

ANTI-MONEY LAUNDERING

Australia



Anti-Money Laundering

Consulting editors

Jonah Anderson

White & Case

Quick reference guide enabling side-by-side comparison of local insights into anti-money laundering laws and regulations, including overview of domestic laws, regulations and investigatory powers; criminal enforcement, including extraterritorial reach of applicable laws; compliance, including due diligence, high-risk categories of customers, business partners and transactions, record-keeping and reporting requirements, and the role of privacy laws; civil claims, including procedures, damages and other remedies; international anti-money laundering efforts; and recent trends.

Generated 02 June 2023

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. © Copyright 2006 - 2023 Law Business Research

Table of contents

DOMESTIC LEGISLATION

Domestic law

Investigatory powers

MONEY LAUNDERING

Criminal enforcement

Defendants

The offence of money laundering

Qualifying assets and transactions

Predicate offences

Defences

Resolutions and sanctions

Forfeiture

Limitation periods on money laundering prosecutions

Extraterritorial reach of money laundering law

AML REQUIREMENTS FOR COVERED INSTITUTIONS AND INDIVIDUALS

Enforcement and regulation

Covered institutions and persons

Compliance

Breach of AML requirements

Customer and business partner due diligence

High-risk categories of customers, business partners and transactions

Record-keeping and reporting requirements

Privacy laws

Resolutions and sanctions

Limitation periods for AML enforcement

Extraterritoriality

CIVIL CLAIMS

Procedure

Damages

Other remedies

INTERNATIONAL MONEY LAUNDERING EFFORTS

Supranational

Anti-money laundering assessments

FIUs

Mutual legal assistance

UPDATE AND TRENDS

Enforcement and compliance

Contributors

Australia



Peter Reeves
preeves@gtlaw.com.au
Gilbert + Tobin



Georgina Willcock
gwillcock@gtlaw.com.au
Gilbert + Tobin

DOMESTIC LEGISLATION

Domestic law

Identify your jurisdiction's money laundering and anti-money laundering (AML) laws and regulations. Describe the main elements of these laws.

In Australia, the regime for detecting, prosecuting and deterring money laundering activities consists of:

- criminal offences for money laundering at the Commonwealth and state or territory levels;
- asset recovery legislation at the Commonwealth and state or territory levels; and
- prevention and detection measures, legislated at the Commonwealth level.

The money laundering offences are defined in Part 10.2 of the Criminal Code Schedule to the Criminal Code Act 1995 (Cth) and encompass a wide range of criminal activity. Similar offences exist in Australia's state and territory criminal legislation. The offences differ according to areas such as relevant predicate offences, the intent of the defendant and penalties.

The asset recovery provisions are contained in the Proceeds of Crime Act 2002 (Cth) (the POC Act), which enables law enforcement to pursue the recovery of assets linked to offences after a conviction. Each Australian state and territory also have asset recovery legislation for funds generated by offences at a state or territory level.

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act) is the primary piece of legislation with respect to the prevention and detection of money laundering and terrorism financing. The AML/CTF Act operates in conjunction with the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth) and associated regulations, each of which are made under the AML/CTF Act.

The Financial Transaction Reports Act 1988 (Cth) operates alongside the AML/CTF Act, and imposes obligations on cash dealers and solicitors to report significant cash transactions (ie, A\$10,000 or more) to the Australian Transaction Reports and Analysis Centre. This Act also requires cash dealers to verify the identities of account signatories.

Australia implements the United Nations Security Council sanctions regime under the Charter of the United Nations Act 1945 as well as the Australian autonomous sanctions regime under the Autonomous Sanctions Act 2011 (Cth) and associated regulations. Sanctions measures include prohibitions on making a sanctioned supply, a sanctioned import, providing a sanctioned service, engaging in a sanctioned commercial activity and dealing with a designated person or entity. Australian sanctions laws establish serious criminal offences, and penalties include up to 10 years in prison and substantial fines.

Law stated - 19 May 2023

Investigatory powers

Describe any specific powers to identify proceeds of crime or to require an explanation as to the source of funds.

Australia has unexplained wealth laws at the Commonwealth, state and territory levels. At the Commonwealth level, Part 2-6 of the POC Act contains the unexplained wealth provisions, where targets of orders must prove on the balance of probabilities that their wealth was not derived from an offence against an Australian law, a foreign indictable offence or a state offence that has a federal aspect. Amendments in 2018 created the National Cooperative Scheme on Unexplained Wealth, aimed at enhancing 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. The scheme currently applies to New South Wales, the Australian Capital Territory and the Northern Territory.

In February 2021, Parliament passed a law to create a new category of proceeds of general crime. The introduction of the proceeds of general crime offence removed the requirement for money or other property to be linked to an indictable offence and lowered the threshold for the prosecution. These amendments commenced on 17 February 2021 and are intended to capture the controllers of modern money laundering networks who do not typically deal with the money or property directly.

Law stated - 19 May 2023

MONEY LAUNDERING

Criminal enforcement

Which government entities enforce your jurisdiction's money laundering laws?

The Commonwealth Department of Public Prosecutions (CDPP), Australia's federal prosecution service, prosecutes money laundering offences at the Commonwealth level. The Australian Transaction Reports and Analysis Centre, the Australian Federal Police and the Australian Border Force act as partner agencies to the CDPP in prosecuting money laundering offences. The Australian Federal Police also leads the Criminal Assets Confiscation Taskforce that, as stated on its website, collaborates with other agencies to 'identify, investigate and litigate appropriate asset confiscation matters at the Commonwealth level'.

State- and territory-based public prosecution services and local police departments enforce and prosecute offences at their respective levels. However, it is unlikely that a prosecution under a state or territory law for money laundering would be pursued if one has already been brought at the federal level. At the state and territory levels, police focus is on the investigation of predicate offences and money laundering prosecution only in simple cases where offenders may be caught in possession of cash.

Law stated - 19 May 2023

Defendants

Can both natural and legal persons be prosecuted for money laundering?

Both natural and legal persons can be prosecuted for money laundering offences.

Law stated - 19 May 2023

The offence of money laundering

What constitutes money laundering?

The relevant division of the Criminal Code Act 1995 (Cth) (the Criminal Code) creates multiple offences that cover a wide range of criminal activity. The offences are based on a person dealing with money or property that is proceeds of crime, or will be (or is at risk of becoming) an instrument of crime. Broadly, the elements of the offence are:

- the existence of money or property;
- a dealing (physical conduct such as receiving, possessing, concealing or disposing of the money or property, importing or exporting it, or engaging in banking transactions) in money or property being unlawful because the proceeds are proceeds of crime, or the proceeds are at risk of being used in the commission of or to facilitate a

crime; and

- the person believed that the money or property was the proceeds of a crime, or was reckless or negligent about that fact.

Generally, a person commits an offence of money laundering if they deal with money or other property that is, or is reasonably suspected of being, the proceeds of crime and one of the following states of mind is present:

- intentionality: the money or property is, and is believed to be, proceeds of crime, or the person intends that the money or property will become an instrument of crime;
- recklessness: the money or property is proceeds of crime, or there is a risk that it will become an instrument of crime, and the person is reckless to this fact; or
- negligence: the money or property is proceeds of crime, or there is a risk that it will become an instrument of crime, and the person is negligent as to this fact.

An offence under section 400.9 of the Criminal Code does not require the element of intention, recklessness or negligence be present. Rather, the offence is established where it is reasonable to suspect that money or property was the proceeds of crime.

'Proceeds of crime' means any money or other property wholly or partly derived or realised, directly or indirectly, by any person from the commission of an offence against a law of Australia 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). Money or other property is an instrument of crime if it is used (or used to facilitate) in the commission of an offence against such a law.

Offences contained in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act) are also used in prosecuting money laundering offences.

The offences at a state and territory level differ according to areas such as relevant predicate offences, the intent of the defendant and penalties attached to the offences.

Financial institutions generally cannot be prosecuted for their customers' money laundering crimes (unless the elements of the offence can otherwise be established). However, crimes committed by customers may cause financial institutions to contravene a regulatory offence under the AML/CTF Act should the offending conduct not be appropriately identified and managed (eg, by failing to report a suspicious matter).

Law stated - 19 May 2023

Qualifying assets and transactions

Is there any limitation on the types of assets or transactions that can form the basis of a money laundering offence?

Provided that the elements of the offence are present, there is no limitation on the types of assets or transactions, and no monetary threshold, for money laundering to constitute an offence. However, increasing penalties apply under the Criminal Code as the value of the money or property that is the subject of the offence increases.

Law stated - 19 May 2023

Predicate offences

Generally, what constitute predicate offences?

The Criminal Code does not limit predicate offences with a specific list and criminal infringements of state, territory or foreign indictable offences can constitute predicate offences. Predicate offences vary between the state and territory levels.

In Australia, the main predicate offences to money laundering are drug-related offences, fraud, tax evasion, people smuggling, theft, arms trafficking and corrupt practices. Criminal infringements of laws of other jurisdictions can serve as predicate offences; however, the 2015 Financial Action Task Force assessment report of Australia's AML regime found that money laundering offences involving proceeds of foreign offences are not frequently prosecuted because Australia does not consider that foreign predicate offences are major such offences for money laundering in Australia.

Law stated - 19 May 2023

Defences

Are there any codified or common law defences to charges of money laundering?

For money laundering offences where there is a stated monetary or property value, or property reasonably suspected of being proceeds of crime, a defence of mistake of fact as to the value of money or property is available. This defence applies if, at or before the time of dealing with the money or property, the person considered what the value was and was under a mistaken but reasonable belief about that value. In this scenario, the defendant has the burden of proof and, if relied upon, the relevant offence will be that which is for the value of the money or property that the defendant believed.

The AML/CTF Act also contains a defence to proceedings for an offence against the regulations to that Act, a contravention of a civil penalty provision under that Act or proceedings under the Proceeds of Crime Act 2002 (Cth) (the POC Act) that relate to the AML/CTF Act where the defendant proves reasonable precautions were taken, and due diligence exercised, to avoid such contravention.

Law stated - 19 May 2023

Resolutions and sanctions

What is the range of outcomes in criminal money laundering cases?

The possible outcomes in criminal money laundering cases range from six months' to life imprisonment. Monetary penalties may be imposed on natural and non-natural persons, ranging from 10 penalty units (currently A\$2,750) to 1,500 penalty units (currently A\$417,500). Under current legislation, the value of penalty units will automatically increase in line with the consumer price index from 1 July 2023.

The levels of outcomes in criminal money laundering cases depend on the value of the money or property involved. The range of potential outcomes is also dependent on the defendant's state of mind, as different penalties exist based on whether the dealing with the proceeds of crime was done so intentionally, recklessly or negligently (reflective of a scale of most to least severe). For example, the Criminal Code states that the maximum penalty for an AML offence relating to money or property with a value of A\$10,000 or more is 10 years' imprisonment if committed intentionally, five years' imprisonment if committed recklessly and two years' imprisonment if committed negligently.

The CDPP may also seek to wind up offending companies.

Forfeiture

Describe any related asset freezing, forfeiture, disgorgement and victim compensation laws.

Under the POC Act, a freezing order can be made by a magistrate against an account with a financial institution if:

- there are reasonable grounds to suspect that the balance of the account is proceeds of a particular offence, or it is wholly or partly an instrument of a serious offence; and
- there is a risk that the account's balance will be reduced so that a person will not be deprived of all or some of such proceeds or such an instrument.

The POC Act also enables forfeiture orders to be made under which property must be surrendered to the government if certain offences have been committed.

Both the freezing and forfeiture orders are part of the POC Act's implementation of a confiscation scheme, which outlines processes relating to confiscation that also include restraining orders (prohibiting disposal of or dealing with property) and pecuniary penalty orders (requiring payment of amounts based on benefits derived from committing offences). The POC Act also has provisions that outline ways in which information can be gathered, such as examining any person about the affairs of people covered by the examination orders and requiring financial institutions to provide information and documents relating to accounts and transactions.

Similar legislation has been enacted in the states and territories of Australia that relates to making such orders and confiscation of profits and other proceeds of crime.

Law stated - 19 May 2023

Limitation periods on money laundering prosecutions

What are the limitation periods governing money laundering prosecutions?

The Crimes Act 1914 (Cth) sets out a time limit for the CDPP to bring proceedings. This limit is one year after the commission of a money laundering offence where the maximum term of imprisonment for an individual is six months or less, or the maximum penalty for a body corporate is 150 penalty units or less. These are generally money laundering offences where the value of the money or property is low and the fault element consists of recklessness or negligence. There is a six-year limitation period applicable to civil prosecutions under the AML/CTF Act.

Law stated - 19 May 2023

Extraterritorial reach of money laundering law

Do the money laundering laws applicable in your jurisdiction have extraterritorial reach?

Australia's criminal money laundering laws have extraterritorial application under the Criminal Code and apply where:

- the relevant conduct constituting the alleged offence occurs;
- wholly or partly in Australia, or on board an Australian aircraft or ship;
- wholly outside Australia and the money or other property is proceeds of indictable crime, or is likely to become or at risk of becoming an instrument of crime, in relation to a Commonwealth, state or territory indictable offence;

- wholly outside Australia and the money or other property is proceeds of general crime in relation to a Commonwealth, state or territory law;
- wholly outside Australia and the person is an Australian citizen, resident or corporation; or
- the alleged offence is an ancillary offence occurring wholly outside of Australia and the conduct constituting the primary offence occurs wholly or partly in Australia, or on board an Australian aircraft or ship.

Law stated - 19 May 2023

AML REQUIREMENTS FOR COVERED INSTITUTIONS AND INDIVIDUALS

Enforcement and regulation

Which government entities enforce the AML regime and regulate covered institutions and persons in your jurisdiction? Do the AML rules provide for ongoing and periodic assessments of covered institutions and persons?

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's financial intelligence agency with regulatory responsibility for AML and counter-terrorist financing. AUSTRAC administers the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act).

AUSTRAC has several Commonwealth, state and territory partner agencies, including the Australian Federal Police, the Australian Criminal Intelligence Commission and the Australian Securities and Investments Commission.

Entities regulated by the AML/CTF Act (reporting entities) are required to comply with reporting obligations, including submitting to AUSTRAC an annual compliance report confirming compliance or identifying instances of non-compliance with the AML/CTF Act. AUSTRAC has information-gathering powers under the AML/CTF Act, and reporting entities have an obligation to adopt procedures to apply any feedback and recommendations received from AUSTRAC as a result of surveillance or assessment.

Law stated - 19 May 2023

Covered institutions and persons

Which institutions and persons must have AML measures in place?

Broadly, the AML/CTF Act regulates reporting entities, which are defined in the Act as persons who provide a designated service (also as defined in the Act). Designated services include financial, bullion and gambling services. The AML/CTF Act was amended in 2017 to include digital currency exchange providers within the scope of providing a designated service.

The AML/CTF Act regulates only those designated services with a connection to Australia, referred to as the geographical link test. The test will be satisfied where:

- the designated service is provided to the customer at or through a permanent establishment of the reporting entity (including any place where it carries on business through an agent) in Australia; or
- the reporting entity is a resident of Australia and the designated service is provided at or through a permanent establishment of the reporting entity in a foreign country, or the reporting entity is a subsidiary of an Australian company and the service is provided at or through a permanent establishment of the subsidiary in a foreign country.

Where the AML/CTF Act applies, reporting entities' obligations include:

- enrolling with AUSTRAC;
- adopting and maintaining a compliant AML and counter-terrorist financing programme (AML/CTF programme);
- conducting customer due diligence (CDD) procedures; and
- reporting to AUSTRAC annually, and as required, on the occurrence of suspicious matters, threshold transactions of A\$10,000 or more, all international funds transfer instructions and record-keeping.

Law stated - 19 May 2023

Compliance

Do the AML laws applicable in your jurisdiction require covered institutions and persons to implement AML compliance programmes? What are the required elements of such programmes?

Under the AML/CTF Act, reporting entities must adopt and maintain an AML/CTF programme that complies with the AML/CTF Act and the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth).

AML/CTF programmes are risk-based and relate to the size and nature of each business, the designated services offered to and its money laundering or terrorism financing (ML/TF) risk profile. Reporting entities must develop and document an AML/CTF programme that is tailored to their specific business needs and is proportionate to the level of ML/TF risk that their businesses face.

An AML/CTF programme generally comprises two parts: Part A and Part B.

The primary purpose of Part A is to identify, mitigate and manage the ML/TF risks arising from the provision of a designated service by a reporting entity. It includes:

- an ML/TF financing risk assessment, which must be periodically reviewed and updated;
- approval and ongoing oversight by boards and senior management;
- appointment of a compliance officer;
- regular independent review of Part A;
- a due diligence programme for employees;
- a risk awareness training programme for employees;
- procedures to respond to and apply AUSTRAC feedback;
- systems and controls to ensure compliance with reporting obligations; and
- ongoing CDD procedures.

Part B of the AML/CTF programme includes a framework to ensure the reporting entity is reasonably satisfied that:

- an individual customer is who they claim to be;
- for a non-individual customer, the customer exists and their beneficial ownership details are known; and
- procedures for collecting and verifying customer and beneficial owner information.

Law stated - 19 May 2023

Breach of AML requirements

What constitutes breach of AML duties imposed by the law?

The AML/CTF Act sets forth that producing false or misleading information or documentation, forging documentation for use in customer identification procedures, providing or receiving a designated service using a false customer name

or customer anonymity, or structuring a transaction to avoid a reporting obligation under the AML/CTF Act are offences. Further, contraventions of obligations under the AML/CTF Act generally result in civil penalty provisions. For example, if a reporting entity provides a designated service to a customer prior to adopting, or where it does not maintain, a compliant AML/CTF programme, that entity has breached a civil penalty provision.

Where a reporting entity has formed a suspicion about a customer, or has submitted a suspicious matter report (SMR) to AUSTRAC about a customer, the AML/CTF Act generally prohibits the reporting entity from disclosing that suspicion or report to the customer. Disclosing such a suspicion or report would constitute the offence of tipping off under the AML/CTF Act.

Law stated - 19 May 2023

Customer and business partner due diligence

Describe due diligence requirements in your jurisdiction's AML regime.

The AML/CTF Act generally requires that a reporting entity adopt and maintain an AML/CTF programme, comprising Part A and Part B.

With respect to due diligence procedures, Part A of an AML/CTF programme must contain an employee due diligence programme that documents procedures for screening staff members to minimise any exposure to risk. The procedures must set out appropriate risk-based systems and controls for the reporting entity to determine whether to screen a prospective employee or rescreen an existing employee (eg, where such employee is promoted or transferred and may be in a position to facilitate the commission of a money laundering or terrorism financing offence). The procedures should enable a reporting entity to identify and verify the identity of prospective or existing employees, confirm their employment history and determine if they are suitable to be employed in a particular position in the business. The procedures should take into account the role of the employee and the nature, size and complexity of the business, and the type of risk it might reasonably face. Additionally, the AML/CTF programme should outline policies for managing employees who fail to comply with any system, control or procedure under the programme.

The primary purpose of Part B is to ensure the reporting entity knows its customers and understands its customers' financial activities. The reporting entity must establish a framework and document its CDD procedures in detail. The purpose of undertaking CDD procedures is to enable the reporting entity to be reasonably satisfied that, in relation to an individual customer, the customer is who they claim to be and, in relation to a non-individual customer, the customer exists and its beneficial ownership details are known.

Broadly, the CDD requirements include:

- collecting and verifying customer identification information;
- identifying and verifying the beneficial owners of a customer;
- identifying whether a customer is a politically exposed person (PEP) (or an associate of a PEP) and establishing the source of funds used during the business relationship or transaction; and
- gathering information on the purpose and intended nature of the business relationship.

The minimum customer information a reporting entity must collect and verify will depend on the type of customer it is dealing with, as prescribed in the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth). The method of verification will also depend on the customer type, but must come from a reliable and independent source.

Part A of an AML/CTF programme must also contain the reporting entity's ongoing customer due diligence (OCDD)

procedures. Reporting entities are required to have in place appropriate OCDD systems and controls to determine whether additional customer information (including beneficial owner information) should be collected or verified on an ongoing basis to ensure that the reporting entity holds up-to-date information about its customers. The decision to apply the OCDD process to a particular customer depends on the customer's level of assessed ML/TF risk.

The OCDD procedures should include implementing a transaction monitoring programme and developing an enhanced CDD programme. The transaction monitoring programme is a risk-based programme of systems and controls to monitor transactions, which is capable of identifying complex transactions, unusually large transactions and unusual patterns of transactions. The enhanced CDD programme is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.

Law stated - 19 May 2023

High-risk categories of customers, business partners and transactions

Do the AML rules applicable in your jurisdiction require that covered institutions and persons conduct risk-based analyses? Which high-risk categories are specified? What level of due diligence is expected in relation to customers assessed to be high risk?

The AML/CTF Act requires reporting entities to undertake a money laundering and terrorism financing risk assessment to measure the level of risk associated with providing each designated service. In particular, a reporting entity must consider the risk posed by:

- customer types, including any customers who are PEPs and their associates;
- the types of designated services it provides;
- how the entity provides its designated services (eg, over the counter or online); and
- the foreign jurisdictions with which it operates or conducts business.

The Australian government has declared via regulations to the AML/CTF Act that Iran and North Korea are prescribed foreign countries for the purposes of the AML/CTF Act and are subject to countermeasures, including enhanced CDD obligations and certain prohibitions on dealings.

Other than in relation to prescribed foreign countries, the AML/CTF Act does not specify high-risk categories of customers or designated services. Rather, it is up to the reporting entity to determine whether a particular designated service or customer is high risk. The risk level determines the risk-based customer identification procedures to be conducted, including whether enhanced CDD procedures will be undertaken and additional identification information collected and verified. Reporting obligations may also apply depending on the nature of a transaction.

For all foreign PEPs and high-risk domestic or international organisation PEPs, reporting entities must closely monitor the transactions conducted by that customer. If a reporting entity suspects that a transaction undertaken by a PEP involves funds that are the proceeds of corruption or other criminal activity, it must submit a SMR to AUSTRAC.

Law stated - 19 May 2023

Record-keeping and reporting requirements

Describe the record-keeping and reporting requirements for covered institutions and persons.

Record-keeping requirements

Reporting entities have record-keeping obligations under the AML/CTF Act. The types of records to be kept depend on the type of designated service provided. Specifically, the types of records that must be retained are records of or about:

- transactions;
- identification procedures;
- electronic funds transfer instructions;
- AML/CTF programmes; and
- due diligence assessments of correspondent banking relationships.

Reporting requirements

The AML/CTF Act creates five reporting obligations:

- annual compliance reports;
- SMRs;
- threshold transaction reports;
- international funds transfer instruction reports; and
- cross-border movement reports.

Annual compliance report

All reporting entities must submit an annual compliance report, unless an exemption applies. Reports are due annually by 31 March, relating to the prior reporting (calendar) year.

Suspicious matter report

The obligation to submit an SMR arises where, in the course of a dealing with a customer, a reporting entity forms a suspicion (on reasonable grounds) that:

- the customer is not who they claim to be;
- information the reporting entity has may be:
 - relevant to investigate or prosecute a person for an evasion of tax law or an offence against a Commonwealth, state or territory law; or
 - of assistance enforcing the Proceeds of Crime Act 2002 (Cth) or a corresponding state or territory legislation; and
- providing a designated service may be:
 - preparatory to committing an offence related to money laundering or terrorism financing; or
 - relevant to the investigation or prosecution of a person for an offence related to money laundering or terrorism financing.

The report must include details about the reporting entity's business, the suspicious matter, the persons to which the matter relates and any related transactions. The report must be submitted within 24 hours of the time the suspicion is formed if relating to terrorism financing. If in relation to any other offence, the relevant reporting time frame is three business days after the day in which the relevant suspicion was formed.

Threshold transaction report

If a reporting entity commences providing, or provides, a designated service to a customer that involves a transfer of physical or digital currency of A\$10,000 or more (or foreign currency equivalent), they must submit a threshold transaction report to AUSTRAC within 10 business days of the day in which the transaction occurred. The threshold transaction report must include the business details of the reporting entity, the customer of the designated service and further details of the transaction, including cash, digital currency and other components.

International funds transfer instruction

A reporting entity that sends an international funds transfer instruction transmitted out of Australia or receives such an instruction transmitted into Australia must report the instruction to AUSTRAC within 10 business days of the day in which the instruction was sent or received.

Cross-border movement reports

All persons, including reporting entities, must report cross-border movements of physical currency of A\$10,000 or more. Such a report must be made before currency is sent or carried out of or into Australia, or within five business days of receiving currency sent into Australia. In addition, if requested by a police or customs officer, a person may be required to give AUSTRAC or the relevant officer a report immediately about any cross-border movement of bearer negotiable instruments (eg, cheques or money orders) of any amount.

Law stated - 19 May 2023

Privacy laws

Describe any privacy laws that affect record-keeping requirements, due diligence efforts and information sharing.

The Privacy Act 1988 (Cth) (the Privacy Act) regulates the handling of personal information by Australian government agencies, Australian Capital Territory agencies and private sector organisations with an aggregate group revenue of at least A\$3 million. The Privacy Act also applies to all reporting entities under the AML/CTF Act regardless of turnover.

The Privacy Act includes 13 Australian Privacy Principles, which create obligations on the collection, use, disclosure, retention and destruction of personal information. The Australian Privacy Principles include:

- open and transparent management of personal information;
- disclosure to a person that their personal information will be collected;
- restrictions on the use and disclosure of personal information;
- obligations to ensure the accuracy of collected personal information; and
- obligations to protect personal information.

Personal information means information or an opinion about an identified individual, or one who is reasonably identifiable whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

The effect of this is that information collected about an individual in the course of undertaking CDD procedures would generally constitute personal information for the purposes of the Privacy Act, and requires that reporting entities

comply with the Privacy Act in relation to personal information collected from customers, personal information recorded by reporting entities and personal information shared with other entities.

Where there has been a breach of data (ie, unauthorised access to or disclosure of information), the Notifiable Data Breaches scheme (introduced in February 2018) requires entities regulated under the Privacy Act to notify any affected individuals and the Office of the Australian Information Commissioner where the breach is likely to result in serious harm to those individuals. The Notifiable Data Breaches scheme applies to agencies and organisations if the Privacy Act requires them to take steps to secure certain categories of personal information.

In addition to complying with the Privacy Act as it relates to the collection, use and handling of personal information, reporting entities must comply with the AML/CTF Act with respect to disclosure of personal information to credit reporting bodies. The AML/CTF Act authorises the use and disclosure of certain personal information held by a credit reporting body to a reporting entity for the purposes of verifying the individual's identity under the AML/CTF Act, provided that the reporting entity discloses certain information to the customer and obtains the customer's express consent prior to disclosing such information.

Law stated - 19 May 2023

Resolutions and sanctions

What is the range of outcomes in AML controversies? What are the possible sanctions for breach of AML laws?

There are a variety of enforcement outcomes that AUSTRAC can pursue in the event of non-compliance with the AML/CTF Act. These include:

- seeking civil penalty orders under the AML/CTF Act and, if the Federal Court of Australia is satisfied that a reporting entity has contravened a civil penalty provision, a pecuniary penalty may be payable to the government (as at May 2023, the maximum pecuniary penalty for bodies corporate is A\$27.5 million, and A\$5.5 million for individuals and other entities);
- accepting an enforceable undertaking, which is a written undertaking that is enforceable in court and used as an alternative to civil or administrative action;
- issuing an infringement notice, whereby payment of the specified penalty will discharge any liability and no criminal or civil penalty proceedings will be brought;
- issuing a remedial direction, which requires a reporting entity to take specified action to ensure that it does not contravene a civil penalty provision in the future; and
- requiring that a reporting entity take certain actions in relation to auditing (eg, appointing an external auditor and arranging for an audit report).

Law stated - 19 May 2023

Limitation periods for AML enforcement

What are the limitation periods governing AML matters?

Proceedings for a civil penalty order under the AML/CTF Act must be commenced no later than six years after the date of contravention.

Law stated - 19 May 2023

Extraterritoriality

Do your jurisdiction's AML laws have extraterritorial reach?

The AML/CTF Act states that, unless the contrary is provided in the Act, it extends to acts, omissions, matters and things outside Australia. However, a geographical link to Australia, with respect to the relevant designated service, must be present.

Law stated - 19 May 2023

CIVIL CLAIMS

Procedure

Enumerate and describe the required elements of a civil claim or private right of action against money launderers and covered institutions and persons in breach of AML laws.

There is no right to bring a civil claim or private action for a breach of AML laws.

Law stated - 19 May 2023

Damages

How are damages calculated?

Not applicable.

Law stated - 19 May 2023

Other remedies

What other remedies may be awarded to successful claimants?

Not applicable.

Law stated - 19 May 2023

INTERNATIONAL MONEY LAUNDERING EFFORTS

Supranational

List your jurisdiction's memberships of supranational organisations that address money laundering.

Australia is a member of the following supranational organisations:

- the Financial Action Task Force (FATF);
- the Egmont Group of Financial Intelligence Units; and
- the Asia/Pacific Group on Money Laundering.

Australia also has observer status within the Middle East and North Africa Financial Action Task Force and the Eastern and Southern Africa Anti-Money Laundering Group.

Law stated - 19 May 2023

Anti-money laundering assessments

Give details of any assessments of your jurisdiction's money laundering regime conducted by virtue of your membership of supranational organisations.

Over the course of 2013 and 2014, the FATF commenced its assessment of Australia's AML and counter-terrorist financing (AML/CTF) regime. A joint evaluation report by the FATF and the Asia/Pacific Group on Money Laundering was published in April 2015. The assessment tested Australia's AML/CTF regime against the 40 FATF recommendations. Australia was one of the first FATF member economies to be subject to a mutual assessment.

The report found Australia was compliant with only 24 of the 40 FATF recommendations. Key findings included that:

- Australia failed to implement the second tranche of AML/CTF regulation covering non-financial businesses and professional sectors (other than gaming and bullion);
- the enforcement and supervision powers of the Australian Transaction Reports and Analysis Centre (AUSTRAC) should be more effective; and
- major reporting entities (including the big four domestic banks) had a good understanding of AML/CTF risks and obligations, but some controls were found to be misaligned with FATF standards.

Australia achieved high results with respect to international cooperation and substantial results in risk, policy and coordination, the use of financial intelligence and combating terrorist financing and proliferation financing.

Following the assessment and publication of the report, the Attorney-General's Department undertook a statutory review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act) to address the recommendations. A report was tabled before Parliament in April 2016.

In November 2018, the FATF published its third report in response to Australia's progress in addressing the technical compliance deficiencies identified in the mutual evaluation report. Australia has been re-rated on the following key recommendations:

- Australia's responsibilities of law enforcement and investigative authorities rating improved from largely compliant to compliant;
- Australia enhanced due diligence with high-risk countries, increasing the rating from partially compliant to largely compliant; and
- Australia improved from largely complaint to compliant after assessing the money laundering risks associated with new products and technologies.

Law stated - 19 May 2023

FIUs

Give details of your jurisdiction's Financial Intelligence Unit (FIU).

AUSTRAC is Australia's Financial Intelligence Unit. It has several offices throughout Australia. The address of its Sydney office is :

AUSTRAC

Level 23, 323 Castlereagh Street

Haymarket

NSW 2000

Australia

International callers can reach the AUSTRAC Contact Centre on +61 2 9950 0055 or via email at contact@austrac.gov.au. Callers in Australia can reach the Centre on 1300 021 037.

Law stated - 19 May 2023

Mutual legal assistance

In which circumstances will your jurisdiction provide mutual legal assistance with respect to money laundering investigations? What are your jurisdiction's policies and procedures with respect to requests from foreign countries for identifying, freezing and seizing assets?

Australia can make requests to any foreign country, and can receive requests from any foreign country, for mutual assistance in criminal investigations and prosecution, including to recover the proceeds of crime. Australia's response to such requests can include executing search warrants to obtain evidence (eg, bank records from financial institutions), taking evidence from a witness for foreign proceedings, arranging for travel for witnesses, and registering and enforcing orders (including restraining and forfeiting proceeds of crime).

Australia has numerous international exchange instruments that outline the sharing of financial intelligence information between regulators, including AUSTRAC and Financial Intelligence Units in foreign jurisdictions. These arrangements are generally effected through memorandums of understanding as well as through letters and statements of cooperation. There are also informal channels between regulators and law enforcement bodies.

The Mutual Assistance in Criminal Matters Act 1987 (Cth) (the MACM Act) is aimed at regulating the provision of international assistance by Australia in criminal matters when a foreign country makes a request, as well as facilitating the obtaining of international assistance by Australia in criminal matters. There are several provisions in the MACM Act that specifically deal with the recovery of property through the registration and enforcement of foreign orders in Australia, including enforcement of foreign forfeiture orders, pecuniary penalty orders, restraining orders, production orders, monitoring orders and search warrants relating to foreign serious offences.

The Mutual Assistance in Business Regulation Act 1992 (Cth) also intends to enable Commonwealth regulators to assist foreign regulators in their administration of foreign business laws by obtaining relevant information and evidence and transmitting this information to foreign regulators. In the context of AML laws, this includes Commonwealth regulators such as the Australian Securities and Investments Commission and the Australian Prudential Regulation Authority, which are relevant in the designated services surrounding financial services institutions.

The process for providing mutual legal assistance generally begins with an assessment by the Attorney-General's Department as to the nature of the request received, and consideration against the mandatory and discretionary grounds for refusal set out in the MACM Act, the relevant treaty and government policy. Assistance may be refused where the request relates to punishment of a person for a political offence, or where granting the request would

prejudice the sovereignty, security or national interest of Australia or essential interests of a state or territory.

Under the AML/CTF Act, AUSTRAC's chief executive officer may also communicate information to the government of a foreign country if they are satisfied that the foreign country's government has given appropriate undertakings regarding the confidentiality, use and purpose of the information, as well as the AUSTRAC information being appropriate in all circumstances to be communicated to the foreign government. AUSTRAC's chief executive officer may also authorise the Commissioner of the Australian Federal Police to have access to AUSTRAC information for the purposes of communicating it to a foreign law enforcement agency.

Law stated - 19 May 2023

UPDATE AND TRENDS

Enforcement and compliance

Describe any national trends in criminal money laundering schemes and enforcement efforts.

Describe any national trends in AML enforcement and regulation. Describe current best practices in the compliance arena for companies and financial institutions.

Review of Australian regime

In April 2023, the Attorney-General announced a public consultation on proposed reforms to Australia's AML and counter-terrorist financing (AML/CTF) financing regime. The proposed reforms include extending the existing AML/CTF legislation to capture additional tranche-two, high-risk entities that are designated non-financial businesses and professions, including:

- lawyers;
- accountants;
- trust and company service providers;
- real estate agents; and
- dealers in precious metals and stones.

These proposed reforms were part of the recommendations in the Senate Standing Committee on Legal and Constitutional Affairs' report on the adequacy and efficacy of Australia's AML/CTF financing regime, published in March 2022. The report recommends changes to bring Australia's regime in line with the Financial Action Task Force's recommendations.

Submissions to the resulting Consultation Paper are due by June 2023 and feedback received will be used to inform subsequent drafting of the reforms over the course of the year. A second consultation paper is expected to be released in late 2023.

Digital assets regulation

The Australian Transaction Reports and Analysis Centre (AUSTRAC) began regulating digital currency exchange providers in April 2018, making Australia one of the first countries to regulate them for AML/CTF purposes. However, in January 2022, AUSTRAC's chief executive officer made statements referring to the challenges and regulatory blind spots in regulating cryptocurrency providers (and businesses providing services to such providers).








In October 2021, the Senate Select Committee on Australia as a Technology and Financial Centre released its final report. The report includes recommendations addressing the lack of fit-for-purpose regulation of cryptocurrencies and

digital assets, and issues relating to the practice of de-banking of crypto and digital assets businesses under the guise of compliance with AML/CTF requirements.

The resulting 2023 Consultation Paper acknowledges that the current AML/CTF regime must be reformed to respond to risks in the digital assets sector. The paper proposes that reforms could include expansion of the regulation of the types of services to cover exchanges between digital currencies; transfers of digital currency on behalf of customers; safekeeping or administration of digital currency; and provision of financial services related to an issuer's offer or sale of a digital currency.

Law stated - 19 May 2023

Jurisdictions

	Australia	Gilbert + Tobin
	Bulgaria	New Balkans Law Office
	Denmark	Poul Schmith/Kammeradvokaten
	Germany	Park Wirtschaftsstrafrecht
	Greece	ANAGNOSTOPOULOS
	Hong Kong	Herbert Smith Freehills LLP
	India	AZB & Partners
	Italy	Studio Legale Pisano
	Japan	Anderson Mōri & Tomotsune
	Luxembourg	Allen & Overy LLP
	South Korea	Yoon & Yang LLC
	Switzerland	Homburger
	United Kingdom	White & Case
	USA	Gibson Dunn & Crutcher LLP