATS.....	22
VULNERABILITIES.....	39
NATIONAL VULNERABILITIES.....	39
SECTORAL/CHANNEL VULNERABILITIES	43
CONSEQUENCES	102
APPENDIX A: SCOPE AND METHODOLOGY	105
APPENDIX B: AUSTRALIAN GOVERNMENT AGENCIES CONSULTED	108
APPENDIX C: GLOSSARY OF TERMS.....	109
APPENDIX D: THREAT AND VULNERABILITY MATRICES	115
APPENDIX E: INDUSTRY SURVEY	117
APPENDIX F: INTERNATIONAL FIU SURVEY	118



EXECUTIVE SUMMARY

The *Money Laundering in Australia National Risk Assessment 2024* (the assessment) is an important contribution to Australia's efforts to counter money laundering and other serious crime. It brings together insights from across Australia's law enforcement, intelligence and regulatory agencies, private sector stakeholders and international financial intelligence units (FIUs) to assess risks associated with money laundering. It assesses crimes that generate illicit proceeds, as well as the methods and channels used to launder funds in Australia. It also examines the international and domestic drivers that influence the Australian environment, and considers how Australia mitigates and combats money laundering activity, including where improvements could be made.

The key theme to emerge from this assessment is persistence: persistent exploitation of channels that have historically been used to launder funds (e.g. banks, remitters and casinos); persistent exploitation of high-value assets like luxury watches, vehicles and real estate; and persistent involvement of professional service providers to help establish complex business structures and associated banking arrangements to help individuals launder funds and conceal wealth.

Another theme to emerge from this assessment is the criminal exploitation of legitimate financial channels, assets and services. Core features of Australia's domestic economy, such as cash, bank accounts, payments technology, business structures and trusts, are also used by money launderers to place, layer and integrate criminal proceeds.

Underpinning many money laundering activities in Australia is opacity, anonymity and a lack of transactional visibility. The use of cash, trusts, identity crime, mule accounts and third-party transactions that obscure identity, beneficial ownership or financial flows continues to be a mainstay of money laundering.

Identity verification, a key pillar of anti-money laundering and counter-terrorism financing (AML/CTF) controls, is likely to become an increasingly contested space with the emergence of artificial intelligence and deep-fakes. This is a key emerging challenge facing Australia and the broader AML/CTF community.

Despite a sustained focus and effort across Australia's public and private sectors, money laundering remains an intractable issue as it is highly intertwined with all profit-generating crimes. The challenges in disrupting money laundering are not unique to Australia. Many of the money laundering threats and risks highlighted in this assessment are noted by other jurisdictions. While the actors may differ, the issues and challenges are strikingly similar.

Australia remains committed to creating a hostile environment for criminal actors who abuse the financial system for money laundering, terrorism financing and other serious crime. This will be achieved through ongoing investigation and prosecution of offenders, confiscation of criminal assets, regulatory reform, capacity building throughout the region, industry outreach and education, and strengthening of partnerships. Further inroads in disrupting money laundering in Australia will only be made through these sustained efforts.







KEY FINDINGS

- Australia's economy is exploited by money launderers. Lawful domestic financial channels remain fundamentally important pathways for money launderers to place, layer and integrate funds domestically and internationally.
- Australia remains an attractive destination to store and integrate criminal proceeds because of its stable political system, open and free economy, independent legal system, well-developed financial services sector and strong real estate market.
- Crimes generating the highest value of illicit proceeds that require laundering are assessed to be drug offences (including cultivation, manufacture and trafficking), tax and revenue crimes, as well as defrauding government-funded programs. The illicit drug market is a key driver of money laundering in Australia.
- Criminals continue to use established channels such as cash, luxury goods, real estate, domestic banks, casinos and remitters to launder funds in Australia.
- Criminal use of digital currency, digital currency exchanges, unregistered remitters and bullion dealers is increasing.
- The increased speed of financial transactions in recent years has made it harder for reporting entities to identify and freeze suspicious transfers before funds leave an account. This is further complicated when individuals open and transact through multiple products across multiple financial institutions.
- Opaque legal structures can be created in Australia and used by criminals to help conceal their identity and illicit activity. These structures can limit or obscure visibility of the ultimate beneficial owners of corporate entities, assets and financial infrastructure. They create a significant money laundering vulnerability for Australian authorities and industry.
- The use of professional service providers, either witting or unwitting, to establish, advise on or operate corporate and financial infrastructure also reduces visibility of the ultimate beneficial owner and creates money laundering vulnerabilities for Australian authorities and industry. The lack of AML/CTF obligations for some designated non-financial businesses and professions means professional service providers are not subject to the due diligence, transaction reporting and supervision requirements outlined in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

SNAPSHOT OF RISK RATINGS

THREATS: PROCEEDS-GENERATING CRIMES










LEGEND



































	Increase		Decrease		Stable
	Low		Medium		High























PREDICATE CRIME	RATING	OUTLOOK
Illicit drugs		
Tax and revenue crime		
Government-funded program fraud		
Scams		
Illicit tobacco		
Pure cybercrime		
Identity crime		
Corruption and bribery		
Superannuation fraud		
Child sexual exploitation		
Environmental crime		
Payment fraud		
Firearms trafficking		
Human trafficking		
Intellectual property crime		

VULNERABILITIES

LEGEND

	Increase		Decrease		Stable		Emerging		
	Very Low		Low		Medium		High		Very high

SECTOR/CHANNEL	RISK	OUTLOOK
Cash - transfer of value		
Cash - store of value		
Luxury goods		
Real estate (domestic)*		
Digital currencies – transfer of value**		
Unregistered remittance dealers		
Cash-intensive businesses		
Cash smuggling (undeclared)		
Registered remittance service providers		
Major banks		
Other domestic banks / foreign subsidiaries		
Casinos		
Bullion and precious metals (physical or securities)		
Lawyers		
Accountants		
Legal structures		
Companies		
Trusts		
Luxury vehicles and watercraft		

Digital currency exchanges**		
Digital currencies – store of value**		
Bullion dealers		
Cash smuggling (declared cash movement)		
Mutual banks		
Foreign bank branches		
Superannuation fund providers		
Stockbrokers and securities dealers		
Wealth and financial assets		
Real estate agents*		
Offshore service providers and trust and company service providers		
Trusted insiders		
Betting agencies / corporate bookmakers		
Pubs and clubs		
Online offshore gambling		
Non-bank lenders and financiers		
Foreign currency exchanges		
Custodians and asset custody services		
Managed investments schemes		
Customs brokers		
Casino junket tour operations		
On-course bookmakers		

* **Real estate (domestic)** refers to the physical real estate asset/good that can be purchased, sold and rented for money laundering purposes. **Real estate agents** are the professional service providers who provide the service for individuals and entities to purchase real estate (domestic). Real estate agents are not currently regulated under the AML/CTF Act.

** **Digital currency exchanges (DCEs)** exchange money for digital currency and vice versa. DCE providers must be registered with AUSTRAC under the AML/CTF Act. **Digital currencies – transfer of value** and **Digital currencies – store of value** refer to digital assets/channels through which value can be transferred and stored for laundering purposes. It refers to the digital currency itself.



INTRODUCTION

This assessment is an important contribution to Australia’s money laundering risk mitigation ecosystem. It provides an intelligence base to better assist policy and operational responses to identified money laundering risks. The assessment also provides contextual guidance to all Australian businesses on the scale and impact of the risks and aims to help regulated businesses to continue improving their AML/CTF programs and their reporting of money laundering activity to relevant authorities. It also provides improved insights for other businesses and channels to help them manage criminal risks they might face. A comprehensive assessment of money laundering risks and channels is also critical to implement the international standards set by the Financial Action Task Force (FATF), the global money laundering and terrorism financing watchdog.¹

Details on the scope and methodology of this assessment are found at [Appendix A](#).



ACKNOWLEDGEMENT

AUSTRAC has completed this assessment as Australia’s FIU. The assessment was made possible by the cooperation and participation of the Australian agencies, authorities and bodies listed at [Appendix B](#). AUSTRAC wishes to acknowledge and thank each participant for their valued contributions to this project.

Please see [Appendix C](#) for a glossary of terms used in this assessment.

¹ The FATF Recommendations require countries to identify, assess and understand money laundering risks at a national level. These risks should be assessed on an ongoing basis and be kept up to date.



WHAT IS MONEY LAUNDERING?

Money laundering encompasses two main elements:

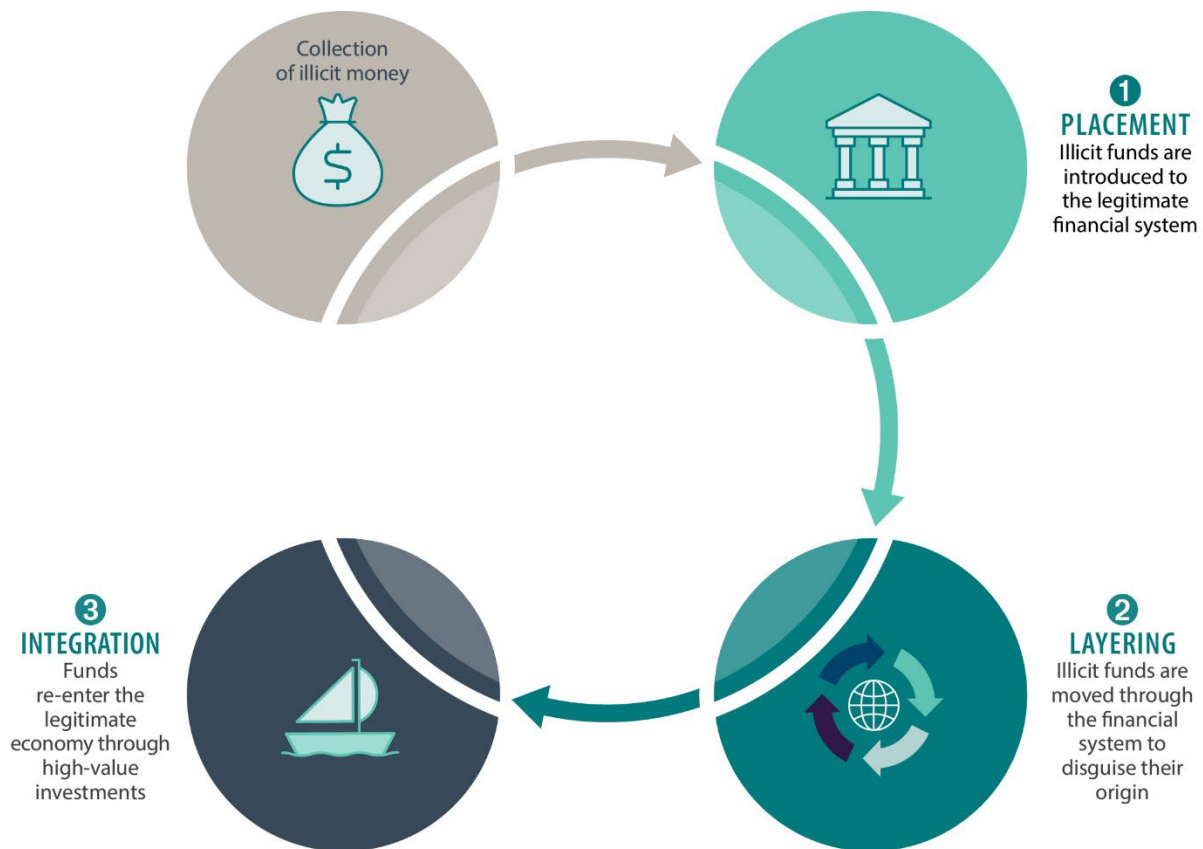
- the process by which illegally obtained funds are given the appearance of having been legitimately obtained
- the use of funds (either illegally obtained or legitimate) as an instrument of crime.

Money laundering is a major component of virtually all criminal activity and adversely affects the Australian community in numerous ways. It perpetuates serious crime by enabling criminals to reinvest in further crime. It diminishes tax revenue and weakens government control over the economy. Money laundering also undermines the integrity of Australia's financial system and other industry sectors and has the potential to damage the credibility and reputation of Australia's regulatory and law enforcement agencies.

The money laundering cycle describes the typical process criminals may use to conceal the source of illicit funds and make funds appear legitimate. It consists of the three stages of placement, layering and integration:

- **Placement** – illegal funds or assets are introduced into the formal financial system. Some common placement techniques include structuring deposits into bank accounts and using cash to purchase assets.
- **Layering** – illegal funds or assets are moved, dispersed or disguised to conceal their true origin. Funds are sometimes layered using a web of complex transactions. Some common layering techniques include using multiple banks and accounts, having professionals act as intermediaries and transacting through corporations and trusts.
- **Integration** – after funds or assets are distanced from their origins, they are made available for investment in further criminal activity, legitimate business or to purchase high-value assets and luxury goods. At this stage the illegal money has achieved the appearance of legitimacy.

FIGURE 1: THE THREE STAGES OF MONEY LAUNDERING



MONEY LAUNDERING OFFENCES

In Australia, money laundering is investigated and prosecuted at the state and territory level as well as Commonwealth level. At the Commonwealth level, the AML/CTF Act and the *Financial Transaction Reports Act 1988* operate in conjunction with the *Criminal Code Act 1995* (Criminal Code) and the *Proceeds of Crime Act 2002* (POCA).

- The Criminal Code and Part 12 of the AML/CTF Act create an offence of dealing with the proceeds and instruments of crime. For a money laundering offence to be committed, a person need only handle illicit funds, not necessarily launder and legitimise criminal earnings.
- The POCA allows confiscation of the proceeds and instruments of crime under civil and criminal provisions. It also allows confiscation of any secondary commercial benefit obtained through commission of a crime (for example, through publicity surrounding the offence).

Unexplained wealth laws require individuals suspected of possessing unexplained wealth to demonstrate that it was legally acquired or have it confiscated. The POCA and *Crimes Legislation Amendment (Serious and Organised Crime) Act (No.2) 2010* include unexplained wealth provisions to strengthen asset-confiscation attempts by the Commonwealth. Unexplained wealth laws also exist at the state and territory level.

Instruments of crime

Division 400 of the Commonwealth Criminal Code defines money laundering broadly to include both dealing with proceeds of crime and instruments of crime. The second limb of this definition focuses on the potential of money and property, irrespective of its provenance, to enable future offending. The application of criminal sanctions to both those who profit from crime and those who engage in illicit financing of criminal endeavours is an important pillar of Australia's response to money laundering.



AUSTRALIA'S AML/CTF REGIME

Australia's AML/CTF regime forms an important part of the national approach to countering money laundering and other serious crime. The AML/CTF regime is a multifaceted and cooperative effort across law enforcement, regulatory, intelligence and policy agencies, as well as industry, international partners and the broader community.

Among other things, the AML/CTF regime aims to:

- provide measures to deter, detect and disrupt money laundering
- provide a disincentive to crime by reducing its profitability
- reduce the pool of money available to finance future criminal activity
- aid in the detection and prosecution of crime
- protect the integrity of the financial system and reputation of Australian businesses.

INTERNATIONAL CONTEXT

Australia's AML/CTF regime is based on international standards developed by the FATF. Australia is a founding member of the FATF, which was established in 1989. FATF is the major inter-jurisdictional body for setting AML/CTF standards known as the FATF Recommendations, and has established a peer review process, known as 'mutual evaluations'. These are undertaken by member countries to assess the effectiveness and compliance of the assessed country's measures to combat money laundering, terrorism financing and proliferation financing.

The FATF Recommendations and its mutual evaluations of Australia have been major catalysts for enhancements to Australia's AML/CTF regime since 2003. Most recently this involved a comprehensive statutory review of the AML/CTF Act and associated Rules and Regulations in 2016. The review report took into account the outcomes of the 2015 FATF mutual evaluation of Australia and made a range of recommendations to modernise and strengthen the AML/CTF regime. These recommendations are being implemented in phases.

COOPERATION AND INFORMATION SHARING

The Australian Government is committed to working with foreign partners to share intelligence and strengthen domestic, regional and global resistance against money laundering threats. This engagement is facilitated by various multilateral and bilateral agreements that the Australian Government has in place through its agencies.

Regional and international cooperation and engagement is channelled through:

- Intelligence exchange and requests for information, including for mutual legal assistance and extradition with foreign counterpart agencies.
- Regional capacity building in Southeast Asia, South Asia, and the Pacific.
- Active involvement in key international forums, including the United Nations, the Association of Southeast Asian Nations (ASEAN), the ASEAN Regional Forum, the East Asia Summit, FATF, the Egmont Group of FIUs, the Asia/Pacific Group on Money Laundering, and the Global Coalition to Fight Financial Crime.
- A network of internationally-deployed officers working closely with counterparts across the globe.

A number of law enforcement and Commonwealth agencies, including AUSTRAC, participate in collaborative international efforts to combat money laundering and other financial crime.

Key groups include:

- The **Egmont Group of FIUs** is a united body of 174 FIUs. The Egmont Group facilitates the secure exchange of expertise and financial intelligence among its members to combat money laundering, terrorist financing and associated predicate crimes. Australia was a founding member and takes a leadership role in a wide range of Egmont work.
- The **Asia/Pacific Group on Money Laundering** is an inter-governmental organisation of 42 member jurisdictions. A key objective is to ensure that individual members effectively implement the international standards against money laundering, terrorist financing and proliferation financing related to weapons of mass destruction.
- The **Financial Intelligence Consultative Group** is a collective regional body of heads and senior representatives of FIUs from ASEAN, New Zealand and Australia. Japan's FIU participates as an observer. This group promotes, enhances and strengthens collaboration to combat serious financial crime in the region.
- The **Pacific Financial Intelligence Community** brings together 12 Pacific FIUs, including Australia and New Zealand. It promotes greater collaboration among members, covering operational engagement, research activities, capacity building and technology enhancement to combat the region's financial crime challenges.
- The **Indo-Pacific Economic Framework** is a regional arrangement to build cooperation and economic integration in the Indo-Pacific region. A primary objective is to progress key international anti-corruption measures, tax evasion initiatives and anti-money laundering (AML) instruments.

- The **Five Eyes Money Laundering Community of Practice** is a law enforcement forum established as a mechanism for Five Eyes countries² to share intelligence, best practice and coordinate actions to mitigate and disrupt international money laundering and financial crime threats.
- The **Asset Recovery Interagency Network - Asia Pacific** facilitates police-to-police collaboration and information sharing across the Indo-Pacific region on asset recovery issues.
- The **Joint Chiefs of Global Tax Enforcement (J5)** brings together leading tax enforcement authorities from member countries to combat international tax crime and money laundering.
- The **International Anti-Corruption Coordination Centre** brings together specialist law enforcement officers from multiple agencies around the globe to combat grand corruption. This includes offences such as bribery of public officials, embezzlement, abuse of office and money laundering.

Australia also engages with the following international public-private partnerships:

- The **Global Coalition to Fight Financial Crime** aims to mitigate financial crime by strengthening global AML/CTF regimes through political and policy reforms.
- The **Bribery Prevention Network** brings together business, civil society, academia and government with the shared goal of supporting Australian businesses to prevent, detect and address bribery and corruption.



AUSTRAC PROGRAMS IN THE INDO-PACIFIC REGION

AUSTRAC delivers tailored programs to FIU partners across the Indo-Pacific region. These programs focus on building AML/CTF capabilities and sharing financial intelligence analytic expertise to strengthen regional resilience against financial crime.

- The **AUSTRAC Pacific Islands Partnership Program** provides AML/CTF capacity- building activities for counterparts across the Pacific region.
- Through **Project Taipan**, AUSTRAC works with Pacific FIUs to develop and install IT systems that uplift their capability.
- The **Mekong-Australia Partnership on Transnational Crime**, coordinated by the Department of Foreign Affairs and Trade (DFAT), aims to counter transnational crime and enhance border security in the Mekong subregion through targeted capacity- building programs.
- The **Strengthening Anti-Money Laundering and Counter-Terrorism Financing Responses in the Philippines Program** is a partnership between AUSTRAC and the Philippines FIU. Program activities support the Philippines to strengthen their response to terrorism and enhance their AML/CTF framework to meet international standards.

² Five Eyes countries include Australia, Canada, New Zealand, the United Kingdom and the United States.

DOMESTIC CONTEXT

AML/CTF REGULATORY AND LEGISLATIVE FRAMEWORK

Australia's AML/CTF legislative framework is tailored to support AUSTRAC's mandate as the dual AML/CTF regulator and FIU. It comprises:

- the AML/CTF Act
- the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules)
- the *Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulations 2018*
- the *Financial Transaction Reports Act 1988* (FTR Act).

The AML/CTF Act mostly focuses on regulating businesses that provide a range of services known as designated services.³ Businesses that provide designated services are known as reporting entities. Reporting entities must comply with obligations under the AML/CTF legislative regime.⁴ There are currently approximately 17,000 reporting entities enrolled with AUSTRAC.

The FTR Act imposes several obligations on cash dealers. These include the requirement to verify the identities of account holders and report cash transactions of \$10,000 or more and suspicious transactions to AUSTRAC. Solicitors must report cash transactions of \$10,000 or more.



A statutory review of the AML/CTF regime was completed in 2016. The review made a number of recommendations to strengthen and simplify Australia's AML/CTF legislative framework. These recommendations are being implemented in phases.

The Australian Government is currently developing legislation for the most substantial phase of proposed reforms. These reforms will aim to simplify and modernise the regime in line with international standards and best practice. The proposed reforms would also extend AML/CTF regulation to additional services that are recognised globally as posing high ML/TF risks. These include certain services provided by businesses such as lawyers, accountants, trust and company service providers, real estate agents, property developers and dealers in precious metals and precious stones. If enacted, these reforms will significantly increase the number of entities reporting to AUSTRAC and bring Australia in line with other FATF member countries.

³ Designated services are defined in section 6 of the AML/CTF Act and include financial services, including remittance and digital currency exchange, gambling and bullion dealing.

⁴ Australia's AML/CTF regime adopts an all-crimes approach to monitoring and reporting suspicious matter reports (SMRs) to AUSTRAC. This approach recognises that while most crimes cause some degree of harm to individuals, businesses or the broader community, not all crimes generate criminal proceeds. All regulated entities must submit a SMR to AUSTRAC when they suspect a customer of being involved in criminal activity including money laundering, terrorism financing, an offence against a Commonwealth, state or territory law, the proceeds of crime, or tax evasion.

ENFORCEMENT ACTIONS⁵

AUSTRAC can take enforcement action against reporting entities who do not comply with the AML/CTF legislative regime. Civil penalty orders imposed by the courts in recent years demonstrate AUSTRAC's increasing compliance investigation capabilities.

- In 2017, the Federal Court of Australia ordered three Tabcorp group companies to pay a penalty of \$45 million for contraventions of the AML/CTF Act.
- In 2018, the Federal Court of Australia ordered the Commonwealth Bank of Australia to pay a penalty of \$700 million for contraventions of the AML/CTF Act.
- In 2020, the Federal Court of Australia ordered Westpac Banking Corporation to pay a penalty of \$1.3 billion for contraventions of the AML/CTF Act. The order represents the largest civil penalty in Australian history.
- In 2023, the Federal Court of Australia ordered Crown Melbourne and Crown Perth to pay a penalty of \$450 million for contraventions of the AML/CTF Act, as well as AUSTRAC's legal costs. The order represents one of the largest civil penalties against a casino globally.
- In 2024, the Federal Court of Australia ordered SkyCity Adelaide Pty Ltd (SkyCity) to pay a penalty of \$67 million for contraventions of the AML/CTF Act, as well as AUSTRAC's legal costs.

AUSTRAC has commenced civil penalty proceedings against The Star Pty Ltd and The Star Entertainment QLD Ltd for alleged serious breaches of the AML/CTF Act. This matter is currently before the Federal Court of Australia.

NATIONAL ANTI-MONEY LAUNDERING (AML) COORDINATION MECHANISMS

Australia's AML efforts form an important part of the *National Strategy to Fight Transnational, Serious and Organised Crime* (the National Strategy).⁶ The National Strategy provides the framework for governments, the private sector, civil society organisations, academia and the community to work together to secure Australia's national interests in combatting transnational serious and organised crime (TSOC).

The **Australian Transnational Serious and Organised Crime Committee** (ATSOCC) is the governance body that oversees and monitors the implementation of the National Strategy. The ATSOCC's mission is to build understanding of key TSOC threats, provide strategic and policy advice on national priorities to combat TSOC, and enhance inter-jurisdictional cooperation and collaboration to disrupt threat actors. Its members include senior officials from each Australian policing agency, and Justice or Attorneys-General agency; New Zealand Police; New Zealand Ministry of Justice; AUSTRAC; the Australian Criminal Intelligence Commission; the Office of National Intelligence; the Australian Border Force; and the Department of Home Affairs.

In addition, a number of inter-agency committees and groups exist to coordinate operational activities, set strategic priorities, and facilitate information sharing to combat money laundering and serious financial crime impacting Australia.

The **Criminal Justice and Law Enforcement Forum** brings together agency heads from across the Australian Government to drive meaningful action on criminal justice and law enforcement issues. Through its broad membership, the Forum provides strategic oversight and guidance for the

⁵ Enforcement actions include civil penalty orders, enforceable undertakings, infringement notices and remedial directions. AUSTRAC publishes information about its enforcement actions, including case outcomes. Details are available on [AUSTRAC's website](#).

⁶ The Council of Australian Governments agreed to the National Strategy to Fight Transnational, Serious and Organised Crime on 12 December 2018. Further information about the National Strategy is available on the [Department of Home Affairs](#) website.

development of whole of government strategies, policies and coordinated activities to protect Australian communities and institutions from harm, including from financial crime.

The **Serious Organised Crime Coordination Committee** supports the prioritisation, endorsement and coordination of operational activities, both nationally and internationally.

The **Council of Financial Regulators** is a coordinating body for financial regulatory agencies, including the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC), the Reserve Bank of Australia (RBA) and the Department of Treasury (Treasury).

PUBLIC-PRIVATE PARTNERSHIPS

Public-private partnerships enable collaboration and information sharing to build industry understanding of the financial crime environment and capability to combat threat actors.

Fintel Alliance is an AUSTRAC initiative established in 2017. A world-first public-private partnership, Fintel Alliance brings together experts from financial institutions, law enforcement and intelligence agencies, and academia, to increase the resilience of the financial sector to criminal exploitation and support investigations into serious crime and national security matters.

The **Australian Financial Crimes Exchange** brings together businesses, government, law enforcement agencies and industry groups to coordinate the fight against financial and cybercrime in Australia. It is also a collaboration platform, allowing the public and private sectors to share and access secure information and intelligence.



SUPPORTING AND COLLABORATING WITH INDUSTRY

AUSTRAC publishes a wide range of practical guidance to help businesses understand, identify and report suspicious activity. Reporting entities and private sector businesses are encouraged to review the full list of available guidance [on AUSTRAC's website](#) and identify products and tools that may be relevant to their operations. In particular, financial crime guides provide information about the financial aspects of different crime types. They include case studies and indicators that can be used to identify potential offences.

Since 2016, AUSTRAC has also published 21 ML/TF risk assessments to help businesses identify, mitigate and manage their risks. This includes 17 sector-based risk assessments, three regional risk assessments and Australia's first national proliferation financing risk assessment. These reports are available on [AUSTRAC's website](#).

OPERATIONAL FRAMEWORK

A number of state, territory and Commonwealth agencies, including AUSTRAC, are responsible for formulating and implementing Australia's operational AML response.⁷ These agencies work closely to support a collaborative cross-agency effort to combat money laundering threats.

Table 1 highlights priority taskforces that drive or support Australia's AML efforts.⁸ These taskforces allow members to share targeted, actionable intelligence to support operational law enforcement outcomes into money laundering activities and related predicate crimes.

⁷ Please refer to [AUSTRAC's website](#) for a list of these agencies.

⁸ This list is not exhaustive. Please refer to [AUSTRAC's website](#) for a full list of Australian taskforces that AUSTRAC contributes to.

TABLE 1: AUSTRALIAN TASKFORCES LINKED TO AML EFFORTS

TASKFORCE	AREA OF FOCUS	JURISDICTION
Australia Centre to Counter Child Exploitation	Child exploitation and human trafficking	National
Serious and Organised Crime Coordination Committee (SOCCC) National Operation Taskforce ATHENA	Illicit firearms	National
Operation AVARUS	Money laundering	National
Shadow Economy Standing Taskforce	Shadow Economy	National
Criminal Assets Confiscation Taskforce	Criminal wealth	National
Fraud Fusion Taskforce	Fraud against government payments programs	National
Illicit Tobacco Task Force	Illicit tobacco	National
SOCCC National Operation Taskforce MORPHEUS	Outlaw motorcycle gangs	National
Phoenix Taskforce	Illegal phoenix activity (corporate fraud, tax evasion)	National
Serious Financial Crime Taskforce	Serious and complex financial crime including tax crime and evasion	National
SOCCC National Operation Taskforce THEMIS	Fraud and serious financial crime	National
SOCCC National Operation Taskforce VITREUS	Illicit drugs	National
SOCCC National Operation Taskforce KUBERA	Money Laundering	National
SOCCC National Operation Taskforce HELIOS	Cybercrime	National

TASKFORCE AVARUS

Officially launched on 17 March 2023, Taskforce AVARUS is an investigative capability established by the Australian Federal Police (AFP) to enhance the operational impact on money laundering. The taskforce is a multi-agency entity with members from the Australian Border Force, the Australian Criminal Intelligence Commission and AUSTRAC. Since the establishment of Taskforce AVARUS, 197 search warrants have been executed with 85 people arrested on 113 counts of money laundering and money laundering-related charges. As a result, organised crime groups have been deprived of more than \$421 million in cash and assets.

An AFP investigation established in early 2022 targeted a global money laundering organisation headquartered in Sydney, New South Wales. The organisation is alleged to have provided money laundering services at an industrial scale to various transnational organised crime groups. The organisation used a range of methodologies, such as 'daigous', casino junket tours and offsetting, to move illicit funds across multiple jurisdictions.

In February 2023, the investigation resulted in the arrest of nine individuals, including the alleged head of the organisation, and the restraint of approximately \$32 million in digital currencies along with multiple luxury items and firearms. The AFP-led Criminal Assets Confiscation Taskforce (CACT) also obtained restraining orders related to more than 20 properties in Sydney. These included multiple commercial buildings, two residential homes worth more than \$19 million combined, a 360-hectare tract of land worth \$47 million and 66 bank accounts. The dual strategy of undertaking criminal prosecutions and civil proceeds of crime litigation ensures the AFP and its partner agencies can deliver maximum impact to criminal groups.

The AFP commenced an investigation in August 2022 to investigate a highly sophisticated global criminal organisation suspected of operating and controlling one of Australia's largest independently-owned remittance businesses. It is alleged the organisation used the vast scale of the remittance business to help mask the movement of at least \$229 million of criminal proceeds into and out of Australia. Unlike other money laundering organisations (MLOs) that prefer to operate covertly, the syndicate was uniquely overt, operating legitimate shopfronts across the country. In addition to servicing thousands of legitimate customers, it allegedly also serviced criminal customers, including helping to create fake business documents, invoices and bank statements to avoid regulatory detection.

In October 2023, the investigation resulted in the arrest of seven members of the organisation, including four Chinese nationals and three Australian citizens. The AFP-led CACT also obtained restraining orders related to more than \$50 million in residential and investment properties, luxury vehicles and other luxury items. AUSTRAC has also initiated regulatory action against the remittance business.



KEY FEATURES OF AUSTRALIA'S MONEY LAUNDERING ENVIRONMENT

This chapter highlights key features of Australia's money laundering environment identified in this assessment. It provides important context for understanding money laundering risks, including factors that drive and enable money laundering activities and those which continue to pose challenges for reporting entities and authorities.

PERSISTENT AND AGILE CRIMINALS

Criminals continue to identify and exploit new opportunities to launder illicit funds through innovation, experimentation and adaptation. By operating without regard to the law, money launderers often remain more agile than those responsible for preventing and enforcing AML/CTF obligations. When one channel is disrupted, the money laundering ecosystem generally offers multiple alternate options for criminals to place, layer or integrate their illicit funds. This is further complicated when criminals share insights and learn from one another.

TECHNOLOGICAL ADVANCEMENTS

Technological advancements over the past decade have complicated the ability to detect and track illicit transactions. The speed of some payment systems enable value to be transferred almost instantaneously across national and international borders and, in some cases, outside regulatory capture. Artificial intelligence (AI) and the widespread access to it will almost certainly create further and more complex challenges for reporting entities and authorities, for example, challenging identity verification processes. Organised crime groups have readily adapted to adopt and exploit new technologies to their advantage. Technologies that can include end-to-end encryption and digital currencies allow money launderers to hide their identities and illicit activities from law enforcement agencies. This makes it difficult to attribute criminal activity to particular individuals, organisations, premises or devices.

STRONG TIES TO CRIMINAL MARKETS IN ASIA

A number of Australia's illicit markets are linked to criminal markets and organisations operating in Asia. These include large and highly functional international drug-trafficking organisations that control supply chains into Australia, as well as professional money laundering organisations (MLOs) with a demonstrated capability to launder funds into and out of Australia. Australia's extensive economic relations and trade with Asian markets also provide legitimate financial pathways that can mask illicit transfers.

HIGH DEMAND FOR ILLICIT GOODS

Australians continue to demonstrate a high demand for illicit goods. For example, Australia is one of the largest consumers of illicit stimulants globally and Australia's illicit drug market generates substantial criminal proceeds that require laundering. The estimated street value of methylamphetamine, cocaine, MDMA and heroin was \$12.4 billion in 2022-23.⁹ Despite ongoing law enforcement efforts, many of Australia's illicit markets, including both drugs and tobacco, remain strong and resilient to large-scale disruption.

ATTRACTIVE DESTINATION FOR ILLICIT FUNDS

Australia enjoys a global reputation as a large, robust and stable economy. While these features attract legal investment, they also make it an attractive destination for foreign proceeds of crime. Australia's desirable lifestyle, strong rule of law and stable institutions including robust legal frameworks that protect assets and wealth from lawful confiscation, are likely major factors in attracting these funds. The country's strong trade and investment ties also create vulnerabilities that are exploited by criminals. For example, asset classes that attract a high volume of international investment, such as real estate, are also highly desirable as a means to transfer and store wealth.

⁹ ACIC, National Wastewater Drug Monitoring Program Report 21, 2024. <https://www.acic.gov.au/publications/national-wastewater-drug-monitoring-program-reports/report-21-national-wastewater-drug-monitoring-program>



THREATS

In the context of this assessment, money laundering threats are predicate crimes that generate illicit proceeds, which are then laundered in, from or through Australia. This chapter discusses threats that have been rated ‘high’ and ‘medium’ *only*. Each risk rating provides the current overall assessment of threat and an assessment of how the threat is likely to change over the next three years. A discussion of regions that are assessed to pose a higher threat to Australia is at the end of this chapter.

AUSTRAC acknowledges that many crime types assessed as posing a low money laundering threat have **very high levels of associated harm**, including child sexual exploitation, human trafficking and environmental crime. AUSTRAC holds and generates a significant volume of financial intelligence regarding many of these crime types and remains committed to detecting and supporting their disruption. AUSTRAC does this by providing financial intelligence and expert analytical support to domestic and international law enforcement and FIU partners.



CHALLENGES IN ESTIMATING THE MONEY LAUNDERING THREAT

Despite consistent efforts, the actual amount of money, property and assets that are laundered in Australia remains difficult to definitively quantify. With respect to domestic criminal proceeds, current best estimates were provided by the Australian Institute of Criminology (AIC) in the report titled *Estimating the costs of serious and organised crime in Australia, 2020-21* (Cost of Crime report).¹⁰ It estimated the amount of criminal proceeds generated in Australia per year could be as high as \$43.7 billion. The AIC estimated the *total* cost of serious and organised crime in Australia, including the prevention and response costs, is as high as \$60.1 billion in 2020-21. With respect to foreign criminal proceeds, estimates remain elusive.

¹⁰ R Smith & A Hickman, *Estimating the costs of serious and organised crime in Australia, 2020-21*. Statistical Report no. 38. Australian Institute of Criminology, 2022. The Cost of Crime report and associated figures are discussed in more depth in the **Consequences** chapter of this assessment.

HOW PROCEEDS OF CRIME MANIFEST IN THE COMMUNITY

Criminals often rely on the use of multiple forms of criminal proceeds for the money laundering process, largely depending on the stage of the money laundering cycle (i.e. placement, layering and integration) and the criminal activity from which the proceeds were generated.

Criminal proceeds generally take one or more of the following forms:







- Cash – typically from the immediate sale of an illicit good or derived from an illicit act.
- Electronic funds transfer – as funds are already in the financial system, the perpetrator will decide whether or not, and in what proportion, the proceeds should be transferred through various payment mechanisms and the ultimate destinations.
- Digital currencies and digital assets – now a notable part of the global financial economy, the conversion of fiat currency to digital currency is largely traceable, but once outside the regulated ecosystem the movement of illicit value becomes relatively opaque. Predicate financial crimes committed in the digital ecosystem may involve money laundering, and individuals may be identifiable when they interact with a centralised digital currency exchange (DCE) or payment services provider.
- Contingent (in-kind) – i.e. where the value is not immediately known and exclusivity (e.g. potential future rents) available to the owner is extinguished, this typically takes one of two forms:
 - withheld payments, or as an in-species exchange of entitlement; or
 - as an intangible, in the form of loss of future entitlement or ownership of economic rents, e.g. intellectual property fraud.

OVERVIEW OF THREATS

TABLE 2: KEY MONEY LAUNDERING THREATS

PREDICATE CRIME	RATING	OUTLOOK
Illicit drugs		
Tax and revenue crime		
Government-funded program fraud		
Scams		
Illicit tobacco		
Pure cybercrime		
Identity crime		
Corruption and bribery		
Superannuation fraud		
Child sexual exploitation		
Environmental crime		
Payment fraud		
Firearms trafficking		
Human trafficking		
Intellectual property crime		

LEGEND

	Increase		Decrease		Stable
	Low		Medium		High

ILLCIT DRUGS

RISK RATING

The domestic illicit drug market is assessed as posing a **high** and **increasing** money laundering threat.

INTELLIGENCE PICTURE

Australia's illicit drug market is large, complex and resilient to wide-scale disruption; and is characterised by persistently strong demand. Money laundering is a key enabler of Australia's illicit drug market, which generates significant volumes of criminal proceeds that require laundering. Wastewater analysis places estimates of the combined street value of Australia's drug markets at \$12.4 billion (Table 3).

TABLE 3: ESTIMATED STREET VALUE IN FOUR DRUG MARKETS, 2022-23¹¹

	METHAMPHETAMINE	COCAINE	MDMA	HEROIN	ALL
Estimated street value (\$)	10.58b	1.31b	99.51m	449.55m	12.4b

Methamphetamine poses the highest money laundering threat. Australians are one of the largest consumers of illicit stimulants globally, and transnational and national serious and organised crime groups are very active in Australia's methamphetamine supply chains. By level of demand and use, cannabis is the largest drug market in Australia. However, the level of organised crime involvement is assessed to be lower compared to other illicit drug markets. The volume of linked criminal proceeds that require laundering is also assessed to be lower. This is because cannabis distribution channels are more dispersed, and individuals in the supply chain are more likely to consume a portion of their illicit profits to fund their lifestyle, compared to other drug markets.

Diversity is a key feature of money laundering linked to Australia's illicit drug markets. Well-established money laundering methodologies persist, such as structuring and the use of cash,¹² third-party accounts and money mules. However, exploitation of digital currencies is increasing. The level of complexity of money laundering schemes ranges from the use of professional criminal organisations with global operations, to simple unsophisticated methods which require minimal skills, knowledge or expertise.

OUTLOOK

Australia's illicit drug markets are entrenched, and levels of consumer demand are unlikely to experience a significant decline in the short to near term. Consequently, illicit drug markets will continue to generate large volumes of criminal proceeds that need to be laundered over the next three years and likely into the longer term.

¹¹ ACIC, National Wastewater Drug Monitoring Program Report 21, 2024. <https://www.acic.gov.au/publications/national-wastewater-drug-monitoring-program-reports/report-21-national-wastewater-drug-monitoring-program>

¹² Alongside the seizure of luxury goods including watches, handbags, vehicles, jewellery and real estate, large cash seizures remain a hallmark of Australian investigations into illicit drugs.

TAX AND REVENUE CRIME

RISK RATING

Tax and revenue crime is assessed as posing a **high** and **increasing** money laundering threat. For the purpose of this assessment, this category of threat includes:

- dishonest activities that target each of the taxation revenue streams administered by the Australian Taxation Office (ATO) including personal income tax, business/company tax, and goods and services tax
- offshore tax evasion
- illegal phoenix activities, in which new companies are created to continue the business of companies that have been deliberately liquidated to avoid paying their debts
- misuse of trusts to conceal income.

The money laundering threat associated with superannuation fraud is considered separately.

INTELLIGENCE PICTURE

The actual value of criminal proceeds generated from tax and revenue crimes is very difficult to determine. However, the Cost of Crime report places estimates between \$1.86 billion and \$6.37 billion per year.

Tax and revenue crime is inextricably linked to money laundering. When criminal proceeds generated from tax and revenue crime already exist in the legitimate financial system (e.g. in a bank account), money laundering techniques are integral to layering and re-integrating the illicit funds. For this reason, many of the financial channels and criminal methodologies that are used to perpetrate tax and revenue crimes are also used to launder the resulting criminal proceeds. For example, professional service providers, such as lawyers, accountants and offshore service providers, are used to establish onshore and offshore business structures and associated banking arrangements to obscure transactions, assets and beneficial ownership.

When cash payments are used for income tax evasion purposes by both individuals and businesses, proceeds are likely to be used to support lifestyle purchases or business expenses. These funds, unless in significant amounts, are unlikely to require laundering.

Tax and revenue crimes are perpetrated by both opportunistic individuals, as well as national and transnational serious and organised crime groups impacting Australia, who leverage both complicit and non-complicit professional service providers. Serious and organised crime groups are generally involved in larger-scale tax and revenue crimes and money laundering schemes.

OUTLOOK

Tax and revenue crime will continue to pose a high money laundering threat over the next three years, given the enduring nature and extent of tax crimes and its perpetrators, and its intrinsic connection to money laundering. The flexibility and array of traditional financial channels and legal intermediaries ensures new opportunities and vulnerabilities are continually identified and exploited by agile and opportunistic criminals to launder illicit funds generated from tax crimes.



Combatting tax and revenue crime is a key government priority. In July 2023, the Australian Government provided \$223.8 million to the ATO to extend the Serious Financial Crime Taskforce through to 30 June 2027 and merge with the ATO's new Serious Organised Crime program. The extension and merging of the Serious Organised Crime program will maximise the disruption of organised crime groups that seek to undermine the integrity of Australia's public finances.

Between 1 July 2015 and 31 March 2024, the ATO's Serious Financial Crime Taskforce has progressed cases that have resulted in:

- completion of 2,152 audits and reviews
- conviction and sentencing of 38 people
- raised liabilities of over \$2.182 billion
- collected \$842 million.¹³

GOVERNMENT-FUNDED PROGRAM FRAUD

RISK RATING

Government-funded program fraud is assessed as posing a **high** and **increasing** money laundering threat. This category of risk includes frauds that are committed against Commonwealth benefit programs and assistance available to the Australian community. These include child care benefits fraud, family day care fraud, Medicare fraud, or fraud against the National Disability Insurance Scheme (NDIS).¹⁴

INTELLIGENCE PICTURE

There are no reliable estimates of the total cost of government-funded program fraud in Australia. However, losses are assessed to be significant. Like tax and revenue crime, criminal proceeds generated from these crimes often already exist in the legitimate financial system, and money laundering techniques are integral to layering and re-integrating the illicit funds. While the criminal methodologies differ (discussed below), many of the financial channels that are used to perpetrate government-funded program fraud are also used to launder the resulting criminal proceeds. For example, the use of professional service providers to help establish onshore and offshore business structures and associated banking arrangements.

Methodologies used vary in complexity and sophistication. They often involve inflating or falsifying invoices, over-claiming for services delivered, using stolen personal information to claim additional benefits, using 'cleanskins' to act as company directors and illegal phoenixing.

OUTLOOK

Government-funded program fraud will continue to pose a high money laundering threat over the next three years. The scale of criminal misuse will likely increase in line with increased government expenditure. Ongoing government funding for programs and services create continued opportunities for individuals and groups to defraud these programs.

¹³ Please refer to the [Serious Financial Crime Taskforce](#) webpage for more details of their work and operational outcomes.

¹⁴ Please refer to the [Commonwealth Department of Public Prosecutions](#) website for a more comprehensive list of types of government-funded program frauds committed in Australia.



The Australian Government will soon provide nearly \$50 billion per year to help individuals and businesses provide critical care and support to millions of Australians. Programs and services will span a range of industries including childcare, aged care, disability support, vocational education and training, and employment.

CASE STUDY 1

Australian authorities investigated a network of individuals suspected of establishing and purchasing companies in order to conduct fraud against the NDIS. The network reportedly claimed payments on behalf of vulnerable participants. Proceeds from the fraudulent claims are believed to have been used to purchase assets such as digital currency and Australian residential/commercial real estate. Key financial controllers of the network conducted rapid transfers between multiple bank accounts, likely in an effort to obscure the transaction chain. Investigations are continuing with charges laid and regulatory responses in progress.

CASE STUDY 2

The Fraud Fusion Taskforce conducted an investigation into several suspected fraudulent NDIS providers based in Western Sydney. The AFP arrested six people allegedly involved in a crime syndicate and are pursuing criminal prosecutions in relation to over \$4 million in allegedly fraudulent NDIS claims. Over \$2 million in suspected tainted assets were seized during the search warrants including eight kilograms of gold bullion from a vault at a secure premises, worth approximately \$600,000.

SCAMS

RISK RATING

Scams are assessed as posing a **medium** and **increasing** money laundering threat. For the purpose of this assessment, this category of threat includes the following scam types: romance, investment, product and service, threats and extortions, job and employment, and unexpected money.¹⁵

INTELLIGENCE PICTURE

Australians are estimated to have lost approximately \$2.7 billion to scams in 2023.¹⁶ This is a 13 per cent decrease in the total value of reported losses in 2022. The true scale and value of scams impacting Australia are almost certainly higher than current estimates, given many victims do not report their losses to authorities.

Scams targeting Australians are largely orchestrated by offshore criminals, including by transnational serious and organised crime groups. Criminal proceeds generated from scams often already exist in the legitimate financial system. Money laundering techniques are then integral to layering and transferring criminal proceeds offshore to the offenders who have orchestrated the scam. Domestic bank accounts, particularly the use of mule accounts, play a key role in these activities and the use of digital currencies as a payment method has increased significantly in recent years (see the call-out box below). While digital currencies can be traced by law enforcement, certain features of the digital currency ecosystem

¹⁵ Please refer to the Australian Government's [National Anti-Scam Centre's Scamwatch](#) website for a detailed explanation of these activities.

¹⁶ Australian Competition & Consumer Commission, Targeted Scams: Report of the ACCC on scams activity 2032, April 2024.

that help increase anonymity, such as mixer services, have added additional challenges for reporting entities and authorities in detecting and stopping the transfer of scam funds.

Scam methods are constantly evolving. Offenders are becoming increasingly sophisticated in their delivery and execution, and criminal activity can be more difficult to detect and disrupt. Offenders leverage emerging technologies and the growing number of customers interacting through digital channels to reach more victims in a cost-effective manner. Examples include impersonating phone numbers, email addresses or websites of legitimate organisations, or creating fake ads, social media profiles and reviews.



KEY ATTRIBUTES OF SCAMS IN AUSTRALIA

The Australian Competition and Consumer Commission (ACCC) produces an annual [Targeting Scams report](#) explaining key trends in scam activity impacting Australia. The most recent report was released in April 2024 and covers the 2023 calendar year. Key findings are summarised below.

- Australians made 600,000 reports of scams, with aggregate losses of more than \$2.7 billion.
- Businesses, including small and micro businesses, reported losses of \$29.5 million to Scamwatch (ACCC).
- The costliest scams to Australians are conducted via phone call, social media and email, although text messages are the most commonly-reported means of scam contact. Bank transfers, cryptocurrency and credit cards are the most common type of payment methods.
- Australians aged 65 and over were the most commonly-targeted victims, followed by Australians aged between 55-64 years. Scams also target vulnerable members of the community such as Indigenous Australians, members of culturally and linguistically diverse communities and people with a disability.
- Investment scams were most commonly reported, accounting for \$1.3 billion in losses, followed by remote-access scams (\$256 million in losses) and romance scams (\$201 million in losses).

OUTLOOK

Scam activity impacting Australia is likely to pose an increasing money laundering threat over the next three years. Australians will remain attractive targets, given the country's comparative wealth in the region. The scale and value of scam activity will almost certainly keep pace with the growth of emerging technologies and the number of customers interacting via digital channels. Scams will also become increasingly challenging to disrupt if criminal groups continue to exploit AI in the delivery and execution of these offences. Bank accounts and digital currency will almost certainly remain the most commonly-used channels to layer scam proceeds, both onshore and offshore.



GOVERNMENT ANTI-SCAM ACTIONS

In July 2023, the Australian Government launched the National Anti-Scam Centre (the Centre). The Centre aims to improve cooperation and information sharing between government and industry to help deliver better protection for Australian consumers and businesses from sophisticated scam activity. The Centre collaborates with other regulators and government agencies, consumer groups and private sector businesses, including telecommunications providers, digital platforms and banks, whose systems are used and subverted by scammers.

The Government has also committed to new industry codes for banks, telecommunications companies and digital platforms to better protect consumers by outlining their responsibilities to prevent, detect, disrupt and respond to scams.

ILLICIT TOBACCO

RISK RATING

The illicit tobacco market is assessed as posing a **medium** and **increasing** money laundering threat.

The illicit tobacco market includes the production of tobacco plant or leaf, or the manufacture of tobacco products. Illicit tobacco may include cigarettes, cigars and loose tobacco (also known as 'chop-chop'), and tobacco leaf and plant matter. Tobacco is illicit when it is grown, manufactured and/or produced in Australia without an appropriate excise licence, even if the tobacco is intended for personal use. Tobacco is also illicit when it is imported into Australia without customs duty being paid. It is illegal to grow tobacco in Australia without the appropriate excise licence. There have been no licenced tobacco growers since 2006 or manufacturers in Australia since 2015.

INTELLIGENCE PICTURE

Australia's illicit tobacco market is driven by high demand and large potential criminal profits. The most recent estimates suggest the illicit market cost Australia approximately \$2.3 billion in lost excise revenue in 2021-22.¹⁷ Serious and organised crime groups have developed an increasing presence in the importation and distribution of illicit tobacco across Australia in recent years. The domestic illicit tobacco market has strong ties to the Middle East and Southeast Asian markets, which are principal sources of tobacco trafficked through Australia.

Money laundering is a key enabler of the illicit tobacco market. Given the strong ties to international markets and transnational crime groups, illicit funds are sometimes moved via trade-based money laundering techniques. Other money laundering methodologies include the use of onshore and offshore business structures, the use of remittance businesses, structured and high-value cash transactions, and third-party transfers.



ILLICIT TOBACCO TASKFORCE

On 1 July 2018, the Illicit Tobacco Taskforce (ITTF) was established to enhance the ability of the ATO and partner agencies to detect, disrupt and dismantle serious and organised crime groups dealing in illicit tobacco. In the financial years 1 July 2018 to 30 June 2023, the ITTF seized over one billion cigarette sticks and over 210 tonnes of loose leaf and molasses tobacco, with an estimated excise duty value of over \$1.7 billion. In addition, approximately 360 acres of domestic illicit tobacco crops were located and destroyed during ITTF operations. These seizures demonstrate the effective effort to stamp out illicit tobacco.

OUTLOOK

Australia's illicit tobacco market is likely to pose an increasing money laundering threat over the next three years. Domestic demand will almost certainly remain high and organised crime groups will almost certainly continue to participate in trafficking and supply activities, given the high value of potential profits.

¹⁷ATO, Illicit Tobacco, Australian Government, 2023, accessed 14 December 2023. <https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/illicit-tobacco>

PURE CYBERCRIME

RISK RATING

Pure cybercrime is assessed as posing a **medium** and **increasing** money laundering threat.

For the purpose of this assessment, pure cybercrime refers to crime directed at computers or other information communication technologies and networks, such as hacking, spreading computer viruses and other malware, ransomware, business email compromise and distributed denial-of-service.

INTELLIGENCE PICTURE

Pure cybercrime is largely driven by large potential profits and relatively easy access to victims. The total proceeds of pure cybercrime to Australian individuals, businesses and Government is estimated to be \$3.9 billion in 2020-21.¹⁸ Individuals account for most of these losses and the number of reported victims is increasing. Ransomware and business email compromise pose the greatest cybercrime threats. They are the most commonly reported offence types and yield the most profits as victims are generally defrauded or extorted for ransom.

The level of serious and organised crime group involvement in pure cybercrime targeting Australians is assessed as high. Estimates provided by the Australian Institute of Criminology suggest it ranges from 50 to 90 per cent.¹⁹ Offences are largely orchestrated by offshore criminals, and money laundering techniques are used to layer criminal proceeds domestically before being transferred overseas. Domestic bank and remittance accounts, particularly the use of mule accounts, play a key role in moving illicitly-gained profits, while the use of digital currency and gold bullion has increased in recent years.

Australian critical infrastructure networks regularly experienced targeted and opportunistic malicious cyber activity in 2022-23. Critical infrastructure networks continue to be targeted by malicious cyber actors worldwide and this is not limited to Australia. Malicious cyber actors steal or encrypt data for ransom, or gain insider knowledge for profit or competitive advantage, and some actors may attempt to degrade or disrupt services. State cyber actors continue to target government and critical infrastructure as well as connected systems and their supply chains as part of ongoing cyber espionage and information-gathering campaigns.



The AUSTRALIAN GOVERNMENT RESPONSE TO CYBERCRIME

On 1 July 2022, the Australian Government committed \$9.9 billion over a decade to fund the Resilience, Effects, Defence, Space, Intelligence, Cyber Enablers (REDSPICE) program. The purpose was to enable the Australian Signals Directorate (ASD) to deliver forward-looking capabilities essential to maintaining Australia's strategic advantage and capability edge in relation to cyber security. This builds on existing investment under the Cyber-Enhanced Situational Awareness and Response (CESAR) Plus Program, which funds the delivery of ASD defensive cyber capability from July 2020 to June 2030.

Key deliverables include:

- improved critical infrastructure resilience against sophisticated cyber attacks

¹⁸ R Smith & A Hickman, *Estimating the costs of serious and organised crime in Australia, 2020-21*. Statistical Report no. 38. Australian Institute of Criminology, 2022.

¹⁹ R Smith & A Hickman, *Estimating the costs of serious and organised crime in Australia, 2020-21*. Statistical Report no. 38. Australian Institute of Criminology, 2022.

- increased visibility of threats to Australia’s critical systems
- improved intelligence-sharing across government and industry; and
- increased nation-wide cyber-incident response capabilities.

On 23 June 2023, the Australian Government appointed the first National Cyber Security Coordinator, led by the Department of Home Affairs. The Coordinator leads national cyber security policy, the coordination of responses to major cyber incidents, whole-of-government cyber incident preparedness efforts and the strengthening of Commonwealth cyber security capability.

OUTLOOK

Pure cybercrime is likely to pose an increasing money laundering threat over the next three years. The scale and value of criminal activity will almost certainly keep pace with emerging technologies, including the rise of AI used to deliver and execute crimes, as well as the growing number of customers acquiring goods and services online.

CASE STUDY 3

AUSTRAC identified an Australian company entity being used by an offshore cybercriminal syndicate to move business email compromise funds offshore. They did this using international shell companies, digital currency and professional service providers, including an accountant. The listed director of the company was highly likely the victim of identity theft or mule activity.

The company attempted to receive the fraudulently obtained proceeds into an Australian bank account, including over \$92,000 from a property settlement-related business email compromise in 2020. The funds were frozen and returned to the victim before they could be sent offshore. However, the account successfully received more than \$290,000 from several different overseas victims over four months in 2020, before layering and moving the funds offshore.

It is highly likely the company used digital currencies to launder the criminal proceeds. The entity deposited funds that were immediately converted into digital currency and withdrawn from the DCE’s custodial account. Two additional offshore corporate accounts were linked to the entity through the DCE and likely used to launder the criminal proceeds through shell companies.

IDENTITY CRIME

RISK RATING

Identity crime is assessed as posing a **medium** and **increasing** money laundering threat.

For the purpose of this assessment, identity crime refers to the use of a fabricated, manipulated, stolen or assumed identity in the commission of a crime, such as fraud. While identity crime is a fundamental enabler of money laundering, this section focuses specifically on the nature and extent of money laundering activities (i.e. the money laundering threat) from proceeds gained through identity fraud.

INTELLIGENCE PICTURE

Identity crime is a pervasive and persistent activity impacting Australian individuals and businesses. During consultations for this assessment, it was noted as a key challenge by law enforcement agencies, reporting entities, government service providers and industry representatives alike. The Cost of Crime report estimates identity crime facilitates the loss of approximately \$2.2 billion in goods, services, credit loans and cash per year.

Identity crime impacting Australia is committed by individuals as well as national and transnational serious and organised crime groups. The level of involvement by serious and organised crime groups is assessed as medium. The Cost of Crime report estimates between 20 and 60 per cent of criminal proceeds linked to identity crime are attributable to these groups. Where transnational serious and organised crime groups are involved, there is often a strong link to cybercrimes. For example, they might commit a cyber attack to steal personal identity information, which is then used to commit other crimes or sold on darknet marketplaces.

Criminal proceeds generated from identity crime are generally already in the legitimate financial system. Money laundering techniques are then used to layer these proceeds domestically, with some funds ultimately being transferred overseas. Domestic bank and remittance accounts, particularly the use of mule accounts, play a key role in these activities.

OUTLOOK

Identity crime is likely to pose an increasing money laundering threat over the next three years. Identities will remain an important and therefore exploitable commodity as the digital economy and interaction through online channels continues to expand. The fundamental role of using stolen identities will remain key to the ongoing increase in identity crime.

CASE STUDY 4

A joint investigation as part of the Serious Financial Crime Taskforce identified a major international criminal syndicate using fraudulently-obtained identities to commit large-scale cybercrimes. The syndicate used stolen identity information purchased from darknet marketplaces, single-use telephone SIM cards and fake email accounts to mimic the identities of victims.

The false identities were used to open at least 60 bank accounts at various Australian institutions. A phishing website that mimicked a superannuation fund was used to harvest members' usernames and passwords. The syndicate used this information to access members' accounts and withdraw funds from the superannuation and share trading accounts of victims, before depositing the stolen funds into the fraudulent bank accounts. The value of stolen funds is estimated to be in excess of \$3.3 million. The group laundered \$2.5 million through transferring the funds to a contact in Asia. The offshore individual purchased, and on-sold luxury goods, prior to remitting the proceeds back to the syndicate in Australia through digital currencies.

A Melbourne woman was subsequently sentenced to five years and six months imprisonment for her central role in the syndicate.

BRIBERY AND CORRUPTION

RISK RATING

Bribery and corruption are assessed as posing a **medium** and **stable** money laundering threat.

INTELLIGENCE PICTURE

The total value of criminal proceeds generated from bribery and corruption is difficult to quantify, but is almost certainly less than other threats considered in this assessment. The Cost of Crime report estimates the amount to be between \$12 million and \$90 million a year. In addition, it is likely that only a smaller portion of criminal proceeds require laundering as individuals may spend a considerable amount on lifestyle expenses.

Known and suspected instances of bribery and corruption continue to be identified across Australia, and the country remains an attractive destination for criminal proceeds generated offshore.²⁰ Particularly vulnerable scenarios include the provision of a service to government (notably where that service is specialised), property development, or in acquiring government approvals or permits.

Common methodologies used to launder the proceeds of bribery and corruption include the use of cash, business structures and trusts, third parties, and intermediaries such as lawyers and accountants. Because bribery and corruption cases often involve a business or commercial enterprise, business structures and associated banking arrangements are often used as vehicles to layer and integrate criminal proceeds.



POLITICALLY EXPOSED PERSONS (PEPs)

A PEP is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas.²¹ They can be an attractive target for bribery and corruption given their capacity to influence government spending and budgets, procurement processes, development approvals and grants. Foreign PEPs are also considered higher-risk customers in terms of money laundering given their potential to receive and handle the proceeds of bribery and corruption. Reporting entities who provide services to foreign PEPs are required to undertake enhanced customer due diligence for these customers. Domestic and international organisation PEPs can also be high-risk customers, and reporting entities must apply enhanced due diligence where they assess high ML/TF risk.

Australia's financial system is mainly exposed to PEPs through domestic and international funds transfers and gambling activity at domestic casinos. In known and suspected cases, PEPs have been observed using the following methodologies to move suspicious funds into Australia:

- use of bank accounts in the names of family members
- purchase of Australian real estate
- large cash transactions
- rapid movement of funds.

²⁰ In 2023, Australia received a score of 75 out of 100 on Transparency International's Corruption Perception Index report (CPI 2023). This is a 10-point decline from ratings in CPI's 2012 report. The CPI 2023 notes that while Australia lags behind its G7 and G20 peers on corporate transparency measures, Australia's Third Open Government Partnership National Action Plan 2024-2025 indicates it is taking steps toward greater corporate transparency by committing to a public beneficial ownership register for companies.

²¹ The AML/CTF Rules defines three types of PEPs: domestic, foreign and international organisation PEPs. Immediate family members and/or close associates of these individuals are also considered PEPs. Refer to the AML/CTF Rules for further details.

OUTLOOK

Bribery and corruption are likely to remain a stable money laundering threat over the next three years. Australia's strong and stable economy, particularly within the region, will continue to attract foreign criminal proceeds. However, the scale and level of involvement of serious and organised crime groups in bribery and corruption impacting Australia is unlikely to increase in the near term.

CASE STUDY 5

In 2019, a foreign PEP reportedly carried \$400,000 in cash into a domestic casino. They refused to disclose information about the source of funds, other than it coming from a friend who owed them money. Due to large cash deposits in the previous 24 hours, the casino accepted only \$100,000 of the cash. The next day, the PEP returned and deposited \$200,000 in cash and again refused to disclose the source of the funds.

SUPERANNUATION FRAUD

RISK RATING

Superannuation fraud is assessed as posing a **medium** and **stable** money laundering threat.

INTELLIGENCE PICTURE

Australia has one of the largest superannuation systems in the world. The superannuation sector manages approximately \$3.7 trillion in assets and approximately 17 million member accounts. Estimates suggest the volume of fraud activity is 0.14 per cent of the total value of superannuation assets under management. Using this estimation, superannuation fraud generates approximately \$4.6 billion per year.

Superannuation fraud is typically committed in two ways. In the first scenario, a legitimate account owner makes a fraudulent claim for early release of their funds. This generally involves submitting numerous financial hardship claims for early withdrawal, falsifying documents and conducting rollovers to other superannuation accounts or self-managed superfunds. Criminal proceeds generated in this scenario usually do not require laundering as the individual simply withdraws and uses the funds for personal expenses. The second scenario involves criminals who illegally access a legitimate superannuation account and submit fraudulent claims to access the funds. This type of fraud is primarily committed by serious and organised criminal groups and criminal proceeds usually require laundering.

Superannuation fraud can also occur in cases of elder abuse and financial abuse associated with domestic and family violence. However, while there is limited evidence of the scale of this activity, any criminal proceeds linked to these cases usually do not need to be laundered.

The level of involvement of national and transnational serious and organised crime groups is assessed to be low to medium. The Cost of Crime report estimates these groups are responsible for between 10 and 50 per cent of criminal proceeds generated from superannuation fraud. These groups primarily use compromised personal information obtained from cybercrime to fraudulently access superannuation funds. The stolen funds are layered through rapid or complex transfers to superannuation staging accounts or self-managed super funds (SMSFs). The proceeds are ultimately withdrawn to bank accounts as seemingly-legitimate superannuation earnings. Other known laundering methodologies include the exploitation of luxury goods and digital currencies to move proceeds between jurisdictions.

OUTLOOK

Superannuation fraud is likely to remain a stable money laundering threat over the next three years. The fundamental role of superannuation for Australia's ageing population, and the ongoing increase in superannuation balances, will ensure this sector remains highly attractive to criminal individuals. Given that money laundering methodologies are used to move superannuation funds that are illegally accessed, the money laundering threat from superannuation fraud will remain an ongoing issue.

AN INTERNATIONAL PERSPECTIVE



To better understand Australia's role in international money laundering funds flows, AUSTRAC sought relevant information and perceptions from partner FIUs as part of this assessment. An overview of survey findings is at [Appendix F](#). Overall, responses suggest Australia is an important destination country for illicit proceeds generated by countries in the region, particularly the Pacific, as well as Asia. Outside of the region, Australia appears to be a comparatively less attractive destination for proceeds of crime. This is likely because Australia has a mid-tier economy and smaller criminal markets compared with other global peers.

Partner FIUs identified the following factors that make Australia an attractive destination for illicit funds:

- ease of travel between Australia and their country
- close associations between organised crime groups in both countries
- favourable border entry arrangements for certain nationalities
- Australia's economic attractiveness, especially its favourable currency conversion
- conditions afforded to foreign investors.

HIGH-RISK JURISDICTIONS

High-risk jurisdictions are those that are considered to pose the greatest threat as a source, conduit or destination country whose nationals generate or move illicit proceeds and laundered funds into Australia. Broadly, their threat can be evaluated by assessing the capability and intent of those foreign nationals for moving funds to Australia. The greater the ease with which illicit funds can be moved from a foreign jurisdiction to Australia, the greater that jurisdiction's capability.

Factors that may facilitate the international movement of illicit funds include:

- proximity (since distance can be a proxy for transport and communication costs)
- shared characteristics (since these make it simpler for countries to do business)
- weak money laundering controls and financial regulation (reducing visibility of money flows and ability to detect and disrupt illicit funds)
- the size and presence of channels and networks through which illicit funds can move (such as trade, foreign investment, diasporas, organised crime links and physical cross-border movements).

The greater the illicit activity within a foreign jurisdiction, the greater its intent to move illicit funds offshore. Factors that may indicate the amount of illicit activity in a country include criminality, resilience, corruption and the size of the shadow economy.

Generally, jurisdictions considered to pose a high threat would be those with high levels of both capability and intent, including those where multi-national serious criminal organisations that conduct

professional laundering activities operate. However, analysis has revealed that a small handful of jurisdictions possess capabilities that far surpass the capabilities of others. These jurisdictions pose the greatest threat to Australia irrespective of their level of intent and even proximity, being located in Asia, Europe and the Americas. They share large volumes of trade with Australia, have high levels of foreign investment and large diaspora communities or volumes of international travellers, or both.

A number of jurisdictions are emerging as a medium threat and are broadly those with fairly high levels of intent combined with medium capabilities. These are located across multiple global regions, in particular Southeast Asia.

Multi-national money laundering organisations (MLOs) and criminal organisations

While it is important to understand the money laundering risk linked to foreign jurisdictions, it is also important to recognise that highly sophisticated MLOs and transnational criminal organisations operate across the world and conduct money laundering in multiple jurisdictions. Transnational criminal groups by definition are not limited to any one country, and generate profits from criminal ventures globally, meaning they can look to launder illicit funds from all over the globe through Australia.

MLOs are increasingly global in their reach, linking criminal groups around the world and enabling these criminal groups to develop in sophistication. While high risk jurisdictions provide one lens of analysis, understanding money laundering risk must also consider MLOs, transnational criminal organisations and their global enterprises.

SECRECY JURISDICTIONS AND TAX HAVENS

Secrecy jurisdictions and tax havens, including countries and regions, pose an enduring money laundering risk given the lack of oversight and the provision of facilities that obscure taxation revenues and illicit funds. These jurisdictions continue to provide the opaque legal structures that allow professional service providers to exploit Australia's taxation and wealth controls. Numerous offshore service providers operating in secrecy jurisdictions and tax havens have been flagged for adverse reporting to AUSTRAC, International Consortium of Investigative Journalists data leaks, regulator breaches and high-risk transactional behaviour.



TRADE-BASED MONEY LAUNDERING (TBML)

Australia's open, stable and liberal trade environment makes TBML an attractive money laundering channel. It is increasingly identified by domestic and international authorities as a significant channel to move criminal proceeds across borders largely hidden from scrutiny by financial regulators.

TBML is broadly defined as disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins. In practice, TBML is a specific type of money laundering frequently used in combination with other money laundering activities such as value transfer and misrepresentation of goods.

TBML operates in the highly-specialised global environment of customs, excise and revenue collection. The international trade system is subject to a range of vulnerabilities that can be exploited. Large volumes of global trade flows provide opportunities to obscure individual illicit transactions, particularly when combined with foreign exchange transactions or diverse trade-financing arrangements.

Common indicators of TBML include:

- evidence of over- or under-invoicing
- companies trading in higher-risk sectors or goods where prices may be highly subjective, such as natural resources, electronics, luxury goods, vehicles, textiles and scrap or precious metals (including bullion)
- trading activity inconsistent with a customer's profile, inconsistent with global market trends, or via relationships that do not make economic sense
- overly complex company or directorship structures
- upon receiving an incoming international transaction, funds are immediately:
 - split and transferred to multiple domestic company bank accounts; or
 - sent back overseas, often to the ordering company or country ('U-turn activity' or 'carouseling')
- funds received from, or exports sent to or through, higher-risk jurisdictions
- significant domestic transfers or cash transactions that exceed expectations for that business
- companies operating in porous border regions close to higher-risk jurisdictions
- use of trade finance products that appears inconsistent with received funds or export history
- discrepancies in the documents supplied to support trade finance, such as:
 - variations in the quantity of shipping containers noted in different documents
 - unusual shipping routes
 - significant gaps between actual shipment dates and payment dates.



VULNERABILITIES

Money laundering vulnerabilities exist at the national, sectoral and channel level, as well as at the individual entity level. This assessment considers national and sectoral/channel vulnerabilities only. Individual businesses must consider the money laundering risks they face in providing their services. Assessments at the sector and channel level will be of benefit to businesses when undertaking their own enterprise risk assessments.

NATIONAL VULNERABILITIES

National vulnerabilities create structural or systemic weaknesses that adversely impact the effectiveness of Australia's AML/CTF framework. This assessment identified five key national vulnerabilities:

- Australia's open, globally-integrated economy
- persistent use of unregulated sectors, channels and mechanisms
- complexity of the financial and payment ecosystem
- gaps in AML/CTF regulation of key designated non-financial businesses and professions
- poor transparency of companies and trusts.

AUSTRALIA'S OPEN ECONOMY

Australia has an open and free economy that provides businesses and investors easy access to its financial system and real assets. However, these same features are exploited by money launderers. Legitimate domestic financial channels are fundamentally important pathways for money launderers to place, layer and integrate criminal proceeds domestically and internationally. The integration of Australia's economy with global goods, services and capital markets, coupled with the increasing speed of financial transactions, creates significant challenges for reporting entities and authorities in discerning illicit funds flows from legitimate transactions. This vulnerability is exacerbated when legitimate financial and business links exist between Australia and higher-risk jurisdictions or countries with weak or ineffective AML/CTF frameworks.

PERSISTENT USE OF UNREGULATED SECTORS, CHANNELS AND MECHANISMS

Money launderers continue to exploit sectors, channels and mechanisms that are subject to little or no AML/CTF regulation or those that deliberately circumvent or avoid regulation. In Australia, this largely includes unregistered remitters, luxury goods retailers, luxury goods, cash-in-transit companies, offshore service providers and unregulated aspects of the digital currency ecosystem, such as peer-to-peer (P2P) traders.²² It also includes other offshore services that Australians transact with, such as online gambling service providers.

Globally and nationally, it is not possible for an AML/CTF framework to have effective oversight of every sector, channel or mechanism that can be used for money laundering. Despite best efforts and intentions, unsighted channels, blind spots and opaque mechanisms remain. These challenges are exacerbated by the persistent evolution and connectedness of global economies and technologies, including the emergence of payment platforms on social media platforms. Increasingly, money launderers exploit AML/CTF vulnerabilities across jurisdictional boundaries, but impacts are felt domestically. Digital currencies and the emergence of decentralised autonomous organisations are good examples of the increasing use of channels that often sit outside AML/CTF regulatory frameworks.

COMPLEXITY OF THE FINANCIAL AND PAYMENTS ECOSYSTEM

Over the past two decades, the payments landscape has undergone a significant transformation with electronic payment instruments displacing both cheques and cash.²³ Funds now move faster, further and more cheaply than ever before; consumers have a range of payment options like contactless payments, digital wallets and the New Payments Platform (NPP). Developments in the payments ecosystem are generally end-user focused, aimed at ensuring consumers and businesses benefit from lower transaction costs and enhanced service delivery. However, these same conveniences are also attractive for quickly placing and layering illicit funds. This creates additional challenges for financial institutions and authorities in detecting, tracing and freezing illicit funds, as well as cancelling or reversing potentially fraudulent transactions.

Online payment services in Australia were initially controlled by major banks, which operated an end-to-end service. This has evolved and now there are numerous and varied online payment service providers (OPSPs) who have one or more roles in the payments ecosystem (see call-out box). The rapid growth of OPSPs in the payments ecosystem exposes Australia to money laundering vulnerability.

²² The Australian Government is proposing legislative reforms that will extend AML/CTF regulation to additional digital asset services. Consultation papers were released in 2023 and 2024. Please refer to the section [Digital currencies](#) for more details.

²³ In the financial year 2020-21 alone, Australians made around 625 electronic transactions per person on average, compared to 275 a decade ago.

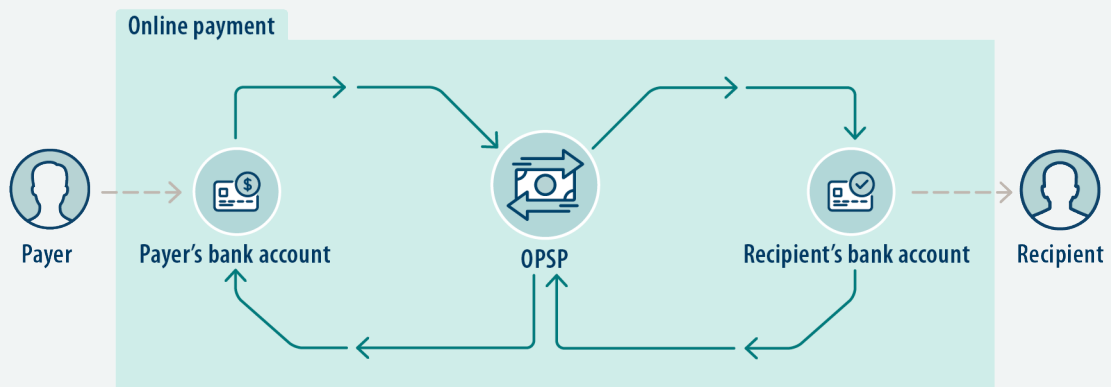
For example:

- The design of some OPSP products and services may not fit within existing regulatory frameworks, or are designed expressly to avoid regulation. It may be difficult for reporting entities to determine whether the OPSPs' product or service meets the definition of a 'designated service' under the AML/CTF Act, whether a provider is required to enrol with AUSTRAC and what reporting obligations they may have.
- The introduction of additional parties to the payment process can reduce end-to-end visibility of the transaction chain. Additionally, some OPSPs require minimal credentials on a receiver.
- From cost and technology perspectives, OPSPs have fewer access barriers for businesses and customers. They can offer merchants more choices and better pricing compared to traditional banks. These commercial benefits are likely to see the continued disruption of traditional payment gateways and the growth of OPSPs.

The complexity and interconnectedness of Australia's financial and payments ecosystem will remain an enduring money laundering vulnerability over the next three years, particularly given the likely growth of the payments ecosystem, including offshore entities providing settlement services to domestic individuals.



WHAT IS AN ONLINE PAYMENT SERVICE PROVIDER?



An OPSP is a third party that provides services for businesses to accept online payments by linking customer payment information to the business account, and facilitating the transaction between their respective financial service providers. OPSPs ensure transactions make it from the customer to the business securely.

OPSPs facilitate a constantly-evolving range of transaction types including:

- purchased payment
- peer-to-peer payments
- micropayments and donations
- crowdfunding
- digital wallets
- Buy Now, Pay Later
- e-commerce
- subscriptions.

GAPS IN AML/CTF REGULATION OF KEY DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Certain types of services provided by designated non-financial businesses and professions are not currently regulated by AUSTRAC, notably those provided by ‘gatekeeper’ professions such as lawyers, accountants and trust and company service providers, as well as real estate agents and dealers in precious metals and precious stones.²⁴ While all Australian entities are subject to Australian sanction laws, many designated non-financial businesses and professions are not currently subject to the due diligence, transaction reporting and supervision requirements outlined in the AML/CTF Act.

Given the role of gatekeeper-type designated non-financial businesses and professions in facilitating money laundering (either wittingly or unwittingly), this regulatory gap creates a vulnerability for Australia. For example, as noted throughout this assessment, criminals often use complex business structures and associated banking arrangements to conceal wealth and obfuscate money laundering activity. Such structures often rely on legal professionals and corporate service providers for their establishment and operation. For real estate assets in Australia, for example, lawyers, accountants and real estate agents play an important role in facilitating the purchase, sale, transfer of ownership and financing arrangements.

The Australian Government is currently developing legislation for the most substantial phase of proposed reforms of the AML/CTF Act. The proposed reforms include extending the AML/CTF Act to certain services provided by businesses such as lawyers, accountants, trust and company service providers, real estate agents, property developers and dealers in precious metals and precious stones.

A detailed discussion of money laundering vulnerability associated with individual types of designated non-financial businesses and professions is provided in the [Professional and other service providers](#) section.

POOR TRANSPARENCY OF TRUSTS AND COMPANIES

There are opportunities for money launderers to create opaque business structures in Australia to help conceal their illicit activity.

Factors that make this easier include:

- The absence of requirements to register ultimate beneficial ownership information for companies, with nominees permitted to register as non-beneficial shareholders and shareholders (beneficial or non-beneficial) permitted to appoint nominee directors.
- The absence of state- or federal-level transparency mechanisms related to trusts.

The inability to access public and timely information on the ultimate beneficial owners of unlisted corporate entities, assets and financial infrastructure creates a significant money laundering vulnerability for Australian authorities and industry. It can prevent financial institutions and other businesses from verifying whether they are engaging with a criminal entity.

The use of professional service providers to establish or operate corporate and financial infrastructure makes it more difficult to identify ultimate beneficial ownership and connections to sanctioned entities. The use of trusts, powers of attorney or third-party authorities also increases the potential for anonymity and increases money laundering risk. The lack of obligations for designated non-financial businesses and professions, such as lawyers and accountants, to undertake due diligence on their clients or monitor for suspicious activities further exacerbates this risk.

A detailed discussion of money laundering vulnerability associated with individual legal structure types is provided in the [Legal structures](#) section.

²⁴ A notable exception relates to solicitors who must report cash transactions of \$10,000 or more – or the foreign currency equivalent – to AUSTRAC under the FTR Act.



IMPROVING AUSTRALIA’S CORPORATE REGISTRATION SYSTEM

Australia is currently stabilising and uplifting its 30 business registers. The program has already introduced the Director identification numbers regime, which is verifying the identity of company directors and will be linked to the companies register in future uplifts.

As part of the Government’s multinational tax integrity election commitment, Australia is in the process of implementing a public register of beneficial ownership information. The aim is to ensure transparency of who actually owns or controls companies and other legal vehicles (such as trusts) reducing Australia’s vulnerability to money laundering and tax evasion.

SECTORAL/CHANNEL VULNERABILITIES

This section assesses money laundering vulnerabilities across the following categories:

- cash
- banking sector
- non-bank financial services
- high-value assets and goods
- digital currencies
- professional service providers
- legal structures
- gambling sector.

Each risk rating provides the current overall assessment of vulnerability and an assessment of how it is likely to change over the next three years.

A detailed discussion is included for vulnerabilities that have been rated ‘very high’, ‘high’ and ‘medium’ *only*. The below legend is used throughout this section.

LEGEND

	Increase		Decrease		Stable		Emerging		
	Very Low		Low		Medium		High		Very high













THE MONEY LAUNDERING ECOSYSTEM: NETWORKED AND ENTRENCHED

This assessment presents vulnerability ratings of individual, separate channels or services. However, these channels and services should be considered as a connected and dynamic ecosystem. When one money laundering channel becomes impeded, illicit funds are swiftly diverted to alternative pathways.

Despite concerted efforts by industry and Australian authorities, many of the key vulnerabilities identified in this assessment are entrenched and were identified in Australia’s money laundering national threat assessment in 2011. These vulnerabilities persist for many reasons. These include their level of accessibility, the capacity to send funds at high speed and scale and the ability to obscure transactions and beneficial ownership.

CASH

SECTOR/CHANNEL	RATING	OUTLOOK
Cash - transfer of value		
Cash - store of value		
Cash-intensive businesses		
Cash smuggling (undeclared)		
Cash smuggling (declared cash movement)		

OVERVIEW

Cash is a mainstay of money laundering in Australia and abroad. Domestically, it is one of the most commonly restrained, forfeited or frozen asset types in criminal asset confiscation matters. It is exploited for its anonymity, accessibility, widespread acceptance and availability. Its use also requires minimal skills, knowledge and expertise.

Common money laundering methodologies involving cash include structuring, third-party deposits, co-mingling by cash-intensive businesses, money mules and bulk cash smuggling. Money laundering endures through channels with the capacity to process high volumes of cash. Notable examples include banks, casinos, pubs and clubs, remitters, cash-intensive businesses and luxury goods retailers. DCEs that accept cash deposits are an emerging channel through which cash is laundered.

Given the utility of cash in money laundering, this section examines the various channels and uses of cash to launder funds. While the underlying attributes of cash make it vulnerable to exploitation, there are individual differences in the vulnerabilities exploited and the subsequent level of risk.

CASH - TRANSFER OF VALUE

Risk rating

The use of cash as a value transfer mechanism, including the use of cash to make payments and exchange of cash between individuals, is assessed as posing a **very high** and **stable** money laundering vulnerability.

Key judgements

- Domestic criminals continue to exploit cash as a value transfer mechanism, using entrenched and highly effective methods that remain resilient to disruption.
- Industries that accept significant cash payments are particularly vulnerable to exploitation. Detecting illicit cross-border payments and bulk cash smuggling will remain difficult.

Domestic context

Despite historically low levels of transactional use of cash in Australia, an estimated \$101 billion remains in circulation.

Cash continues to be a key value transfer mechanism for opportunistic and serious and organised criminals alike because it:

- has one of the lowest levels of sophistication
- requires no specific knowledge skills or expertise

- is readily available and accessible
- carries minimal risk or costs (apart from the risk of theft or seizure)
- can be laundered quickly and at scale.

Businesses and sectors with limited or no AML/CTF oversight and high acceptance of cash payments are particularly vulnerable to criminal exploitation, including the transfer of cash to real estate, cryptocurrency, luxury and high-value goods.

CASE STUDY 6

Over a 12-month period, the director of a jewellery company deposited over \$1.6 million in cash into his business account. In the same reporting period, the company was recorded in more than 400 international funds transfer instructions (IFTIs) to a range of individuals and companies. The majority of them referenced jewellery or invoice numbers.

The company was also the subject of five suspicious matter reports (SMRs). These related to depositing high volumes of cash, receiving payments unauthorised by the *other* financial institution's customer and receiving, sending funds from or to an individual known to facilitate money laundering on behalf of organised crime groups.

Outlook

The use of cash as a transfer of value mechanism will continue to pose a very high money laundering vulnerability over the next three years, particularly as it will remain very difficult to identify the source of cash payments. The minimal skills, knowledge and expertise required to exploit cash will remain attractive to criminals of all sophistication levels.

CASH – STORE OF VALUE

Risk rating

The use of cash as a store of value mechanism is assessed as posing a **very high** and **stable** money laundering vulnerability.

Key judgement

- Cash hoarding is an attractive money laundering strategy for criminals of all sophistication levels. It has low barriers to entry, avoids interactions with reporting entities and allows rapid access to funds.

Domestic context

Cash is commonly hoarded in both the legitimate and illicit economies.²⁵ As a criminal instrument, cash hoarding is a simple and effective strategy for storing proceeds of crime. When funds are needed to pay associates, fund lifestyle expenses or further criminal activities, value is easily accessible. Cash hoarding does not require specialist skills, knowledge or expertise, and minimal costs are involved. It occurs outside of the regulated financial system and subsequently carries little risk apart from possible theft or seizure.

²⁵ Estimates by the Reserve Bank of Australia in 2018 suggested that between 50 to 75 per cent of all Australian banknotes in circulation were hoarded, mainly \$50 and \$100 banknotes.

CASE STUDY 7

As part of AFP's Taskforce AVARUS, a woman was sentenced to 2 years and 11 months' imprisonment for money laundering offences. She was involved in a Vietnamese alleged organised crime network, was the signatory to 89 individual bank accounts and was responsible for coordinating criminal funds across Australia.

Search warrants executed at a unit complex led to the discovery of more than \$2.6 million in cash concealed in several compartments in one of the units, including in a cavity beneath a religious shrine. A cash-counting machine, multiple phones and other items linked to money laundering were also discovered. This arrest disrupted the activities of a significant MLO which was servicing numerous criminal groups in Sydney.

CASE STUDY 8

In April 2022, three members of an Asia-based organised crime group were arrested and charged with money laundering and drug supply offences. \$4.7 million in cash was seized, indicating high levels of cash hoarding. Three digital currency ATMs and 5kg of illicit drugs were also seized in NSW.

The arrested individuals were likely sending funds to the USA for conversion into digital currency through a Latin American MLO. Intelligence indicates the MLO had a number of onshore associates to assist in laundering proceeds.

While the domestic network was temporarily disrupted, broader elements of the network likely remain active.

Outlook

The use of cash as a store of value mechanism will continue to pose a very high money laundering vulnerability over the next three years. There is limited opportunity for detection because these funds generally do not interact with regulated entities. The lack of skills, knowledge and expertise required to store cash also means it will remain attractive to criminals of all levels of sophistication.

CASH-INTENSIVE BUSINESSES

Risk rating

Cash-intensive businesses are assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Cash-intensive businesses remain an attractive channel to launder funds given their capacity to co-mingle and obscure illicit cash with legitimate revenue.
- Cash-intensive businesses have low barriers to entry and are exploited by criminals of all sophistication levels. More sophisticated criminals use professional service providers to create complex legal structures to hide beneficial ownership of and links to cash-intensive businesses.
- Cash-intensive businesses that also operate as remitters provide further opportunities to launder illicit proceeds through domestic and international networks.

Domestic context

Cash-intensive businesses provide a high volume of legitimate cash flows in which the proceeds of crime are integrated or co-mingled prior to entering financial institutions. Higher-risk cash-intensive businesses exist across a range of industries in Australia, most notably luxury goods retailers, daigou²⁶ operators and the labour-hire sector. The untraceable and anonymous nature of cash allows funds to be placed with limited oversight or detection, creating difficulties in differentiating genuine business earnings from proceeds of crime. Traditional cash-related money laundering strategies are commonly observed, including structured withdrawals, third-party deposits as well as withdrawals and funds transfers between business and third-party accounts.

Cash-intensive businesses are exploited by criminals of all sophistication levels. More sophisticated criminals use professional service providers to establish and control businesses, create complex structures to obfuscate ownership and conduct transactions on behalf of the criminal entity.

Further money laundering vulnerabilities exist where businesses offer other cash-intensive services in addition to their main commercial activity. These include:

- the operation of private ATMs
- remittance services, which extends the networks and systems available to facilitate cash deposits below threshold amounts and increases the risk of cuckoo smurfing.

Cash-in-transit businesses are fundamentally cash-intensive and enable the secure movement of high volumes of funds. This exposes operators to money laundering vulnerability, although the extent of criminal misuse is difficult to estimate.

CASE STUDY 9

A joint-partner agency taskforce led to the disruption of serious criminal behaviour by four foreign nationals in the construction industry. Their companies allowed for high volumes of legitimate cash flow to be combined with the frequent transfer of illicit funds and phoenixing of companies to avoid regulatory compliance and law enforcement interest. The syndicate used complex legal entity structures to layer and integrate funds.

CASE STUDY 10

In October 2018, a search warrant was conducted on a daigou business operating out of an Australian warehouse where large volumes of concealed cash, infant formula, pharmaceutical products and make-up and shoes were discovered. The co-owners of the daigou business were then charged under proceeds of crime laws. Investigations revealed that the co-owners had received cash proceeds from organised crime groups and further profited from the illicit cash on selling it to other daigou and to intermediaries who distributed it to gamblers at Australian casinos.

Outlook

Given the ease with which illicit funds can be co-mingled with legitimate profits, cash-intensive businesses will continue to pose a high money laundering vulnerability over the next three years. Financial data and monitoring profiles will help detect suspicious operators. However, it will remain difficult for authorities to distinguish illicit proceeds from legitimate revenue.

²⁶ Daigou literally translated means 'buying on behalf of' and refers to persons who buy items in one jurisdiction for residents of a second jurisdiction in which the items are difficult or costly to obtain.

CASH SMUGGLING (UNDECLARED)

Risk rating

Undeclared cash smuggling is assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgement

- Passenger, cargo and international mail channels are vulnerable to processing and moving large volumes of illicit cash out of Australia. These channels are attractive for money laundering as overall visibility and capacity to detect illicit movements is limited.

Domestic context

Undeclared cash smuggling is a long-standing method for moving domestic criminal proceeds offshore via sea cargo, air cargo, international mail and aviation travellers. Cash couriers and concealment techniques are core features of these activities. Smuggling through air passenger movements typically involves lower values, which are often structured to avoid reporting requirements. Bulk cash smuggling requires more sophisticated planning. Once offshore, it is very difficult to track money movements and determine the ultimate destination or use of funds.

CASE STUDY 11

An organised crime group syndicate was known to collaborate with domestic and transnational entities to import and distribute illicit drugs using a variety of money laundering methodologies including cash smuggling and bulk cash export.

Members of the syndicate arranged for the movement of over \$3 million in cash offshore with the aid of foreign cash couriers. In December 2016, the cash couriers were arrested in their attempted departure out of Australia. In April 2017, over \$1 million in cash was seized after it was discovered concealed within a modified aircraft transport stand. The sea freight container was destined for export to an Asian country.

Outlook

Undeclared cash smuggling will continue to pose a high money laundering vulnerability over the next three years. It requires minimal technical expertise or skills to execute, and will remain challenging to detect and disrupt at scale.

CASH SMUGGLING (DECLARED CASH MOVEMENT)

Risk rating

Declared cash smuggling is assessed as posing a **medium** and **stable** money laundering vulnerability.

Key judgements

- Australia's cross-border declaration system is open to misuse by money launderers. Voluntary declaration provides the appearance of legitimacy to the movement of illicit money. It can be very difficult for border authorities to discern the criminal proceeds from legitimate funds in the absence of additional information.
- Cash-in-transit services may be particularly vulnerable to criminal exploitation, given their ability to securely transport bulk cash offshore and hide the original source of funds.

Domestic context

Australia's cross-border declaration system is misused to provide a veneer of legitimacy to outgoing illicit cash movements. When illicit cash is co-mingled and/or transported with legitimate cash, it is very difficult for border authorities to discern one from the other without additional information on the traveller. The extent to which criminals and serious and organised crime groups use this method is unknown. However, the method is attractive given its ease of use, the capacity to move large sums of money and challenges for authorities in detecting criminal exploitation.

Cash-in-transit services providing offshore cash-freighting services are vulnerable to criminal misuse. This vulnerability increases when cash is moved to higher-risk jurisdictions or when the ultimate customer is difficult to determine. An example is when the cash-in-transit business freights cash on behalf of a registered remittance service provider or other cash-intensive business.



AUSTRALIA'S CROSS-BORDER DECLARATION SYSTEM

In Australia, all individuals and reporting entities must report cross-border movements of monetary instruments in Australian or foreign currency if the combined value is A\$10,000 or more.

There are two types of cross-border movement reports:

- Cross-border Movement – A Monetary Instrument (Carrying) report must be made if you depart or enter Australia via an international airport or seaport with a combined monetary instrument value of \$10,000 or more. This includes bearer negotiable instruments (BNIs) and physical currency.
- Cross-border Movement – A Monetary Instrument (Sending/Received) report must be made if you send or have received monetary instruments by ship or courier, or mail it into or out of Australia.

CASE STUDY 12

In 2022, an individual travelling from a foreign jurisdiction declared they were carrying \$140,000 when they entered Australia. They had also declared they were carrying cash into Australia on a number of other occasions between 2015 and 2022. In total, they were recorded as carrying more than \$400,000 into the country.









Third parties also deposited over \$2.3 million in cash into the individual's Australian accounts, and transferred over \$780,000 from the foreign jurisdiction to Australia. The reason for these deposits and transfers is unknown.

The individual has also been reported in eight SMRs related to large cash deposits and the purchase of Australian property.

Outlook

Declared cash smuggling will continue to pose a medium money laundering vulnerability over the next three years. It requires minimal technical expertise or skills to execute and will remain challenging to detect and disrupt at scale.

BANKING SECTOR

SUBSECTOR	RATING	OUTLOOK
Major banks		
Other domestic banks / foreign subsidiaries		
Mutual banks		
Foreign bank branches		

OVERVIEW

Given their central role in the Australian economy and the global payments ecosystem, most money laundering activity will intersect with reporting entities in the banking sector at some point in the transaction chain. The nature and extent of the risk is largely proportional to a reporting entity's size, the types and location of its customers, products and services, and its global reach. Risk profiles are also impacted by the maturity of a bank's AML/CTF risk culture and compliance program.

Despite ongoing and, in some instances, significant investments in sophisticated monitoring and detection systems and specialised AML/CTF staff, many banks remain exposed to a high level of inherent vulnerability to money laundering. The sheer volume of transactions that the sector processes makes it challenging to detect suspicious activity. Technological innovations have increased transaction speed and convenience in recent years. The rollout of the New Payments Platform (NPP) allows for near real-time transfers. This makes it harder for banks to identify and freeze suspicious transfers before funds leave an account. The exploitation of multiple NPP-enabled accounts across different banks makes it difficult to trace transactions to investigate and prosecute money laundering offences. Additionally, the increasing reliance on remote delivery channels, such as ATMs and internet and phone banking, provides criminals with convenient and sometimes anonymous methods to launder money.

Most large banks offer retail and corporate banking streams, which carry different money laundering risks. Retail banking is exposed to high volumes of low-to-moderate value transactions, including anonymous cash transactions, and often incorporates digital channels for service delivery. Corporate banking is generally exposed to money laundering through large transactions and higher-risk customers, such as complex legal structures or the use of professional service providers. Corporate banking products such as trade finance are also exposed to trade-based money laundering activity.

Transaction accounts are key transit points in and out of the banking system, making them the most commonly and persistently misused product. They are highly exposed to cash placement, enable fast layering activity domestically and internationally and provide accessible, low-cost funds storage. Accounts can be established quickly and easily online, a feature exploited by criminals using stolen, rented or purchased identities to create mule accounts to launder money. Other common retail banking products and services misused for money laundering include electronic funds transfers and credit or debit cards. These products are readily accessible, cheap and easy to use, highly exposed to cash transactions and can facilitate the movement of funds/value domestically and across borders. The use of bank cheques and letters of credit for money laundering is in decline. These products are much less accessible, more complex to exploit and generally may be subject to higher levels of scrutiny by banks.



In 2021, AUSTRAC published four national ML/TF risk assessments of Australia's banking sector. These included Australia's major banks, other domestic banks, foreign subsidiary banks and foreign bank branches. Please refer to [these assessments](#) for a comprehensive overview of each sub-sector, including the distinct terrorism financing risks they face. An [overview of key findings and snapshot of risk ratings](#) from each assessment is also available.

In 2019, AUSTRAC published a national ML/TF risk assessment of [Australia's mutual banks](#). The size and composition of this sub-sector has changed since this assessment, but the money laundering risks remain relevant.

MAJOR BANKS²⁷

Risk rating

Major banks are assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Major banks are almost certainly exposed to the majority of money laundering risk facing the banking sector, given the size of their customer base, scale of operations, cash transaction infrastructure²⁸ and global reach.
- Major banks are also the key conduit for international transactions into and out of Australia,²⁹ and serve as correspondent banks for other financial institutions. These links to offshore institutions and customers expose them to a high level of foreign jurisdiction risk.
- Major banks invest heavily in their AML/CTF capabilities, including transaction monitoring systems. They also report more suspicious transactions than any other sector, providing significant amounts of financial intelligence to law enforcement and intelligence bodies.

Domestic context

Major banks are the largest financial institutions in Australia. They offer the largest range of financial products, most extensive delivery channel networks and serve the largest customer base of any sector regulated under the AML/CTF Act.

They offer the most extensive and accessible cash transaction infrastructure in Australia and facilitate more cash transactions *than all other regulated sectors combined*. The major banks also process the majority of international transactions. Given these features, they remain highly vulnerable to money laundering. For example, they:

- are widely exposed to cash-based money laundering methodologies, such as cuckoo smurfing³⁰
- are key conduits for international transactions in and out of Australia, and serve as correspondent banks for other financial institutions. This exposes major banks to a high level of foreign jurisdiction risk
- offer versatile and varied products that are exploited to quickly place and layer criminal proceeds across multiple financial institutions, both in Australia and offshore

²⁷ Australia's major banks are the four largest authorised deposit-taking institutions (ADIs) in Australia, including wholly-owned subsidiaries of the four major banks. This subsector sits at the centre of the financial services industry, together controlling approximately 75 per cent of assets held by all ADIs and serving approximately 47 million customers.

²⁸ Major banks have the most extensive and accessible cash transaction infrastructure in Australia. They facilitate more cash transactions than all other regulated sectors combined. This results in extreme exposure to cash-based money laundering methodologies.

²⁹ For example, major banks facilitated \$4 trillion worth of international funds transfers in 2022.

³⁰ Cuckoo smurfing is a money laundering process where criminal proceeds are used to make a cash deposit to an innocent person in Australia who is expecting to receive a money transfer from overseas. This deposit is made on behalf of a complicit remittance provider. The remittance provider makes the equivalent payment to the criminal overseas. Using this method, funds do not physically move internationally and there is no money trail.

- offer products that can be used to integrate criminal proceeds, such as the purchase of high-value assets and real estate.

Criminals use varied and sometimes sophisticated methodologies to launder funds through the sector. This includes the use of money mule networks,³¹ cuckoo smurfing, accounts owned by shell companies or cash-intensive businesses, and using bank products to store funds used for offsetting. Sophisticated money launderers often combine methods and use the expertise of professional service providers to help conceal their illicit activity.

Some major banks had failures in their AML/CTF systems and controls in recent years. As a result, ongoing significant investments in their AML/CTF programs are being made. They report more suspicious transactions than any other financial sector, providing significant amounts of financial intelligence to law enforcement and intelligence bodies.

CASE STUDY 13

In 2023, the AFP disrupted a transnational, Australian-based MLO and restrained millions of dollars held in accounts with major Australian banks. Members of the organisation had used the banks to receive laundered funds and purchase Australian real estate and fund their lifestyle here. The organisation had exploited trusted insiders, professional service providers and the Australian financial system to facilitate the laundering and moving of billions of dollars of illicit funds around the world for its clients.

Outlook

Major banks will continue to pose a high money laundering vulnerability over the next three years given their importance in the financial services industry and connectivity with the global financial system.

OTHER DOMESTIC³² AND FOREIGN SUBSIDIARY BANKS³³

Risk rating

Other domestic banks and foreign subsidiary banks are assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Larger banks in this subsector are generally exposed to higher levels of criminal exploitation. They offer more extensive and diverse products, services and delivery channels, providing money launderers with more options to move large volumes of funds.
- Instances of account closures by major banks may cause money laundering risk to be displaced to this subsector.
- Key money laundering vulnerabilities in the subsector include the use of agent banking arrangements, acceptance of cash and other third-party product delivery arrangements.
- There is a wide variation in the effectiveness of AML/CTF systems controls across the subsector.

³¹ Money mules are third parties that are employed to transfer illicit value between jurisdictions. They do this by either transporting physical cash or goods on their person or in their luggage; or undertaking transactions through a bank or remittance service or electronically.

³² Other domestic banks are Australian-owned ADIs that are not major banks, community owned or mutual banks. As at May 2024, there are 89 registered other domestic banks enrolled with AUSTRAC.

³³ Foreign subsidiary banks operating in Australia are ADIs licensed by APRA. Foreign subsidiary banks carry on business through a locally-incorporated subsidiary that is a separate legal entity from its foreign bank parent. As at May 2024, there are seven foreign subsidiary banks enrolled with AUSTRAC.

Domestic context

Domestic banks and foreign subsidiary banks primarily offer retail banking products. However, the nature and extent of money laundering risk across the subsector varies significantly. Risk is largely proportional to a bank's size, the types and location of customers it services, its products and services and its global reach. For example:

- Banks that offer corporate banking products and services in addition to retail products and services are exposed to unique money laundering vulnerabilities, such as misuse of trade finance facilities.
- Banks that operate branchless models and rely on third-party agents to facilitate cash transactions are exposed to heightened vulnerability. These arrangements lengthen the product delivery chain and can complicate detection of suspicious persons or transactions.
- The largest banks generally offer more products and services that are open to exploitation, have an extensive national presence and are exposed to more cash transactions than smaller banks. Cash exposure is generally concentrated in banks that operate large ATM and branch networks.
- Foreign subsidiary banks are generally more exposed to foreign jurisdiction risk because they offer products like foreign currency exchange accounts. They are also likely favoured by customers with links to offshore entities.

Common money laundering methods observed in the subsector include the use of money mules, significant cash or cheque deposits and large domestic transfers into personal and business accounts. Funds are often then transferred to other domestic or international financial institutions.

Account closures by major banks is highly likely displacing higher-risk customers to domestic and foreign subsidiary banks. Larger entities in this subsector may be particularly attractive because they offer similar products, services and the same delivery channel as major banks.

CASE STUDY 14

A foreign bank with no branches or ATMs in Australia reported money laundering concerns in relation to cash deposits at Australia Post outlets. AUSTRAC identified a customer who deposited more than \$126,000 into two bank accounts over a six-month period. The majority of the funds were used to purchase digital currency from a DCE.

AUSTRAC analysis identified that the customer was the subject of a number of SMRs by three reporting entities. Previous suspicious behaviour included frequent cash deposits and large transfers to and from third parties, including DCEs. The reporting entities appear to have closed the customer's accounts, prompting the switch to the foreign bank.

Outlook

Over the next three years, other domestic banks and foreign subsidiary banks will continue to pose a high money laundering vulnerability, given:

- the versatility and variety of product and service offerings
- the delivery channels that can be criminally exploited.

The subsector will also likely remain attractive to customers who are looking for alternative banking services away from major banks.

MUTUAL BANKS

Risk rating

Mutual banks are assessed as posing a **medium** and **stable** money laundering vulnerability. Mutual banks are ADIs owned by their customers, such as building societies and credit unions.

Key judgements

- The extent of money laundering through mutual banks is moderated by the subsector's limited size and reach compared to other banking subsectors.
- Many mutual banks are able to move large volumes of funds quickly and easily. However, the subsector has fewer customers and facilitates fewer transactions than other retail banks. This makes it harder for criminals to conceal large-scale money laundering activity among legitimate transactions.
- Some mutual banks may not have the resources to operate sophisticated AML/CTF systems and controls.

Domestic context

Over the past decade, the number of mutual banks operating in Australia has declined due to consolidation and mergers of banks in the subsector. As of May 2024, there are 49 mutual banks enrolled with AUSTRAC.

Historically, mutual banks primarily serviced members of particular professions or residents of specific regions. However, many of them now provide services to a wider customer base. While this evolution has increased the subsector's exposure to higher-risk customers, criminal exploitation is moderated by the subsector's smaller customer base, restricted product offerings and limited financial footprint.

Mutual banks primarily offer retail banking products and services, which are highly vulnerable to money laundering. Larger mutual banks are likely exposed to a higher level of vulnerability due to their size and multiple options for products, services and delivery channels. However, smaller mutual banks that offer simple-yet-versatile products such as transaction accounts, loan products and term deposits are also exposed. Criminal exploitation of mutual banks generally involves incoming electronic transfers from accounts held at major banks or other large domestic banks. Mutual banks that offer cash facilities are also exposed to direct placement of illicit cash into customer accounts.

Mutual banks may be vulnerable to criminal entities seeking alternative banking arrangements from other larger financial institutions. This applies in particular to mutual banks that offer a variety of retail banking products and cash facilities.

Historically, mutual banks maintained regional branch networks. However, many have since reduced their physical presence and increasingly rely on online banking for product applications and use third-party agents like Australia Post to facilitate cash transactions for customers. These outsourcing arrangements lengthen the service delivery chain and reduce end-to-end visibility of transactions.

The effectiveness of risk mitigation strategies varies across the subsector with some mutual banks having undertaken AML/CTF capability uplifts in recent years.

CASE STUDY 15

In 2022, a regionally-focused mutual bank was likely exploited by a known criminal and money mule to layer funds and buy digital currency on behalf of a money laundering network. A major bank submitted an SMR on the individual for receiving over \$78,000 from himself and third parties. This money was rapidly moved to other accounts, including one held with the member bank.

The mutual bank suspected layering activity and identified several money laundering indicators, including large transactions to and from the customer's accounts with other banks and an unknown source of wealth. The account received over \$280,000 from third parties over four months.

The individual was also named in six SMRs from five different institutions across mutual, major and other domestic banks. This illustrates how money launderers exploit multiple institutions to try and obscure the criminal source of funds.

Outlook

Mutual banks will continue to pose a medium money laundering vulnerability over the next three years. The extent of vulnerability is somewhat moderated, given the smaller size and scale of many banks in the sector. However, the retail products they offer will likely continue to be attractive for criminal exploitation.

FOREIGN BANK BRANCHES³⁴

Risk rating

Foreign bank branches are assessed as posing a **medium** and **stable** money laundering vulnerability.

Key judgements

- The risk profile of foreign bank branches is distinct from the rest of Australia's banking sector, given their primary focus on corporate banking.
- Money laundering vulnerability primarily stems from the use of complex products to execute high-value international transactions, including to higher-risk jurisdictions or into high-value assets.
- Their AML/CTF programs are often based on a global policy designed by an overseas-based head office. While some foreign bank branches customise their programs to the Australian environment, some do not. This can impede their ability to detect and report suspicious transactions that are specific to the Australian context.

Domestic context

The foreign bank branch subsector faces a distinct money laundering risk profile compared to other banking subsectors. This is because they generally provide complex, customised financial products and services for cross-border trade and investment to a smaller number of high-value customers.

There is limited evidence of wide-scale criminal exploitation of foreign bank branches. However, they may be attractive to more sophisticated actors with the access and expertise to establish necessary structures to exploit them for money laundering.

Key vulnerabilities include:

- exposure to higher-risk customers, in particular respondent banks and other financial institutions, high net-worth individuals including commercial companies and trusts, foreign-based customers, professional service providers and PEPs

³⁴ Foreign bank branches operating in Australia are foreign ADIs licensed by the APRA. They are not separate entities incorporated and independently capitalised in Australia, but part of a foreign bank incorporated overseas. As at May 2024, there are 49 foreign bank branches enrolled with AUSTRAC.

- products and services that can be used to store and move funds in and out of the subsector such as:
 - accounts, including transaction, savings and foreign currency accounts
 - international funds transfers
 - correspondent banking services.

Having a small number of customers and overall transactions, employees of foreign bank branches often have direct relationships with their customers and a detailed understanding of them. These staff are very well placed to identify and report unusual behaviour. Foreign banks may be more vulnerable to money laundering if their staff do not identify and report potentially suspicious matters.

Some foreign bank branches may lack a comprehensive understanding of the Australian money laundering environment. While the majority of them have well-established AML/CTF programs, they often maintain a strong reliance on their overseas head offices. This can result in AML/CTF programs that are not adequately tailored to the Australian risk environment.

Outlook

Foreign bank branches will continue to pose a medium money laundering vulnerability over the next three years.

The level of vulnerability is unlikely to increase in the short to medium term due to:

- limited access to the subsector
- the level of expertise required to exploit its products
- the long-term persistence of its corporate-focused business model.

NON-BANK FINANCIAL SERVICES

SECTOR/CHANNEL/SERVICE	RATING	OUTLOOK
Unregistered remittance dealers		
Registered remittance service providers		
Bullion dealers		
Superannuation fund providers		
Stockbrokers and securities dealers		
Non-bank lenders and financiers ³⁵		
Foreign currency exchanges		
Custodians and asset custody services		
Managed investments schemes		

³⁵ This assessment does not discuss money laundering threats that have been rated low. For a comprehensive overview of money laundering risks for non-bank lenders and financiers, please refer to AUSTRAC’s [ML/TF risk assessment of the non-bank lending and financing sector](#), which was released in 2021.

UNREGISTERED REMITTANCE DEALERS³⁶

Risk rating

Unregistered remittance dealers (unregistered remitters) are assessed as posing a **high and increasing** money laundering vulnerability.

Key judgements

- Unregistered remitters pose a significant and persistent money laundering risk to Australia. They are highly attractive to money launderers as transactions evade AML/CTF regulatory oversight. Therefore, illicit transactions are more difficult to disrupt.
- In general, unregistered remitters specialise in moving funds to or from foreign jurisdictions with underdeveloped or quarantined financial systems. Criminals exploit this to launder domestically-generated proceeds of crime through jurisdictions with weak AML/CTF regimes.
- Unregistered remitters who use offsetting arrangements or provide cash-to-**digital currency services** pose a heightened money laundering risk.

Domestic context

Despite concerted law enforcement attention, unregistered remitters continue to operate in Australia and often feature in money laundering investigations. In some instances, strong links exist between unregistered remitters and international money laundering organisations. These remitters are capable of laundering large amounts of illicit cash, often transact through offsetting arrangements (see discussion in **Registered remittance service providers**) and use cuckoo smurfing to move funds offshore.

Unregistered remitters operate outside of AML/CTF regulatory oversight. Transactions are highly opaque and therefore difficult to detect or disrupt. Visibility is further reduced when unregistered remitters use offsetting arrangements or provide unregistered cash-to-digital currency services, which bypass the formal financial system. Unregistered remittance activities may accompany the establishment of companies posing as cash-intensive or international businesses to provide an appearance of legitimacy for international transactions.

In addition to the level of anonymity they can provide criminals, unregistered remitters are attractive because they:

- specialise in moving funds to or from foreign jurisdictions with weak AML/CTF regimes
- are generally willing and able to ingest large amounts of cash
- offer alternative transfer solutions for individuals and entities that have been de-banked or de-risked by regulated financial institutions or remittance providers.

³⁶For the purposes of this assessment, ‘unregistered remitter’ and ‘unregistered remittance dealer’ refer to an individual, business or organisation that carries on a business of providing a designated remittance arrangement in Australia and is not registered on AUSTRAC’s Remittance Sector Register. Individuals and entities that provide remittance services in Australia do not always comply with registration and regulatory requirements. A variety of businesses operate as unregistered remitters. They often pose as cash-intensive businesses or international trading businesses to provide a veneer of legitimacy for international transactions. Some unregistered remitters specialise in moving funds to or from foreign jurisdictions that have underdeveloped or quarantined financial systems.



WHAT IS OFFSETTING?

Offsetting is a method of value transfer using reciprocal debit and credit arrangements between businesses. It is a legitimate method of exchanging value that is used by both unregistered remittance dealers and registered remittance service providers.

For some businesses, offsetting is a viable alternative to formal banking channels, particularly if the customer has been unable to maintain an account with a financial institution. The use of offsetting for money laundering is well documented globally and has been observed in Australia as well.

AUSTRAC'S UNREGISTERED REMITTER CAMPAIGN

Between August and November 2019, AUSTRAC ran a community campaign targeting unregistered remitters. During this time, more than 130 AUSTRAC staff visited at least 400 registered remittance service providers across the country. These visits gave businesses the opportunity to provide feedback and ask questions about their obligations.

More than 240 people attended town hall meetings including local community leaders, multicultural organisations, registered remittance service providers, Australian government agencies and journalists.

At each event, AUSTRAC staff shared information and provided materials in 11 languages that explained the threat of using unregistered remitters. Participants shared this information with their communities to help them identify unregistered remitters and make informed decisions about how they transfer money overseas.

CASE STUDY 16

The AFP identified a money laundering organisation operating as a criminal remittance and banking service able to make significant sums of money available to clients almost anywhere in the world within 24 hours. The organisation moved an estimated \$10 billion over four years and had the capacity to move up to \$1 million an hour during business hours.

The organisation had a sophisticated informal value transfer system in place to make funds available overseas. By exploiting digital currency trading, domestic and foreign shell companies, and multiple offshore bank accounts held with various institutions, the organisation effectively operated as an underground bank with global reach, managing credit and debits internally and setting its own exchange rates. The MLO was ultimately shutdown after the AFP arrested senior members and commenced asset restraint action.

Outlook

Unregistered remitters will pose an increasing money laundering vulnerability over the next three years. This is likely to be driven by continued displacement of criminal customers to the sector and the use of new technologies like digital currency to move illicit funds offshore.

REGISTERED REMITTANCE SERVICE PROVIDERS



AUSTRALIA'S REMITTANCE SECTOR

Remittance service providers operating in Australia offer fast and relatively low-cost methods of transferring funds domestically and overseas. They are a crucial component of global financial inclusion and particularly important for migrant and expatriate communities supporting families in their countries of origin. As at May 2024, 4,294 remittance service providers were registered with AUSTRAC.

Remittance service providers must register with AUSTRAC as one or more of the following:

- A **Remittance Network Provider (RNP)** operates a network of affiliates that use its brand, products, platforms or systems to provide remittance services to customers. An RNP is responsible for an affiliate's registration and reporting obligations to AUSTRAC and must ensure the affiliate has an appropriate AML/CTF program.
- An **affiliate** has an agreement with an RNP to provide remittance services. Under the agreement, the affiliate accepts instructions directly from customers to send funds to a recipient in another location. Affiliates are independently-owned and the RNP does not have control over other activities or services they provide.
- **Independent remittance dealers** are typically registered as a single entity or sole trader, operating independently, or own and operate multiple branches. They use their own products, platforms or systems to provide remittance services directly to customers.

In 2022, AUSTRAC published two ML/TF risk assessments covering:

- [independent remittance dealers in Australia](#)
- [remittance network providers and their affiliates in Australia.](#)

Please refer to these assessments for a comprehensive look at each subsector, including their size, scale of operations and the distinct money laundering risks they face.

Risk rating

Registered remittance service providers are assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Registered remittance service providers will remain attractive to money launderers because they can move funds offshore quickly, easily and at low cost. Key vulnerabilities include:
 - high exposure to cash and foreign jurisdictions
 - the complexity of product delivery arrangements, which can hide the source and ultimate beneficiary of funds.
- Registered remittance service providers who use offsetting arrangements or provide cash-to-digital currency services likely pose a heightened money laundering risk.

Domestic context

Criminals of all sophistication levels use registered remittance service providers to launder illicit funds in Australia. Common money laundering methods include the use of mule accounts, cuckoo smurfing, offsetting and structuring cash deposits.

Registered remittance service providers are attractive to money launderers for the same reasons they appeal to regular customers. They provide a fast, affordable and reliable channel to move funds overseas.

Other core features that make them highly vulnerable to money laundering include:

- High exposure to cash.
- High exposure to high-risk foreign jurisdictions, particularly those whose customers have strong ties to high-risk countries or jurisdictions that border a conflict zone.
- Certain outsourcing arrangements³⁷ and operational structures. An example is the RNP-affiliate structure used by some reporting entities, which lengthens the product-delivery chain and reduces the level of oversight a reporting entity might have.
- The trend towards remote product delivery channels, such as websites or mobile applications, which provides a layer of anonymity for customers. This has been accelerated by COVID-19.
- The adoption of mobile technology has also increased global accessibility to services and provides an additional element of anonymity that may be attractive to money launderers. Criminals can exploit online remittance account applications to establish mule accounts, in some cases using stolen identities, and use them to send illicit funds offshore.

Some registered remittance service providers are also registered with AUSTRAC as a DCE. Businesses offering these dual services may be more attractive for criminals who wish to spread their money laundering activities across multiple channels in an effort to obscure end-to-end visibility of transactions.³⁸ Remittance service providers who use offsetting arrangements may also be targeted by criminals who wish to bypass the formal financial system. Offsetting provides greater anonymity and transactions are often subject to less scrutiny, particularly if the reporting entity has poor or limited record-keeping practices. Offsetting also increases the ability of a criminally-complicit business to avoid reporting requirements.³⁹

The effectiveness of AML/CTF programs and associated detection capabilities are uneven across the remittance sector. Some businesses are unwilling or unable to detect and report suspicious matters and mitigate the money laundering risks they face.⁴⁰

CASE STUDY 17

In 2021, AUSTRAC cancelled the registration of an affiliate of a remittance network provider after its director and owner was convicted of conducting structured deposits. The individual conducted six structured cash deposits totalling \$50,000 into the bank account of a student visa holder within a two-hour period.

³⁷ For example, the use of super agents, correspondent institutions or third-party service providers. Please refer to the two national ML/TF risk assessments of the remittance sector for details of vulnerabilities posed by outsourcing arrangements.

³⁸ Vulnerabilities associated with the DCE-remittance corridor are further discussed in the [Digital currencies](#) section.

³⁹ Reporting entities must still submit relevant reports to AUSTRAC when using offsetting arrangements. AUSTRAC expects remitters to know and understand their AML/CTF reporting obligations when using these arrangements.

⁴⁰ This can be influenced by a range of factors such as language barriers, poor understanding of AML/CTF obligations, mistrust of the government, a belief that submitting SMRs makes their business look bad, or apprehension to report suspicious matters regarding customers who are well-known to them.

Outlook

Registered remittance service providers will continue to pose a high money laundering vulnerability over the next three years. There is little evidence to suggest criminal actors will be deterred from using these services as long as they offer quick, accessible and affordable transfers overseas.

Businesses offering dual remittance and DCE services may be increasingly targeted by criminals.

BULLION DEALERS



AUSTRALIA'S BULLION INDUSTRY

In 2022, AUSTRAC published its national [ML/TF risk assessment of Australia's bullion industry](#). Please refer to this assessment for a comprehensive view of the sector including its size, scale of operations and the distinct money laundering risks posed.

A bullion dealer is an individual, business, or organisation that buys or sells bullion as a bullion-dealing business. AUSTRAC defines bullion as gold, silver, platinum or palladium authenticated to a specified fineness. It comes in the form of bars, ingots, plates, wafers or similar forms, or in coins. Gold is overwhelmingly the dominant precious metal in the bullion sector followed by silver, platinum and palladium.

Bullion dealers include businesses enrolled with AUSTRAC in the precious metal traders sector and in the bullion cohort.⁴¹ Under the AML/CTF Act, reporting entities in the bullion sector are required to maintain and implement a compliant AML/CTF program and are obliged to submit transaction reports to AUSTRAC. As at May 2024, there are 308 businesses in the bullion sector enrolled with AUSTRAC.

Risk rating

Bullion dealers are assessed as posing a **medium** and **increasing** money laundering vulnerability.

Key judgements

- Criminals buy and sell precious metals, such as gold bullion, through complicit and non-complicit dealers to launder money.
- Bullion dealers are increasingly being identified in criminal investigations by Australian authorities. In some instances, individual dealers are strongly linked to known or suspected criminals and/or criminal groups.
- The bullion sector submits a relatively low number of SMRs and the number submitted varies greatly between individual reporting entities of a similar size and scale. Reports often lack detailed information about the grounds for suspicion.

Domestic context

Australian investigations suggest criminals are increasingly exploiting the precious metals industry to launder money. This includes exploiting bullion dealers, wittingly and unwittingly, to export gold bullion and precious metals out of Australia.

The AML/CTF Act does not require individuals or entities to declare the carrying of gold bullion at the border. This is consistent with FATF Standards but can create blind spots to potential money laundering movements.

⁴¹ AUSTRAC does not regulate the purchase or sale of precious metals that are not defined as bullion. For example, granules of fine gold typically used for the manufacture of jewellery are not considered to be bullion because they are not bars, ingots, plates, wafers, coins or similar forms.

Other features that make bullion dealers vulnerable to money laundering:

- High exposure to cash transactions, with many bullion dealers operating cash-intensive business models.
- Bullion is easy to purchase with cash, easy to transport and can be difficult for authorities to trace.
- Certain bullion dealers provide bullion-refining services for gold sourced from Australia (e.g. scrap jewellery) and gold ore mined in other countries. This can make it difficult to determine the legitimacy of the source, particularly after the gold has been refined.
- Exploitation by money mules. In this scenario, the criminal provides the third-party with funds, in some cases cash, to buy gold bullion. The third-party uses their own identification details to buy the gold bullion and hands it to the criminal. In other cases, the third-party sells the gold bullion and transfers the proceeds to the criminal. The use of money mules helps criminals to distance themselves from transactions and reduce their chance of detection.

CASE STUDY 18

An individual extensively recorded in law enforcement intelligence indices for involvement in drug trafficking activity deposited more than \$200,000 in cash into the bank account of a bullion dealer over two days.

Law enforcement discovered that this individual was in fact incarcerated at the time of the transactions. This led them to believe that a money mule had made the deposits using the account holder's details.

Outlook

Bullion dealers will likely pose an increasing money laundering vulnerability over the next three years. This increase will be driven largely by criminal targeting of the sector. Bullion will remain an attractive mechanism to store and/or transfer value, particularly alongside other accessible and transferrable assets such as cash and small luxury goods.

Criminals, in addition to legitimate investors, will likely continue regarding gold bullion as a relatively stable asset and a hedge against inflation and currency risk, given the current economic uncertainty.

SUPERANNUATION FUND PROVIDERS



AUSTRALIA'S SUPERANNUATION SECTOR

Australia's superannuation sector is diverse and made up of funds that vary in size, complexity and regulatory oversight.

This includes:

- APRA-regulated superannuation funds, such as corporate funds, industry funds, public sector funds and retail funds that have chosen to be regulated by APRA
- exempt public sector superannuation schemes that choose not to be regulated by APRA and have an exemption under the *Superannuation Industry (Supervision) Act 1993*
- self-managed super funds (SMSFs), which are private superannuation funds regulated by the ATO.

In 2016, AUSTRAC published its national [ML/TF risk assessment of Australia's superannuation sector](#). In 2022, AUSTRAC published an abridged [update to the risk assessment](#), outlining the criminal threat environment facing the sector.

Please read these assessments for a comprehensive overview of the sector, including the distinct money laundering threats and risks it faces.

Risk rating

Superannuation fund providers are assessed as posing a **medium** and **stable** money laundering vulnerability.

Key judgements

- The superannuation sector is vulnerable to criminal exploitation due to its large customer base, use of remote and online delivery channels and difficulties in verifying sources of funds for voluntary contributions. This limits visibility and allows criminals to conduct transactions without raising suspicion.
- Both APRA-regulated and self-managed super funds are subject to the same access restrictions. However, APRA-regulated superannuation funds are likely less attractive to money launderers due to the involvement of an independent third-party to release and invest the monies in these funds.
- Superannuation accounts will continue to be used to store criminal proceeds derived from other predicate offences — fraud, in particular.

Domestic context

The scale of money laundering through superannuation funds is likely very low compared to other financial services and sectors such as banking and remittance, largely because superannuation accounts are subject to various access rules and restrictions under superannuation laws. For example, members have limited access to funds held in their superannuation before they reach preservation age and voluntary contribution caps limit the amount of funds that can be deposited each year.

Nonetheless, the superannuation sector is vulnerable to money laundering. For instance, criminal proceeds can be placed into a superannuation account via voluntary contribution or can be fraudulently accessed by individuals known to the member or by criminals using stolen identities.

Illicit funds can then be stored or layered through staging accounts⁴² or SMSFs and ultimately withdrawn disguised as superannuation benefits or transferred to third party accounts, including to accounts in foreign jurisdictions.

SMR submissions by the superannuation sector are relatively low compared to their vast customer base and the significant value of assets under management.⁴³ This may stem from reduced visibility of customers and transactions, driven by remote or online delivery channels, outsourcing of administration and transaction monitoring processes to third parties and from the timing of conducting Know Your Customer (KYC) procedures.

When entities in the superannuation sector outsource KYC, transaction monitoring or other AML/CTF obligations to third parties, they must ensure these arrangements are fit for purpose and allow the entity to manage and mitigate its ML/TF risks.

Generally, SMSFs carry a higher level of money laundering vulnerability compared to APRA-regulated super funds as they do not have reporting obligations under the AML/CTF Act.⁴⁴ SMSF regulation typically focuses on compliance with superannuation and tax legislation, rather than the detection of suspicious financial behaviours or sources of illicit funds. In addition, SMSFs are more accessible as they are controlled by the trustees, members or a trusted advisor such as an accountant or lawyer.

CASE STUDY 19

Between April and July 2023, \$500,000 was sent to a personal bank account, including \$350,000 from the account of the SMSF. Around \$500,000 was reportedly transferred back to the SMSF account—an indication of layering. The SMSF trustee was referenced in seven other SMRs between 2010 and 2023. The activity was linked to transfers involving a remitter and currency exchange that itself was the subject of 30 SMRs between 2019 and 2023 for various concerns, including money laundering.

Outlook

Superannuation funds will continue to pose a medium money laundering vulnerability over the next three years. Superannuation accounts are unlikely to become more attractive for large-scale money laundering activities but they will remain vulnerable to other predicate offences such as fraud.

Superannuation accounts will also continue being used to layer fraudulently-obtained funds through rollover activities and ultimately accessed through illegal use of early release schemes.

⁴² Staging accounts are established for the purpose of consolidating funds before they are further transferred or withdrawn from the superannuation system. SMSF staging accounts can also be set up to receive unauthorised or illegal superannuation benefits.

⁴³ Reporting improved as a result of COVID early-access to superannuation schemes, which saw an increase in superannuation withdrawals and subsequent improved SMR reporting and CDD checks. AUSTRAC released industry specific guidance and indicator reports, and ran education campaigns to uplift industry capability.

⁴⁴ SMSF accounts are not captured under the AML/CTF Act. However, reporting entities that provide services to SMSFs, such as banks, are obligated to report certain information and transactions to AUSTRAC.

STOCKBROKERS AND SECURITIES DEALERS



AUSTRALIA'S SECURITIES AND DERIVATIVES SECTOR

In 2017, AUSTRAC published its national [ML/TF risk assessment of Australia's securities and derivatives sector](#). Please refer to this assessment for a comprehensive overview of the sector including its size, scale of operations and the distinct money laundering risks.

In 2016, AUSTRAC published a national [ML/TF risk assessment of Australia's financial planning sector](#). This report contains information relevant to financial planners who provide stockbroking services.

Risk rating

Stockbrokers and securities dealers are assessed as posing a **medium** and **stable** money laundering vulnerability.

Key judgements

- The extent of observed money laundering by stockbrokers and securities dealers is relatively low. However, the sector is exposed to a range of inherent money laundering vulnerabilities. These include exposure to high-risk customers and jurisdictions, and complex and increasingly remote online service delivery channels.
- Where detected, money laundering generally involves placement of illicit cash and layering through trading accounts.
- There is evidence of limited understanding of money laundering risk and under-developed AML/CTF systems and controls among some entities.

Domestic context

There are generally two scenarios where stockbrokers and securities dealers are involved in money laundering. The first involves dealers wittingly laundering funds on behalf of criminal clients. This scenario can involve placement of illicit cash, layering through multiple trading accounts, loss-making trading activity and funds transfer requests to third parties.

The second scenario involves stockbrokers and securities dealers being exploited by customers to generate criminal proceeds from fraudulent activities, such as market manipulation and insider trading as well as tax evasion. In these instances, criminal proceeds are generally already placed in an investment product and are either withdrawn or layered and integrated into the wider financial ecosystem.

Detection of money laundering and wider criminality by stockbrokers and securities dealers is relatively low. Nonetheless, they are exposed to a range of money laundering vulnerabilities. These include:

- the relative ease with which cash can be moved into and between trading accounts, and accepting cash to purchase investments for clients
- the volume and speed of transactions, coupled with the increasing use of online services and trading platforms, which create additional challenges for transaction monitoring
- reduced visibility of underlying customers in transactions with:
 - multi-layered trading chains, legal persons and arrangements with complex ownership structures
 - the use of overseas-based agents
 - funds transfer requests to third parties

- customers using multiple brokers and market participants, limiting visibility of their overall trading activity
- the availability of services enabling off-market transfers, where ownership and value in shares can be transferred directly between entities, including across jurisdictions
- the common industry practice of ‘white labelling’ can lead to uncertainty over AML compliance and reporting responsibilities
- a high level of foreign jurisdiction risk due to offshore market participants.

Stockbrokers and securities dealers in Australia are subject to AML/CTF reporting obligations. However, there is evidence of limited understanding of money laundering risk and under-developed AML/CTF systems and controls among some sector entities. For example, AUSTRAC has observed a lack of rigour and analysis by decision makers when deciding to take on or continue relationships with high-risk customers. Staff engaging with customers, such as front office staff and wealth advisers, are well placed to identify and report potentially suspicious matters. This should be a key control for these entities in managing and mitigating risks.

SMR submissions are relatively low, and may reflect a focus on trading risks such as market manipulation and insider trading by clients, rather than suspected money laundering, tax evasion and other predicate offences.



REPORTING OBLIGATIONS TO AUSTRAC AND ASIC

Reporting entities have an obligation to report SMRs to AUSTRAC if they form a suspicion on reasonable grounds that the services they are providing may be relevant to an investigation or prosecution of a person for taxation offences, offences against a law of the Commonwealth, State or Territory, the enforcement of proceeds of crime legislation, money laundering or the financing of terrorism. Suspicious activity reports (SARs) are also reportable to ASIC for activity relating to insider trading and market manipulation.

Market participants are *not* required to submit a SAR to ASIC if the information has been reported to AUSTRAC in an SMR. However, they must always report an SMR to AUSTRAC to satisfy their AML/CTF obligations, even if they have already reported the matter in a SAR to ASIC.

Some matters are reportable to ASIC in a SAR but not required to be reported to AUSTRAC, for example, where a person or entity is not a customer of the market participant and where there is no ‘customer’ (such as when a market participant is engaged in proprietary trading).

CASE STUDY 20

Between April and June 2022, an Australian company received nearly \$12 million in domestic and international transfers. The funds were possibly obtained through ‘Sha Zhu Pan’ investment scams targeting China-based WeChat and Alipay users. They appeared to finance transfers to online trading platforms that offer contracts for difference in commodities such as digital currency, forex and shares. Some of the online trading platforms are linked to financial secrecy jurisdictions and tax havens.











Outlook

Stockbrokers and securities dealers will continue to pose a medium money laundering vulnerability over the next three years. They are unlikely to become highly attractive to criminals seeking to launder large volumes of illicit funds. However, they will continue to be exposed to inherent vulnerability. In addition, customers of stockbrokers and securities dealers who generate criminal proceeds from fraudulent activities will almost certainly continue to use investment products to store, layer and integrate illicit funds.

HIGH-VALUE ASSETS AND GOODS

For the purposes of this assessment, high-value assets and goods include luxury goods, which are further defined as:

- precious stones
- jewellery
- fashion designer goods
- watches
- artworks
- other collectable assets and asset classes used for investment purposes, including shares in publicly- listed companies and other investment products.

ASSET TYPE	RATING	OUTLOOK
Luxury goods		
Real estate (domestic)		
Luxury vehicles and watercraft – store of value		
Bullion and precious metals (physical or securities) – transfer of value		
Wealth and financial assets – store of value		

LUXURY GOODS

Risk rating

Luxury goods are assessed as posing a **very high** and **stable** money laundering vulnerability.

Key judgements

- Luxury goods are a highly effective money laundering mechanism. There is a global market for and acceptance of these goods. They are easily obtained and transported across domestic and international borders, and regulatory oversight is limited.
- Luxury goods are widely exploited for money laundering purposes by domestic and international criminals alike.

Domestic context

Luxury goods are an effective and low-cost channel to launder funds. Criminal use of luxury goods to both store and transfer criminal proceeds is widely documented by national and international partners. In Australia, high-value watches are commonly identified by authorities in money laundering investigations. High-value jewellery, designer accessories and apparel are also observed.

Luxury goods are attractive for money laundering for a range of reasons:

- They require minimal to no knowledge, skills or expertise to acquire, store and maintain.
- They are easily moved into and out of both licit, including second-hand, and illicit markets. The global second-hand market for many luxury goods is expansive. It features many private sellers and traders, including those based offshore.
- They often retain very high value, and in some cases appreciate in value.
- In many cases, they are easily transported.

The purchase and selling of luxury goods is not captured in Australia's AML/CTF regime. Therefore, mitigating vulnerability relies on individual businesses understanding their risk exposure and implementing controls to prevent and detect criminal misuse.

CASE STUDY 21

A luxury goods business was identified as part of a network likely involved in money laundering and the transfer of illicit proceeds by the global brokering and smuggling of high-value watches and border-controlled drugs.

Within the span of a year, the business director deposited over \$1.6 million in cash into the business account, with the funds ultimately used for business expenses. Due to ongoing high value-cash deposits and other suspicious transfers, the business was recorded in a number of SMRs.

The business also received funds from an individual suspected of laundering funds through luxury cars and watches for clients, including organised crime groups. Both the director and the business are recorded in multiple intelligence holdings.

CASE STUDY 22

The AFP charged nine members of a Sydney-based MLO, alleging the syndicate laundered funds on behalf of multiple TSOC groups in addition to \$150 million of their own profits. The AFP alleged the group moved illicit funds through multiple jurisdictions and channels, including daigous, casino junkets and informal value transfer systems.

Search warrants at 13 Sydney locations seized 18 designer watches, 17 designer handbags and at least 46 items of luxury jewellery in addition to \$29 million in cryptocurrency and unlawfully stored firearms. In total, the AFP restrained more than \$150 million in property, cash and luxury goods.

Outlook

Luxury goods will continue to pose a very high money laundering vulnerability over the next three years. As long as they are easy and legal to obtain and maintain, they will remain a favoured channel for storing and transferring criminal proceeds.

REAL ESTATE (DOMESTIC)

Risk rating

The real estate sector is assessed as posing a **very high** and **stable** money laundering vulnerability.

Key judgements

- Real estate is a widely-exploited asset type for money laundering in Australia. This is due to the market stability and value appreciation, profit-generation, negative gearing benefits, housing and rental income functions of the sector. It can be exploited at all stages of the money laundering cycle.
- Methods of laundering funds through real estate include:
 - manipulating property values
 - reselling in quick succession at a higher price
 - using illicit funds to pay for improvements and renovations to increase house prices prior to selling
 - using rental payments to legitimise income
 - the use of complex legal structures to purchase real estate and/or obfuscate property ownership.
- Law enforcement confiscation of criminally-linked assets, including both residential and commercial real estate purchased with domestic and/or foreign proceeds of crime, continues to be challenging due to the use of legal structures and ‘cleanskins’ to conceal property ownership.
- The involvement of professional service providers who enable real estate purchases, such as lawyers, conveyancers and real estate agents, pose a significant risk for money laundering. This is because of the absence of measures to enhance transparency of beneficial ownership and AML obligations, as they are not currently subject to AML/CTF regulation (see [Professional Services Providers](#) section).

Domestic context

The actual value of money laundering through Australia’s real estate market is difficult to estimate. However, it is reportedly one of the most expensive and commonly-identified asset types in criminal confiscation investigations, and is one of the most attractive real estate markets globally.

Between 2020-21 and 2022-23, over \$55 million of residential real estate and over \$7 million in commercial real estate was forfeited⁴⁵. The same features that make this sector attractive for legitimate investment also make it a highly desirable destination for placing, layering and/or integrating criminal proceeds. Advantages include appreciation in value, negative gearing benefits and income from rental and commercial leasing. This is in addition to holding a tangible high-value and stable asset.

Cases of money laundering through Australian residential real estate are well known. While cases involving commercial real estate have been historically less common, they are increasingly identified in criminal investigations.

The Australian real estate sector is also identified as a common destination for foreign proceeds of crime. Concealing foreign ownership through onshore ownership structures poses a high money laundering vulnerability.

⁴⁵ Forfeiture of restrained real estate occurs at the conclusion of the relevant court (criminal or civil) proceedings.

Given the current lack of measures to enhance transparency of beneficial ownership, the use of trusts, shell companies and complex legal structures to purchase and own real estate in Australia remains a prominent challenge for law enforcement.

Real estate services in Australia are not currently regulated under the AML/CTF Act and therefore pose a significant money laundering vulnerability due to the lack of visibility of activity. Visibility of real estate transfer of ownership is only partially available on a state-by-state basis, with most states not collecting beneficial ownership information.

CASE STUDY 23

An investigation into the purchase of a commercial property in NSW worth several million dollars revealed it was likely purchased with proceeds of crime. An offshore service provider (OSP) facilitated its purchase by transferring several million dollars from an offshore jurisdiction to the accounts of a domestic law firm. The law firm settled the property, with the total amount of funds settled for the purchase exceeding \$5 million. Settlement documentation obfuscated the source of funds by indicating they were obtained from a loan arrangement.

Outlook

Real estate will continue to pose a very high money laundering vulnerability over the next three years, driven largely by the market's stability and high value. Residential and commercial property real estate transactions are subject to proposed AML/CTF legislative reforms. If implemented, their impact on the extent of money laundering in the sector will need to be re-assessed.

LUXURY VEHICLES AND WATERCRAFT – STORE OF VALUE⁴⁶

Risk rating

The use of luxury vehicles and watercraft as a store of value mechanism is assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Luxury vehicles, and to a lesser extent boats and yachts, hold an enduring appeal for criminals. They are a lifestyle purchase, projecting status and prestige while being an effective method to store criminal wealth.

Domestic context

Luxury vehicles have an enduring appeal to criminals as lifestyle purchases projecting status and prestige and the capacity to be used to conceal and store illicit funds. Their appeal endures despite a number of attributes unfavourable for money laundering. These include regulatory requirements on purchase and transfer of ownership, depreciation in value over time and traceability.

Luxury vehicles feature regularly in asset restraints and confiscations, with Australian government agencies identifying them as an asset type preferred by those laundering drug-related proceeds of crime.

⁴⁶ In this section, high value assets refers to luxury vehicles and watercraft, e.g. cars, boats, yachts. The focus on the luxury car industry is due to operational insights.

Despite some regulatory coverage under the FTR Act,⁴⁷ the acceptance of large cash payments in the luxury vehicle industry also carries appeal for laundering activity.

Luxury cars are also used as a transfer of value mechanism in the criminal community when on sold. Criminal infiltration of businesses across the retail and wholesale luxury car industry, and related luxury goods sectors, also enables them to move funds across business networks and diversify across various asset types.

Luxury yachts and boats also feature in asset restraints, with Australian government agencies seeing them as a destination for investing proceeds of crime. Watercraft can serve an additional purpose to storing value when they are used to facilitate illicit drug importations.

CASE STUDY 24

Operation Elbrus was a joint ATO and AFP investigation into a large scale tax fraud and money laundering scheme. The investigation involved a syndicate that conspired to withhold and launder \$105 million owed to the ATO.

Illicitly obtained funds were invested into luxury assets including a boat, cars, motorbikes and an aeroplane. A legitimate payroll company, run by the syndicate members, accepted money from legitimate clients to process payroll, transferring funds to sub-contracted companies (Tier 2 companies), which made payroll payments to workers of clients. The Tier 2 companies were fronts, with straw directors, but effectively controlled by syndicate members. These companies partially remitted tax obligations to the ATO, but redirected remaining funds through a complex series of companies and trusts to accounts controlled by syndicate members. These funds were used to purchase the luxury items, with syndicate members being joint or principal beneficiaries. Investigators estimate unpaid funds to total approximately \$105 million.

The methods used to enable the laundering and asset purchases included: use of separate foreign secrecy jurisdictions for banking and company incorporation; use of corporate vehicles including trusts and shell companies; use of financial centres overseas; use of multiple professional facilitators including solicitors, accountants and company service providers; the use of false invoices and descriptions of funds transfers as loans.

Outlook

The use of luxury goods as a store of value mechanism will continue to pose a high money laundering vulnerability over the next three years. The primary driver for luxury vehicles and watercraft being used as a store of value mechanism for laundered funds is their lifestyle appeal. Coupled with the relative ease of transacting in these sectors due to limited AML oversight, their criminal exploitation will almost certainly persist.

⁴⁷ Motor vehicle dealers who provide insurance or act as insurance intermediaries **must** report to AUSTRAC significant cash transactions of \$10,000 or more (or foreign currency equivalent), as well as suspect transaction reports.

BULLION AND PRECIOUS METALS (PHYSICAL OR SECURITIES) – TRANSFER OF VALUE⁴⁸

Risk rating

The use of bullion and precious metals as a value transfer mechanism is assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Domestic criminals buy and sell bullion and precious metals to launder money as they have a high intrinsic value, can be purchased with cash and provide anonymity when transferring value.
- The buying and selling of bullion and precious metals allows criminals to easily invest, transfer and conceal the proceeds of crime with a low risk of detection.

Domestic context

As with luxury goods, bullion and precious metals are a multi-purpose asset that can be used as a store of value mechanism and as a value transfer mechanism. They have a number of features that make them attractive to criminals. These include:

- their universal acceptance in extensive domestic and global regulated and unregulated markets where prices are easily established
- the relative ease to acquire them
- the comparatively large values and ease to transport them
- the ease to store and conceal them, including through the use of precious metal certificates⁴⁹
- their status as a safe haven investment, meaning that the benefits of these assets to the legitimate investor apply equally to criminals.

Bullion and precious metals are relatively easy to conceal and move across domestic and international borders and convert back to legitimate funds.

Bullion is easily purchased with cash and purchased anonymously from bullion dealers who are not required to carry out customer identification procedures when the retail value of the transaction is less than \$5,000.⁵⁰ Furthermore, criminals are known to make cash-only purchases of bullion below \$10,000 to avoid AML/CTF reporting obligations.

⁴⁸ AUSTRAC regulates the buying or selling of bullion where the buying or selling is in the course of carrying on a bullion-dealing business. For the purposes of this assessment, bullion is defined as gold, silver, platinum or palladium authenticated to a specified fineness in the form of bars, ingots, plates, wafers or similar forms including coins. Precious metals, such as granules of fine gold typically used for the manufacture of jewellery or gold dust, are not regulated under the AML/CTF Act. Businesses buying and selling precious metals that are not classified as bullion are not subject to AML/CTF regulation.

⁴⁹ Precious metal certificate products verify the ownership of a certain amount of precious metal, usually gold, silver or platinum. The authority that issues the certificate typically offers a storage service for the physical metal that the certificate represents. Criminals can use third parties to purchase the certificates and launder the proceeds of crime. This allows them to distance themselves from the asset and obfuscate the true source of funds used to acquire the certificate.

⁵⁰ As per Chapter 33 of the AML/CTF Rules, this exemption to application customer identification procedures does *not* apply where the bullion dealer determines that they should collect further KYC for ongoing customer due diligence (OCDD) purposes, or update and verify that KYC for OCDD purposes.

CASE STUDY 25

The AFP, in partnership with the National Disability Insurance Agency, AUSTRAC and Services Australia, conducted an investigation into several suspected fraudulent NDIS providers based in Western Sydney. The AFP arrested six people allegedly involved in a crime syndicate and are pursuing criminal prosecutions in relation to over \$4 million in allegedly fraudulent NDIS claims. Over \$2 million in suspected tainted assets were seized during the search warrants including eight kilograms of gold bullion from a vault at a secure premises, worth approximately \$600,000.

Outlook

The use of bullion and precious metals as a value transfer mechanism will continue to pose a high money laundering vulnerability. This will be driven by strong international markets for these goods, their intrinsic value and their attractiveness as a hedge against current economic uncertainty.

WEALTH AND FINANCIAL ASSETS – STORE OF VALUE

Risk rating

The use of wealth and financial assets as a store of value mechanism is assessed as posing a **medium** and **stable** money laundering vulnerability.

This category of vulnerability includes the use of securities and derivatives (including fixed-interest financial products and debt-based assets), APRA-regulated superannuation funds and SMSFs for the purposes of storing value.

Key judgements

- Australians have access to a diverse range of wealth and financial assets. This includes securities, derivatives, superannuation and SMSFs. Each asset has varying levels of risk, costs and ease of use for money laundering, as well as different regulations and restrictions. The risk of criminal exploitation therefore depends on the type and purpose of the assets used.
- For store of value purposes, criminals likely favour securities associated with a lower level of investment risk. Higher-risk investments, such as derivatives, are likely more suitable for layering activity rather than for the long-term store of wealth.
- Superannuation and SMSFs are also attractive vehicles for storing illicit funds. SMSFs are likely exposed to an increased level of money laundering risk as they are not regulated under the AML/CTF Act and allow members to store value in assets such as cash and real estate. However, these have a long-term investment horizon.

Domestic context

Securities and derivatives

The risk of criminals using securities and derivatives to legitimise and integrate illicit funds into the financial system is assessed as medium. Australian government agencies indicate they have occasionally restrained, forfeited or frozen securities over the past two years, and estimate a moderate risk of proceeds of crime being used to purchase securities.

Securities and derivatives are open to exploitation as illicit funds can be moved into these financial assets under the guise of being legitimate investment strategies. In addition, some stockbrokers and securities dealers likely have less knowledge of their AML/CTF obligations compared to more sophisticated sectors such as banking, limiting their ability to detect and report suspicious matters (see [Stockbrokers and securities dealers](#)).

Securities and derivatives carry varying levels of risk, ease of use and investment durations. Investing in low-risk securities such as fixed interest products, government and corporate bonds, or shares in large and well established blue-chip companies, provides a recurring income and requires minimal skill and expertise. Low-risk securities carry a higher money laundering risk as they have more stability and are suitable for holding value over a longer period of time, including some debt-based assets that allow funds to be held for up to 30 years.

In contrast, the risk of exploitation for store of value purposes is lower for derivatives and high-risk securities such as small cap shares, contracts for differences, options and futures. They require more knowledge of markets and expertise given their high volatility, speculative nature and potential for significantly larger losses. They are likely more suitable for layering funds to create an appearance of gains or losses from trading activity, rather than for the long-term store of wealth.

Where securities are used for storing illicit funds, they can be held by opaque legal structures such as shell companies, entities with straw directors, or entities incorporated in secrecy jurisdictions. The lack of transparency is ideal for holding illicit funds for long periods of time while masking the true beneficial ownership and control of assets (see [Legal structures](#)).

The extent to which securities and derivatives are exploited is highly likely to be lower than other store of wealth mechanisms that are less volatile, more accessible and not as reliant on market conditions. However, SMR reporting in the stockbroker and securities dealers sector remain an important mechanism to detect money laundering, frauds and other predicate crimes through this channel (see [Stockbrokers and securities dealers](#)).

CASE STUDY 26

A registered retail funds provider likely allowed the investment of illicit funds into their mortgage-managed investment schemes via cash deposits. The schemes allow investors to pool funds together, with a fund manager appointed to loan funds to borrowers for property purchases and development in Australia.

Between 2018 and 2021, the fund received many large cash deposits totalling almost \$460,000 into their three mortgage-managed investment schemes, some from unknown sources. A related party authorised to receive funds for loans on its behalf also received nearly \$250,000 in large cash deposits from similar sources.







Superannuation and SMSFs

Superannuation and SMSFs are probably used to store criminal wealth to a lesser extent compared to other mechanisms. This is due to product restrictions such as limited access to funds and maximum contribution caps. Nonetheless, it requires very little skill or expertise to store criminal proceeds in these products, and transactions may appear legitimate and therefore not trigger suspicion. SMSFs are more vulnerable to exploitation, in comparison to APRA-regulated super funds, as they are not regulated under the AML/CTF Act, and they allow members to invest in assets not available in regular superannuation funds. This includes assets that pose a high money laundering risk, such as cash, real estate, unlisted trusts and lifestyle assets.

Outlook

Wealth and financial assets will continue to pose a medium money laundering vulnerability over the next three years. They can provide a long-term mechanism for storing wealth, as well as a veneer of legitimacy when withdrawn as an investment or retirement earnings. However, criminals will likely find other high-value assets more appealing, particularly those with fewer restrictions and lower exposure to volatile market conditions. The individual financial motivations of criminal individuals is a key determinant of the exploitation of these assets.

DIGITAL CURRENCIES

SECTOR/CHANNEL/SERVICE	RATING	OUTLOOK
Digital currencies – transfer of value		
Digital currency exchanges		
Digital currencies – store of value		

DIGITAL CURRENCIES – TRANSFER OF VALUE

Risk rating

The use of digital currency as a value transfer mechanism is assessed as posing a **high** and **increasing** money laundering vulnerability.

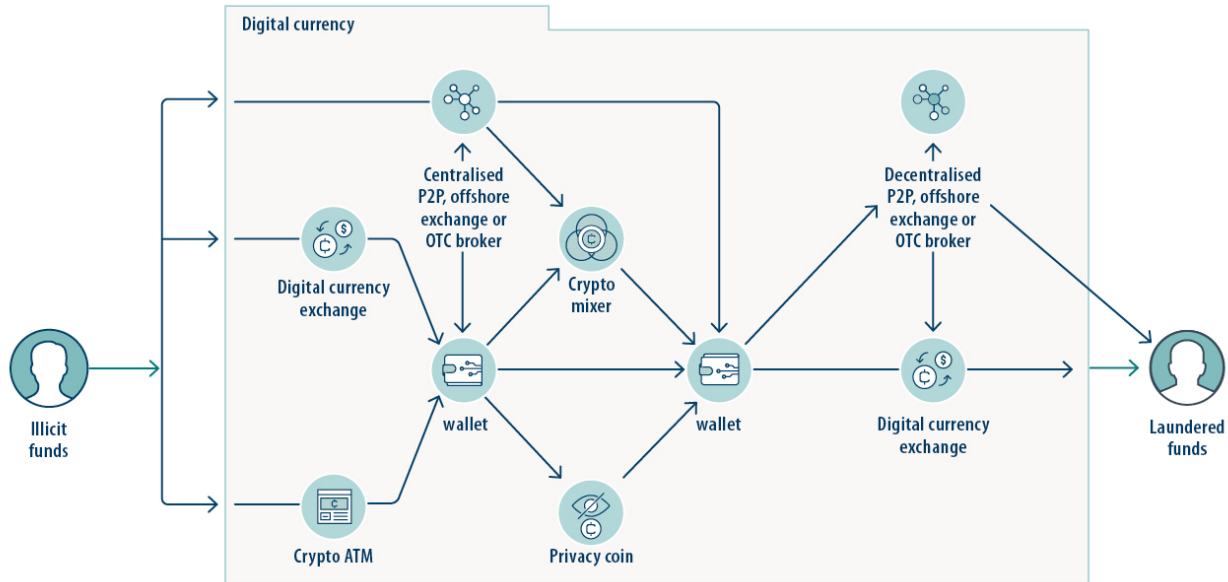
Key judgements

- Under the AML/CTF Act, regulation of digital currencies is currently limited to digital currency-to-fiat currency (and vice versa) transactions provided by DCEs. This means digital currency-to-digital currency payments, such as those made between criminal groups, are only visible to law enforcement and regulators with blockchain monitoring tools where the wallet address is known.
- Digital currencies allow criminal groups to move funds across borders quickly, cheaply and pseudonymously. Digital currency as a transfer of value mechanism is a complementary channel to traditional and entrenched money laundering channels.
- Criminals laundering in the digital currency market use unsophisticated methods to move funds offshore quickly. They favour:
 - fast transfers between fiat currencies and stablecoins
 - mixers and tumblers
 - offshore and unregulated peer-to-peer traders
 - money mules
 - remitters
 - cash-to-digital currency contracts (see [Figure 2](#)).
- Criminal groups' persistent reliance on the traditional fiat economy means regulated on and off ramps will continue to be used to cash out of digital currency. This will allow law enforcement visibility of regulated cash-to-digital currency activity conducted through DCEs.

Domestic context

In the domestic context, the pseudonymity⁵¹ of digital currency presents a vulnerability for law enforcement where digital currency-to-digital currency payments and transfers are involved without the use of on or off ramps. The use of unregulated over-the-counter (OTC) and peer-to-peer (P2P) trading services creates a gap in Australia’s visibility of criminal digital currency activity.

Figure 2 – Common money laundering transactions in the digital currency ecosystem



P2P exchanges present a heightened risk for the transfer and layering of illicit cash. These platforms have large customer bases and act as focal points to swap digital currency between users, including in-person exchanges using physical cash or third-party services. The anonymity and lack of regulatory oversight of informal P2P trading networks create key opportunities for criminals to recruit and use both complicit and unwitting formal P2P traders to launder funds.

OTC broker services enable high-volume and high-value transactions outside the open exchange, and present a high capability to move or hide wealth for criminal purposes.

Reporting by Chainalysis shows a steady increase in the volume of digital currency laundered since 2020, with a significant increase in 2022.⁵² Digital currency remains the primary currency used in scams and ransomware payments due to its borderless, pseudonymous and immutable nature and speed of transfers. In 2022, the share of ransomware funds going to mainstream exchanges increased by 10 per cent and the use of mixers to launder ransomware payments also increased slightly.⁵³

⁵¹ Pseudonymity can be defined as ‘traceable anonymity’, where under ordinary evaluation, identity cannot be determined. However, with technical procedures, association to an individual can be made.

⁵² Chainalysis, The 2023 Crypto Crime Report, Chainalysis, 2023.

⁵³ Ibid

CASE STUDY 27

AUSTRAC recently identified a matter in which it was alleged multiple digital currency ATM operators and financial institutions were being used to move substantial funds gained through suspected scam activity into cryptocurrency. There were reportedly over 100 transactions involving a significant transfer of funds. One of the scam victims alone deposited a substantial amount into an account set up to facilitate the scam. The perpetrators transferred those funds through multiple accounts, including depositing into the digital currency ATMs to layer and create distance from the source of funds. Multiple unique wallets were also used to layer and cloak the existence of the scam activity through the digital currency ATMs.

Outlook

The use of digital currency as a value transfer mechanism will pose an increasing money laundering vulnerability over the next three years. As the use of digital currency expands for legitimate use, opportunities for criminal use will also increase.

DIGITAL CURRENCY EXCHANGES



Digital currency exchanges (DCEs) have been regulated under the AML/CTF Act since 2018. As at March 2024, 389 DCE providers were registered with AUSTRAC.⁵⁴

DCE providers must comply with AML/CTF obligations, including identifying their customers, maintaining records and reporting transactions including suspicious matters to AUSTRAC.

However, the regulatory framework only applies to the exchange of digital currency to fiat currency, and vice versa. Australia is currently consulting on AML/CTF reforms, including the range of digital currency services that are captured in legislation. In addition, Australia is consulting on requirements that would extend FATF's 'Travel Rule' to digital currency transactions. The Travel Rule would require regulated businesses to identify all parties involved in transactions. Implementing this would provide greater visibility of the ultimate beneficial ownership of digital currency assets, as well as parties to transactions.

Risk rating

Digital currency exchanges are assessed as posing a **medium** and **increasing** money laundering vulnerability.

Key judgements

- Criminals exploit DCEs for money laundering as an extension of, and in addition to, traditional layering methodologies.
- DCEs offer speed, global reach, pseudonymity and can facilitate funds flows to and from foreign jurisdictions with low visibility. The near-instant and irreversibility of transactions present a persistent challenge in detecting and disrupting illicit transactions before funds leave wallets.
- Digital currency ATMs and the DCE-remittance corridor are emerging trends that present a heightened money laundering vulnerability.

⁵⁴ This register is not publicly available. AUSTRAC publishes details of cancelled, suspended and refused registrations on its website.

- DCEs provide critical on and off ramping services between fiat currency and digital currency. This presents reporting entities and Australian government agencies with key targeting and intelligence collection opportunities.

Domestic context

Australian criminals largely exploit DCEs to move relatively low-value criminal proceeds offshore. The volatility and low liquidity of the broader digital currency market generally makes them a less attractive channel for high-value money laundering. Criminals often obscure transactions by transferring digital currency through multiple registered exchanges and decentralised exchanges. Once the funds have been sent to an external address, the original DCE can no longer attribute the digital currency to their customer.

Other features that can increase anonymity for customers and decrease visibility for authorities include:

- the use of offshore P2P platforms
- transactions to un-hosted or self-hosted wallets
- transactions to unregulated, offshore exchanges and decentralised exchanges
- transactions involving mixers and tumblers
- the operation of undisclosed nested platforms
- the use of brokers to conduct anonymous trades on behalf of third parties.

The DCE-remittance corridor is an emerging money laundering vulnerability.⁵⁵ When value is moved offshore through digital currency without a cash-out mechanism at either side, visibility of the transfer chain is reduced. Another emerging vulnerability is the operation of digital currency ATMs, which allow criminals or their victims to buy and sell digital currency with cash. Reporting entities offering this service are therefore exposed to many cash-related money laundering vulnerabilities highlighted in this assessment.

The effectiveness of AML/CTF controls in DCE providers are generally of a moderate standard. Given the sector's infancy, many reporting entities assess their products, delivery channels and customers as low risk by default. Understanding of money laundering risk exposure may therefore be poor among some reporting entities.

Outlook

DCEs will likely pose an increasing money laundering vulnerability over the next three years. As the digital currency ecosystem continues to evolve, domestic criminals will undoubtedly identify new opportunities to launder and conceal illicit funds from law enforcement. While Australian government agencies have access to blockchain analytics tools to detect and track criminal abuse of digital currency, technological advancements ensure criminal groups continue to obfuscate their activity.

If adopted, proposed regulatory reforms aligning Australia's regulation of DCEs with FATF requirements will help reduce money laundering vulnerability in the sector. However, if broader criminal adoption of digital currency continues, they will almost certainly become a high risk money laundering channel.

⁵⁵ As at March 2024, 151 reporting entities are registered with AUSTRAC as dual DCE and remittance service providers in Australia.

DIGITAL CURRENCY – STORE OF VALUE

Risk rating

The use of digital currency as a store of value mechanism is assessed as posing a **medium** and **increasing** money laundering vulnerability.

Key judgements

- Intelligence suggests that Australian criminal groups are less likely to use digital currency as a store of value mechanism. This is due to its volatility and low liquidity compared to other traditional mechanisms. Stablecoins are favoured by some domestic criminals due to their perceived stability and use as a hedge against price volatility.
- Algorithmic stablecoins may be appealing to groups looking to invest long-term in the digital currency market but Australian criminal groups will likely favour asset-backed stablecoins for laundering illicit funds.
- Storing digital currency in cold wallets assists criminals to hide their wealth from regulatory and law enforcement agencies. However, cold wallets are often tangible and therefore easier to restrain and confiscate by law enforcement once detected.

Domestic context

The accessibility and pseudonymity of storing value through digital currency is a key money laundering vulnerability. However, exploitation by domestic criminals is less than other more established and stable channels. This is due to the volatile prices of digital currency and therefore the potential impact on the value of their holdings over the short, medium and long-term. On-chain data reports that criminal balances in wallets significantly declined in value in 2022, likely due to cases of DCE collapses and hacking, and the 'crypto winter', highlighting the reduction in criminals storing digital currency. Unlike the traditional financial system, the nature of the public blockchain ensures stored criminal proceeds cannot hide in opaque networks and structures and can be visible.

Criminal groups favour the use of stablecoins to store value on the blockchain without the concern of it losing significant value. While digital currency adoption rates have increased in the past few years, the market has faced severe volatility and reputational damage more recently with a major exchange collapsing and others hacked, leading to the fall in value of the major currencies, including Bitcoin and Ether.

Non-fungible token (NFT) ownership is predominantly used for collection or investment purposes and has been highlighted internationally as vulnerable to criminal exploitation for fraud. However, there is insufficient evidence to indicate domestic criminals are widely exploiting NFTs for money laundering activities.

The use of cold wallets is a favourable mechanism to store and hide value off the blockchain from law enforcement visibility. Cold wallets allows criminal groups to store digital currency without the need to connect to a regulated cash-to-DCE, which can be monitored more easily by law enforcement.

Capacity and facilities to access and store confiscated digital currency assets remain a persistent challenge for law enforcement.

CASE STUDY 28













In February 2023, nine members of an MLO were arrested by the AFP and millions of dollars' worth of cash, assets and digital currency were seized. The organisation exploited digital currency trading, domestic and foreign shell company structures and informal value transfer systems to move significant volumes of money for transnational and serious and organised crime groups around the world, primarily through Asian countries. The AFP restrained a number of digital currency assets worth over \$32 million dollars stored in wallets on hard drives and mobile phones.

Outlook

The use of digital currency as a store of value mechanism will pose an increasing money laundering vulnerability over the next three years. The exploitation of asset-backed stablecoins and mainstream digital currency is likely to continue due to their price stability, high accessibility and ease and speed in converting to other coins and fiat currency.

Mass adoption of stablecoins and mainstream digital currency would likely provide greater opportunities to cover up the origins of criminal proceeds. It would also likely reduce the need for criminal use of regulated service providers to convert proceeds to fiat currency. This would likely raise the risk level of money laundering to high.

PROFESSIONAL SERVICE PROVIDERS

PROFESSION	RATING	OUTLOOK
Lawyers		
Accountants		
Real estate agents		
Offshore service providers and trust and company service providers		
Trusted insiders		
Customs brokers		



Professional service providers are uniquely positioned to provide insights into suspicious behaviour through the provision of professional services, helping to build a more complete picture of money laundering activities and assist law enforcement activities. The implementation of impending AML reforms will also harden currently unregulated sectors against exploitation by criminals who use the services provided by professional service providers to facilitate money laundering activities. Regulation will also make it more difficult for professional service providers who are complicit in facilitating money laundering activities to continue to do so undetected.

LAWYERS



In Australia, lawyers are not currently regulated under the AML/CTF Act. They are not currently subject to customer due diligence, transaction reporting and requirements outlined in the Act. A notable exception relates to solicitors, who must report cash transactions of \$10,000 or more, or the foreign currency equivalent, to AUSTRAC under the FTR Act.

Each Australian state and territory has its own regulatory laws and individual organisations that receive complaints, regulate and represent solicitors and barristers. At the Commonwealth level, the profession is governed by the Legal Profession Uniform Law, which states and territories are encouraged to join and which provides regulatory arrangements for the legal profession. Trust accounting rules and regulations can vary from state to state.

Risk rating

Lawyers are assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Lawyers can facilitate money laundering, including unwittingly, through the provision of their professional services. Law enforcement agencies are consistently identifying criminals seeking and exploiting the advice and services of lawyers to legitimise their activity and obfuscate proceeds of crime.
- Domestic criminals rely on lawyers, who often work alongside other professionals such as accountants, financial advisers and offshore service providers, to conceal illicit funds and beneficial ownership.
- Key vulnerabilities associated with lawyers include the criminal use of law firm trust accounts, facilitation of real estate transactions and the creation and administration of legal structures.

Domestic context

The involvement of legal professionals as gatekeepers or facilitators for money laundering is recognised both domestically and internationally as an enduring vulnerability. Australian government agencies report the exploitation of lawyers, along with a range of other professional service providers, as a key component of the criminal business model.

Lawyers conduct a range of services that benefit criminals in the money laundering process, including:

- operating trust and other accounts to deposit, hold and disburse client funds
- facilitating real estate, business and asset transactions including purchase, sale, transfer of ownership and financing arrangements
- establishing and administering complex domestic and offshore legal structures (including trusts and companies, the use of straw directors and nominee shareholders).

AUSTRAC's visibility of suspicious transactions involving lawyers is limited. Estimates of the number of criminally-complicit lawyers, or the volume of funds laundered by these individuals, are not available. However, secondary reporting to AUSTRAC by Australian banks demonstrates lawyers handle large volumes of cash and facilitate a large volume of incoming and outgoing international funds transfers. This increases vulnerability to money laundering by both complicit and non-complicit professionals.

Clients of lawyers pose differing levels of money laundering risk. Vulnerability is increased when a client uses a third party to help obscure identity and/or beneficial ownership. The absence of customer due diligence obligations under the AML/CTF Act exacerbates this vulnerability.

CASE STUDY 29

Operation Elbrus was a joint ATO and AFP investigation into a large-scale tax fraud and money laundering scheme. Two lawyers have been convicted of money laundering offences as part of a number of Elbrus prosecutions, which involved more than \$105 million defrauded from the ATO.

A partner at a law firm used his access to the practice's trust account to knowingly launder over \$24 million in criminal proceeds from the syndicate's activities. He created a false document trail using straw directors to 'authorise' trust distributions.

Separately, a commercial and taxation lawyer and accountant, who was a partner at a different law firm, became a critical trusted adviser to the principal conspirators. He used his legal and accounting skills and status as a solicitor to facilitate laundering and tax fraud. The lawyer misused his firm's trust account to transfer criminal proceeds and supply funds to co-conspirators. He set up and facilitated funds transfers through fraudulent companies, committed legal document fraud and destroyed evidence. The lawyer also instructed syndicate members in misleading authorities, supervising straw directors and processing payments.

Outlook

Lawyers will continue to pose a high money laundering vulnerability over the next three years. They provide access to a range of critical products, services and structures desired by money launderers and criminals alike.

ACCOUNTANTS

Risk rating

Accountants are assessed as posing a **high** and **stable** money laundering vulnerability.

This assessment includes tax accountants, also referred to as tax agents or tax advisors, in the scope of accounting professionals.

Key judgements

- Accountants remain among the most frequently and consistently identified professional facilitators of money laundering, internationally and domestically. Their services are particularly valuable in the layering and integration stages of the money laundering cycle.
- Criminal groups misuse the services provided by accountants for money laundering activities. These include mainstream bookkeeping to legitimise illicit funds and managing complex banking and corporate arrangements to conceal beneficial ownership (including schemes involving multiple facilitators and jurisdictions).
- Structuring of fund movements using complex corporate structures to send and receive funds through accountants' client-trust accounts remains a high money laundering risk.
- Although frequently identified in money laundering investigations, the true extent to which accountants are used in laundering schemes is unknown. Accountants are not currently subject to AML/CTF regulation. Investigations traditionally focus on law enforcement targets and funds flows, rather than the role played by professional service providers.

Domestic context

Australian authorities identify accountants as key professional service providers embedded in criminal business models enabling money laundering, along with lawyers, financial advisors and real estate agents.

Accountants can facilitate money laundering schemes by:

- creating and using complex and multi-layered corporate structures and registered companies to layer illicit funds
- moving large volumes of funds rapidly through multiple company accounts
- obscuring and falsifying the source of structured cash deposits
- obscuring parties to a transaction where trust accounts are used
- transacting with large volumes of cash and structuring.

The accounting industry is diverse, with a number of specialisations. It is also highly accessible across a range of economic activities, given the critical business functions they perform and the interconnected nature of the profession. Australian government agencies have observed an increase in the provision of multifaceted services through consultancy firms. They have identified lawyers and accountants in such arrangements, and cooperation with broader professional networks such as mortgage brokers.

Accountants' vulnerability to money laundering is elevated by the risk profile of clients and transactions. This is especially the case where cash-intensive businesses or complex transactions involving multiple jurisdictions and high-risk clients are involved. Accountants also have dual capability to assist in predicate crimes such as tax evasion and fraud that create illicit funds, as well as enabling the laundering of these proceeds.

Compared to mandatory legal professional auditing and reconciliation of client-trust accounts, accountants and tax agents lack these requirements. Some may voluntarily be members of professional associations that require audits be undertaken.

Accountants are not currently regulated under the AML/CTF Act, creating a significant visibility gap of financial activity for law enforcement agencies. The extensive use of complex legal structures set up by accountants and lawyers remains a key challenge in identifying beneficial ownership and investigating money laundering schemes.

CASE STUDY 30

An investigation into a transnational MLO that was exploiting banking, casino, cryptocurrency, real estate and investment sectors identified the involvement of professional facilitators including accountants and bank employees.

It is alleged the MLO's Australian based accountant provided advice and assistance to the syndicate on how to avoid bank triggers and alerts for funds entering the Australian financial system from overseas institutions.

Alleged assistance provided by the professional facilitators also included:

- opening bank accounts to receive international funds transfers
- creating fraudulent financial documents to legitimise incoming international transactions in response to source of funds questions from the recipient Australian banks
- communicating with bank personnel on behalf of the syndicate
- sourcing and applying for a loan from a financial institution.

Accountants located offshore were also used to establish companies in their local jurisdictions, particularly shell companies, to obscure the source of the funds transferred into Australia.

Outlook

Accountants will continue to pose a high money laundering vulnerability over the next three years. Their centrality across the financial system and provision of professional services are desired by money launderers and other criminals alike.

REAL ESTATE AGENTS

Risk rating

Real estate agents are assessed as posing a **medium** and **stable** money laundering vulnerability.

Key judgements

- The purchase of real estate is a key money laundering methodology, exposing real estate agents to significant amounts of criminal proceeds in holding deposits (see [Real estate \(domestic\)](#)).
- While real estate is assessed as a very high vulnerability, real estate agents play a different role to lawyers, accountants and conveyancers who are able to facilitate purchases and obfuscate sources of funds and beneficial ownership.
- Real estate agents have a different relationship with buyers and sellers to other parties involved in a property transaction, and can provide unique insights to regulators and law enforcement agencies.
- Criminals seeking to purchase real estate with large amounts of cash may give the cash to an agent or deposit it into the agency's statutory trust account directly. Due to the nature of these accounts, criminal proceeds can be co-mingled with legitimate client funds and the source and beneficiary of criminal proceeds can also be concealed from reporting entities.

- While real estate agents are not currently regulated under the AML/CTF Act, they hold valuable intelligence related to real estate purchases that can assist law enforcement to combat money laundering through this sector.

Domestic context

While it is difficult to measure the extent and prevalence of criminal exploitation of real estate agents in Australia, it is assessed to be moderate. Although real estate agents are considered gatekeepers to the real estate market, criminals also exploit lawyers and conveyancers to:

- facilitate property purchases and launder funds through the market
- facilitate purchases directly between a buyer and seller, to remove third party involvement.

Real estate agents have the capacity to manipulate house values for the benefit of money laundering and facilitate rental payments to legitimise rental arrangements for criminals.

Real estate agents may have visibility of:

- deposits, purchases or rental amounts made by cash
- any legal structures relating to the ownership or effective control of a property
- indications that a purchaser may not be the true beneficial owner or in effective control of a property
- how the property has been or is being used (particularly for rental property).

Real estate agents are not currently subject to AML/CTF regulation, creating a visibility gap for law enforcement where agents are exploited by criminals. This is partially offset by banks reporting threshold transaction reports (TTRs) from real estate agencies. However this does not provide a holistic view of cash use in the sector, nor provide insight into customers' identities or source of wealth. Businesses licensed as real estate agencies also use cash for other business functions from the same accounts as real estate transactions. This creates an opportunity for co-mingling legitimate and possibly illicit funds.

The absence of obligated due diligence or beneficial ownership checks on clients is a key vulnerability for professional service providers, including real estate agents, in enabling money laundering through the sector. Given a large proportion of high-value real estate purchases by foreigners use cash, the absence these checks elevates the risk of money laundering.

CASE STUDY 31

In one AFP investigation, a member of a transnational MLO had been living in a rented luxury property while their own was being renovated. A rental payment of more than \$70,000 was transferred from an international company. Members of the MLO regularly made payments for living expenses and other goods in Australia from overseas companies to obfuscate the source of the funds.

Outlook

Real estate agents will continue to pose a medium money laundering vulnerability over the next three years. This will be driven by continued demand for Australian property by criminals. So long as criminals can invest their proceeds into the Australian property market, real estate agents and other professionals will remain vulnerable to criminal exploitation, both wittingly and unwittingly.

OFFSHORE SERVICE PROVIDERS AND TRUST AND COMPANY SERVICE PROVIDERS

Risk rating

Offshore service providers (OSPs) and trusts and company service providers (TCSPs) are assessed as posing a **medium** and **stable** money laundering vulnerability.

OSPs are businesses and professionals that offer business creation, administration and financial services. They are typically based in secrecy jurisdictions or larger financial centres. TCSPs assist in the creation, operation and management of corporate and trust structures.

Key judgements

- Given their technical expertise and knowledge, OSPs and TCSPs provide a gateway for criminals to exploit legal structures, including companies and trusts.
- Complex legal and financial structures obfuscate beneficial ownership, conceal wealth and can move significant volumes of funds domestically and offshore. Criminals therefore often exploit them to launder funds. OSPs and TCSPs are vulnerable to enabling money laundering through the creation and management of these mechanisms.
- OSPs operating in secrecy jurisdictions and foreign financial hubs are highly attractive to criminals of various sophistication levels. These highly-accessible professional service providers enable criminals to launder illicit funds through financial products and systems across jurisdictions.

Domestic context

Given their expertise in wealth protection and the administration of trust and company structures, OSPs and TCSPs are often exploited by criminals. Whether they are complicit or non-complicit, they provide an appearance of legitimacy to criminal activity and create further distance between a criminal and their illicit proceeds.

Although companies can generally be set up without a professional service provider, the creation of more complex legal structures, including trusts, often require the expertise of professional advisors such as OSPs or TCSPs (see [Legal structures](#)). These structures are highly attractive to criminals as they obfuscate beneficial ownership, conceal the origin and purpose of financial transactions and move significant volumes of funds domestically and offshore. As more sophisticated criminals consistently exploit these mechanisms, OSPs and TCSPs remain vulnerable to enabling money laundering.

Many of the established methodologies used to conceal wealth, circumvent financial obligations and ultimately launder money are enhanced by an OSP or TCSP.

Key methodologies include:

- establishing corporate structures in jurisdictions with lax regulatory and legislative frameworks, including secrecy jurisdictions
- creating complex chains of companies across multiple jurisdictions
- appointing straw directors and shareholders
- acting as trustees on behalf of a client
- providing loans secured by client funds.

Services provided by OSPs and TCSPs are not currently regulated under the AML/CTF Act, creating difficulties in detecting criminal activity in the industry. However, reporting entities in Australia should be able to identify when non-individual customers incorporated offshore are associated with an OSP, and must manage and mitigate this risk. This includes determining company structures and beneficial ownership. As TCSPs enable more sophisticated and complex laundering methodologies, authorities face further obstacles in disentangling these structures and entities to uncover beneficial owners.

CASE STUDY 32

In response to the public release of the Pandora Papers data leak in 2021, an Australian government agency conducted an investigation into the criminal activities of an individual and his network, both in Australia and abroad.

The individual is the beneficial owner of an inactive company registered by an OSP in the British Virgin Islands. He also established offshore companies in multiple other jurisdictions and is recorded as former officeholder or shareholder of multiple Australian proprietary companies.

The directors of his companies likely act as OSPs or advisors, rather than fulfilling the role of director. Skilled third-party directors provide the individual with access to services and advice from professional service providers while distancing himself from the companies.

The individual has an extensive history of business misconduct, criminality and non-compliance with tax obligations.

Outlook

OSPs and TCSPs agents will continue to pose a medium money laundering vulnerability over the next three years, given their provision of services and expertise desired by money launderers and criminals alike. The lack of regulation and the difficulties in disentangling corporate structures will continue to be key challenges for AML authorities.

TRUSTED INSIDERS

Risk rating

Trusted insiders are assessed as posing a **medium** and **stable** money laundering vulnerability.

Trusted insiders are individuals who misuse their legitimate access to an organisation's services, products, information or facilities for unauthorised and/or illegal purposes.

Key judgements

- Trusted insiders enhance money laundering capability given their high levels of access and specialist knowledge.
- Criminals use trusted insiders in key sectors to source funds, move cash, falsify documentation and provide advice on evading law enforcement and regulatory detection. Particularly vulnerable sectors are those with a high capacity to accept and/or move large-scale funds.
- Criminals likely use a range of methods and techniques to recruit trusted insiders. Depending on the channel exploited and the level of engagement required, they may cold approach individuals, or begin a legitimate relationship and develop trust over time.

Domestic context

Given their inside knowledge and/or access, trusted insiders can misuse a legitimate entity's systems, services, products or facilities for criminal activity. By providing crucial links to the licit world, trusted insiders facilitate, protect and enhance a criminal's capabilities.

Complicit and well-placed individuals can undermine or subvert their organisation's AML/CTF controls, creating vulnerabilities open to exploitation. Regulated industries with the capacity to process high volumes of funds, such as banks and casinos, are attractive channels for criminals to source or place







trusted insiders. Unregulated industries, such as transport and logistics, are also vulnerable to trusted insiders.

Detection of money laundering can be difficult as criminals often target insiders with the required access and knowledge to circumvent internal policies and procedures. Trusted insiders within reporting entities are able to weaken detection and reporting of money laundering to authorities.

Outlook

Trusted insiders will continue to pose a medium money laundering vulnerability over the next three years given their critical links to legitimate services and markets.

LEGAL STRUCTURES

CHANNEL	RATING	OUTLOOK
Legal structures		
SUB-CHANNEL		
Companies		
Trusts		

LEGAL STRUCTURES

Risk rating

Legal structures are assessed as posing a **high** and **stable** money laundering vulnerability.

For the purpose of this assessment, ‘legal structures’ is an umbrella term that includes various types of companies and trusts. Companies are legitimate vehicles and are regulated through the *Corporations Act 2001* and under the *Australian Securities and Investments Commission Act 2001*.

This section provides an overview of money laundering vulnerabilities posed by the collective use of legal structures. Individual vulnerabilities associated with companies and trusts are addressed in separate sub-categories below.

Key judgements

- Legal structures and associated banking arrangements are persistently exploited by criminals to store and move large volumes of criminal proceeds, including offshore.
- Legal structures can be established with relative ease and can help mask beneficial ownership.
- Australia does not have comprehensive mechanisms for the systematic collection, verification and release of beneficial ownership information. This restricts government agencies’ ability to detect and investigate money laundering through legal structures. Restraining and confiscating criminal assets held by companies or trusts can also be challenging and resource-intensive.
- Offshore legal structures can help further obscure financial flows and beneficial ownership, particularly when legal structures are established in secrecy jurisdictions or across multiple jurisdictions.
- Professional service providers play a key role in establishing and managing complex legal structures used to conceal wealth and launder funds.

Domestic context

The misuse of legal structures is frequently and persistently observed in Australian money laundering investigations. Company and trust structures are versatile and can be tailored to complement criminal operations, obscure financial flows and protect criminal assets.

Legal structures are generally highly-accessible, easy and cheap to establish. They can be exploited to move significant volumes of funds domestically and offshore. Companies can operate their own bank accounts and independently engage in transactions.

Common money laundering activities include:

- placing cash into bank accounts held by legal structures to co-mingle funds
- rapid layering of funds between domestic and foreign legal structures to obscure the true source or provide legitimacy to offshore funds transfers
- integration of funds where legal structures are used to purchase or invest in high-value assets, such as real estate.

Complex legal structures can be established through one or more of the following lawful activities:

- the use of parent and subsidiary entities
- the establishment of trust, trading and operational business accounts
- the use of 'holding companies', joint ventures, partnerships, inter-party 'loans', service agreements and 'lines of credit'
- the use of other structures or arrangements such as franchisor/franchisee structures, multi-level marketers, licensor/licensee arrangements and financial and legal instruments (e.g. powers of attorney, deeds and contracts).

Complex company structures can also be established through the use of de facto and shadow directors. A **de facto director** is a person who operates in the capacity of a director but is not named on ASIC's corporate records. They may have titles such as 'business development director', 'chairman' or 'principal'. A **shadow director** is a person who operates through a straw or dummy director. The use of de facto and shadow directors is not legal.

Uncovering ownership and control of legal structures is challenging for law enforcement agencies and reporting entities. Forty per cent of industry respondents surveyed for this assessment said this was a key challenge to detecting and responding to money laundering. Criminals exploit this by sheltering assets behind various types and layers of legal structures to conceal true ownership and avoid confiscation. This includes the use of shell companies or shelf companies with straw directors or straw shareholders (see [Companies section](#)). The Australian Government has committed to establishing a beneficial ownership register for companies and other legal vehicles, which will almost certainly improve transparency.

Money launderers often leverage the expertise of professional service providers to establish and manage complex legal structures, such as lawyers, accountants, or trust and company service providers (TCSPs). Facilitators can create straw director and shareholder arrangements, or act as trustees to provide a veneer of legitimacy to otherwise suspicious transactions (see [Professional and other service providers](#)).

Legal structures established offshore likely carry increased money laundering risks, especially where multiple jurisdictions or secrecy jurisdictions are involved. Using offshore structures increases opportunities for cross-border movement of funds and creates additional layers of legal entities that can hold assets. This hampers the ability for authorities to investigate and prosecute money laundering, especially where jurisdictions have limited corporate oversight, lenient licensing regimes, or weak AML/CTF frameworks.

CASE STUDY 33

Operation Elbrus was a joint ATO and AFP investigation into a large scale tax fraud and money laundering scheme. The investigation involved a syndicate that conspired to withhold and launder \$105 million owed to the ATO. This involved the establishment and operation of a legitimate payroll services company and a number of second tier subcontracting companies the syndicate controlled. Vulnerable individuals were appointed as straw directors of these companies to obscure beneficial ownership.

Funds were concealed and disposed of through bank accounts owned by the companies, or through trust accounts associated with members of the syndicate. Funds were used to purchase 18 residential properties, luxury cars, two aeroplanes and other luxury items. In some instances, transactions were accompanied by false invoices and descriptions. Some funds were also transferred back to Plutus to create the appearance that it was a legitimate and profitable company.

All matters have now been dealt with before the court, pending any future appeals. 15 people have been sentenced over their roles in the scheme.

Outlook

Legal structures will continue to pose a high money laundering vulnerability over the next three years given their critical capacity to conceal wealth, protect criminal assets and obscure illicit financial transactions. Despite the Australian Government's commitment to establish a public beneficial ownership register, complexities associated with legal structures will continue to make disruption difficult.

COMPANIES

Risk rating

Companies are assessed as posing a **high** and **stable** money laundering vulnerability.

For the purposes of this assessment, companies include:

- Australian listed incorporated entities
- Australian unlisted incorporated entities
- foreign incorporated entities operating in Australia
- foreign-owned subsidiaries operating in Australia.

Key judgements

- Companies may be attractive to money launderers because they are easy to establish or purchase with limited knowledge, skills or expertise. They also provide criminals with the capacity to launder high volumes of funds.
- Domestic and foreign shell companies commonly feature in Australian money laundering investigations. Straw and shadow directors or shareholders are also commonly observed. These individuals are used to conceal beneficial ownership and complicate the identification and disruption of money laundering.
- Australian unlisted incorporated entities and foreign owned subsidiaries are exposed to the highest level of money laundering risk relative to other types of company structures in Australia.

Domestic context

The exploitation of company structures is frequently observed in Australian money laundering investigations. This often includes complex structures comprising front and shell companies, which are used to co-mingle or conceal criminal proceeds, protect assets, reduce visibility of beneficial ownership and obscure financial transactions. In addition, bank accounts linked to companies may be used to move higher volumes of illicit funds without flagging suspicion.

The ease of establishing companies in Australia may be attractive to money launderers. The process is fast, inexpensive and can be conducted online or with the assistance of a professional service provider. Existing unlisted companies can also be purchased by criminals and used as legitimate fronts to place and layer proceeds of crime (see [Cash-intensive businesses](#)).

Companies are separate legal entities that can be used to cloak criminal activity and protect illicitly-obtained assets and income. Authorities must lift the corporate veil to identify illicit activity conducted through companies. This creates barriers for investigators and asset confiscation.

Since November 2021, all company directors have been required to register and verify their identities with Australian Business Registry Services. However, this process may be undermined when criminals appoint a family member or 'cleanskin' associate as a straw director, compel vulnerable individuals to register companies or use stolen personal information to establish companies. This allows criminals to maintain control and place or layer funds from a distance. Straw directors can also be appointed to offshore companies controlled by domestic criminals to further conceal beneficial ownership.

Australian unlisted incorporated entities and foreign owned subsidiaries are likely more vulnerable to criminal exploitation compared to publicly-listed or foreign-incorporated companies, which are subject to requirements under the *Corporations Act 2001*. Unlisted incorporated entities are privately owned and subject to less regulatory oversight and public disclosure obligations. This may be an attractive feature for money launderers. It is also harder to determine beneficial ownership of a foreign subsidiary because ultimate control is typically held by an offshore entity.

CASE STUDY 34

An AFP investigation found that the controllers of an MLO utilised shell companies and dummy directors to launder significant amounts of illicit funds worldwide. The MLO used professional service providers to assist in the creation and management of these shell companies. Shell companies can be registered with stolen third party identities without the victims ever knowing that their details have been used by the money laundering syndicate. Bank accounts are then opened in the company names and used to transfer illicit funds until they are frozen by banks or detected by law enforcement.

The MLO also used foreign shell companies to transfer their profits into Australia for investment. The shell companies provided a valuable means of obfuscating the origins of the funds and accommodating large volumes of transactions. The MLO allegedly used companies to purchase a large number of properties around Sydney totalling more than \$90 million.

CASE STUDY 35

A government agency identified persons of interest establishing numerous shell companies to layer and move illicit funds offshore. Funds were highly likely derived from tobacco importation, drug supply or fraud offences.

The shell companies and associated bank accounts were registered under the name of a person of interest and their acquaintances. Recycled phone numbers, mailing addresses and email addresses were also used to circumvent identification requirements by financial institutions.

No genuine business activity was undertaken by the shell companies, however the bank accounts were used to receive bulk cash deposits and large credit transfers. Funds were then transferred to a high-risk jurisdiction via remittance dealers. Accounts were also used to facilitate cross-border transfers of value through offsetting arrangements between foreign and onshore bank accounts.

Outlook

Companies will continue to pose a high money laundering vulnerability over the next three years. This risk rating may increase in the longer term if mitigation strategies do not sufficiently address the ease with which complex company structures can be created in Australia.

TRUSTS

Risk rating

Trusts are assessed as posing a **high** and **stable** money laundering vulnerability.

For the purpose of this risk assessment, trusts include Australian-domiciled trusts and other non-legal persons, and foreign trusts and other non-legal persons.

Key judgements

- Limited oversight of trust structures in Australia makes them attractive to money launderers. Assets can be hidden in trusts easily and uncovering beneficial ownership is challenging, especially when concealed behind a complex structure that has multiple layers.
- Establishing and managing trusts may require a level of technical expertise and involve professional assistance to help draft trust deeds, navigate complex legal frameworks and adhere to administrative obligations.
- Foreign trusts and trusts with foreign trustees or foreign beneficiaries are likely less appealing to criminals holding Australian assets. These arrangements may be more expensive and complex to establish and come with additional regulatory barriers, such as foreign investment notification requirements.

Domestic context

Australian authorities report that trusts are often exploited alongside companies to create complex and opaque legal and group structures. Trusts can be exploited at all stages of the money laundering cycle, including by placing cash into bank accounts, layering funds to and from accounts held domestically and offshore, and purchasing and holding high-value assets.

Trusts are attractive vehicles for money laundering as they separate the legal owner of the assets (the trustee) from the beneficiary, helping conceal the beneficiary's interests. This is a barrier to identification and confiscation of criminal assets in Australia. Trusts with corporate trustees also allow

criminals to use shell companies and straw directors in trust arrangements to create additional layers of obfuscation (see [Companies](#)).

Uncovering the beneficial owners of trusts is difficult, particularly when they are concealed behind multiple layers of legal structures or have multiple beneficiaries. It is challenging for authorities to attribute trust assets or interests in trust assets to specific individuals. While beneficial owners may be outlined in a trust deed (if any exists), access to these documents is limited and often held by lawyers and may attract claims of legal professional privilege (see [Lawyers](#)).

Professional service providers, such as lawyers and accountants, may play a key role in creating and managing trusts because of the complexity and technical expertise that may be required. This includes distinguishing between trusts that have different purposes, restrictions, requirements and risks. Facilitators may also act as trustees to create distance between a trust and its criminally-linked beneficial owners.

The complexities associated with trusts may make some more costly to establish and manage in comparison to companies. However, more sophisticated money launderers seeking to create complex structures are likely to have significant financial resources and unlikely to find the cost prohibitive.

Offshore trusts increase money laundering risks where they allow criminals to hold assets beyond the reach of Australian law enforcement. This complicates beneficial ownership identification, especially when secrecy jurisdictions are involved. In contrast, foreign trusts and trusts with foreign trustees or foreign beneficiaries that are used to hold Australian investments are likely less attractive to criminals. This is because they may be subject to foreign investment notification requirements, or lead to additional taxes for certain assets.

CASE STUDY 36

An investigation into persons of interest allegedly involved in importing illicit drugs identified a property likely belonging to the individuals of interest. However, it was held by a family trust that appeared to be unrelated to them. The trust deed indicated the beneficiaries were the person of interest's brother, his children and spouse. It was determined the trust was established with the sole purpose of concealing assets and avoiding proceeds of crime proceedings.

Outlook

Trusts will continue to pose a high money laundering vulnerability over the next three years. They will remain desirable for criminals wishing to conceal wealth and illicit proceeds as long as they limit regulatory oversight and risk of detection.

GAMBLING SECTOR

SECTOR/CHANNEL	RATING	OUTLOOK
Casinos		
Betting agencies/corporate bookmakers		
Pubs and clubs		
Online offshore gambling		
Casino junket tour operations		
On-course bookmakers		

CASINOS

Risk rating

Casinos are assessed as posing a **high** and **stable** money laundering vulnerability.

Key judgements

- Despite sustained regulatory and law enforcement efforts, casinos continue to be exploited for large-scale money laundering by sophisticated criminal entities and small-scale opportunistic offenders.
- Casinos are exposed to a wide range of inherent money laundering vulnerabilities, and aspects of their operating models make them very attractive to criminals. These include the capacity to ingest large amounts of cash, high-stakes wagering and an environment where large transactions are normalised.
- The effectiveness of AML/CTF programs and associated detection capabilities are uneven across the sector. Therefore, casinos' ability to detect and report suspicious matters and mitigate their risks varies.

Domestic context

Australia's casino sector is large and diverse. In the 2020-21 financial year, it recorded a turnover value of over \$14.91 billion.⁵⁶ The sector is subject to a complex regulatory landscape at national, state and territory levels. Each jurisdiction has its own regulator, unique tax arrangements, licensing rules, legislative provisions and limitations on gambling. This influences casinos' product offerings and configuration, both in terms of venue layout and the variety and nature of gambling services offered.

In recent years, the sector has been the subject of numerous commissions of inquiry, enforcement actions by AUSTRAC, regulatory actions by ASIC, and intense media scrutiny following identified AML/CTF deficiencies. As a result, many casinos are undergoing reforms.⁵⁷

Despite industry reforms and sustained regulatory and law enforcement efforts, casinos continue to be exploited for money laundering on a large scale by criminal entities. They range from sophisticated transnational serious and organised crime groups to opportunistic, low-level offenders. Key money

⁵⁶ Queensland Government Statisticians Office, Australian Gambling Statistics, 38th edition, 1995–96 to 2020–21, Queensland Government, <https://www.qgso.qld.gov.au/issues/2646/australian-gambling-statistics-38th-edn-1995-96-2020-21.pdf>.

⁵⁷ For example, a proposal to lower the customer due diligence (CDD threshold) from \$10,000 to \$5,000, mandatory carded play and pre-commitments on gaming machines at Crown Casino Melbourne.

laundering methodologies include structuring, the exchange of chips between parties and the buying and selling of tickets from electronic gaming machines (EGMs).

Across the sector, casinos are exposed to a wide range of money laundering vulnerabilities.

The key vulnerabilities include:

- high-risk customers, notably high-value customers, criminal entities, PEPs and anonymous customers in public gaming areas who do not hold casino accounts
- a capacity to accept large transactions, including in cash
- high-stakes wagering and high-volume gambling
- a diverse suite of products and services that facilitate rapid transfer of value between customers. This includes funds both within and outside of casino venues, enabling the proceeds of crime to be legitimised as casino winnings
- a high level of exposure to higher-risk foreign jurisdictions, including those with currency or gambling restrictions and where informal remittances such as offsetting or community funding are used.

CASE STUDY 37

Between 2016 and 2021, an Australian casino provided designated services to a customer who it understood to be the owner of a 'sushi shop'. During this period, the casino recorded significant turnaround of over \$19 million for this customer. The casino reported that the customer had engaged in large and unusual transactions in the casino, including transactions indicative of structuring, loan sharking, and using other customers to conduct threshold transactions on their behalf to avoid reporting requirements.

Outlook

The casino sector will continue to pose a high money laundering vulnerability over the next three years, despite sustained regulatory and law enforcement disruption efforts. As the impact of regulatory and supervision reforms become more apparent and individual casino AML/CTF systems and controls mature, criminal exploitation will almost certainly evolve in response. Ongoing monitoring and assessment of the sector's resilience to criminal exploitation will be important in understanding the trajectory of this risk.

BETTING AGENCIES AND CORPORATE BOOKMAKERS

Risk rating

Betting agencies and corporate bookmakers are assessed as posing a **medium** and **stable** money laundering vulnerability. The risk picture between betting agencies and corporate bookmakers differ slightly given that betting agencies are online, whereas corporate bookmakers predominantly provide face-to-face and often trackside services.

Key judgements

- The extent of criminal exploitation of betting agencies and corporate bookmakers by serious and organised criminals is likely lower than other gambling channels. However, these service providers are highly exposed to money laundering vulnerabilities. They are easy to access, process a high volume and value of transactions, and service high-risk customers.

- Money launderers and legitimate gamblers use similar methodologies and strategies which requires increased diligence and monitoring to identify suspicious activity.
- It is likely that proceeds of crime are being spent predominantly for lifestyle choices.



This category of risk includes totalisator organisations, betting exchanges and corporate bookmakers. The cohort is dominated by several entities. These corporate bookmakers have the largest customer bases and most sophisticated business operations. There is much less stability in this cohort, as entities are frequently merging and consolidating. This can create or exacerbate existing compliance vulnerabilities and risks.

In 2018, AUSTRAC published its national [ML/TF risk assessment of on-course bookmakers in Australia](#). An on-course bookmaker is an entity who carries on a business of a bookmaker at a racecourse, under a licence from a competent state-based licencing authority. The assessment is relevant for on-course bookmakers working at thoroughbred, greyhound and harness racing events in Australia. Please refer to the assessment for a comprehensive overview of the money laundering risks these entities face.

Domestic context

Gambling on Australian sport and racing events has experienced significant and sustained growth for at least the past decade, particularly through online channels. Recent estimates found the Australian interactive onshore wagering market generated \$6.5 billion in 2022 across racing and sports betting.⁵⁸

Domestic wagering platforms are very accessible and easy to use. Mobile applications and the internet now dominate how customers interact with domestic betting agencies and corporate bookmakers, meaning minimal face-to-face interaction.

The movement of funds into and out of bookmakers is also relatively easy. Typically, accounts are funded through bank transfers, cards issued by third parties and online payment platforms, which are highly visible. These funds flows are subject to monitoring by both bookmakers and banking institutions in order to manage gambling-related harm. However, various other payment platforms and methods used to place and move funds have significantly less visibility and likely create money laundering vulnerability. They include cash bets and electronic betting terminals and vouchers.

Detection of money laundering activity involving betting agencies and corporate bookmakers remains relatively low compared to other gambling channels. Criminals are more likely to spend their illicit proceeds on lifestyle activity with these entities. Nonetheless, strategies that could be used to launder funds include:

- the use of third-party betting accounts, also known as ‘bowler accounts’
- structuring bets across multiple domestic bookmakers
- structuring bets with a bookmaker/s by a syndicate, which may include bowler accounts
- placing structured cash wagers through electronic betting terminals and retail betting outlets
- transferring betting vouchers
- using cashed-out winnings to place further bets or purchase a betting voucher
- the use of arbitrage betting strategies to minimise losses.

⁵⁸ H2, Australia Offshore Wagering Market Analysis (<https://responsiblewagering.com.au/wp-content/uploads/2023/05/H2-Australia-Offshore-Wagering-Market-Analysis-2023-Report.pdf> 2023) H2, 2023, accessed 6 June 2023.



CASH BETTING AND ELECTRONIC BETTING TERMINALS (EBT)

Cash betting is exploited by professional gamblers and criminals alike and remains difficult to disrupt. It carries higher money laundering vulnerability compared to account-based betting offered by corporate bookmakers. Specific vulnerabilities include ease of use and challenges in monitoring and oversight of bets, particularly when EBTs are used to place and settle wagers. Common methodologies to launder funds include structuring cash bets through EBTs and payouts structured to remain under reporting thresholds.

CASE STUDY 38

A reporting entity triggered an alert in relation to the director of a business linked to over 100 bowler accounts that facilitated gambling transactions using multiple bookmakers. The director was also the ultimate beneficial owner of the business. The bowler accounts were opened under the name of third parties in order to conceal the true identity of the individual responsible for placing the bets.

The reporting entity submitted an SMR as the true source of funds was unclear, raising concerns that the syndicate could be laundering illicit funds through gambling platforms on behalf of others.

The bowlers were likely recruited using social media and instructed on how to disguise their identities from betting agencies. Funds were transferred into the bowlers' bank accounts with advice on what bets to place. Bowlers received a portion of the profits for the placing of the bets.

Outlook

Betting agencies and corporate bookmakers will continue to pose a medium money laundering vulnerability over the next three years. These entities are very dynamic, have a high risk appetite, and provide a service that has historically been exploited by criminals. Cash betting through EBTs will almost certainly remain a specific point of vulnerability and exploitation in the broader bookmaking sector.

PUBS AND CLUBS



Pubs and clubs are hospitality venues that offer gambling services. They are subject to different state or territory-based regulations related to EGM entitlements and customer payout amounts. As at May 2024, there are 4,013 pubs and clubs enrolled with AUSTRAC.

In 2022, AUSTRAC embarked on a nationwide education campaign to help pubs and clubs that operate EGMs understand their AML/CTF obligations. AUSTRAC reached over a thousand venues, answered questions specific to the operation of each business and shared practical tips on how to identify and report suspicious customer behaviour. Following the completion of the campaign, SMR submissions by businesses increased, helping us detect and disrupt criminal activity across the sector.

To support these efforts, AUSTRAC has updated and developed several new resources to help businesses in this sector improve their SMR submissions. Reporting entities are encouraged to view these [resources on the AUSTRAC website](#).

Risk rating

Pubs and clubs are assessed as posing a **medium** and **stable** money laundering vulnerability.

Key judgements

- Pubs and clubs are likely used by a small number of criminals to launder funds at scale, however significant proceeds of crime are being spent for lifestyle choices. Opportunistic offenders also likely use them to launder smaller amounts of criminal proceeds.
- Pubs and clubs are widely available, easy to access, and money laundering methods are well established and require very little expertise or knowledge. Their money laundering vulnerability primarily stems from a high volume and value of transactions (including cash transactions) and exposure to high-risk customers.
- AML/CTF capability and capacity across the sector could be improved. A number of entities remain highly vulnerable to money laundering. The ability to detect and report suspicious transactions to AUSTRAC remains low.

Domestic context

The scale of funds moving through the pubs and club sector is significant, with annual turnover exceeding \$124 billion for the 2019-20 financial year. Australian pubs and clubs offer a range of gambling services, including EGMs and cash redemption terminals. They present a money laundering vulnerability as illicit funds can be easily transferred between various gambling formats in the one venue. This can complicate tracking and tracing of fund movements.

Key gambling services they offer include:

- EGMs⁵⁹
- totalisator betting (betting services provided by entities are discussed in the previous section [Betting agencies or corporate bookmakers](#))
- Keno (rapid draw lottery game) and other lotteries⁶⁰
- social poker tournaments.⁶¹

⁵⁹ Australia is renowned internationally for the scale of gambling through EGMs and the high number of EGMs per capita. However, the density of EGMs and EGM play are concentrated in New South Wales, followed by Queensland and Victoria.

⁶⁰ Keno and other lottery type product are expressly excluded from Australia's AML/CTF regime as it is considered a very low money laundering risk. Such products are more a lifestyle pastime and destination for the use of illicit funds, rather than a known viable method of money laundering.

⁶¹ Money laundering risks relating to poker are assessed as limited.

EGMs have been identified as one of the higher-risk gambling services offered, due mainly to the scale of funds that can be moved. Many EGMs have limits on the volume that can be processed, ranging from \$100 to \$10,000.

Observed money laundering methodologies include:

- high-volume cheque payouts
- machine payouts with little or no play
- collecting the machine credit in the form of a ticket, cheque payout or funds transfer
- cheque-buying
- collecting payouts from EGMs played by third parties
- buying and selling winning tickets.

However, large-scale money laundering through EGMs, while occurring, is *not* widespread.



NEW SOUTH WALES CRIME COMMISSION PROJECT ISLINGTON

In 2022, the New South Wales Crime Commission released the final report of its inquiry into the use of EGMs at pubs and clubs for money laundering. Notably, the inquiry found that large scale dealing with the proceeds of crime through EGMs is occurring, but money laundering (which includes the intent to conceal) is not widespread. The inquiry noted that using EGMs to launder large amounts of criminal proceeds is probably too high risk and inefficient.

The inquiry also found that EGMs were being misused at a much higher extent by individuals spending their criminal proceeds, including by people who became involved in criminal activity to fund their gambling.

The true extent of money laundering through pubs and clubs is an intelligence gap. However, it is likely that they are used by a small number of criminals laundering large amounts of illicit funds. In addition, opportunistic offenders use pubs and clubs to launder smaller amounts of criminal proceeds.

CASE STUDY 39

The NSW Inquiry into Money Laundering via EGMs in Hotels and Clubs (Project Islington) identified an individual likely laundering proceeds of crimes via EGMs. On one occasion, they inserted over \$10,000 worth of \$20 notes into an EGM at a club. They then gambled a small portion of the funds, requested winning tickets and redeemed the tickets for larger denomination notes.

The individual had been recruited by a third party to transfer \$100,000 overseas to pay for an illegal shipment of e-cigarettes in the form of \$20 and \$50 notes. Financial reports indicated that the individual structured cash deposits into their bank account and then proceeded to gamble and refine the notes at the club. Both the structuring activity and the winning ticket redemption with little or no play suggest likely money laundering activity.

As the individual gave this evidence in a NSWCC coercive hearing, it could not be used against them to prosecute them for those offences.

Outlook

Pubs and clubs will continue to pose a medium money laundering vulnerability over the next three years. The sector is likely to be persistently exploited and remains a moderately attractive channel through which to launder funds. However, it is more likely to remain at higher risk of dealing in proceeds of crime given the predominance of EGMs in these venues.

ONLINE OFFSHORE GAMBLING

Risk rating

Online offshore gambling is assessed as posing a **medium** and **stable** money laundering vulnerability.

Key judgements

- Online offshore wagering platforms have opaque settlement channels and are not currently captured by Australia's AML/CTF regime.
- While criminal exploitation of online offshore gambling platforms by Australians is occurring, there is no evidence that it is widespread. Nonetheless, these platforms are exposed to money laundering vulnerabilities given the likely correlation between offline online platforms and existing online betting agencies that are regulated in Australia.
- Settlement through digital currency is becoming increasingly prevalent, further obscuring the channels used by online offshore gambling platforms.

Domestic context

Numerous money laundering vulnerabilities exist in the offshore online bookmaking ecosystem. These services are hosted by gambling platforms based in jurisdictions where the strength and effectiveness of licensing, regulation and AML/CTF controls vary widely. Many offshore online platforms have absent or illusory AML controls. They also contravene Australian legislation by offering gambling services to Australians in the absence of a domestic licence.

Online offshore wagering platforms are not currently covered by the AML/CTF Act when they do not have a geographical link to Australia. They can be broadly divided into two principal groups:

- online offshore bookmakers and betting platforms who offer wagering markets on sports and racing events from around the world
- online offshore casinos and poker platforms.

Recent estimates suggest that flows from Australian customers to offshore sports and racing wagering platforms alone is \$1.1 billion.⁶² Furthermore, Australians were estimated to have spent \$80 million across the mobile casino-style game sector in the second quarter of 2022, equating to \$240 million a year. Offshore sports and racing wagering is not covered by the AML/CTF Act, however offshore wagering and online casinos are captured under the *Interactive Gambling Act 2001*, regulated by the Australian Communications and Media Authority.

With online gambling illegal in many jurisdictions including in Australia, the platforms have the capability to move funds through an array of regulated and unregulated channels with varying levels of visibility from an AML perspective.

Key money laundering vulnerabilities include:

- opaque settlement channels, such as the use of off-setting
- the use of third parties to settle bets
- the mis-description of credit card transactions

⁶² H2, Australia Offshore Wagering Market Analysis (<https://responsiblewagering.com.au/wp-content/uploads/2023/05/H2-Australia-Offshore-Wagering-Market-Analysis-2023-Report.pdf>) H2, 2023, accessed 6 June 2023.

- the use of business accounts through which funds are transacted
- the use of affiliate or agent structures through which funds are settled, usually in bulk settlements on a regular basis.

Digital currency adds an additional layer of complexity. Its use to fund offshore wagering is estimated to have grown strongly in recent years. Between 2019 and 2023, the number of websites offering racing and sports wagering accepting digital currency increased by 85 per cent.

CASE STUDY 40

In addition to offshore online wagering platforms, other services that act as gateways to offshore online bookmakers through a single portal are also prominent. Brokers offer access to multiple offshore partner wagering sites, yet have absent or deceptive KYC requirements. These portals also place the bets, similar to commission agents, thereby obscuring the actual bettor. Additionally, the actual jurisdiction in which these portals are located cannot be established.

Through the use of payment processors including digital currency, brokers allow customers to effectively hide their origin from the bookmaker accepting the bet. One of the main appeals of the offshore market is the anonymity it provides, potentially for a number of illicit reasons including money laundering.

SMRs have identified related suspicious activity with concerns that offshore gambling sites are being used by money launderers as a mechanism to present illicit funds as legitimate gambling winnings.

Outlook

Online offshore wagering platforms will continue to pose a medium money laundering vulnerability over the next three years, particularly given their demonstrated resilience to disruption. This sector will remain vulnerable to money laundering, given the opacity of their settlement channels, their accessibility and their capacity to move funds between parties at scale. However, it will likely not be as attractive as other gambling channels to money launderers because of the required level of sophistication and specialist knowledge and skills required.



CONSEQUENCES

This assessment recognises that the consequences of money laundering are complex and difficult to measure. Reliable estimates of the amount of laundered funds impacting Australia are elusive, and socio-economic harms stemming from money laundering activity are extremely challenging to quantify. This makes assessing consequences associated with money laundering largely approximate.

For example:

- Money laundering is a function of a predicate crime. It can be difficult, if not impossible, to estimate the consequences of a predicate crime separate to its linked money laundering activity. In addition, the level of impact and harm arising from some predicate crimes are visible and generally significant (e.g. illicit drug trafficking), while those of other crimes, including money laundering, can be far less obvious, immediate or severe.
- The financial impact of money laundering and predicate crime is often diluted in prosperous economies.
- Incoming foreign criminal proceeds can have little negative financial impact on public revenues. However, they could give rise to other socio-economic harms or reputational loss for Australia.

To address these challenges, this assessment uses a mix of quantitative and qualitative inputs and, where possible, case studies and inductive methods are used.

This assessment does not provide an overall rating for the consequences of money laundering. Discussion in this section applies to the *national level only*. Consequences were not considered at the sector level or in relation to each individual money laundering channel or method assessed in this report.

Discussion covers two areas:

1. **Financial impact** provides best contemporary estimates of the cost of domestic and foreign money laundering and predicate crimes impacting Australia in the financial year 2020-21 (FY2020-21).
2. **Broader socio-economic harm** is more theoretical in nature and includes potential and actual harms arising from money laundering activity only. For reasons noted above, it does not include socio-economic harm linked to all predicate crimes.⁶³

FINANCIAL IMPACT: THE COST OF PREDICATE CRIMES

As mentioned on page 22, the Australian Institute of Criminology (AIC) released its Cost of Crime report in 2022. It provides the best contemporary estimates of the financial impact of both domestic and foreign predicate crime affecting Australia in the 2020-21 financial year. Estimates should be interpreted with caution. Please refer to the full report for a comprehensive explanation of data limitations and caveats. The figures included in this assessment represent the highest value of the range of estimates provided in the Cost of Crime report.

Estimates were made across three main categories and include the likely value of illicit criminal proceeds in the Australian economy, as well as the likely value of indirect costs resulting from criminal activity.

Direct serious and organised crimes were estimated to cost up to \$37.3 billion. These crimes have a clear and direct link with serious and organised criminals and include illicit drug activity, organised financial crime, some violent crimes committed against individuals, human trafficking and other crimes involving illicit goods, identity crime and pure cybercrime.

Various crime enablers are also directly linked to serious and organised crime. These include money laundering, violence, corruption, the misuse of identity and the use of professional service providers.

Consequential serious and organised crimes were estimated to cost up to \$6.4 billion. These are conventional crimes committed to support, facilitate or as a result of involvement in serious and organised criminal activities. Examples include crimes by illicit drug users to finance drug purchases, violence to intimidate businesses, or identity theft for financial fraud.

Indirect costs of preventing and responding to serious and organised crime were estimated to be up to \$16.4 billion. These include costs incurred by law enforcement, the criminal justice system, other government agencies, the private sector and individuals in the community in preventing and responding to crime.

⁶³ Social harm linked to criminal activity is well-documented and can manifest at personal, community and societal levels. It ranges from minor to severe.

SOCIO-ECONOMIC HARM FROM MONEY LAUNDERING

This assessment considered a range of socio-economic harms that may arise from money laundering activities impacting Australia.

In 2020, AUSTRAC commissioned the AIC to conduct research into the social and economic impacts arising from money laundering in Australia. Three factors were identified as the most relevant and significant in the Australian context. They are outlined below.

FINANCING AND FACILITATING CRIME

Money laundering enables criminals to fund other illicit activities like drug and weapons trafficking, and allows criminal organisations to grow and expand. Both outcomes increase the potential to endanger more Australians. Money laundering also facilitates other high-harm crimes such as human trafficking and smuggling, where laundered funds support solicitation, transportation and illicit transactions.

LOSS OF PUBLIC REVENUE

Money laundering reduces public revenue by enabling tax evasion. This loss affects governments' ability to fund essential services like healthcare, education and infrastructure development. This is further intensified when public revenue is diverted to implement policing and preventive measures to combat criminal offending. Vulnerable individuals and communities likely experience higher levels of harm when critical services cannot be provided.

REPUTATION OF THE FINANCIAL SECTOR

Financial institutions that have been linked to significant money laundering activity have likely suffered some reputational and economic damage. This is especially when regulatory action has been taken or an institution incurs costs necessary to repair brand image or increase capability to mitigate threats. In some instances, reputational damage can arbitrarily (and perhaps unfairly) extend to other reporting entities in financial sectors that have come under regulatory scrutiny.

APPENDIX A: SCOPE AND METHODOLOGY

SCOPE

This assessment considers all money laundering risks. This includes predicate crimes that generate criminal proceeds ('proceeds-generating crimes'), as well as methods, channels and mechanisms used in money laundering activities impacting Australia. This assessment does not include lawful activities that help individuals and businesses minimise their tax obligations.

The assessment examines money laundering across two contexts:

1. **Domestic proceeds of crime** that are generated in Australia. These funds may stay in Australia ('domestic' funds flows), be moved offshore ('outgoing' funds flows), or be moved offshore then sent back to Australia ('returning' funds flows).
2. **Foreign proceeds of crime** that are generated outside of Australia. These funds are moved into Australia ('incoming' funds flows), or are moved into Australia then sent back offshore ('through' funds flows).

Please see [Appendix C](#) for a glossary of terms used in this assessment.

METHODOLOGY

This assessment employs the standard risk assessment framework developed by the FATF as a general guide. It assesses money laundering risks as a function of threats and *inherent* vulnerabilities. Consequences of money laundering are also considered, but ratings are not provided. There is insufficient contextual data needed to accurately estimate the level of consequence for each risk factor.

RISK MODEL

	RISK FACTORS
THREAT An assessment of the likely amount of criminal proceeds generated, and the nature and extent of associated money laundering activities.	Threat ratings are based on an assessment of three factors: <ul style="list-style-type: none"> • The estimated amount of funds generated by the crime type, and the need for those funds to be laundered. • The type and diversity of money laundering methods used to move funds generated by the crime type. • The nature of actors and participants operating within the illicit market, including the level of involvement of serious and organised criminals and their resilience to law enforcement disruption.
VULNERABILITY An assessment of regulated and unregulated methods, channels and mechanisms used to launder illicit funds. It also includes national vulnerabilities such as Australia's AML/CTF framework.	Vulnerability ratings are based on an assessment of seven factors across three dimensions: <ul style="list-style-type: none"> • Prevalence <ul style="list-style-type: none"> – <i>Extent of criminality</i>: the scale of money laundering occurring through the channel, and whether it is increasing. – <i>Nature of criminality</i>: the extent to which serious and organised criminals use the channel. • Vulnerability <ul style="list-style-type: none"> – <i>Profitability</i>: the scale and capacity of the channel to move large volumes of licit/illicit funds. – <i>Accessibility</i>: the cost of a channel or other barriers to access, for example, getting funds to a higher-risk region.




	<ul style="list-style-type: none"> - <i>Ease of use</i>: the level of expertise or technical skills required to use a particular channel. • Mitigation <ul style="list-style-type: none"> - <i>Detection</i>: the level of anonymity provided by the channel, including reporting entities' ability to detect and report misuse to authorities. - <i>Disruption</i>: the ability of AUSTRAC and law enforcement authorities to triage, investigate and prosecute instances of money laundering through the channel.
<p>CONSEQUENCE</p> <p>The level of financial impact or socio-economic harm caused by money laundering events.</p>	<p>Consequence is considered across two factors:</p> <ul style="list-style-type: none"> • <i>Financial impact</i> provides best contemporary estimates of the cost of domestic and foreign money laundering and predicate crimes impacting Australia in the financial year 2020-21. • <i>Broader socio-economic harm</i> includes potential and actual harms arising from money laundering activity.
<p>OUTLOOK</p> <p>An assessment of the risk for the next three years.</p>	<p>A risk may be assessed as likely to 'increase' or 'decrease', usually based on known and evident drivers.</p> <p>A risk may be assessed as 'emerging' if it is relatively new and likely to be used for money laundering. Generally, further intelligence collection and monitoring is required.</p> <p>Risks that are likely to remain unchanged are considered 'stable'.</p> <p>This approach will help AUSTRAC monitor and track changes in the risk environment.</p>

ASSESSING AND RATING THREAT

A threat matrix was developed to assess and rate the nature and extent of proceeds-generating crimes.

Appendix D provides details of the threat matrix and an explanation of how scores were achieved. Final threat assessments were weighted as follows: 'low', 'medium', and 'high'. Conditional threat statements are provided in Table 4.






TABLE 4: CONDITIONAL THREAT STATEMENTS

CONDITIONAL THREAT STATEMENT		
	High	A high volume of illicit funds are generated that require laundering. Money laundering methodologies are highly varied and/or there is a high level of involvement by serious and organised crime groups and other criminal entities.
	Medium	A moderate volume of illicit funds are generated that require laundering. Money laundering methodologies are somewhat varied and/or there is some level of involvement by serious and organised crime groups and other criminal entities.
	Low	A low volume of illicit funds are generated that require laundering. Minimal variety of money laundering methodologies are used, and there is little to no involvement by serious and organised crime groups and other criminal entities.

ASSESSING AND RATING INHERENT VULNERABILITY

A matrix was developed to assess and rate the level of *inherent* vulnerability of 79 individual channels, methods and mechanisms to exploitation for money laundering. **Appendix D** provides details of the vulnerability matrix and an explanation of how scores were achieved. Final vulnerability assessments were weighted as follows: 'very low', 'low', 'medium', 'high', and 'very high'. Conditional vulnerability statements are provided in Table 5.

TABLE 5: CONDITIONAL VULNERABILITY STATEMENTS

CONDITIONAL VULNERABILITY STATEMENT		
	Very high	Risk requires immediate and sustained attention. The channel/method is used in the majority cases of money laundering and there are many barriers to detecting and disrupting criminal actors.
	High	Risk requires ongoing attention and assessment. The channel/method is used in many cases of money laundering and there are barriers to detecting and disrupting criminal actors.
	Medium	Risk requires ongoing monitoring and further assessment. The channel/method is frequently used for money laundering and there are barriers to detecting and disrupting criminal actors.
	Low	Risk is acceptable but may require monitoring. There is limited evidence the channel/method is used for money laundering but inherent vulnerabilities could be exploited by criminal actors.
	Very low	Risk is acceptable and does not require monitoring. There is very limited or no evidence the channel/method is used for money laundering.

INFORMATION SOURCES

This assessment draws on a range of intelligence and data sources including:

- A formal request for information and/or survey to contributing agencies.
- Survey responses provided by 111 reporting entities and industry representatives. **Appendix E** provides an overview of the industry survey findings.
- Survey responses provided by 35 international FIU partners. **Appendix F** provides an overview of these findings.
- A review of significant money laundering investigations and prosecutions.
- Financial transaction reporting to AUSTRAC.
- Financial and criminal intelligence holdings.
- International reporting on money laundering trends.
- Feedback and professional insights from interviews and consultation with key stakeholders.

VALIDATION OF RESULTS

To ensure accuracy of the risk ratings and key findings, AUSTRAC developed this assessment in close consultation with the key contributors noted in **Appendix B**. This included engagement across three main stages of the project:

1. Collection: stakeholders completed a money laundering risk perception survey, questionnaire and/or a formal request for information.
2. Analysis: AUSTRAC collated all collection responses and developed draft risk ratings. AUSTRAC then coordinated and hosted multiple workshops with contributors to validate and finalise findings and risk ratings.
3. Review: a consultative draft of the final assessment was provided to government partner agencies for review, feedback and (where appropriate) final endorsement.

APPENDIX B: AUSTRALIAN GOVERNMENT AGENCIES CONSULTED

- Attorney-General's Department (AGD)
- Australian Border Force (ABF)
- Australian Competition and Consumer Commission (ACCC)
- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Institute of Criminology (AIC)
- Australian Prudential Regulation Authority (APRA)
- Australian Securities and Investments Commission (ASIC)
- Australian Security Intelligence Organisation (ASIO)
- Australian Taxation Office (ATO)
- Department of Foreign Affairs and Trade (DFAT)
- Department of Home Affairs (DHA)
- Department of Treasury (Treasury)
- National Anti-Corruption Committee (formerly ACLEI) (NACC)
- National Disability Insurance Agency (NDIA)
- New South Wales Crime Commission (NSWCC)
- Office of National Intelligence (ONI)
- Reserve Bank of Australia (RBA)
- Services Australia (SA)
- State & Territory Police agencies
- State & Territory Anti-Corruption Commissions
- State & Territory gambling regulators
- State & Territory Departments of Public Prosecutions
- Tax Practitioners Board

APPENDIX C: GLOSSARY OF TERMS

TERM	DEFINITION
Accountants	In Australian intelligence reporting, 'accountant' is used broadly and as an umbrella term, in part reflecting the breadth of the profession and its specialisations, particularly across tax, advisory and consulting functions. This assessment includes tax accountants (also referred to as 'tax agents/advisors') in the scope of accounting professionals.
Affiliates	Affiliates are independently-owned businesses that have an agreement with a remittance network provider (RNP) to use the network's brand, products, platforms or systems to provide remittance services.
Authorised deposit-taking institution (ADI)	An authorised deposit-taking institution (ADI) is a body corporate authorised under the Banking Act 1959 to carry on banking business in Australia (e.g. a bank, building society or credit union), the Reserve Bank of Australia or a person who carries on state banking.
Australian unlisted incorporated entities	Proprietary-limited companies are unlisted, privately-held entities which have an increased exposure to being used for money laundering because they have less regulatory oversight, fewer reporting and public disclosure obligations, and reduced public scrutiny in comparison to publicly-listed companies, cooperatives and not-for-profit organisations. This creates an environment where money laundering can occur more easily without attracting attention from the public and makes it harder for authorities to detect illicit activity.
AML/CTF	Anti-money laundering and counter-terrorism financing.
AML/CTF program	A document that sets out how a reporting entity meets its AML/CTF compliance obligations.
Barriers to entry	The economic hurdles new entrants face while entering the market. The types of barriers to entry are capital costs, competition, legal barriers, marketing barriers, limited market, predatory pricing, finding suppliers, master of technology, learning curve and economies of scale.
Beneficial owner	An individual who owns 25 per cent or more, or otherwise controls the business of an entity.
Bowler account	A betting account that allow gamblers to anonymise their betting activity, overlaying the risks associated with betting accounts with the risks associated with gambling agents.
Bulk cash smuggling	Bulk cash smuggling is the process of moving the instruments or proceeds of crime as physical cash between international jurisdictions. The purpose is usually to pay for illicit products or to move the cash via jurisdictions with weak AML systems into the international financial system. Methods of bulk cash smuggling typically involve concealing cash in cargo shipments containers.
Bullion and precious metals	Gold, silver, platinum or palladium authenticated to a specified fineness in the form of bars, ingots, plates, wafers or similar forms including coins. Precious metals, such as granules of fine gold typically used for the manufacture of jewellery or gold dust, are not regulated under the AML/CTF Act. Businesses buying and selling precious metals that are not classified as bullion are not subject to AML/CTF regulation.
Cleanskin	Complicit third parties who do not have criminal records.
Cold wallet	Cold wallets are physical devices, like USBs or hard drives that hold digital currencies. They are not connected to the internet, and are therefore less prone to hacker attacks or technical malfunctions. The opposite of cold wallets, are 'hot' wallets, which are digital wallets that needs an internet connection to function and store digital currencies.
Corporate bookmakers	Businesses that offer fixed odds betting via digital or telephone platforms on sports, racing or novelty events.
Crypto mixer	A service that blends the digital currencies of many users together to obfuscate the origins and owners of the funds.
Cuckoo smurfing	A money laundering process where criminal proceeds are used to make a cash deposit to an innocent person in Australia who is expecting to receive a money transfer from overseas. This deposit is made on behalf of a complicit remittance provider. The remittance provider

	<p>makes the equivalent payment to the criminal overseas. Using this method, funds do not physically move internationally and there is no money trail.</p>
Customer due diligence (CDD)	<p>Customer due diligence (CDD) is the process where pertinent information of a customer's profile is collected and evaluated for potential ML/TF risks.</p>
Cash couriers	<p>Cash couriers are people who physically transport cash on their person, internally or as part of their luggage between international jurisdictions. Couriers may be directly connected to the predicate offences and cash proceeds, or may be third parties (mules) recruited specifically to move the money offshore.</p>
Casino junkets tour operations (or casino-based gaming tours)	<p>Derived from casino marketing programs, a junket is an organised gaming tour for people who travel to the casino primarily to gamble. It may include transport, accommodation, incentives to gamble and the movement of funds to and from the casino.</p> <p>Casino-based junkets may be part of the casino's in-house marketing program or run by independent operators who have a contract with the casino.</p>
Daigou	<p>Daigou literally translated means 'buying on behalf of' and refers to persons who buy items in one jurisdiction for residents of a second jurisdiction in which the items are difficult or costly to obtain.</p>
Decentralised autonomous organization	<p>A decentralised autonomous organization (DAO) has no central governing body and members share a common goal to act in the best interest of the entity. Popularised through digital currency enthusiasts and blockchain technology, DAOs are used to make decisions in a bottom-up management approach.</p>
De facto director	<p>A person who operates in the capacity of a director albeit not named on ASIC's corporate records. They may have names like business development director, chairman, principal, etc.</p>
Designated remittance arrangement	<p>Refers to non-financiers that accept instructions from a transferor to transfer money or property and then arranges for it to be made available to an ultimate transferee – s10 AML/CTF Act.</p>
Digital currencies	<p>A type of currency that only exists in digital rather than physical form (not coins or notes, for example). Digital currency can be exchanged for goods, services or physical currency and is not issued by or under the authority of a government.</p>
Enhanced customer due diligence (ECDD)	<p>Enhanced customer due diligence (ECDD) is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.</p>
Enablers	<p>Refers to aspects that allow criminals to abuse a feature to achieve their own ends.</p>
Facilitators and gatekeepers	<p>Includes financial service professionals, insiders and politically exposed persons (PEPs).</p>
Fiat currency	<p>Fiat currency is legal tender currency, authorised and backed by the issuing government. It is a type of currency that is not backed by a physical commodity. The Australian dollar is an example of fiat currency.</p>
Financial Action Task Force (FATF)	<p>The Financial Action Task Force (FATF) is an intergovernmental body focused on fighting money laundering, terrorism financing and other related threats to the integrity of the international financial system by ensuring the effective implementation of legal, regulatory and operational measures.</p>
Financial institutions	<p>FATF defines a financial institution as any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:</p> <ul style="list-style-type: none"> • acceptance of deposits and other repayable funds from the public • lending • financial leasing • money or value transfer services • issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money) • financial guarantees and commitments • participation in securities issues and the provision of financial services related to such issues • individual and collective portfolio management safekeeping and administration of cash or liquid securities on behalf of other persons

	<ul style="list-style-type: none"> • otherwise investing, administering or managing funds or money on behalf of other persons • underwriting and placement of life insurance and other investment-related insurance • money and currency changing • trading in money market instruments, foreign exchange, exchange, interest rate and index instruments, transferable securities, commodity futures trading.
Foreign-owned subsidiaries (foreign subsidiary banks)	Authorised deposit-taking institutions (ADIs) licensed by the Australian Prudential Regulation Authority (APRA). Foreign subsidiary banks conduct business through a locally-incorporated subsidiary that is a separate legal entity from its foreign bank parent.
Foreign incorporated branch (foreign bank branch)	Foreign authorised deposit-taking institutions (ADIs) licensed by the Australian Prudential Regulation Authority (APRA). Foreign bank branches are <i>not</i> separate entities incorporated and independently capitalised in Australia, but a part of a foreign bank incorporated overseas.
Front company	A company that is a fully functional, physically present business that helps to hide and mask illegal financial activity. Its primary goals are to conceal illicit activities that could be compromised if the actual beneficiaries or stakeholders were made public, and to protect the parent company from negative publicity in the event of a problem.
High-value assets and goods	Luxury goods such as precious stones, jewellery, fashion designer goods, watches, luxury vehicles and watercraft, domestic real estate, artworks and other collectables. Also includes assets and asset classes that are used for investment purposes, including shares in publicly-listed companies and other investment products.
Identity crime	Identity crime, also known as identify theft, fraud or misuse, is a common cyber threat worldwide. Identity crime exploits vulnerabilities in personal identification credentials, consumer payment systems and technological advances in computing and communications, generally for financial gain.
Illicit tobacco	Loose-leaf tobacco ('chop-chop') and pre-rolled cigarettes, which include counterfeit tobacco manufactured illegally, contraband tobacco illegally smuggled into Australia and 'illicit whites' smuggled into Australia illegally and sold without payment of tax. All locally-grown tobacco in Australia is now illicit, as no licences to grow tobacco have been issued since 2015.
Independent remittance dealer (IRD)	Remittance service providers that use their own products, platforms or systems to provide services directly to customers. IRDs can be registered as a single entity operating independently, or own and operate multiple branches.
Instrument(s) of crime	Money or other property is an instrument of crime if it is used in the commission of, or used to facilitate the commission of, an offence against a law of the Commonwealth, a state, a territory or a foreign country that may be dealt with as an indictable offence (even if it may, in some circumstances, be dealt with as a summary offence).
Integration	The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.
International funds transfer instruction (IFTI)	An international funds transfer instruction (IFTI) involves either: <ul style="list-style-type: none"> • an instruction that is accepted in Australia for money or property to be made available in another country, or • an instruction that is accepted in another country for money or property to be made available in Australia.
Legal entity structures	Include corporations and trusts that may be set up in simple or highly-complex structures.
Layering	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin
Luxury goods	Precious stones, jewellery, fashion designer goods, watches, luxury vehicles and watercraft, domestic real estate, artworks and other collectible, and assets and asset classes that are used for investment purposes including shares in publically listed companies and other investment products.
Middle East	Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestinian territories, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen

Mixers and tumblers	Services that collect, pool and pseudo-randomly shuffle cryptocurrencies of many users to obfuscate the origins and ownership of funds. The use of mixers makes it difficult for law enforcement and regulators to untangle transactions and identify ownership and funds flows
Mule	A law enforcement term for third parties used to move illicit goods or value. These activities are usually high-risk illegal activities that have the potential to be detected by law enforcement or regulatory bodies. 'Money mules' are third parties that are employed to transfer illicit value between jurisdictions. They do this by either transporting physical cash or goods on their person or in their luggage; or undertaking transactions through a bank or remittance service or electronically.
Mutual banks	Approved deposit-taking institutions (ADIs) that are owned by their customers, such as building societies and credit unions.
Offshore bank	Refers to a bank located outside the country of residence of the depositor (typically in a low-tax jurisdiction), providing financial and legal advantages. Such advantages typically include greater privacy, low or no taxation, limited or no regulation of account activities and protection against local political or financial instability.
Offsetting	An alternative remittance practice that enables the international transfer of value without actually transferring money. This is possible because the arrangement involves a financial credit and debit (offsetting) relationship between two or more dealers operating in different countries. Hawala and hundi are common alternative remittance practices.
On and off ramps	On ramps relate to services converting fiat currency into digital currency. Off ramps relate to services converting digital currency into fiat currency.
Organised crime group (OCG)	A criminal network engaged in serious and organised crime, as defined by the <i>Australian Crime Commission Act 2002</i> .
Other domestic banks	Australian-owned authorised deposit-taking institutions (ADIs) that are not major banks, community owned or mutual banks.
Payment fraud (card fraud)	The fraudulent acquisition and/or use of debit and credit cards, or card details, for financial gain. Card fraud may involve acquiring legitimate cards from financial institutions by using false supporting documentation or stealing legitimate cards before the designated customers receive them. This may also involve phishing, card-not-present fraud, the creation of counterfeit cards, hacking to steal customer financial data and card skimming.
Peer-to- peer trading (P2P)	Direct transfer of assets between two parties without the need for a third party to facilitate the transactions. Over-the-counter transactions allows people to bulk trade cryptocurrencies directly, with assistance and negotiation of the exchange.
Phishing	Phishing involves scammers contacting victims and pretending to be from a legitimate business in an attempt to obtain personal information. The information is then used to fraudulently gain access to a banking product, commonly a transaction account or credit card.
Phoenixing	Phoenixing occurs when a new company is created to continue the business of a company that has been deliberately liquidated to avoid paying its debts, including taxes, creditors and employee entitlements.
Placement	The first stage of the money laundering cycle in which illicit funds enter the formal financial system.
Precious metal certificates	Verify the ownership of a certain amount of precious metal, usually gold, silver or platinum. The authority that issues the certificate typically offers a storage service for the physical metal that the certificate represents. Criminals can use third parties to purchase the certificates and launder the proceeds of crime. This allows criminals to distance themselves from the asset and hide the true source of funds used to buy the certificate.

Proceeds of crime	Any money or other property that is wholly- or partly-derived or realised, directly or indirectly, by any person from the commission of an offence against a law of the Commonwealth, a state, a territory or a foreign country that may be dealt with as an indictable offence (even if it may, in some circumstances, be dealt with as a summary offence).
Professional service provider	A ‘professional service provider’ is a business professional who provides specialist services that may facilitate money laundering, either complicity or non-complicity. In the context of money laundering, this generally includes lawyers, accountants and trust and company service providers, as well as real estate agents and other high-value goods dealers.
Professionals	Persons able to provide financial expertise – may include lawyers, accountants, tax advisers and trust and company service providers.
Pure cybercrime	Crime directed at computers or other information communication technologies and networks, such as hacking, spreading computer viruses and other malware, ransomware, business email compromise and distributed denial-of-service.
Pubs and clubs	Hospitality venues that offer gambling services. Pubs and clubs are subject to different state- or territory-based regulatory requirements related to electronic gaming machine (EGM) entitlements, the total funds machines can accept and store while being played, and customer payout amounts. The profile of these entity types also differs, with clubs operating on a membership basis and having associated identification requirements, and pubs being accessible to the general public and having fewer customer identification requirements.
Remittance network provider (RNP)	Businesses that allow affiliates to use their brand, products, platforms or systems to provide remittance services. Affiliates are independently-owned businesses that have an agreement with an RNP to use the network’s brand, products, platforms or systems to provide remittance services. The RNP is responsible for an affiliate’s registration and reporting obligations to AUSTRAC, and must ensure they have an appropriate AML/CTF program.
Reporting entity (regulated entity)	An entity that provides any designated services listed under section 6 of the AML/CTF Act. These entities generally provide financial, gambling, bullion or digital currency exchange services. All reporting entities must meet obligations under the Act.
Retail payment service (systems)	Payment systems that facilitate transactions between two consumers, between consumers and businesses, or between two businesses. Retail payment systems allow for funds to be transferred electronically from person to person, to pay for goods or to get cash.
Retail banking	Retail banking provides financial services to individual customers, as opposed to large institutions. Services offered generally include savings and checking accounts, mortgages, personal loans, debit and credit cards and certificates of deposit.
Secrecy jurisdictions	While AUSTRAC does not have a definition of secrecy jurisdictions in the AML/CTF Act, for the purposes of this NRA, secrecy jurisdictions are jurisdictions that enable people or entities to escape or undermine the laws, rules and regulations of other jurisdictions.
Serious and organised crime (SOC)	An offence that involves two or more offenders, substantial planning and organisation, is of a kind that ordinarily involves the use of sophisticated methods and techniques and is usually committed in conjunction with other offences of a like kind; and is a serious offence within the meaning of the Proceeds of Crime Act 2002 or of the Criminal Code and that is punishable by imprisonment for a period of three years or more.
Sha Zhu Pan	Sha Zhu Pan, or romance baiting, is a scam in which offenders often devote long period of time to gain the trust of victims before encouraging them to invest in the share market, digital currency or foreign currency exchanges.
Shadow director	A shadow director is a person who operates through a ‘straw’ or ‘dummy’ director, effectively the puppeteer to the puppet. Placing a puppeteer at the top of a multi-level entity, on or offshore, creates a puppet master to domestic puppets who may be onshore puppeteers.

Shell company	<p>A company that, at the time of incorporation, has no significant assets or operations. Shell companies can be set up domestically or offshore and ownership structures can take several forms.</p> <p>Shell companies have no physical presence, employees or products and may be owned by corporations, nominee owners and bearer shares, obscuring beneficial ownership.</p>
Shelf company	<p>A company that is already registered but has never traded or conducted business and holds no assets or liabilities. The primary purpose is to achieve perceived longevity and credibility with potential clients, investors and lenders.</p> <p>Shelf companies are used to bypass the time-consuming process of creating a new corporation and to give an appearance of corporate longevity.</p>
Southeast Asia	<p>Brunei, Burma (Myanmar), Cambodia, East Timor, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand and Vietnam.</p>
Staging account	<p>Superannuation accounts established by members for the purpose of consolidating funds prior to being further transferred or withdrawn from the superannuation system.</p>
Suspicious matter report (SMR)	<p>A reporting entity must submit an SMR under the AML/CTF Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law. An SMR must also be submitted if the reporting entity has reasonable grounds to suspect the customer or an agent of the customer is not who they say they are.</p>
Tax crime	<p>The abuse of the tax and superannuation system for financial benefit. This includes hiding cash wages, avoiding tax (including GST), using complex offshore secrecy arrangements to avoid tax, and falsely claiming refunds and benefits.</p>
Tax havens	<p>While AUSTRAC does not have a definition of tax havens in the AML/CTF Act, for the purpose of this NRA, tax havens are countries, regions or states that have minimal tax for non-residents and do not share financial or banking information with foreign tax authorities.</p>
Third party (business structure)	<p>A relationship where a business is transferred to a third party who has legal control and a duty to run that business to benefit someone else. A trust is an example of a third party business structure.</p>
Threshold transaction report (TTR)	<p>A report submitted to AUSTRAC about a designated service provided to a customer by a reporting entity that involves a transfer of physical or digital currency of \$10,000 or more, or the foreign currency equivalent.</p>
Trade-based money laundering (TBML)	<p>Broadly defined as ‘disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins’. In practice, TBML is a specific type of money laundering frequently used in combination with other money laundering activities, such as value transfer and misrepresentation of goods.</p>
Transnational, serious and organised crime (TSOC)	<p>Transnational, serious and organised crime covers a wide range of the most serious crime threats impacting Australia including:</p> <ul style="list-style-type: none"> • manufacture and trade of illicit commodities, including drugs and firearms • sexual exploitation of children • human trafficking and slavery • serious financial crime • cybercrime. <p>Key enablers of TSOC include money laundering, identity crime and public sector corruption.</p>
Trusted insiders	<p>Individuals who misuse their legitimate access to an organisation's services, products, information or facilities for unauthorised and/or illegal purposes.</p>
White labelling	<p>White labelling is an agreement between two parties where one party provides services or products to another party under the other party's brand name.</p>

APPENDIX D: THREAT AND VULNERABILITY MATRICES

THREAT MATRIX

THREAT FACTORS			
	LOW	MEDIUM	HIGH
EXTENT (e.g. the estimated volume of criminal proceeds generated by the crime type that require laundering)	LOW Crime/illicit market generates a small amount of domestic proceeds that require laundering, particularly in comparison to other crimes/illicit markets.	MEDIUM Crime/illicit market generates a moderate amount of domestic proceeds that require laundering, particularly in comparison to other crimes/illicit markets.	HIGH Crime/illicit market generates a large amount of domestic proceeds that require laundering, particularly in comparison to other crimes/illicit markets.
NATURE (e.g. the diversity and sophistication of methods used to launder funds generated by the crime type)	LOW Minimal variety of money laundering (ML) methods used and/or methods used do not require specialist skills, access or expertise to execute.	MEDIUM Several ML methods are used which require some specialist skills, access or expertise to execute.	HIGH A wide range of ML methods are used and generally require specialist skills, access or expertise to execute.
ACTORS (e.g. the level of serious and organised crime (SOCG) involvement in the illicit market and/or linked money laundering activity)	LOW Little to no involvement of SOCGs and/or other higher-risk entities in the crime/illicit market and linked ML.	MEDIUM SOCGs and/or other higher-risk entities control some aspects of the crime/illicit market and linked ML.	HIGH SOCGs and/or other higher-risk entities control a large portion of the crime/illicit market and linked ML.

VULNERABILITY MATRIX

VULNERABILITY FACTORS			
	LOW	MEDIUM	HIGH
LEVEL OF CRIMINALITY (e.g. the scale of ML occurring through the channel and whether it is increasing)	LOW The scale of money laundering occurring through the channel, method or mechanism is low, particularly compared to other channels, and is not likely to increase in the near future.	MODERATE The scale of money laundering occurring through the channel, method or mechanism is moderate, particularly compared to other channels, and might increase in the near future.	HIGH The scale of money laundering occurring through the channel, method or mechanism is high, particularly compared to other channels, and is not likely to decrease in the near future.
LEVEL OF INVOLVEMENT (e.g. the extent that SOCGs exploit the sector/mechanism as a preferential means to launder funds)	LOW SOCGs rarely use the sector/mechanism as a preferential means to launder funds.	MODERATE SOCGs sometimes use the sector/mechanism as a preferential means to launder funds.	HIGH SOCGs often use the sector/mechanism as a preferential means to launder funds.
PROFITABILITY (e.g. opportunity to raise/move/store large volumes of funds)	LOW The channel/method likely limits only small amounts to be raised/moved/stored.	MODERATE The channel/method likely enables modest amounts to be raised/moved/stored.	HIGH The channel/method likely enables larger amounts to be raised/moved/stored.
ACCESSIBILITY (e.g. relative cost and barriers to access, including to/from foreign jurisdictions)	DIFFICULT Many barriers to access and/or costs more than other financing options.	MODERATE Some barriers to access and/or may cost more than other financing options.	EASY Few or no barriers to access and/or costs less than other financing options.
EASE OF USE (e.g. knowledge and/or technical expertise and support required)	DIFFICULT Requires more planning, knowledge and/or technical expertise than other options.	MODERATE Requires some planning, knowledge and/or technical expertise.	EASY Requires little planning, knowledge and/or technical expertise compared to other options.
DETECTION (e.g. ability for terrorism financing to be identified and reported to authorities)	LIKELY Illicit transactions are relatively easy to detect and are routinely reported or visible to authorities.	LIMITED Illicit transactions are sometimes detected and reported or visible to authorities.	DIFFICULT Illicit transactions are difficult to detect and/or are rarely reported or visible to authorities.
DISRUPTION (e.g. ability for authorities to investigate and prosecute or disrupt terrorism financing offences)	LIKELY Authorities face few challenges in successfully investigating and prosecuting or disrupting offences.	LIMITED Authorities face some challenges in successfully investigating and prosecuting or disrupting offences.	DIFFICULT Authorities face a number of challenges in successfully investigating and prosecuting or disrupting offences.

APPENDIX E: INDUSTRY SURVEY

The industry survey was issued to Fintel Alliance industry partners, representatives and industry association members to gauge views of the current domestic money laundering environment and measures currently in place to mitigate the risks.

111 entities responded, representing 95 per cent of regulated sectors. To maintain anonymity, respondents were aggregated into their industry sector's money laundering vulnerability strata (referred to as "money laundering vulnerability group/s") as assessed through this report.

AWARENESS AND CONCERNS

Across all "awareness" factors⁶⁴ each money laundering vulnerability group has a proportion of entities that do not fully understand their risk factors or threats. Across all money laundering vulnerability groups, respondents acknowledge their money laundering risks are equal to or less than other commercial risks they may encounter in their sphere of operations.

Respondents all appear not to be too concerned about their ability to address money laundering in their organisation should it arise.

GUIDANCE AND COLLABORATION

In terms of current levels of guidance, all money laundering vulnerability groups are generally positive. Those with negative responses called for better guidance on indicators, as well as a consistent approach to Know Your Customer/Customer Due Diligence across all sectors.

A somewhat similar picture is painted for information sharing with government agencies. The positive perception was approximately 60 per cent, while respondents generally highlighted a lack of feedback – typically a one-way communication flow from reporting entity to AUSTRAC.

EXTERNAL CHALLENGES

Industry participants identified information sharing as a principal external challenge to countering money laundering, followed by a lack of financial intelligence and investigative capabilities, and weak beneficial ownership and legal person transparency.

⁶⁴ Awareness factors asked respondents if they are aware of money laundering risk indicators and red flags generally, relevant to their sector and relevant to Australia and the region in which they operate and transact.

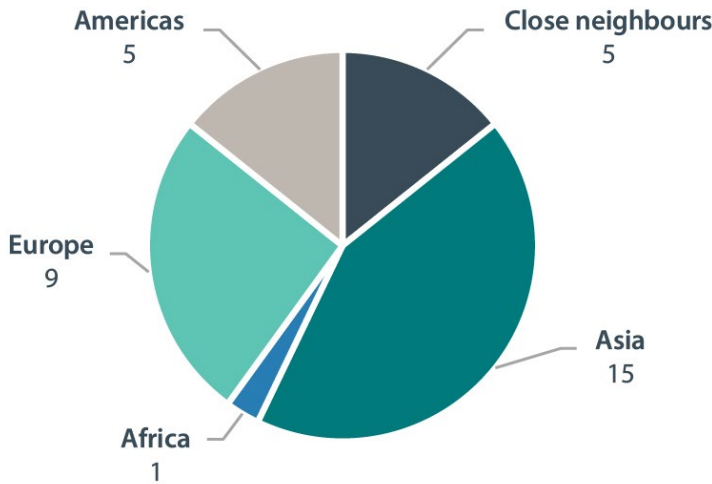
APPENDIX F: INTERNATIONAL FIU SURVEY

67 international partner FIUs were invited to participate in a perceptions survey to gain insights into Australia’s status as a source and destination of criminal proceeds. Figure 3 below shows the locations of the FIUs who contributed to the assessment. Close neighbours include countries within Oceania, Micronesia and Melanesia.

Figure 3 - Number of FIUs who responded to international FIU ML NRA 2023 survey by principal region

Countries responding to survey by regional grouping

35 countries



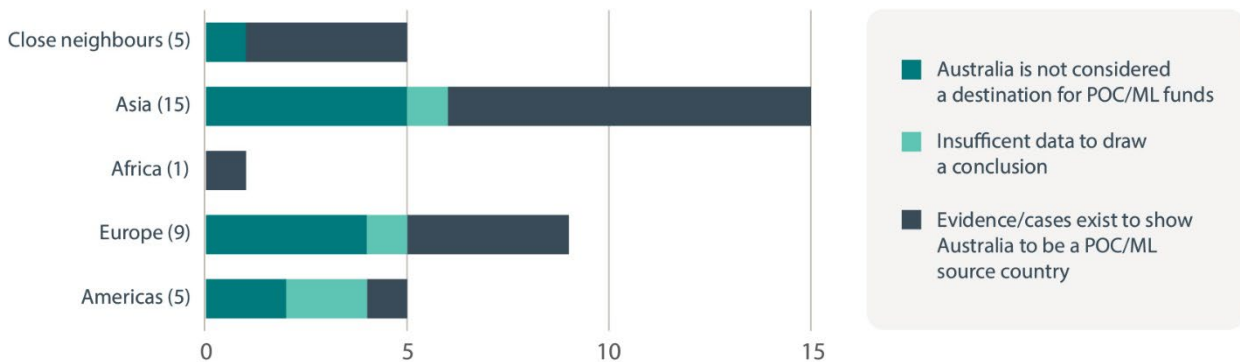
AUSTRALIA AS A DESTINATION OF ILLICIT PROCEEDS

50 per cent of respondents have sufficient evidence or cases to confirm Australia is a destination country for laundered funds. While Australia has been identified as a destination of illicit funds, the scale of funds is not quantifiable.

Figure 4 - Number of countries by region and how they perceive Australia as an attractive destination for illicit proceeds

How Australia is perceived as a destination country for POC/ML proceeds

(n)= participating countries



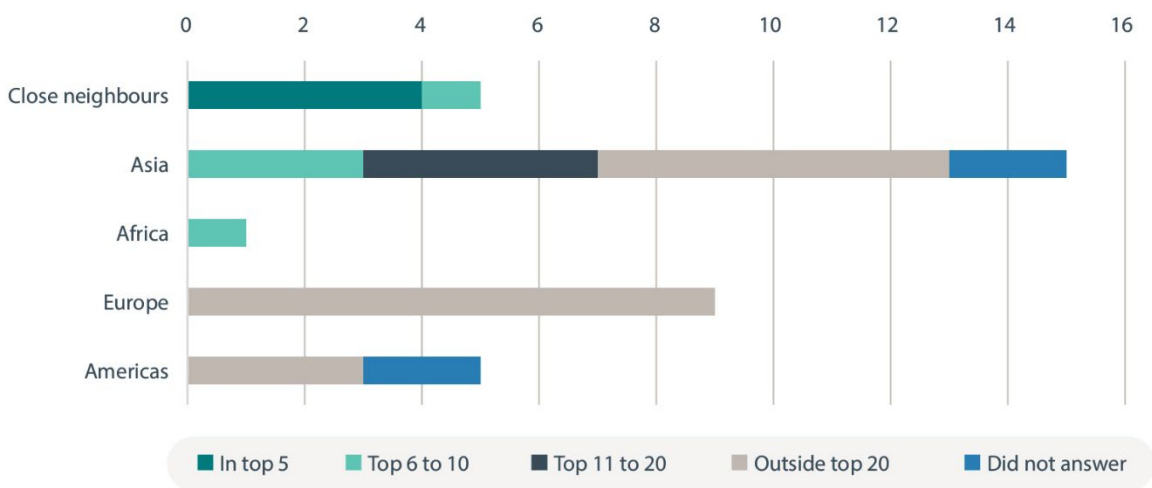
Australia is an important country *within* our region from both an economic and illicit proceeds perspective. However, *outside* of our region, Australia is a comparatively less attractive destination for proceeds of crime.

Ranking Australia as a destination for proceeds of crime or money laundering proceeds among global peers:

- more than 50 per cent place Australia outside their top 20 destination countries, most notably this includes six Asian countries
- 25 per cent of countries consider Australia to be in their top 10 destination countries for proceeds of crime or money laundering
- 80 per cent of Australia’s closest neighbours rate Australia in their top five destinations for illicit proceeds.

Figure 5: Number of countries by region and where they rank Australia as a destination of illicit funds

Where Australia ranks as a POC/ML destination country
(country count by ranking cohort)



Predicate offences behind foreign sourced illicit proceeds

21 countries provided feedback about predicate crimes in their country that generate illicit proceeds that are sent to or transited through Australia.

The top three predicate crimes identified by respondents were fraud (90 per cent), bribery and corruption (52 per cent) and illicit drugs (38 per cent).

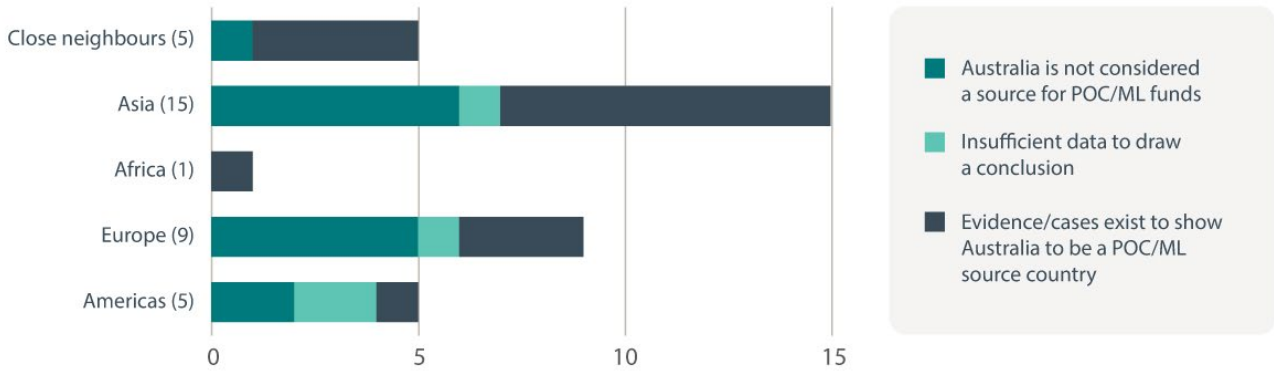
AUSTRALIA AS A SOURCE OF ILLICIT PROCEEDS

In addition to considering Australia as a destination of proceeds of crime or money laundering, FIUs were also asked to consider Australia as a *source* of illicit proceeds *sent to their* jurisdiction.

Approximately 40 per cent of respondents do not consider Australia to be a source for proceeds sent to their country, while 50 per cent of respondents have sufficient evidence or cases to confirm Australia as a source or conduit country. The remaining 10 per cent did not have sufficient information or data to make an assessment.

Figure 6 - Number of countries by region and how they perceive Australia as a source of illicit proceeds

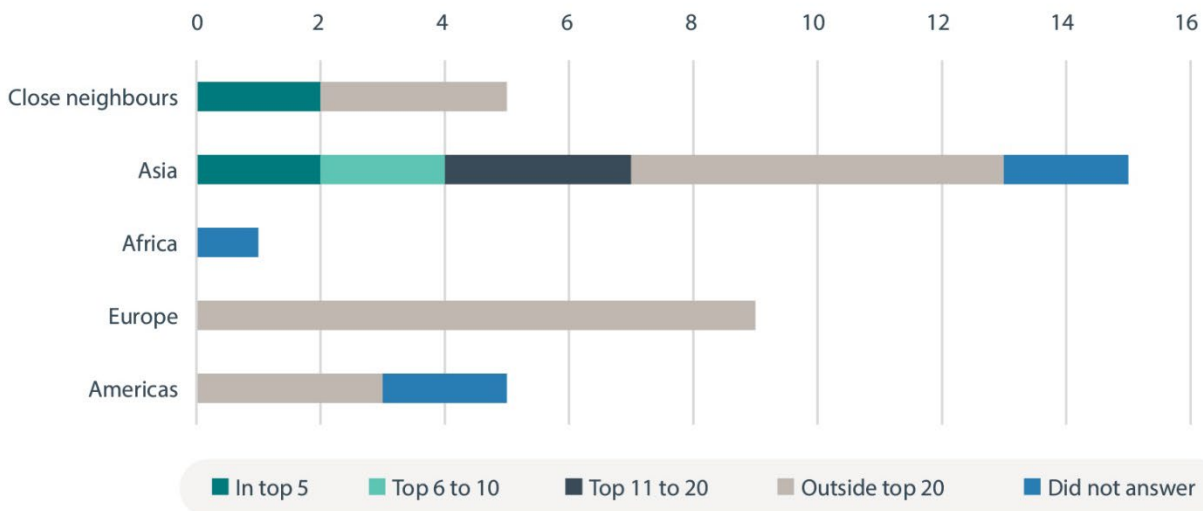
How Australia is perceived as a source country for POC/ML proceeds
(n)= participating countries



Only six countries consider Australia to be among the top 10 of source countries, with two of Australia’s closest neighbours and two Asian countries considering Australia in their top five destinations for illicit proceeds. 60 per cent of respondents place Australia outside their top 20 destination countries; this most notably includes three close neighbours and six Asian countries.

Figure 7: Number of countries by region and where they rank Australia as a source of illicit funds

Where Australia ranks as a POC/ML source country
(country count by ranking cohort)



FIUs considered Australia to represent a medium to low money laundering threat in terms of being both a source or destination country. Close proximity, mutual entry arrangements, Australia’s open investment markets and legal structures, and mutual ties between criminal groups feature heavily as the basis for money laundering activity with many countries.



AUSTRAC.GOV.AU

