GIR Global Investigations Review

The Guide to Anti-Money Laundering - Third Edition

Australia: a closer look at the regulatory environment in the face of new reforms and 'Tranche 2' amendments

The Guide to Anti-Money Laundering - Third Edition

The Guide to Anti-Money Laundering is one of the first publications to simultaneously tackle both sides of the money laundering conundrum. Edited by Sharon Cohen Levin of Sullivan & Cromwell, the third edition covers global enforcement and compliance trends – with specific practical advice for corporations and their counsel throughout. It also features a new Spotlight section, which takes a deep dive into the anti-money laundering regimes of key jurisdictions around the world.

Generated: May 29, 2025

GIR Global Investigations Review

Australia: a closer look at the regulatory environment in the face of new reforms and ‘Tranche 2’ amendments

Dennis Miralis, Dennis Miralis, **Jasmina Ceic**, Jasmina Ceic and **Jack Dennis**

Nyman Gibson Miralis

Summary

MONEY LAUNDERING

WHAT LAWS IN YOUR JURISDICTION PROHIBIT MONEY LAUNDERING?

In Australia, money laundering is prohibited under two key pieces of federal legislation and various state and territory laws.

The first piece of federal legislation is the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (the AML/CTF Act), which is accompanied by the Anti-Money Laundering and Counter-Terrorism Financing Rules 2007 (the AML/CTF Rules). These two instruments set out the legal requirements and obligations for 'reporting entities' and prohibit non-compliance (and money laundering) in respect of these entities.

Criminal offences under the AML/CTF Act predominately fall under Part 12 and regulate designated entities providing false or misleading information concerning their reporting obligations. These instruments regulate reporting entities by way of a series of compliance and reporting obligations.

Regulated entities are defined in Section 5 of the AML/CTF Act as persons who provide a 'designated service'. Broadly speaking, a designated service is considered to be a business operating in financial services, gambling, bullion services, remittance service providers and digital currency services. These businesses under the AML/CTF Act are known as reporting entities.

The second federal legislation is the Criminal Code Act 1995 (the Criminal Code). The Criminal Code sets out criminal offences targeting the conduct of more than just reporting entities, covering all Australian citizens, residents and body corporates, among others, depending on where the alleged money laundering or related offences occur.

Chapter 10, Part 10.2, Division 400 of the Criminal Code contains over 40 money laundering offences covering proceeds of crime (funds generated by an illegal activity) and instruments of crime (funds used to conduct an illegal activity).

Beyond the two above-mentioned federal instruments, Australian state and territory criminal legislation also contains money laundering offence provisions, as below:

- New South Wales: Crimes Act 1900, Part 4AC;
- Victoria: Crimes Act 1958, Part I, Division 2A;
- Queensland: Criminal Proceeds Confiscation Act 2002, Chapter 9;
- South Australia: Criminal Law Consolidation Act 1935, Part 5, Division 4;
- Western Australia: Criminal Code Act 1913, Part VII, Chapter LIX;
- Tasmania: Crime (Confiscation of Profits) Act 1993, Part 6A;
- Australian Capital Territory: Crimes Act 1900, Part 6, Division 6.2A; and
- Northern Territory: Criminal Code Act 1982 (NT): Part VII, Division 3.

WHAT MUST THE GOVERNMENT PROVE TO ESTABLISH A CRIMINAL VIOLATION OF THE MONEY LAUNDERING LAWS?

To prove a money laundering offence, the Commonwealth Director of Public Prosecutions (CDPP) must prove the existence of physical elements that create the offence and the fault element in respect of each physical element.

Generally speaking, there are two principal kinds of money laundering offences under the federal Criminal Code.

The first, concerns 'dealing' with money or other property reasonably believed to be the proceeds of crime or that will become an instrument of crime. Under the Code, dealing occurs when a person receives, possesses, conceals, disposes, imports or exports the money or property or otherwise engages in a banking transaction relating to the money or other property.

The second concerns a person concealing or disguising certain things about money or property reasonably believed to be proceeds of crime, such as the nature, value, source or identity of the owner.

For each kind, there are different tiers of money laundering offence depending on whether the value of the money or property is A$10 million or more. The CDPP does not have to prove that a defendant knew the value of the offence or the predicate offence itself (i.e., the particular offence (or kind of offence) that was committed in relation to the money or property).

WHAT ARE THE PREDICATE OFFENCES TO MONEY LAUNDERING? DO THEY INCLUDE FOREIGN CRIMES AND TAX OFFENCES?

While the Criminal Code does not specify offences that predicate money laundering offences, predicate offences in Australia usually involve drugs and narcotics trafficking, fraud, theft and identity theft, tax evasion, people smuggling, arms trafficking and corruption offences. Criminal breaches of state and territory laws and foreign laws can also be predicate offences.

IS THERE EXTRATERRITORIAL JURISDICTION FOR VIOLATIONS OF YOUR JURISDICTION'S MONEY LAUNDERING LAWS?

Yes. As a starting point, the money laundering offences defined by the Criminal Code apply where the conduct occurs partly in Australia or wholly or partly on board an Australian aircraft or ship irrespective of the vehicle's location.

For conduct occurring wholly outside Australia, the money laundering offences defined by the Criminal Code apply where:

- the money or property is likely to become, or is at risk of becoming, proceeds of indictable crime[1] in relation to a Commonwealth, state, or territory law;
- the money or property is proceeds of 'general crime' in relation to Commonwealth, state or territory law;
- the person is an Australian citizen, resident or body corporate; and
- the offence is an ancillary offence, and the primary offence relevant to the ancillary offence occurred, or was intended to occur, wholly or partly either in Australia or on board an Australian aircraft or ship.

Unique defences are available where the alleged conduct occurs wholly in a foreign country (but not on board an Australian aircraft or ship).

IS THERE CORPORATE CRIMINAL LIABILITY FOR MONEY LAUNDERING OFFENCES, OR IS LIABILITY LIMITED TO INDIVIDUALS?

Yes. The Criminal Code applies equally to bodies corporate and individuals. Accordingly, a corporation can be liable for any of the money laundering offences under the Criminal Code.

WHICH GOVERNMENT AUTHORITIES ARE RESPONSIBLE FOR INVESTIGATING VIOLATIONS OF THE MONEY LAUNDERING LAWS?

At the federal level, agencies tasked with investigating money laundering include the Australian Criminal Intelligence Commission, the Australian Federal Police (AFP), the Australian Taxation Office, the Australian Transaction Reports and Analysis Centre (AUSTRAC), and the Australian Securities and Investments Commission (ASIC).

At the state and territory level, the respective state and territory law enforcement agencies and police investigate violations of their own money laundering laws.

AUSTRAC is Australia's primary anti-money laundering (AML) financial intelligence agency and has two main functions. Its primary function is to monitor and enforce AML and counterterrorism financing (CTF) laws in Australia. Its secondary function is the collection of analyses and dissemination of financial intelligence to relevant government departments in Australia and overseas.

AUSTRAC's role in Australia is vital in assisting domestic and international enforcement agencies in the investigation of money laundering offences. At the time of writing, it regulates over 17,000 designated service entities across Australia that provide financial, gambling bullion, remittance and digital currency services to prevent and track money laundering offences. This number is set to increase by more than 90,000 on 1 July 2026 as new reforms impose regulatory obligations onto new areas (e.g., real estate, lawyers, conveyancers, accountants, and trust and company service providers).

WHICH GOVERNMENT AGENCIES ARE RESPONSIBLE FOR THE PROSECUTION OF MONEY LAUNDERING OFFENCES?

At the national level, the CDPP is the primary government agency that is responsible for the prosecution of money laundering offences. Its remit includes prosecuting money laundering offences that are criminalised under the Criminal Code.

The CDPP is assisted by AUSTRAC, the AFP and the Department of Home Affairs in prosecuting money laundering offences.

At the state and territory level, the respective state or territory public prosecutions offices are responsible for prosecuting money laundering offences that breach state or territory laws.

WHAT IS THE STATUTE OF LIMITATIONS FOR MONEY LAUNDERING OFFENCES?

At the national level, there are no time limits on commencing proceedings for money laundering offences specifically, but there are general limitations. Under Section 15B of the Criminal Code, the CDPP can commence criminal proceedings within one year after the commission of an offence or, for offences against:

- an individual, at any time if the maximum penalty that may be imposed for the offence in respect of an individual is at least six months' imprisonment; or
- a body corporate, at any time if the maximum penalty that may be imposed for the offence in respect of a body corporate is at least 150 penalty units.[2]

These limits only apply in the case of first convictions. As such, these limits do not apply to most money laundering offences: these limits are not relevant where an alleged offender has had previous convictions, and most money laundering offences are punishable by maximum penalties greater than these limits.

At the state and territory level, the prosecution of money laundering offences may also have time limits. For example, in New South Wales, proceedings for summary offences must be commenced no later than six months from the date when the offence was allegedly committed; however, money laundering offences are considered indictable offences.

WHAT ARE THE PENALTIES FOR A CRIMINAL VIOLATION OF THE MONEY LAUNDERING LAWS?

The Criminal Code provides different penalties for money laundering offences. The maximum penalty depends on the value of the relevant money or property that has allegedly been laundered and what the offender reasonably believed at or before the time of the offence. The penalties may include imprisonment and fines.

For example, for a money laundering offence with money or property worth A$10 million or more, the maximum penalty is:

- for individuals, life imprisonment or 2,000 penalty units, or both; and
- for body corporates, 10,000 penalty units.

At the lower range of value, Section 400.8(3) is an offence for a person convicted of dealing with money or property (without specifying any value) where they were negligent to the fact that the money or property was proceeds of indictable crime or that there was a risk that it will become an instrument of crime. This offence has a maximum penalty of 10 penalty units.

ARE THERE CIVIL PENALTIES FOR VIOLATIONS OF THE MONEY LAUNDERING LAWS? WHAT ARE THEY?

The AML/CTF Act contains the civil penalties for violations of money laundering laws. Under the Act, individuals can face penalties up to A$6.6 million for breaches of a civil penalty provision, while corporations can face penalties up to A$33 million.

IS ASSET FORFEITURE POSSIBLE UNDER THE MONEY LAUNDERING LAWS? IS IT PART OF THE CRIMINAL PROSECUTION? WHAT PROPERTY IS SUBJECT TO FORFEITURE?

At the national level, there are existing mechanisms that can be used in relation to money laundering offences. The Proceeds of Crime Act 2002 (Cth) (the POC Act) enables law enforcement to pursue the recovery of assets linked to offences after a conviction through freezing orders, restraining orders, forfeiture orders and pecuniary penalty orders, among other things. This legislation has a broad definition of someone's 'property', which includes any money, real property and personal property, tangible or intangible, located in Australia or elsewhere.

An important component of the POC Act is the unexplained wealth provisions at Part 2-6. These provisions can be used to obtain orders, and persons must prove on the balance of probabilities that their wealth was not derived from an offence against a law of the Commonwealth, a foreign indictable offence, or certain state and territory offences.

Since 2018, the National Cooperative Scheme on Unexplained Wealth has operated to enhance the ability of the Commonwealth, state and territory law enforcement agencies to trace, identify and seize assets that cannot be connected to a lawful source.

At the state and territory level, each Australian state and territory also has asset recovery legislation for funds generated by offences at a state or territory level. For example, in New South Wales, there are the Confiscation of Proceeds of Crime Act 1989 (NSW) and the Criminal Assets Recovery Act 1990 (NSW).

IS CIVIL OR NON-CONVICTION-BASED ASSET FORFEITURE PERMITTED UNDER THE MONEY LAUNDERING LAWS? WHAT PROPERTY IS SUBJECT TO FORFEITURE?

At the national level, the POC Act enables law enforcement to pursue the restraint and recovery of assets suspected of criminal origins without the necessity of securing a criminal conviction. This includes obtaining a forfeiture order, which can be granted by a court even where the court is satisfied that there is suspicious conduct constituting a serious offence (without needing to actually prove a particular offence or conviction).

The definition of property is not impacted by whether the forfeiture is conviction or non-conviction based.

ANTI-MONEY LAUNDERING

WHICH LAWS OR REGULATIONS IN YOUR JURISDICTION IMPOSE ANTI-MONEY LAUNDERING COMPLIANCE REQUIREMENTS ON FINANCIAL INSTITUTIONS AND OTHER BUSINESSES?

The Australian AML compliance regime is imposed by the AML/CTF Act and related rules and regulations, including the AML/CTF Rules.

On 29 November 2024, the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024 (the AML/CFT Amendments) was passed by Parliament. The AML/CTF Amendments implement a range of changes, commonly referred to in Australia as the 'Tranche 2' reforms. These reforms reflect recommendations by the Financial Action Task Force and changes already seen in other jurisdictions and include amendments to:

- extend the regime to additional high-risk service providers;
- simplify the Australian AML and CTF (AML/CTF) obligations; and
- modernise the AML/CTF regime to reflect changing business structures, technologies and illicit financing methodologies.

WHAT TYPES OF INSTITUTIONS ARE SUBJECT TO THE AML RULES?

The AML rules apply to reporting entities. A reporting entity is a person or institution that provides a designated service.

Section 6 of the AML/CTF Act lists the designated services subject to the AML/CTF obligations, which cover various financial, bullion and gambling services. For example, the financial services covered include accepting money on deposits, making loans and exchanging digital currency for fiat currency (or vice versa) in the course of carrying on a digital currency exchange business.

In other words, the institutions subject to the current AML/CTF regime are authorised deposit-taking instructions, banks, building societies, credit unions, superannuation funds,

casinos, crypto exchanges and any other body that provides one or more of the services listed in Section 6.

Under the AML/CFT Amendments, the AML/CTF regime will extend to Tranche 2 entities, including:

- real estate professionals;
- professional service providers, including lawyers, accountants, and trust and company service providers; and
- dealers in precious stones and metals, as well as products comprising, containing or having attached to it any of the same (e.g., jewellery or watches).

MUST PAYMENT SERVICES AND MONEY TRANSMITTERS BE LICENSED IN YOUR JURISDICTION? ARE PAYMENT SERVICES AND MONEY TRANSMITTERS SUBJECT TO THE AML RULES AND COMPLIANCE REQUIREMENTS?

Yes.

Payment services and money transmitters are subject to the AML rules and compliance requirements. Under Section 6 of the AML/CTF Act, the following services are considered designated services:

- carrying on a business of giving effect to remittance arrangements; and
- exchanging foreign currencies as a currency exchange business.

As providers of one or more of these services, payment services and money transmitters are reporting entities and must comply with the AML rules and requirements.

Payment services and money transmitters must be registered with AUSTRAC, the principal AML Australian agency, under Part 6 of the AML/CTF Act. An entity or person who conducts an unregistered money remittance business can be liable for a civil penalty under Section 51B of the AML/CTF Act.

ARE DIGITAL ASSETS SUBJECT TO THE AML RULES AND COMPLIANCE REQUIREMENTS?

In part, yes, and there are important changes under the AML/CTF Amendments.

Under the current AML/CTF Act, 'digital currency' is expressly recognised and defined as a digital representation of value that:

- functions as a medium of exchange, a store of economic value or a unit of account;
- is not government-issued;
- is interchangeable with money; and
- is generally available to members of the public.

Certain digital currency exchange service providers are subject to the AML rules and compliance requirements. Specifically, the AML rules apply only to the exchange of digital currency for 'money' (or vice versa) that is provided in the course of carrying on a digital currency exchange business. It is therefore generally understood that the current AML rules only cover crypto-to-fiat exchanges and not crypto-to-crypto exchanges; however, whether the AML rules apply ultimately depends on the specific details of each exchange.

Part 6A of the AML/CTF Act imposes registration and reporting obligations specifically onto providers of the relevant digital currency exchange services.

The AML/CTF Amendments introduce critical changes, including the following:

- The term 'digital currency' is replaced by the term 'virtual asset', thereby significantly changing and expanding the scope of the assets covered. For example, such assets are no longer required to be interchangeable with money, can function as an investment and now include certain digital representations of value that enable a person to vote on the management, administration or governance of arrangements connected with digital representations of value (which will likely include certain decentralised autonomous organisation governance tokens).
- The services that are covered by the AML/CTF Amendments include crypto-to-crypto exchanges and any designated service in connection with the offer or sale of a virtual asset provided in the course of carrying on a business participating in the offer or sale.

WHAT ARE THE SPECIFIC AML COMPLIANCE REQUIREMENTS FOR COVERED INSTITUTIONS?

AML compliance under Australian law falls under three categories: an AML/CTF programme, ongoing reporting and record-keeping.

Under the current AML/CTF regime, reporting entities must implement an AML/CTF programme identifying and mitigating the money laundering and terrorism financing risks faced by the business. Although the content varies depending on the nature of the business and its designated service, each AML/CTF programme must include the following:

- a comprehensive assessment of the money laundering and terrorism financing risks;
- the appointment of an AML/CTF compliance officer;
- an independent review of the programme;
- an employee due diligence programme;
- AML/CTF training for employees;
- an enhanced customer due diligence programme for when the money laundering and terrorism financing risk is high;
- a transaction monitoring programme; and
- 'know your customer' procedures.

The AML/CTF Amendments retains the obligation to have an AML/CTF programme, reformulating it around a money laundering and terrorism financing risk assessment and AML/CTF policies. This reformulation is said to move away from the current tick-box exercise.

Like under the existing regime, the risk assessment must identify and assess the risks of money laundering, terrorism financing and proliferation financing that the reporting entity may reasonably face. This assessment must be appropriate to the nature, size and complexity of the business; have regard to several considerations, including service type,

customer type, delivery channels, countries and any matters specified in the AML/CTF Rules; and be updated at least once every three years.

AML/CTF policies are policies, procedures, systems and controls that reflect aspects already required by the existing regime set out above. The AML/CTF Amendments introduce increased flexibility in the handling of these assessments and policies, such as allowing reporting entities to organise themselves into reporting groups to centralise these obligations.

Under the current regime, reporting entities have ongoing reporting obligations. These include obligations to submit:

- threshold transaction reports for transfers of A$10,0000 or more;
- international funds transfer instruction reports for fund transfers into or out of Australia made electronically or under a designated remittance arrangement;
- suspicious matter reports if there are suspicions that a customer or transaction is related to criminal activity; and
- compliance reports when requested by AUSTRAC, providing details of the entity's compliance efforts under the AML regime.

Under the AML/CTF Amendments, these obligations remain largely the same, and exemptions may apply (e.g., certain entities that operate no more than 15 gaming machines).

Reporting entities must also keep records about transactions, customer identification procedures and their AML/CTF programme. The specific record-keeping obligations depend on the reporting entity's particular designated services. The record-keeping obligations remain largely the same under the AML/CTF Amendments.

ARE THERE DIFFERENT AML COMPLIANCE REQUIREMENTS FOR DIFFERENT TYPES OF INSTITUTIONS?

The precise AML compliance requirements for a reporting entity depend on the designated service that it provides. The content of an AML/CTF programme may vary substantially between entities that provide different designated services.

Money remittance and digital currency exchange institutions have unique additional compliance requirements. Both types of institution must register with AUSTRAC and renew their registration every three years. Both types of institutions must also keep an original or certified copy of a national police certificate for all key personnel and details of the institution's business structure.

WHICH GOVERNMENT AUTHORITIES ARE RESPONSIBLE FOR THE EXAMINATION AND ENFORCEMENT OF COMPLIANCE WITH THE AML RULES?

The government authority responsible for the examination, administration and enforcement of Australian AML law is AUSTRAC. AUSTRAC is also responsible for disseminating intelligence to other law enforcement, national security, revenue and regulatory agencies for further investigation.

ARE THERE REQUIREMENTS TO MONITOR AND REPORT SUSPICIOUS ACTIVITY? WHAT ARE THE FACTORS THAT TRIGGER THE REQUIREMENT TO REPORT SUSPICIOUS ACTIVITY? WHAT IS THE PROCESS FOR REPORTING SUSPICIOUS ACTIVITY?

Reporting entities must monitor and report suspicious activity. Activity is suspicious and must be reported if the reporting entity suspects that a person using their services is not who they claim to be or that information concerning the activity may be relevant to investigate or prosecute a criminal offence.

Suspicious activity must be reported to the AUSTRAC CEO either within 24 hours or within three days of the reporting entity forming the relevant suspicion, depending on the nature of the activity. The report must be in an approved form and contain specific information about the suspicious activity and a statement outlining the grounds on which the reporting entity has formed the suspicion.

A suspicious matter report can be lodged online through the AUSTRAC online portal.

Under the AML/CTF Amendments, this requirement remains the same, except there are now codified exceptions for information that the reporting entity reasonably believes is subject to legal professional privilege.

ARE THERE CONFIDENTIALITY REQUIREMENTS ASSOCIATED WITH THE REPORTING OF SUSPICIOUS ACTIVITY? WHAT ARE THE REQUIREMENTS? WHO DO THE CONFIDENTIALITY REQUIREMENTS APPLY TO? ARE THERE PENALTIES FOR VIOLATIONS OF THE CONFIDENTIALITY REQUIREMENTS?

Yes.

Under the current regime, a reporting entity must not disclose that they have given or are required to give AUSTRAC a suspicious matter report. There are certain exceptions to this confidentiality requirement, such as for the purposes of crime prevention, seeking legal advice or an audit or review of the AML/CTF programme. Breaching this confidentiality requirement is a criminal offence and is known as 'tipping off'. Tipping off is punishable by imprisonment for up to two years or a fine of up to 120 penalty units.

Similarly, it is an offence for government officials to disclose information they have obtained through AUSTRAC, except as authorised under AML law. This includes reports of suspicious activity. This offence is punishable by imprisonment for up to two years or a fine of up to 120 penalty units.

The AML/CTF Amendments reform the offence for breaching the confidentiality requirement such that information-sharing is allowed except where disclosure relates to certain information (e.g., certain AML/CTF reports and notices) and disclosure 'would or could reasonably be expected to prejudice and investigation' for an offence under Australian law or proceeds of crime proceedings. Similar exemptions still apply. The offence regarding disclosure by government officials remains largely unchanged.

ARE THERE REQUIREMENTS FOR REPORTING LARGE CURRENCY TRANSACTIONS? WHO MUST FILE THE REPORTS, AND WHAT IS THE THRESHOLD?

Yes. Part 3 of the AML/CTF Act imposes reporting obligations on reporting entities. Section 43 of the Act requires entities to provide designated services report threshold transactions. The threshold is the transfer of physical currency (cash) of A$10,000 or more (or equivalent in the foreign currency equivalent) as part of providing a designated service. Regulations can apply this obligation to transactions involving digital currency.

In addition, affiliates of remittance network providers, motor vehicle dealers who act as insurers, or insurance intermediaries and solicitors must also report threshold and significant cash transactions.

ARE THERE REPORTING REQUIREMENTS FOR CROSS-BORDER TRANSACTIONS? WHO IS SUBJECT TO THE REQUIREMENTS AND WHAT MUST BE REPORTED?

Yes.

Under the current regime, cross-border transactions must be reported where they comprise:

- monetary instruments of A$10,000 or more; or
- certain international funds transfer instructions transmitted out of or into Australia, which may include certain electronic funds transfer instructions and instructions given by a transferor for the transfer of money or property under a designated remittance arrangement.

These are relevant for financial institutions and other entities, such as remittance service providers and casinos.

Although there are some indirect amendments under the AML/CTF Amendments for these obligations, the obligations remain largely the same, except references to 'international funds transfer instructions' will be changed to 'information about international value transfer services'.

IS THERE A FINANCIAL INTELLIGENCE UNIT OR OTHER GOVERNMENT AGENCY RESPONSIBLE FOR ANALYSING THE INFORMATION REPORTED UNDER THE AML RULES?

Yes. AUSTRAC functions as Australia's financial intelligence unit and AML/CTF regulator. It is responsible for analysing information reported under Australia's AML rules.

WHAT ARE THE PENALTIES FOR FAILING TO COMPLY WITH YOUR JURISDICTION'S AML RULES, AND ARE THEY CIVIL OR CRIMINAL?

There are various penalties for failing to comply with the Australian AML/CTF regime, including the following:

- *Criminal penalties*: these apply to the most serious AML/CTF violations. The maximum penalties range from six months to 10 years' imprisonment, or 30 to 10,000 penalty units, or both.
- *Civil penalties*: the Federal Court of Australia determines the total civil penalties, taking into consideration factors listed at Subsection 175(3) of the AML/CTF Act. The maximum penalty is 100,000 penalty units for body corporates and 20,000 penalty units for natural persons.
- *Other options*: these include enforceable undertakings, remedial directions and infringement notices for certain violations, which can be up to:
    - for body corporates, 120 penalty units or another amount specified in the AML/CTF Rules; and
    - for individuals, 24 penalty units.

Throughout 2024, the full range of non-criminal penalties could be seen in action. In 2024, AUSTRAC:

- obtained an enforceable undertaking from Sportsbet Pty Ltd;
- issued at least 19 infringement notices;
- successfully concluded civil penalty proceedings totalling A$67 million against SkyCity Adelaide Pty Ltd in June 2024 for alleged serious and systemic non-compliance with Australia's AML/CTF laws; and
- commenced in December 2024 civil penalty proceedings against Entain Group Pty Ltd for other serious AML/CTF violations.

ARE COMPLIANCE PERSONNEL SUBJECT TO THE AML RULES? CAN AN ENFORCEMENT ACTION BE BROUGHT AGAINST AN INDIVIDUAL FOR VIOLATIONS?

The AML/CTF Act requires reporting entities to appoint compliance officers who are at management level; however, compliance officers are not specifically subject to the AML rules in the same manner as reporting entities.

Most compliance obligations are imposed on the reporting entity and not on its individual employees, and violations of such will accordingly be enforced by way of a fine against the company, not a specific individual.

However, there are offences throughout the AML/CTF Act targeted towards an individual's own violations of AML rules. These include:

- moving or receiving monetary instructions into or out of Australia over a certain value (e.g., A$10,000) without making the required report;
- knowingly giving or producing false or misleading information to AUSTRAC;
- providing or receiving a designated service using a false customer name or customer anonymity; and
- being involved in conducting transactions conducted in such a manner as to avoid reporting requirements.

Section 235 of the AML/CTF Act provides protection to employees of a reporting entity from civil or criminal liability for acts or omissions carried out in good faith in some circumstances.

Separately, a company's violations of AML/CTF obligations may lead to action against directors and other company officers for breach of duties under Australian corporation law.

WHAT IS THE STATUTE OF LIMITATIONS FOR VIOLATIONS OF THE AML RULES?

Civil penalty proceedings under the AML/CTF Act and its rules can be commenced no later than six years after the contravention.

Infringement notices must be given within 12 months after the day on which the contravention allegedly took place.

DOES YOUR JURISDICTION HAVE A BENEFICIAL OWNERSHIP REGISTRY OR AN ENTITY OR OFFICE THAT COLLECTS INFORMATION ON THE BENEFICIAL OWNERSHIP OF LEGAL ENTITIES?

No. Australia does not currently have a beneficial ownership registry; however, there are legislative reforms on the horizon, including:

-

a new regulatory regime for a public registry of beneficial legal owners of corporations to be enforced by ASIC, which has been being considered since as early as 2022; and

- a potential registry of trusts, which is at the very early stages of developing.

ENDNOTES

[1] An 'indictable offence' is a type of offence under Australian law for which each jurisdiction may have a varying definition. Under federal law, it is generally defined as '[o]ffences against a law of the Commonwealth punishable by imprisonment for a period exceeding 12 months are indictable offences, unless the contrary intention appears' (Crimes Act 1914 (Cth)- , Section 4G).

[2] At the time of writing, since 7 November 2024, one penalty unit is equivalent to A$330, (Crimes Act 1914 (Cth), Section 4AA).

Dennis Miralis dm@ngm.com.au
Dennis Miralis dm@ngm.com.au
Jasmina Ceic jc@ngm.com.au
Jasmina Ceic jc@ngm.com.au
Jack Dennis jd@ngm.com.au

Australia

https://ngm.com.au/