

Anti-Money Laundering

Consulting editor
Barry Vitou



2018

GETTING THE
DEAL THROUGH 

GETTING THE
DEAL THROUGH 

Anti-Money Laundering 2018

Consulting editor

Barry Vitou

Pinsent Masons LLP

Reproduced with permission from Law Business Research Ltd

This article was first published in May 2018

For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com



Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

© Law Business Research Ltd 2018
No photocopying without a CLA licence.
First published 2012
Seventh edition
ISBN 978-1-912377-50-3

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between March and April 2018. Be advised that this is a developing area.

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112



CONTENTS

Australia	5	Nigeria	67
Peter Reeves and Georgina Willcock Gilbert + Tobin		Babajide O Ogundipe and Chukwuma Ezediaro Sofunde, Osakwe, Ogundipe & Belgore	
Chile	12	Portugal	72
Jorge Bofill, Daniel Praetorius and Libertad Triviño Bofill Escobar Abogados		Hélder Frias and Manuel Barbosa Moura Úria Menéndez – Proença de Carvalho	
France	18	Russia	79
Arut Kannan, Jean-Baptiste Poulle and Rudolf Efremov Spitz Poulle Kannan AARPI		Vasily Torkanovskiy Ivanyan & Partners	
Greece	24	Singapore	86
Ilias G Anagnostopoulos and Jerina (Gerasimoula) Zapanti Anagnostopoulos Criminal Law & Litigation		Eric Chan and Agnes Lim Shook Lin & Bok LLP	
India	30	Switzerland	93
Aditya Bhat and Pankhuri Govil AZB & Partners		Flavio Romerio and Katrin Ivell Homburger	
Italy	41	United Arab Emirates	99
Roberto Pisano, Valeria Acca and Chiara Cimino Studio Legale Pisano		Ibtissem Lassoued Al Tamimi & Co	
Japan	49	United Kingdom	105
Yoshihiro Kai Anderson Mōri & Tomotsune		Anne-Marie Ottaway, Michael Ruck, Elena Elia and Jenny Burton Pinsent Masons LLP	
Korea	54	United States	113
Soonghee Lee, Ju Yong Lee, Bo Hyun Lee and Hye Jin Hwang Yoon & Yang LLC		Gregory C Lisa, Peter S Spivack and Ashley Hutto-Schultz Hogan Lovells US LLP	
Luxembourg	60		
Laurent Lenert Kayser, Lenert & Becker, Avocats à la Cour			

Preface

Anti-Money Laundering 2018

Seventh edition

Getting the Deal Through is delighted to publish the seventh edition of *Anti-Money Laundering*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Chile, Korea and Portugal.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the consulting editor, Barry Vitou of Pinsent Masons LLP, for his assistance with this volume. We also extend special thanks to Lamia R Matta, Leila Babaeva and Ann K Sultan of Miller & Chevalier Chartered, who contributed the original format from which the current questionnaire has been derived, and who helped to shape the publication to date.

GETTING THE 
DEAL THROUGH

London
April 2018

Australia

Peter Reeves and Georgina Willcock

Gilbert + Tobin

Domestic legislation

1 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 legislative regime for detecting, prosecuting and deterring money laundering activities consists of:

- criminal offences for money laundering at both the Commonwealth and state or territory levels;
- asset recovery legislation at both 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 Federal Criminal Code Act 1995 (Cth) (Criminal Code) 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) (POC Act), which enables law enforcement to pursue the recovery of assets linked to offences after a conviction. Each Australian state and territory also has 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) (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) (AML/CTF Rules) and associated regulations, each of which are made under the AML/CTF Act.

The Financial Transaction Reports Act 1988 (Cth) (FTR Act) operates alongside the AML/CTF Act. The FTR Act 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 (AUSTRAC), and also requires cash dealers to verify the identity of account signatories.

Sanction laws comprise part of Australia's AML legislative framework. Australia implements the United Nations Security Council sanctions regime under the Charter of the United Nations Act 1945 and 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 sanction laws establish serious criminal offences, and penalties include up to 10 years in prison and substantial fines.

2 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 both the Commonwealth and state and territory levels. At the Commonwealth level, Part 2-6 of the

POC Act contains the unexplained wealth provisions, where targets of these orders 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 a state offence that has a federal aspect.

The following states have also enacted unexplained wealth laws. Only the Australian Capital Territory has yet to implement specific provisions relating to unexplained wealth under the Confiscation of Criminal Assets Act 2003 (ACT).

New South Wales

The New South Wales (NSW) Crime Commission is responsible for obtaining unexplained wealth orders from the Supreme Court of NSW under the Criminal Assets Recovery Act 1990 (NSW). In granting the order, the court must have a reasonable suspicion that the person against whom the order is sought has engaged in a serious crime-related activity or acquired property derived from any serious crime-related activity of another person (whether or not the person against whom the order is made knew or suspected this). A finding under this section need not be based on a reasonable suspicion as to the commission of a particular offence and can be based on a reasonable suspicion that some offence constituting a serious crime-related activity was committed.

Northern Territory

The Director of Public Prosecution (DPP) may apply to the Supreme Court of the Northern Territory for an unexplained wealth declaration where the value of the person's total wealth is greater than the value of the person's lawfully acquired wealth. The onus is placed on the person against whom the unexplained wealth declaration was sought.

Queensland

Under Part 5A of the Criminal Proceeds Confiscation Act 2002 (Queensland), the state may apply to the Supreme Court of Queensland for an unexplained wealth order, which may be granted if the court is satisfied that there is a reasonable suspicion that the person has engaged in a serious crime-related activity or has acquired property derived from a serious crime-related activity without sufficient consideration (even if the person did not know or suspect the property was derived from illegal activity).

South Australia

The DPP may authorise the Crown Solicitor to apply for an unexplained wealth order under the Serious and Organised Crime (Unexplained Wealth) Act 2009 (South Australia) if the DPP reasonably suspects that a person has wealth that has not been lawfully acquired.

Tasmania

Part 9 of the Tasmanian Crime (Confiscation of Profits) Act 1993 empowers the Supreme Court of Tasmania to make unexplained wealth declarations. There is a general presumption that any part of a person's wealth is presumed not to have been lawfully acquired by the person unless the person proves otherwise under the declaration.

Victoria

The DPP or another appropriate officer may apply for an unexplained wealth restraining order under the Confiscation Act 1997 (Victoria). In respect of property located outside of Victoria, an unexplained wealth

restraining order can be made where a police officer reasonably suspects that a person has engaged in serious criminal activity, that the person has an interest in the property, the criminal activity happened within Victoria and the total value of the property is A\$50,000 or more. For property located in Victoria, the DPP may apply for an unexplained wealth order if a police officer suspects on reasonable grounds that the property was not lawfully acquired and either the property is located in Victoria or the person who has acquired the property is ordinarily a resident in Victoria.

Western Australia

Western Australia (WA)'s unexplained wealth regime is established by the Criminal Property Confiscation Act 2000 (WA). The DPP may apply to the Supreme Court of WA for an unexplained wealth declaration against a person where it is more likely than not that the total value of the person's wealth is greater than the value of the person's lawfully acquired wealth. The person against whom the order is sought bears the onus of proof and the DPP does not need to prove reasonable grounds for suspecting that the person committed an offence.

Money laundering

3 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. AUSTRAC, the Australian Federal Police (AFP) and the Department of Home Affairs act as partner agencies to the CDPP in prosecuting money laundering offences. The AFP also leads the Criminal Assets Confiscation Taskforce, which collaborates with other agencies to 'identify, investigate and litigate' asset confiscation matters at the Commonwealth level.

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

4 Defendants

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

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

5 The offence of money laundering

What constitutes money laundering?

The relevant division of the Criminal Code creates multiple offences that encompass a wide range of criminal activity. The offences are based on a person dealing with money or property which 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 - being physical conduct such as possessing the money or property, concealing or disposing it or engaging in banking transactions;
- such dealing in money or property is 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 the money was the proceeds of a crime or was reckless or negligent about that fact.

A person commits an offence of money laundering if the person deals 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:

- intentional - 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;
- reckless - 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
- negligent - 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.

Owing to the state of mind element, a strict liability standard does not apply.

'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. 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 AML/CTF Act (see question 16) are also often used in prosecuting money laundering.

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).

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

7 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 a predicate offence. Predicate offences do vary at the state and territory level.

In Australia, the three main predicate offences to money laundering are drugs, fraud and tax evasion. Criminal infringements of laws of other jurisdictions can serve as predicate offences; however, the 2015 Foreign 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 predicates for money laundering in Australia.

8 Defences

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

For money laundering offences where there is a stated money or property value of A\$1,000 or more, 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.

Other defences apply where the defendant is able to prove the relevant geographical connection was not present in relation to the alleged offence.

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 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.

9 Resolutions and sanctions

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

Broadly, the possible outcomes in criminal money laundering cases range from 25 years' to six months' imprisonment. Monetary penalties may be imposed on natural and non-natural persons, ranging from 1,500 penalty units (currently A\$315,000) to 10 penalty units (currently A\$2,100). It is anticipated that the penalty units will be reviewed in late 2018, and the value of penalty units is increased annually from 1 July.

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 severe 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 done so intentionally, five years' imprisonment if done so recklessly and two years' imprisonment if done so negligently.

The CDPP may also seek to wind up offending companies.

10 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, forfeiting property to the Commonwealth 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.

11 Limitation periods

What are the limitation periods governing money laundering prosecutions?

Under Australia's Commonwealth and state and territory laws, there are generally no time limitations for when prosecutions can be brought for indictable criminal offences, such as money laundering.

12 Extraterritorial reach

Do your jurisdiction's money laundering laws have extraterritorial reach?

Australia's criminal money laundering laws apply where:

- the relevant conduct constituting the alleged offence occurs wholly or partly in Australia or on board an Australian aircraft or ship;

- the relevant conduct constituting the alleged offence occurs wholly outside Australia and the money or other property is proceeds of 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;
- the relevant conduct constituting the alleged offence occurs 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.

AML requirements for covered institutions and individuals

13 Enforcement and regulation

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

AUSTRAC is Australia's financial intelligence agency with regulatory responsibility for anti-money laundering and counter terrorism financing. AUSTRAC administers the AML/CTF Act.

AUSTRAC has several federal, state and territory partner agencies, including the AFP, the Australian Crime Commission and the Australian Securities and Investments Commission (ASIC).

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.

14 Covered institutions and persons

Which institutions and persons must carry out AML measures?

Broadly, the AML/CTF Act regulates reporting entities, which are defined in the AML/CTF Act as persons who provide a 'designated service' (also as defined in the AML/CTF Act). Designated services include financial services (eg, account/deposit taking services, cash carrying/payroll services, currency exchange services, life insurance services, loan services, remittance services, investment services and Australian financial services licence holders arranging for another entity to provide a designated service), bullion services 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' (see 'Update and trends' for further information).

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 service provider in Australia, or the service provider is a resident of Australia and the designated service is provided at or through a permanent establishment of the service provider in a foreign country or the service provider 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 to enrol with AUSTRAC, adopt and maintain a compliance anti-money laundering and counter-terrorism financing programme (AML/CTF programme), conduct customer due diligence procedures, report to AUSTRAC annually and following the occurrence of suspicious matters, threshold transactions or international funds transfer instructions and record keeping.

15 Compliance

Do the AML laws 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 AML/CTF Rules.

AML/CTF programmes are risk-based and relate to the size and nature of each business, the designated services it offers customers 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 the specific business needs and that is proportionate to the level of ML/TF risk the business faces.

An AML/CTF programme generally comprises a Part A and a Part B.

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

- a ML/TF financing risk assessment, which must be periodically reviewed;
- 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 customer due diligence 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.

16 Breach of AML requirements

What constitutes breach of AML duties imposed by the law?

The AML/CTF Act creates an offence to produce false or misleading information or documentation, forge documentation for use in customer identification procedures, provide or receive a designated service using a false customer name or customer anonymity or structure a transaction to avoid a reporting obligation under the AML/CTF Act.

Further, contraventions of obligations under the AML/CTF Act generally constitute civil penalty provisions. For example, a reporting entity that provides a designated service to a customer prior to adopting, or where it does not maintain, a compliant AML/CTF programme breaches a civil penalty provision.

Where a reporting entity has formed a suspicion about a customer, or has submitted a suspicious matter report 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 suspicion or report would constitute the offence of 'tipping off' under the AML/CTF Act.

17 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 a Part A and a 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.

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 customer due diligence (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 their 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, and this information is prescribed in the AML/CTF Rules. The method of verification will also depend on the customer type, but generally 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 customer due diligence 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 customer due diligence programme is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.

18 High-risk categories of customers, business partners and transactions

Do your jurisdiction's AML rules require that covered institutions and persons conduct risk-based analyses? Which high-risk categories are specified?

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 the following:

- 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 (for example, 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 the Democratic People's Republic of Korea are prescribed foreign countries for the purposes of the AML/CTF Act and are subject to AML/CTF countermeasures, including enhanced customer due diligence 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 customer due diligence procedures will be undertaken and additional identification information collected and verified (see question 17). Reporting obligations may also apply depending on the nature of a transaction (see question 19).

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 suspicious matter report (SMR) to AUSTRAC.

19 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

AML/CTF compliance reports provide AUSTRAC with information about a reporting entity's compliance with the AML/CTF Act and associated rules and regulations. All reporting entities must submit an annual compliance report unless an exemption applies (eg, for Australian financial services licence holders that arrange for customers to receive a designated service from another reporting entity, and do not provide any other designated service). As at the date of writing, AUSTRAC is designing (with input from industry) a revised annual compliance report designed to collect better and more informative responses and reduce any unnecessary administrative burden on the reporting population.

Suspicious matter report

The obligation to submit a 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 POC Act 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 after 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 to provide, or provides, a designated service to a customer which involves a transfer of physical currency or e-currency of A\$10,000 or more (or foreign currency equivalent), they must submit a threshold transaction report to AUSTRAC within 10 business days after the day the transaction occurred. A 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 and other components.

International funds transfer instruction

A reporting entity that sends an international funds transfer instruction transmitted out of Australia or receives an international funds transfer instruction transmitted into Australia must report the instruction to AUSTRAC (IFTI) within 10 business days of the day the instruction was sent or received. Different information must be included in an IFTI report depending on whether the IFTI is categorised as an international electronic funds transfer instruction or as instructions given under a designated remittance arrangement.

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. Also, if requested by a police officer or a 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.

20 Privacy laws

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

The Privacy Act 1988 (Cth) (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 (APPs), which create obligations on the collection, use, disclosure, retention and destruction of personal information. The APPs 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 customer due diligence procedures would generally constitute personal information for the purposes of the Privacy Act, and require 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.

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 the reporting entity discloses certain information to the customer and obtains the customer's express consent prior to disclosing such information.

Update and trends

Anti-money laundering is a core focus for the Australian government. The government recently announced that an additional A\$43.4 million would be given to AUSTRAC to recruit staff to ensure AML/CTF compliance from financial institutions. In April 2016, the *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations* (AML/CTF Report) was released. Key findings were that the AML/CTF Act and AML/CTF Rules are too complex and that industry requires more assistance to understand and comply with their obligations. The AML/CTF Report contained 84 recommendations to streamline and strengthen Australia’s AML/CTF regime.

The AML/CTF Report contemplated two phases of consultation and implementation, with Phase 1 including priority projects scheduled for completion in 2017, while Phase 2 progresses major, long-term reforms.

After Phase 1 consultation in relation to expanding the objects of the AML/CTF Act, the government passed the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017, which has brought digital currencies within the scope of Australia’s anti-money laundering regime. These amendments are focused on the point of intersection between cryptocurrencies and the regulated financial sector, namely digital currency exchanges. At the time of writing, the amendments are not in force; however, they are expected to commence on 3 April 2018. Once implemented, digital currency exchange providers will be required to register with AUSTRAC in order to operate. Registered exchanges will be required to implement know-your-customer processes to adequately verify the identity of their customers,

with ongoing obligations to monitor and report suspicious and large transactions. Exchanges will also be required to keep certain records relating to customer identification and transactions for up to seven years. The offence for operating a registrable digital currency exchange service without registering with AUSTRAC will carry a penalty of up to two years’ imprisonment or a fine of up to A\$105,000, or both.

Phase 2 of AUSTRAC’s project plan for implementing recommendations strengthening Australia’s AML/CTF regime is due to begin this year with consultation on the proposed simplification of the AML/CTF Act and Rules. This should, among other things, clarify record-keeping requirements and reporting obligations for reporting entities. The public consultation on the draft amendments to the AML/CTF Rules closed on 13 February 2018 but broader consultation, design and implementation for the AML/CTF reforms will continue through to 2019.

AUSTRAC has also implemented a new dedicated webpage that provides information about the AML/CTF regime and AUSTRAC’s role to assist businesses wishing to create a new financial service product or to understand their AML/CTF obligations. In its annual report for 2016–17, AUSTRAC noted that the webpage had been successful, garnering over 40 direct enquiries from entities developing innovative new approaches to providing ‘designated services’ as defined under the AML/CTF Act. AUSTRAC also noted that it met representatives of start-ups throughout the year to enable those businesses to discuss proposed business models and provide guidance on how their businesses could comply with obligations under the AML/CTF Act.

21 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 Commonwealth. As at the date of this publication, the maximum pecuniary penalty for body corporates is A\$21 million and A\$4,200,000 for individuals and other entities;
- acceptance of an enforceable undertaking, which is a written undertaking that is enforceable in court and used as an alternative to civil or administrative action;
- issuance of an infringement notice, whereby payment of the specified penalty will discharge any liability and no criminal or civil penalty proceedings will be brought;
- issuance of 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).

22 Limitation periods

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.

23 Extraterritoriality

Do your jurisdiction’s AML laws have extraterritorial reach?

The AML/CTF Act states that, unless the contrary intention appears within the act, it extends to acts, omissions, matters and things outside Australia. However, note that the geographical link to Australia, with respect to the relevant designated service, must be present (see question 14).

Civil claims

24 Civil claims and private enforcement

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.

International anti-money laundering efforts

25 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);
- Egmont Group of Financial Intelligence Units; and
- the Asia/Pacific Group on Money Laundering (APG).

26 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.

During 2013–2014, the FATF commenced its assessment of Australia’s AML/CTF regime. A joint evaluation report by the FATF and the APG 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 in only 24 out of the 40 FATF recommendations. Key findings included that:

- Australia has failed to implement the second tranche of AML/CTF regulation covering non-financial businesses and professional sectors (other than gaming and bullion);
- AUSTRAC’s enforcement and supervision powers 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 AML/CTF Act to address the recommendations and a report was tabled before Parliament in April 2016. See 'Update and trends' for further information.

27 FIUs

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

AUSTRAC is Australia's FIU. It has several offices throughout Australia. The details of its Sydney office are:

Level 7, Tower A, Zenith Centre
821 Pacific Highway
Chatswood, NSW 2067
Australia
Tel: +61 2 9950 0055

AUSTRAC Contact Centre
Tel: +61 2 9950 0055
Fax: +61 3 8636 0508
contact@austrac.gov.au
www.austrac.gov.au

28 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 prosecutions, including to recover the proceeds of crime. Australia's response to such a request 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 which outline the sharing of financial intelligence information between regulators, including AUSTRAC and FIUs in foreign jurisdictions. These arrangements are generally effected through memoranda of understanding and also 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) (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. Relevantly in the context of AML laws, this includes Commonwealth regulators such as ASIC 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, the AUSTRAC CEO may also communicate information to the government of a foreign country if it is 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. The AUSTRAC CEO 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.



Peter Reeves
Georgina Willcock

preeves@gtlaw.com.au
gwillcock@gtlaw.com.au

Level 35, Tower Two, International Towers Sydney
200 Barangaroo Avenue
Barangaroo, NSW 2000
Australia

Tel: +61 2 9263 4000
Fax: +61 2 9263 4111
www.gtlaw.com.au

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com