

GETTING THE DEAL THROUGH

Anti-Money Laundering

in 24 jurisdictions worldwide

2014

Contributing editors: James G Tillen and Laura Billings



Published by
Getting the Deal Through
in association with:

Anagnostopoulos Criminal Law & Litigation

Anderson Mōri & Tomotsune

Angara Abello Concepcion Regala & Cruz Law Offices
(ACCRALAW)

Ashurst Australia

AZB & Partners

Conlin Bedard LLP

Estudio Beccar Varela

Financial Action Task Force

Gorrissen Federspiel

Herdem Attorneys at Law

Ivanyan & Partners

Knierim | Huber Rechtsanwälte

Laurent Lenert, Avocat à la Cour

Maestre & Co Advocats

Miller & Chevalier Chartered

Niederer Kraft & Frey Ltd

Quiñones, Ibarguen, Luján & Mata SC

Rubio Villegas y Asociados, SC

Simmons & Simmons LLP

Sjöcrona Van Stigt Advocaten

Sofunde, Osakwe, Ogundipe & Belgore

Studio Legale Pisano

The Law Firm of Salah Al-Hejailan

Wilson Harle

Zingales & Pagotto Sociedade de Advogados (ZISP Law)

Anti-Money Laundering 2014**Contributing editors:****James G Tillen and Laura Billings
Miller & Chevalier Chartered**

Getting the Deal Through is delighted to publish the third edition of *Anti-Money Laundering*, a volume in our series of annual reports, which provide international analysis in key areas of law and policy for corporate counsel, cross-border legal practitioners and clients.

Following the format adopted throughout the series, the same key questions are answered by leading practitioners in each of the 24 jurisdictions featured. New jurisdictions this year include Argentina, Germany, Guatemala, Luxembourg and Turkey. This edition includes a global overview authored by James G Tillen, Laura Billings and Jonathan Kossak of Miller & Chevalier Chartered as well as an introduction written by the secretariat of the Financial Action Task Force.

Every effort has been made to ensure that matters of concern to readers are covered. However, specific legal advice should always be sought from experienced local advisers. *Getting the Deal Through* publications are updated annually in print. Please ensure you are referring to the latest print edition or to the online version at www.gettingthedealthrough.com.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We would also like to extend special thanks to contributing editors James G Tillen and Laura Billings of Miller & Chevalier Chartered for their assistance with this volume.

Getting the Deal ThroughLondon
May 2014**Publisher**Gideon Robertson
gideon.roberton@lbresearch.com**Subscriptions**Rachel Nurse
subscriptions@gettingthedealthrough.com**Business development managers**George Ingledew
george.ingledew@lbresearch.comAlan Lee
alan.lee@lbresearch.comDan White
dan.white@lbresearch.comGlobal Overview – The cutting edge:
keeping abreast of the global AML/CFT
legal and regulatory landscape 3**James G Tillen, Laura Billings and
Jonathan Kossak**
Miller & Chevalier Chartered

FATF: the global standard-setter 5

The Secretariat
Financial Action Task Force

Andorra 7

Marc Maestre
Maestre & Co Advocats

Argentina 12

Maximiliano D'Auro and Lucía Degano
Estudio Beccar Varela

Australia 19

Philip Trinca and James Morris
Ashurst Australia

Brazil 25

**Leopoldo Pagotto and
Marina Troncoso Esposito**
Zingales & Pagotto Sociedade de Advogados
(ZISP Law)

Canada 31

Benjamin P Bedard and Paul D Conlin
Conlin Bedard LLP

Denmark 38

Anne Birgitte Gammeljord
Gorrissen Federspiel

Germany 42

Daniel Gutman and Christian Rathgeber
Knierim | Huber Rechtsanwälte

Greece 49

**Ilias G Anagnostopoulos and
Jerina (Gerasimoula) Zapanti**
Anagnostopoulos Criminal Law & Litigation

Guatemala 55

Estuardo Mata Palmieri
Quiñones, Ibargüen, Luján & Mata SC

India 61

Aditya Bhat and Richa Roy
AZB & Partners

Italy 71

Roberto Pisano and Chiara Cimino
Studio Legale Pisano

Japan 80

Yoshihiro Kai
Anderson Mōri & Tomotsune

Luxembourg 85

Laurent Lenert
Laurent Lenert, Avocat à la Cour

Mexico 91

**Juan Carlos Partida Poblador,
Alejandro Montes Jacob and
Marcela Trujillo Zepeda**
Rubio Villegas y Asociados, SC

Netherlands 96

Enide Z Perez and Max J N Vermeij
Sjöcrona Van Stigt Advocaten

New Zealand 103

Gary Hughes and Rachel Sussock
Wilson HarlePublished by
Law Business Research Ltd87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910© Law Business Research Ltd 2014
No photocopying: copyright licences do not apply.
First published 2012
Third edition
ISSN 2050-747X

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. Although the information provided is accurate as of May 2014, be advised that this is a developing area.

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

CONTENTS

Nigeria 112

**Babajide O Ogundipe and
Chukwuma Ezediario**

Sofunde, Osakwe, Ogundipe & Belgore

Philippines 116

Chrysilla Carissa P Bautista

Angara Abello Concepcion Regala & Cruz
Law Offices (ACCRALAW)

Russia 124

Vasily Torkanovskiy

Ivanyan & Partners

Saudi Arabia 131

Robert Thoms and Sultan Al-Hejailan

The Law Firm of Salah Al-Hejailan

Switzerland 135

Adrian W Kammerer and Thomas A Frick

Niederer Kraft & Frey Ltd

Turkey 141

Şafak Herdem

Herdem Attorneys at Law

United Kingdom 148

**Nick Benwell, Cherie Spinks, Emily Agnoli
and David Bridge**

Simmons & Simmons LLP

United States 156

**James G Tillen, Laura Billings and
Jonathan Kossak**

Miller & Chevalier Chartered

New Zealand

Gary Hughes and Rachel Sussock

Wilson Harle

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.

New Zealand's domestic legislation and legal processes used to counter money laundering can be separated into two main categories. The first contains the criminal money laundering offences and provisions related to those offences. The second contains the AML civil compliance regime by which regulated businesses, primarily in the financial and gaming sectors, are required to take steps to deter, detect and report possible money laundering activity. This civil regime contains comprehensive regulatory provisions, breach of which can itself be a criminal offence.

The main criminal provisions are in the Crimes Act 1961. Section 243 makes it an offence to engage in a money laundering transaction in respect of property that is the proceeds of a serious offence, knowing or believing that all or part of the property is the proceeds of a serious offence or being reckless as to whether or not the property is so tainted. A 'serious offence' is defined as one punishable by imprisonment for a term of five years or more (including overseas actions that would be so punishable were they committed in New Zealand). Money laundering is punishable by a term of imprisonment of up to seven years.

There is also a separate offence of obtaining property that is the proceeds of a serious offence with intent to engage in money laundering, knowing or believing (or being reckless as to whether) the property is the proceeds of a serious offence.

Other relevant provisions can be found in:

- the Misuse of Drugs Act 1975, where section 12B very much follows the structure of section 243, but relates specifically to laundering the proceeds of drug offences;
- the Terrorism Suppression Act 2002, with criminal offences for providing or collecting funds to be used for terrorist acts; and
- the Criminal Proceeds (Recovery) Act 2009, which relates to the forfeiture of assets and funds that may be derived from the profits of crime.

The criminal offence provisions for laundering money are reasonably settled and have been largely unchanged for a number of years. The laws relating to the recovery of money or property that are the proceeds of crime were substantially reformed in 2009 and there is a growing body of case law on these types of confiscation or recovery action.

New Zealand's AML regulatory regime for the financial sector has also been through a period of major recent transition, designed to greatly enhance New Zealand's degree of compliance with the FATF's 40+9 Recommendations (October 2004 version). The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) introduced a modern and broad risk-based

framework that has led to a major overhaul of this country's AML regime. The new law had a long implementation period and only came into full force and effect from 30 June 2013.

The substantive AML/CFT legal obligations and powers for most types of regulated institutions are now found in the AML/CFT Act 2009 and the Regulations made under it. The Act contains the key principles and umbrella provisions, with significant matters of detail being addressed in the Regulations and Gazette notices made under it. The regulatory supervisors have also issued a Code of Practice for Identity Verification (now amended), which if complied with provides a safe harbour to institutions when verifying information for customers considered to be low to medium risk.

The AML/CFT Act imposes significantly more onerous obligations on reporting entities than the previous regime and expands the range of commercial enterprises brought under coverage of the regime as reporting entities. In a brief summary, the main obligations on such entities include to:

- conduct and document a written risk assessment on money laundering and terrorist financing risks arising from the customers, the products and services, the delivery channels, countries and institutions dealt with and intermediary risks;
- develop a written AML compliance programme containing policies, procedures and controls to manage and mitigate the risks of money laundering and the financing of terrorism;
- vet senior managers and staff hired to perform AML/CFT related duties;
- train senior managers and relevant staff in AML/CFT related matters;
- comply with detailed customer due diligence (CDD) requirements, including customer identification and verification processes, and determine when enhanced CDD is required, when simplified CDD might be permitted and when CDD can be carried out by a person other than the reporting entity;
- have a process to detect and to ensure reporting of suspicious transactions, and to make such reports when appropriate;
- monitor, on an ongoing basis, customer activity, especially in relation to specified high-risk transactions and business relationships;
- ensure there are processes for full record keeping to enable reconstruction of accounts or transactions if required; and
- make an annual report to the AML supervisor on compliance issues, and arrange for biennial independent auditing of compliance with the AML/CFT programme.

The requirements in the previous regime, the Financial Transactions Reporting Act 1996 (FTR Act), continue in effect for lawyers, accountants, real estate agents, precious metals dealers and other luxury asset dealers or brokers. It is intended that these industries will be brought under the AML/CFT regime via a second round of coverage regulation, probably not before 2016.

Money laundering

2 Criminal enforcement

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

The New Zealand police are responsible for enforcing the criminal offence provisions relating to money laundering. A specialist unit within the police, the Organised and Financial Crime Agency New Zealand, is involved in most of the major operations, and for criminal proceeds recovery and forfeiture, regional Specialised Asset Recovery Units exist within the police.

Money laundering is an indictable offence and can be prosecuted on a summary basis in the district court (under the Summary Proceedings Act 1957). New procedural rules that remove the distinction between indictable and summary offences have come into effect following the commencement of the Criminal Procedure Act 2011 in October 2013.

The three AML/CFT supervisory bodies (the Reserve Bank, the Financial Markets Authority and the Department of Internal Affairs) are not involved in prosecuting or enforcing the criminal law relating to money laundering, but they supervise the anti-money laundering regulatory regime and may bring civil actions to enforce the obligations under the AML/CFT Act. There can also be criminal prosecutions for some offences under the AML/CFT Act, which would be brought by the New Zealand police.

3 Defendants

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

The Crimes Act offence provisions for money laundering refer to a 'person' engaging in a money laundering transaction (section 243(4)). The Crimes Act defines a person as including any public body or local authority and any board, society or company in relation to acts that it is capable of doing. Therefore, both legal and natural persons can be prosecuted for money laundering. Although the penalty for money laundering is a term of imprisonment, under section 39 of the Sentencing Act 2002, a court may impose a fine instead. The requisite knowledge and intention to commit the offence can be imputed to a body corporate through its human agents. Thus both natural and legal persons can be subject to an appropriate punishment for money laundering. Most cases in the past have been taken against individuals.

4 The offence of money laundering

What constitutes money laundering?

A money laundering transaction is engaged in if, for the purpose of concealing any property, or enabling another person to conceal property, a person deals with that property or assists another person to deal with that property (whether directly or indirectly). 'Property' is widely defined as including real and personal property of any description, whether situated in New Zealand or elsewhere and whether tangible and intangible, and includes an interest in any such property. 'Conceal' is defined as concealing or disguising the property and includes (without limitation) converting the property into another form and concealing or disguising the nature, source, location, disposition or ownership of the property, or of any interest in the property. 'Deal with' means to deal with the property in any manner and by any means and includes (without limitation) disposal, transferring possession or bringing the property into or removing it from New Zealand.

The state of mind required for money laundering is a knowledge or belief that all or part of the property is the proceeds of an offence punishable by a term of imprisonment of five years or more,

or being reckless as to whether the property is the proceeds of such an offence. There must also be an intention to conceal the property or to assist another to do so.

There is also a lesser offence of possession of property for money laundering purposes. In order to establish this offence, it must be proven that the property was the proceeds of a serious offence and that the accused had the requisite knowledge or was reckless, and intended to engage in a money laundering transaction in respect of that property (section 243(3)).

5 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?

There is no monetary threshold or other limitation on the types of assets or transactions for prosecution under section 243 of the Crimes Act (see the discussion of the definition of 'property' and 'deal with' in question 4).

6 Predicate offences

Generally, what constitute predicate offences?

Under section 243 a predicate offence must be a 'serious offence', which means an offence punishable by imprisonment for five or more years. The definition expressly includes acts, wherever committed, which, if they had been committed in New Zealand, would constitute an offence punishable by imprisonment for five or more years. Acts committed outside New Zealand can constitute a predicate offence, but must, at the time of being committed, constitute an offence under the law of the jurisdiction in which they are committed (section 245). There is a presumption that the act will constitute an offence under the relevant foreign laws unless the accused puts the matter in issue.

There are proposals expected to be put forward to Parliament soon for consideration in an Organised Crime and Anti-Corruption Legislation Bill, that may do away with the 'serious offence' threshold and mean that any criminal offence could qualify as a predicate offence.

Under the Misuse of Drugs Act 1975, the relevant predicate offences are offences relating to dealing in controlled drugs, cultivating prohibited plants, supplying or manufacturing equipment that is capable of being used to manufacture controlled drugs or cultivating prohibited plants and knowingly importing or exporting precursor substances for unlawful use. Again, the predicate offence can be committed outside New Zealand and, if it was, the burden is on the accused to show that the act was not an offence in the relevant foreign jurisdiction at the relevant time.

From October 2013, a new provision came into effect, which clarifies that a person may be charged with money laundering whether or not the person who committed the predicate offence has been charged or convicted or is otherwise amenable to justice (section 243A).

7 Defences

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

In addition to the ability to establish that the relevant act committed outside New Zealand was not an offence in the foreign jurisdiction at the time it was done (section 245 Crimes Act 1961), there is also a codified defence under section 244. The defence is established if the accused can prove that the act to which the charge relates was done by them in good faith for the purpose of, or in connection with, the enforcement or intended enforcement of:

- any enactment relating to a serious offence;
- the Criminal Proceeds (Recovery) Act 2009;

- the AML/CFT Act; or
- the Financial Transactions Reporting Act.

This typically relates to directions from the police on how to deal with funds or with customers after a suspicious transaction report (STR) has been made.

Additional general defences are set out in the Crimes Act, and common law defences (such as insanity, compulsion and duress) are preserved unless abrogated expressly. The codified defences include infancy (sections 21 and 22), insanity (section 23) and compulsion by another (section 24).

8 Resolutions and sanctions

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

The maximum penalty for the offence of money laundering is seven years' imprisonment. For the related offence of possession with the intention of money laundering it is five years' imprisonment. Under section 39 of the Sentencing Act a fine may be imposed instead of a term of imprisonment.

9 Forfeiture

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

The Criminal Proceeds (Recovery) Act 2009 sets out a detailed legislative scheme relating to forfeiture orders. Unlike the previous forfeiture law, a criminal conviction is not required for the imposition of a forfeiture order – all that is required is proof of 'significant criminal activity' on the balance of probabilities. A significant criminal activity is activity that would amount to either an offence punishable by a term of imprisonment of five years or more, or from which property or proceeds of NZ\$30,000 or more have been directly or indirectly obtained. Several types of orders are covered in the Act, including assets forfeiture orders, profit forfeiture orders and instrument forfeiture orders.

Prior to forfeiture, the Act provides for restraining orders in respect of property. The police can then apply for a civil forfeiture order in respect of certain property, including orders relating to both assets and profits. If the court is satisfied that the property was obtained as a result of a significant criminal activity, then it must make an assets forfeiture order, which vests the property in the Crown. If it is shown that a respondent has benefited from significant criminal activity, and has an interest in property, then the court must make a profit forfeiture order. A profit forfeiture order is enforceable as an order made as a result of civil proceedings instituted by the Crown against the person to recover a debt due to it. Relief can be granted, following application by a person other than the respondent to the forfeiture order, in the case of undue hardship.

An order for the forfeiture of property used to commit or facilitate a serious offence may also be made under section 142N of the Sentencing Act 2002 and form part of the sentence imposed on an offender. The effect of such an order is also to vest the property in the Crown absolutely.

10 Limitation periods

What are the limitation periods governing money laundering prosecutions?

There are no limitation periods governing the prosecution of money laundering offences under the Crimes Act. They do not come within the range of offences subject to a 10-year limitation period under section 10B of that Act.

11 Extraterritorial reach

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

As a general rule, the criminal jurisdiction applies only to acts or omissions that occur in New Zealand and does not extend beyond domestic borders (section 6 Crimes Act). All acts committed in New Zealand may form the basis of an offence and so non-citizens and non-residents that commit a crime in New Zealand can be prosecuted (section 5 Crimes Act). Although generally actions outside New Zealand would not be an offence, sections 243 and 245 specifically provide that the predicate offences for money laundering can be offences committed outside New Zealand.

Further, the money laundering conduct itself may occur outside New Zealand as it may involve property being brought into or moved outside New Zealand, and the property may be situated in New Zealand or elsewhere. However, some connection to New Zealand is required; some relevant act or event forming part of dealings with the property must have taken place in the jurisdiction.

AML requirements for covered institutions and individuals

12 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?

New Zealand makes use of a multi-supervisor model under the AML/CFT Act, whereby three existing regulatory agencies that each have responsibility for regulating certain sectors in other areas of law have added AML/CFT to their existing responsibilities. In this respect, New Zealand differs from other countries (eg, Australia) that have chosen to establish a new singular enforcement agency.

The three AML/CFT Supervisors are:

- the Reserve Bank of New Zealand – for banks, life insurers and non-bank deposit takers;
- the Financial Markets Authority – most other financial institutions including issuers of securities, trustee companies, futures dealers, collective investment schemes, brokers and financial advisers; and
- the Department of Internal Affairs – for casinos, non-bank deposit taking lenders, money changers, card issuers and any other reporting entities that do not clearly fall within the remit of the other supervisors.

The three supervisors have had greatly enhanced supervisory, investigation and enforcement powers from 30 June 2013 when the AML/CFT Act came properly into force. Over several years previously, they had worked to create a large number of guidelines and advisory notes for entities grappling with their new compliance responsibilities and the Supervisors' new enforcement functions. Further guidelines have continued to be issued since the Act came into effect to assist entities to better understand their obligations under the law, most recently on the topics of wire transfers and persons acting on behalf of customers (August 2013).

The Commissioner of Police is also involved in the civil AML/CFT regulatory regime as the recipient of any STRs for investigation and as ultimate enforcement arm if there is a breach of the AML/CFT compliance regime that necessitates criminal prosecution. The Police Financial Intelligence Unit (NZFIU) issued new Suspicious Transaction Guidelines in 2013.

The Ministry of Justice also has an active role in the development and implementation of the AML regime. The Ministry manages an AML/CFT Coordination Committee that includes the three supervisors, New Zealand customs service, New Zealand police and other invited agencies.

13 Covered institutions and persons

Which institutions and persons must carry out AML measures?

At present, reporting entities under the AML/CFT Act are defined to include financial institutions and casinos. Section 5 provides that 'financial institution', means a person, who in the ordinary course of business, carries on one or more of the financial activities set out there, including:

- accepting deposits or other repayable funds from the public;
- making a loan to or for a customer;
- issuing a debit or credit card;
- managing the means of payment;
- supplying goods through a finance lease (other than for consumer products);
- providing remittance services that transfer money or property;
- issuing or accepting liability under life insurance policies;
- issuing or selling securities and derivatives;
- safekeeping or administering cash or liquid securities on behalf of other persons; and
- exchanging foreign currency.

A firm that carries on one or more of those activities and does so 'in the ordinary course of business' will have to comply with the AML/CFT Act. The AML/CFT supervisors issued a guideline to clarify how they intend to apply the phrase 'ordinary course of business'. It sets out a number of contextual factors, which, when considered together, may indicate whether an activity is in the usual course of business of that firm. These involve whether the financial activity:

- is normal or otherwise unremarkable for the particular business (including as indicated by the firm's internal processes and marketing materials);
- is frequent or is regular;
- involves significant amounts of money;
- is a source of revenue for the firm;
- involves significant allocation of the firm's resources; or
- involves a service or product that is offered to customers or third parties.

In addition, any person who holds a casino operator's licence under the Gambling Act 2003 is covered by the AML/CFT Act.

There is also power to include or exclude other types of business by regulation without having to formally amend the Act in Parliament. An illustration of this flexibility came when the AML/CFT Regulations 2011 added trust and company service providers (formation and secretariat services) to the list of covered reporting entities, largely in response to concerns raised by the alleged involvement of some New Zealand registered companies in overseas criminal activities using rogue trust or company service providers. The regulations have also brought some types of financial advisers (and firms that provide financial advice) within the new regime.

There are also a growing number of carve outs and exemptions from coverage being made in the Regulations for low-risk products or services or some functions of a covered entity, for example, debt collection services. In addition, there is a process to apply for special ministerial exemption for a particular business or sector. At the time of writing, almost 40 of these individual or ad hoc ministerial exemptions have been granted.

At a later date, lawyers, accountants, real estate agents, precious metals dealers and other luxury asset dealers or brokers will be brought under the new AML/CFT regime via a second round of regulation. The Ministry of Justice has said it intends to commence policy work in 2014 to bring this second tranche into place. In the meantime these people will continue to be regulated by the FTR Act.

14 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?

Reporting entities must establish, implement and maintain an AML compliance programme. They must first conduct their own detailed written risk assessment of their business operations, products or services, customers, distribution methods, countries and institutions dealt with, and then base their compliance programme on those identified risks. This means the programme can be proportionate and risk based, having regard to the nature, size and complexity of their individual business.

The compliance programme must include adequate and effective processes, policies and controls in a number of specified areas, including:

- training and vetting processes for staff involved in AML/CFT procedures;
- ensuring that customer due diligence (CDD) measures are carried out;
- reporting suspicious transactions;
- ensuring safe retention of account and transaction records and keeping written findings on unusual transactions or business relationships;
- prevention of products or transactions that might favour anonymity; and
- monitoring and managing ongoing compliance with its AML/CFT programme (section 57 of the AML/CFT Act).

Entities must also appoint an AML/CFT compliance officer to administer and maintain the programme.

15 Breach of AML requirements

What constitutes breach of AML duties imposed by the law?

Breach of AML obligations can cover a wide variety of matters, a number of which are listed in question 20. Some specific prohibitions are set out in the AML/CFT Act:

- if unable to conduct CDD, an entity must not establish a new customer relationship, must terminate an existing relationship, must not carry out an occasional transaction over certain thresholds and must consider whether to make a STR;
- an entity must not knowingly or recklessly set up a facility for an anonymous customer or under a false name; and
- an entity must not establish or continue relationships with a foreign shell bank, or correspondent bank of a shell bank.

Tipping off customers is also prohibited in New Zealand. The legislation sets out a duty not to disclose or tip off, together with an offence of tipping off, and the substantial potential penalties that may follow.

Under the AML/CFT Act, section 46 requires a reporting entity not to disclose certain information in relation to suspicious transactions reports to anyone except the police, the entity's AML/CFT supervisor, an officer or employee of the entity for any purpose connected with their duties, a lawyer advising on the matter or members of a designated business group in order to decide whether to make a STR. Section 47 prevents disclosure of that information in any judicial proceeding unless the judge is satisfied that disclosure is necessary in the interests of justice.

16 Customer and business partner due diligence

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

A key feature of the AML/CFT Act is to force reporting entities to develop more detailed CDD (or 'know your customer') processes. While there is ability to apply a risk-based approach somewhat

flexibly in many areas, there are also minimum requirements set out in the statute. Sections 10 to 17 contain the main requirements for standard CDD, with additional requirements or relaxations in certain circumstances for simplified CDD (sections 18 to 21) or for enhanced CDD (sections 22 to 30).

Generally, the CDD required was not retrospective as it did not require all existing customers to be verified upon the law coming into force, with some exceptions if and when the nature of the relationship changes, suspicion is raised or an entity realises it holds inadequate information.

CDD will typically apply to new customers or accounts where there is a business relationship that has an element of duration or to 'occasional transactions' that are one-offs outside of a business relationship over a dollar threshold of NZ\$10,000 and where insufficient information is held about a customer or the business relationship changes.

Section 15 sets out the minimum information required for standard CDD: the person's full name, date of birth, if not the customer, that person's relationship to the customer, address or registered office and the person's company identifier or registration number, as well as any information prescribed by the Regulations. The entity must then verify that information and verify additional details depending on the level of risk in certain situations (or as prescribed in the Regulations).

An Identity Verification Code of Practice was issued by the AML/CFT supervisors and amended in 2013, containing detailed options of the type of documentary evidence or electronic verification methods that may be considered acceptable when verifying the identity of low to medium-risk individuals during CDD. The code is not compulsory but, if followed, acts as a safe harbour, providing a business with a way of establishing likely compliance with the AML/CFT obligations. Reporting entities must still consider further, and potentially develop additional mechanisms for verifying, any high-risk customers.

Beneficial ownership is a challenging area of compliance in New Zealand, given the relatively high proportion of trust structures used in commercial and individual enterprises. A balance has been struck in the AML/CFT Act and Regulations that will require entities to verify beneficial ownership by obtaining the name and date of birth of each beneficiary of a trust or, for charitable or discretionary trusts with more than 10 beneficiaries, a description of the class and types of beneficiary and trust objectives. A Guidance Note indicating the AML supervisors' likely approach to beneficial ownership was issued in December 2012.

17 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 risk-based approach is enshrined in much of the AML/CFT Act. Reporting entities must carry out a written risk-based assessment, which must be the platform and reference point for the rest of their Compliance Programme, and available to the Supervisor on request. It must also be independently audited every two years. Reporting entities must also develop processes and filters to determine if more stringent CDD measures are required in high risk cases, or where the Act prescribes that enhanced CDD must be carried out, such as:

- dealing with a trust, or company with nominee shareholders or bearer shares;
- non-resident account holders from a country with an insufficient AML regime;
- 'politically exposed persons' (prominent foreign public individuals, as specifically defined); and

- wire transfers, correspondent banking or customer relationships involving new or developing technologies or products that might favour anonymity.

Enhanced CDD means, in most of those cases, making further enquiry into the customer's source of funds or wealth, although there are some additional specific data requirements, for example, in the case of wire transfers.

As noted in question 16, the safe harbour Code of Practice for identity verification does not extend to high risk customers (or corporate entities).

18 Record keeping and reporting requirements

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

New Zealand reporting entities and their auditors have specific obligations under sections 40–43 of the AML/CFT Act to make STRs where suspicion is raised in certain situations. The legal trigger for reporting is when a transaction or proposed transaction gives the reporting entity reasonable grounds to suspect that it is or may be relevant to the investigation or prosecution of money laundering or related offences.

The STR must be made as soon as practicable and no more than three working days after forming the suspicion. The NZFIU has developed a secure online XML-based IT platform that entities must use to make STRs, known as 'goAML'. The detailed contents of an STR form are now prescribed in the Regulations. Other parties who are not yet directly covered by the new regime (including lawyers, accountants and real estate agents) still have generic obligations under the old FTR Act to make STRs upon suspicion being formed when any person conducts or seeks to conduct any transaction giving reasonable grounds to suspect money laundering activity.

Where terrorism financing is suspected, a Suspicious Property Report must be completed under section 43 of the Terrorism Suppression Act 2002.

Reporting entities must also:

- keep transaction records enabling reconstruction of any transaction within the last five years, specified financial information, and identity and verification evidence;
- make annual reports on their risk assessment and compliance programme, in the detailed format required by the AML supervisors for this reporting function; and
- subject their risk assessment and compliance programme to independent audits every two years, or as requested by their AML/CFT supervisor.

19 Privacy laws

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

Reporting entities under the AML/CFT Act must have regard to privacy issues and protect personal information they may hold. This is expressly required in relation to the sharing of information among members of a designated business group (eg, related companies).

Privacy is also an important consideration under the Amended Identity Verification Code of Practice 2013 jointly issued by the AML/CFT supervisors. This recognises and endorses New Zealand's well-developed personal privacy principles contained in the Privacy Act 1993, whenever reporting entities are carrying out due diligence. The Privacy Act governs personal information held by any agency in New Zealand and sets out 12 Information Privacy Principles (IPPs). The IPPs govern all phases of collection, handling and ultimate use and disposal of information about identifiable individuals by both private and public agencies. The IPPs require good reasons

for disclosing personal information to anyone other than the data subject and for use of the information for any reason other than the purpose for which it was collected. The definition of personal information is very wide and includes any 'information about an identifiable individual'.

Before issuing STR guidelines for each type of reporting entity, setting out examples and features of transactions that may give rise to suspicion of any money laundering offence, the New Zealand police must consult with the Privacy Commissioner. Such guidelines were issued by the NZFIU in 2013.

New legislation has been passed – the Identity Information Confirmation Act 2012 – that enables access to a consent-based service to allow both public and private sector agencies to check whether identity information presented by customers is the same as that recorded by the Department of Internal Affairs through its citizenship, passports, and births, deaths and marriages registry functions. The Act provides for quite strict privacy controls on the circumstances in which the registries can be accessed. This service is still in its formative stages. However, another initiative, a secure online identity verification service introduced by the government called 'RealMe' is up and running, and some leading banks have begun using it. A RealMe verified account is intended to be the online equivalent of a passport or drivers licence. The service was introduced to not only allow the government to provide services online but to also be used by the private sector to verify identity. Separately, some IT service providers are compiling databases that can be subscribed to for a fee in order to assist with verification information about New Zealand citizens and residents.

20 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 mix of enforcement sanctions with differing levels of potential penalty outcomes, depending on the factual circumstances and the attitude of the AML/CFT supervisor to the transgression. Regulators can consider legal action for civil liability acts and also criminal offences, and these can be taken against senior managers and individuals within corporate entities as well as the corporation.

Civil liability acts include:

- failing to ensure branches and subsidiary businesses comply with AML/CFT requirements, entering or continuing a business relationship without adequate evidence of identity, inadequate account and transaction monitoring and entering or continuing a correspondent banking relationship with a shell bank. For these matters, statutory maximum pecuniary penalties are set at NZ\$100,000 for individuals or NZ\$1 million for corporate bodies; and
- failing to keep records as required, failing to establish, implement or maintain an AML compliance programme and failing to carry out CDD. Here, statutory maximum pecuniary penalties are set at NZ\$200,000 for individuals or NZ\$2 million for corporate bodies.

Rather than apply to the court for a pecuniary penalty or an injunction, the AML/CFT supervisor may elect to issue a formal warning, or accept a court-enforceable undertaking from the reporting entity. At the time of writing, there have not yet been any such formal enforcement actions made public, although that may well change later in 2014. It is expected that, initially at least, the supervisors are likely to make use of warnings and enforceable undertakings rather than punitive court action, except in the most egregious of cases.

Criminal offences for breaches of the AML/CFT regulatory regime include:

- recklessly, knowingly or repeatedly carrying out a civil liability act as above;

- failing to make STRs when required;
- providing false or misleading information concerning STRs;
- tipping off unauthorised third parties about STRs;
- failing to keep adequate records concerning STRs; and
- obstructing an STR investigation.

For these more serious matters, the statutory maximum sanction is a criminal fine of up to NZ\$300,000 or up to two years' imprisonment for individuals, or fine of up to NZ\$5 million for corporate bodies.

There are also offence provisions relating to the cross-border transportation of cash, which are considered more minor offences and have a penalty of not more than three months' imprisonment or a fine of up to \$10,000, or both, for an individual or a fine of up to \$50,000 for a body corporate. The first prosecutions under the new AML/CFT Act have been made by the New Zealand customs service, based on the non-declaration of cross-border cash movements.

21 Limitation periods

What are the limitation periods governing AML matters?

If seeking a civil penalty, an application must be made by an AML/CFT supervisor within six years of the conduct that gives rise to the liability to pay the civil penalty.

The time limit for the majority of offences under the AML/CFT Act is three years 'after the time when the matter of the information arose'. For the more minor offences relating to the cross-border transportation of cash the time limit for laying the charging document is only six months after the date on which the offence was committed.

22 Extraterritoriality

Do your jurisdiction's AML laws have extraterritorial reach?

Generally speaking, the AML/CFT Act measures apply to entities carrying on the defined types of business or services within New Zealand's borders. However, this applies equally to subsidiaries or branches of foreign financial institutions seeking to operate in New Zealand. Further, in some specific respects a limited form of extraterritoriality applies, for instance:

- New Zealand domestic reporting entities must ensure that branches and subsidiaries in a foreign country apply, to the extent that the country's law permits, broadly equivalent AML compliance measures; or
- cross-border transportation of cash (NZ\$10,000 or more) into or out of the country.

The AML/CFT supervisors issued a brief guidance note in December 2012 on how they perceive the territorial scope of the Act as it affects their functions. Some uncertainty, however, remains over the exact extent of extraterritorial reach, and this may be ultimately only resolved as case law develops in future.

Civil Claims

23 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.

The field of private claims or civil liability for AML breaches is very underdeveloped in New Zealand. In the past, the FTR Act has been seen as primarily a police or criminal matter, and there have been few attempts to press private claims. However, as part of the criminal process, victims can seek reparation payments or courts can order that part of the fine be paid to victims.

In relation to civil liability acts under the new AML regime, the primary right and responsibility to take action rests with the AML/CFT supervisor and the civil 'balance of probabilities' onus of proof applies. However, if a pecuniary penalty is sought, the court has the ability to order it to be paid to the Crown 'or to any other person specified by the court', which allows payment to be directed to victims of crime or others affected.

In practice, the usual court order would probably be a payment to the Crown, similar to a fine. But it is possible that as the enhanced AML/CFT regime gets bedded in, and as the financial consequences become more serious for reporting entities in future, more civil claims are likely.

Reporting entities have immunity from civil suit for actions taken to comply with the Act, as long as they were acting in good faith and reasonably (section 77 of the AML/CFT Act). For plain cases of non-compliance or breach, potential common law causes of action may remain available, such as equitable tracing remedies, claims of knowing assistance or knowing receipt of property from the proceeds of crime, fraud or breach of trust or even the tort of breach of statutory duty.

At a practical level, increasing use by the Crown of the Criminal Proceeds (Recovery) Act regime tends to preclude or 'crowd out' the likelihood of private claims, because the Crown usually targets those assets of an offender with the most realistic prospect of realising value, frequently leaving few viable assets for a private claimant.

International anti-money laundering efforts

24 Supranational

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

New Zealand has been a member of the FATF since 1991. New Zealand is also closely engaged with the Asia-Pacific Group on Money Laundering (APG), a FATF-styled regional body that coordinates regional development and liaison under FATF auspices.

25 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.

The FATF has carried out country assessments of New Zealand in 2003, 2009 and in 2013, in conjunction with the APG.

Following delays in implementing the new AML/CFT legislation, New Zealand had been placed on a more frequent follow-up schedule for mutual evaluations, however following the most recent October 2013 Mutual Evaluation Report finding there had been significant progress, New Zealand is back on to the regular evaluation path.

A copy of that Report can be found at www.fatf-gafi.org/countries/n-z/newzealand/documents/fur-new-zealand-2013.html.

The FATF Report's summary section in October 2013 records that:

Since the adoption of its mutual evaluation report in 2009, New Zealand has focused its attention on:

- *Strengthening the AML/CFT legislative framework with the adoption of new preventive AML/CFT Legislation – the AML/CFT Act, 2009 – which came into full force and effect on 30 June 2013.*
- *Issuing a set of implementing preventive AML/CFT measures, a National Risk Assessment and comprehensive guidance material to assist reporting entities with the implementation of the Act.*
- *Introducing several changes to its supervisory framework, including establishing three statutory supervisors for reporting*

entities subject to the Act: The Reserve Bank of New Zealand; the Financial Markets Authority; and the Department of Internal Affairs.

- *Strengthening its registration and licensing regime for financial service providers and the insurance sector.*
- *Introducing a new cross-border cash reporting regime.*

In October 2013, the FATF recognised that New Zealand had made significant progress in addressing the deficiencies identified in the 2009 mutual evaluation report and could be removed from the regular follow-up process. The decision by the FATF to remove a country from the regular follow-up process is based on procedures agreed in October 2009.

26 FIUs

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

The NZFIU collects suspicious transaction reports that come from banks and other financial institutions. It also monitors reportable amounts of cash crossing New Zealand borders, and supports investigations into money laundering activity. The NZFIU is a member of the Egmont Group.

The NZFIU address and contact details are:

New Zealand Police National Headquarters

180 Molesworth Street

PO Box 3017

Wellington

New Zealand

Tel: +64 4 474 9499

Fax: +64 4 498 7405

www.police.govt.nz/service/financial/index.html

The NZFIU has a bespoke online secure system named 'goAML' that reporting entities must use, and it does not accept simple e-mail reports or oral reports (other than in situations of extreme urgency). Reporting entities must enrol in and interface with the goAML system operated by the FIU in order to satisfactorily meet their obligations to make secure electronic reporting.

27 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?

In New Zealand, the Mutual Assistance in Criminal Matters Act 1992 allows government authorities to receive and consider requests for assistance from an appropriate and legally competent foreign body, such as police or regulatory agencies and courts. The statute is designed to facilitate the provision and obtaining of international assistance in criminal cases, and is being increasingly resorted to in cases of international fraud and money laundering.

In the interests of international comity, the New Zealand attorney-general (as the New Zealand central authority) has the discretion to receive such requests and to exercise powers under New Zealand domestic legislation on behalf of the foreign authority. This may include going to the New Zealand courts to obtain search warrants on a without notice (ex parte) basis or seeking interim or permanent restraining and seizure orders over assets and property, or both.

The usual sequence of events in a request for international assistance would be as follows:

- a foreign legal basis for action is established by decision or order of a foreign court;
- the foreign court order or indictment or foreign restraining order, or both, provide the source material for the foreign agencies to

Update and trends

With the implementation of a complex new regulatory regime, reporting entities and their customers have had plenty of ‘teething troubles’ to grapple with during the early period of the AML/CFT Act being in force. In particular, even as we approach the one-year anniversary of the implementation, there remains considerable confusion among some firms, their advisers and the public over aspects of customer due diligence rules.

By far the biggest problem area surrounds trust structures and the legislative requirement to identify and verify the upstream beneficial ownership and persons acting on behalf of others. There are a large and varied number of trust structures traditionally used in New Zealand commerce. Confusion over these issues seems to have been exacerbated by the decision to exclude lawyers and other professionals from the first round of coverage under the Act, in that some professionals acting as trustees appear unclear on the extent to which new requirements apply to them.

To date, the AML/CFT supervisors have taken a sensible and pragmatic approach to enforcement, in effect, telling the supervised entities that if a ‘genuine and reasonable attempt to comply’ has been made, immediate enforcement action will be unlikely. It may be expected that, to the extent this has allowed any ‘honeymoon period’ of transition, it is perhaps coming to an end during 2014, especially in cases where there has been wilful or deliberate breaches of the compliance rules.

The first prosecution under the AML/CFT Act to reach the High Court (acting as appellate body) is the case of *New Zealand Customs Service v Huang* [2013] NZHC 3277. This concerned an example of large amounts of cash being transported across the country’s borders. Mr Huang’s appeal against conviction, for failing to declare or report cash well in excess of the threshold of NZ\$10,000 being moved in or out of New Zealand by him, failed. This was an offence under

section 106 of the Act dealing with cross-border transactions, rather than the more mainstream AML compliance obligations applicable to private financial institutions. However, the court confirmed the general approach to enforcement under the Act, including that the offence was one of strict liability, with no requirement to prove Huang had actual knowledge of being required to report, and that the Act clearly allows a charge of an ‘attempt’ to be brought. The interpretative approach of the court indicates heavy reliance on the explicit public welfare regulatory nature of the Act’s purpose statement and also holds useful judicial analysis of its offence structure.

Looking ahead, a proposed Organised Crime and Anti-Corruption bill is expected to be introduced into Parliament during 2014. This will make some important amendments to the present AML compliance regime, including potentially:

- clarifying that intent to conceal the money or property is not an element of the money laundering Crimes Act offence;
- removing the requirement that the predicate offence must be one punishable by five years’ or more imprisonment namely, any type of offence potentially qualifies;
- requiring reporting entities to report to the NZFIU all international wire transfers over NZ\$1,000 and all physical cash transactions over NZ\$10,000;
- creating new offences to address gaps in New Zealand’s criminal law framework for identity crime and people trafficking;
- extending the time frames for foreign restraining orders and providing the ability to register such orders without notice (eg, to cover a *Dotcom* case scenario); and
- allowing police to share personal information and DNA databank information with international counterparts, in order to further inter-agency cooperation efforts and treaty agreements.

make a request for assistance to the attorney-general under the Mutual Assistance in Criminal Matters Act;

- the New Zealand attorney-general receives and considers the request on the basis of the information provided, and can then apply to the court for various orders, including registration of any interim foreign restraining orders on a without notice basis;
- once accepted and registered, the foreign orders allow New Zealand’s asset restraining powers under the Criminal Proceeds (Recovery) Act to be engaged; and
- any actual seizure operation would then be executed by the New Zealand police.

The mutual assistance regime was invoked in 2012 to provide assistance to the United States’ authorities investigating the business of a German internet tycoon who was resident in New Zealand, known as Kim Dotcom, and this has generated considerable recent case law in this area.

The FBI alleges that Kim Dotcom’s business, Megaupload.com, a file-sharing or ‘cyberlocker’ website, was an international criminal organisation responsible for massive worldwide online piracy. After obtaining an indictment from a grand jury in West Virginia on charges of breach of copyright, conspiracy to breach copyright, conspiracy to racketeer, wire fraud and money laundering, the United States Department of Justice (as that country’s central authority) requested assistance from the attorney-general to search the property of Dotcom and his associates in New Zealand and to seize evidence. New Zealand police were then authorised to apply for search warrants to effect that assistance. Having obtained the warrants in the district court, police executed them at three separate addresses and seized a large number of documents and digital storage devices.

The subjects of those search warrants subsequently applied for judicial review of the warrants, alleging that they were unlawful.

Dotcom and his co-accused had sought, prior to a hearing on their eligibility for extradition to the USA, disclosure of the



Gary Hughes
Rachel Sussock

gary.hughes@wilsonharle.com
rachel.sussock@wilsonharle.com

64 Fort Street
Auckland City 1010
New Zealand

Tel: +64 9 915 5700
Fax: +64 9 915 5701
www.wilsonharle.com

documents on which the United States' case against them was based. After several appeals, in *Dotcom & Ors v United States of America* [2014] NZSC 24, the Supreme Court, by a majority, held that the United States is not required to disclose to the appellants, prior to their extradition hearing, the documents, records and information upon which their criminal case in the United States relies.

In its application for extradition, the United States is able to make use of a procedure for submitting evidence called the 'record of the case'. A record of the case is relied on as establishing a prima facie case against those facing extradition and comprises a summary of the evidence that the requesting state says implicates them. It is not available to every country that applies for extradition and is designed to provide a streamlined procedure for those to whom it applies. In this case the record of the case contained extracts from emails, data stored on servers, an analysis of how Megaupload's websites operated and proposed evidence of investigators and experts.

The majority in the Supreme Court has held that the record of case procedure does not require disclosure of all the documents it summarises and there is no general obligation of disclosure on a foreign state requesting extradition. Further, it held that the lower courts did not have the power to make disclosure orders in extradition cases, as the statutory powers in the Criminal Disclosure Act are not incorporated into the Extradition Act. The majority also noted, however, that the requesting state has a duty of good faith to disclose any information that would seriously undermine the evidence upon which it relies.

At the time of writing, Mr Dotcom and his associates are still awaiting an extradition hearing on the grand jury charges. Despite the final resolution of the collateral dispute regarding the extent of disclosure required in the context of extradition proceedings, other judicial review proceedings and challenges to the extradition process remain under appeal to the Supreme Court.

GETTING THE DEAL THROUGH

Annual volumes published on:

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Shipbuilding
Shipping
Tax Controversy
Tax on Inbound Investment
Telecoms and Media
Trade & Customs
Trademarks
Vertical Agreements



**For more information or to
purchase books, please visit:**
www.gettingthedealthrough.com



Strategic Research Partner of the
ABA Section of International Law



THE QUEEN'S AWARDS
FOR ENTERPRISE:
2012



Official Partner of the Latin American
Corporate Counsel Association