Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Public Act	2009 No 35
Date of assent	16 October 2009
Commencement	see section 2

Contents

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

2 Commencement

(1) Parts 1 and 4 (except section 162) come into force on the day after the date that this Act receives the Royal assent.

(2) Sections 68 to 71, 106 to 115, and 163 come into force 12 months after the date on which this Act receives the Royal assent.

(3) Except as provided in subsection (5), the rest of this Act comes into force on a date to be appointed by the Governor-General by Order in Council.

(4) One or more Orders in Council may be made appointing different dates for the commencement of different provisions.

(5) However, section 162 may not be brought into force unless every provision of Part 2 has been brought into force.

Part 1
Preliminary provisions

3 Purpose

(1) The purposes of this Act are—

(a) to detect and deter money laundering and the financing of terrorism; and

(b) to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force; and

(c) to contribute to public confidence in the financial system.

(2) Accordingly, this Act facilitates co-operation amongst reporting entities, AML/CFT supervisors, and various government agencies, in particular law enforcement and regulatory agencies.

4 Overview

(1) This section is a guide to the general scheme and effect of this Act, but does not affect the interpretation or application of the other provisions of the Act.

(2) Part 1 deals with preliminary matters such as definitions of terms used in the Act. It sets out the purpose of the Act and the extent to which it applies to reporting entities.

(3) Part 2 deals with AML/CFT requirements and compliance and has 6 subparts, as follows:

(a) subpart 1 includes provisions dealing with requirements on reporting entities to conduct due diligence on customers and certain other persons, the ability of reporting entities to rely on third parties to carry out customer due

diligence and other AML/CFT functions, and prohibitions on establishing or continuing business relationships and setting up facilities in certain circumstances:

(b) subpart 2 includes provisions dealing with requirements on reporting entities to report suspicious transactions, protection of persons making suspicious transaction reports, and disclosure of information relating to such reports:

(c) subpart 3 sets out requirements on reporting entities to keep records and includes provisions concerning the storage and destruction of records:

(d) subpart 4 deals with reporting entities' internal policies and procedures relating to the prevention of money laundering and the financing of terrorism, including provisions setting out requirements for reporting entities to have an AML/CFT programme for detecting and managing the risk of money laundering and the financing of terrorism, to carry out a risk assessment before conducting customer due diligence or establishing an AML/CFT programme, and to review, audit, and report on their risk assessment and AML/CFT programmes:

(e) subpart 5 deals with codes of practice and includes provisions relating to the preparation of codes by AML/CFT supervisors, approval of codes of practice, and their legal effect:

(f) subpart 6 contains provisions relating to the reporting of certain movements of cash into and out of New Zealand.

(4) Part 3 deals with enforcement and contains provisions relating to civil liability acts, offences, search and seizure, penalties, and immunity of certain persons from civil and criminal proceedings.

(5) Part 4 deals with institutional arrangements and miscellaneous matters and has 2 subparts, as follows:

(a) subpart 1 includes provisions that identify the AML/CFT supervisors and their functions, powers, and ability to delegate supervisory functions; the financial intelligence functions of the Commissioner of Police and a requirement on that person to issue guidelines

relating to suspicious transaction reports; the roles and responsibilities of the Ministry, the AML/CFT co-ordination committee required to be established by the chief executive of the Ministry, and other agencies concerning monitoring, evaluating, and advising on the operation of the AML/CFT regulatory system:

(b) subpart 2 includes regulation-making powers and provisions relating to the Minister's power to grant exemptions from the requirements of the Act.

5 Interpretation

In this Act, unless the context otherwise requires,—

AML/CFT means anti-money laundering and countering the financing of terrorism

AML/CFT programme means a compliance programme established under section 56(1)

AML/CFT requirements means the requirements set out in Part 2

AML/CFT supervisor, in relation to a reporting entity, means the person referred to in section 130(1) that is responsible for supervising the reporting entity under Parts 3 and 4

applicable threshold value means the threshold value that—

(a) is prescribed in regulations; and

(b) applies to a particular person, class of persons, transaction, class of transactions, financial activity, or class of financial activities prescribed in regulations

bearer-negotiable instrument means—

(a) a bill of exchange; or

(b) a cheque; or

(c) a promissory note; or

(d) a bearer bond; or

(e) a traveller's cheque; or

(f) a money order, postal order, or similar order; or

(g) any other instrument prescribed by regulations

beneficial owner means the individual who—

(a) has effective control of a customer or person on whose behalf a transaction is conducted; or

(b) owns a prescribed threshold of the customer or person on whose behalf a transaction is conducted

beneficiary institution, in relation to a wire transfer from an ordering institution, means any person who receives those funds and then makes those funds available to a person (the **payee**) by—

(a) crediting it to an account held by the payee; or

(b) paying it to the payee

business relationship means a business, professional, or commercial relationship between a reporting entity and a customer that has an element of duration or that is expected by the reporting entity, at the time when contact is established, to have an element of duration

cash means—

(a) physical currency:

(b) bearer-negotiable instruments

cash report means a report made under subpart 6 of Part 2

casino means the holder of a casino operator's licence under the Gambling Act 2003

chief executive means the chief executive of the Ministry

civil liability act has the meaning set out in section 78

code of practice and **proposed code of practice** have the meanings set out in section 62

Commissioner means the Commissioner of Police

constable has the same meaning as in section 4 of the Policing Act 2008

correspondent banking relationship has the meaning set out in section 29(3)

country includes any State, territory, province, or other part of a country

customer—

(a) means a new customer or an existing customer; and

(b) includes—

(i) a facility holder:

(ii) a person conducting or seeking to conduct an occasional transaction through a reporting entity:

(iii) a junket organiser as defined in section 4(1) of the Gambling Act 2003:

(iv) a person or class of persons declared by regulations to be a customer for the purposes of this Act; but

(c) excludes a person or class of persons that is declared by regulations not to be a customer for the purposes of this Act

Customs officer has the same meaning as in section 2(1) of the Customs and Excise Act 1996

designated business group means a group of 2 or more persons where—

(a) each member of the group has elected, in writing, to be a member of the group and the election is in force; and

(b) each election was made in accordance with regulations (if any); and

(c) no member of the group is a member of another designated business group; and

(d) each member of the group is—

(i) related to each other member of the group within the meaning of section 2(3) of the Companies Act 1993 and is—

(A) a reporting entity resident in New Zealand; or

(B) a person that is resident in another country with sufficient anti-money laundering and countering the financing of terrorism systems and is supervised or regulated for anti-money laundering and countering the financing of terrorism purposes; or

(ii) providing a service under a joint venture agreement, to which each member of the group is a party; or

(iii) a government department named in Schedule 1 of the State Sector Act 1988, a State enterprise under the State-Owned Enterprises Act 1986, or a Crown entity under section 7 of the Crown Entities Act 2004; or

(iv) related to 1 or more of the entities in subparagraph (iii) through the provision of common products or services; or

(v) an entity or class of entities prescribed by regulations to be a member of a designated entity; and

(e) each member of the group satisfies any conditions that may be prescribed by regulations and that apply to that member

domestic wire transfer has the meaning set out in section 27(7)

existing customer, in relation to a reporting entity, means a person who was in a business relationship with the reporting entity immediately before the commencement of Part 2

facility—

(a) means any account or arrangement—

(i) that is provided by a reporting entity; and

(ii) through which a facility holder may conduct 2 or more transactions; and

(b) without limiting paragraph (a), includes—

(i) a life insurance policy:

(ii) membership of a superannuation scheme:

(iii) the provision, by a reporting entity, of facilities for safe custody, including (without limitation) a safety deposit box:

(iv) an account or arrangement declared by regulations to be a facility for the purposes of this Act; but

(c) excludes an account or arrangement declared by regulations not to be a facility for the purposes of this Act

facility holder, in relation to a facility,—

(a) means the person in whose name the facility is established; or

(b) if that facility is a life insurance policy, means any person who for the time being is the legal holder of that policy; or

(c) if that facility consists of membership of a superannuation scheme, means any person who is a member of the scheme within the meaning of member in section 2(1) of the Superannuation Schemes Act 1989

financial institution—

(a) means a person who, in the ordinary course of business, carries on 1 or more of the following financial activities:

(i) accepting deposits or other repayable funds from the public:

(ii) lending to or for a customer, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions (including forfeiting):

(iii) financial leasing (excluding financial leasing arrangements in relation to consumer products):

(iv) transferring money or value for, or on behalf of, a customer:

(v) issuing or managing the means of payment (for example, credit or debit cards, cheques, traveller's cheques, money orders, bankers' drafts, or electronic money):

(vi) undertaking financial guarantees and commitments:

(vii) trading for the person's own account or for the accounts of customers in any of the following:

(A) money market instruments (for example, cheques, bills, certificates of deposit, or derivatives):

(B) foreign exchange:

(C) exchange, interest rate, or index instruments:

(D) transferable securities:

(E) commodity futures trading:

(viii) participating in securities issues and the provision of financial services related to those issues:

(ix) managing individual or collective portfolios:

(x) safe keeping or administering of cash or liquid securities on behalf of other persons:

(xi) investing, administering, or managing funds or money on behalf of other persons:

(xii) underwriting or placement of life insurance or other investment related insurance:

(xiii) money or currency changing; and

(b) includes a person or class of persons declared by regulations to be a financial institution for the purposes of this Act; but

(c) excludes a person or class of persons declared by regulations not to be a financial institution for the purposes of this Act

financing of terrorism has the same meaning as in section 4(1) of the Terrorism Suppression Act 2002

gambling inspector has the same meaning as in section 4(1) of the Gambling Act 2003

government agency means—

(a) a government department named in Schedule 1 of the State Sector Act 1988; or

(b) a Crown entity under section 7 of the Crown Entities Act 2004; or

(c) the Reserve Bank, the Parliamentary Counsel Office, the New Zealand Police, and the New Zealand Security Intelligence Service; or

(d) any international counterpart of the entities in paragraphs (a) to (c)

identity information means information obtained under sections 15, 19, 23, and 27(1) and (2) and any other information relating to identity prescribed by sections 29(2)(g) and 30(b)

individual means a natural person, other than a deceased natural person

intermediary institution, in relation to a wire transfer, is a person that participates in a transfer of funds that takes place through more than 1 institution but is not an ordering institution or a beneficiary institution

law enforcement purposes means—

(a) the administration of this Act:

(b) the detection, investigation, and prosecution of—

(i) any offence under this Act; or

(ii) a money laundering offence; or

(iii) any offence under section 143B of the Tax Administration Act 1994; or

(iv) any serious offence (within the meaning of section 243(1) of the Crimes Act 1961)

(c) the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009:
(d) the enforcement of the Misuse of Drugs Act 1975:
(e) the enforcement of the Terrorism Suppression Act 2002:
(f) the administration of the Mutual Assistance in Criminal Matters Act 1992:
(g) the investigation of matters relating to security under the New Zealand Security Intelligence Service Act 1969:
(h) any action referred to in paragraphs (a) to (g) taken in respect of legislation of an overseas jurisdiction that is broadly equivalent to the enactments listed in those paragraphs

Minister means the Minister who is, with the authority of the Prime Minister, for the time being responsible for the administration of this Act

Ministry means the department of State that, with the authority of the Prime Minister, is for the time being responsible for the administration of this Act

money laundering offence means an offence against section 243 of the Crimes Act 1961 or section 12B of the Misuse of Drugs Act 1975 or any act committed overseas that, if committed in New Zealand, would be an offence under those sections of those Acts

occasional transaction—

(a) means a cash transaction that occurs outside of a business relationship and is over the applicable threshold value (whether the transaction is carried out in a single operation or several operations that appear to be linked); and
(b) includes a transaction or class of transactions declared by regulations to be an occasional transaction for the purposes of this Act; but
(c) excludes—
  (i) cheque deposits; and
  (ii) a transaction or class of transactions declared by regulations not to be an occasional transaction for the purposes of this Act

ordering institution—

(a) means any person who has been instructed by a person (the **payer**) to electronically transfer funds controlled by the payer to a person (the **payee**) who may or may not be the payer on the basis that the transferred funds will be made available to the payee by a beneficiary institution; and

(b) includes a person declared by regulations to be an ordering institution for the purposes of this Act; but

(c) excludes a person or class of persons declared by regulations not to be an ordering institution for the purposes of this Act

physical currency means the coin and printed money (whether of New Zealand or of a foreign country) that—

(a) is designated as legal tender; and

(b) circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue

Police employee has the same meaning as in section 4 of the Policing Act 2008

politically exposed person means—

(a) an individual who holds, or has held at any time in the preceding 12 months, in any overseas country the prominent public function of—

(i) Head of State or head of a country or government; or

(ii) government minister or equivalent senior politician; or

(iii) Supreme Court Judge or equivalent senior Judge; or

(iv) governor of a central bank or any other position that has comparable influence to the Governor of the Reserve Bank of New Zealand; or

(v) senior foreign representative, ambassador, or high commissioner; or

(vi) high-ranking member of the armed forces; or

(vii) board chair, chief executive, or chief financial officer of, or any other position that has comparable influence in, any State enterprise; and

(b) an immediate family member of a person referred to in paragraph (a), including—
  (i) a spouse; or
  (ii) a partner, being a person who is considered by the relevant national law as equivalent to a spouse; or
  (iii) a child and a child's spouse or partner; or
  (iv) a parent; and
(c) having regard to information that is public or readily available,—
  (i) any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close relationship, with a person referred to in paragraph (a); or
  (ii) any individual who has sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of a person described in paragraph (a)

registered bank has the same meaning as in section 2(1) of the Reserve Bank of New Zealand Act 1989

regulations means regulations made under this Act

reporting entity—
(a) means—
  (i) a financial institution; and
  (ii) a casino; and
(b) includes—
  (i) a person or class of persons declared by regulations to be a reporting entity for the purposes of this Act; and
  (ii) any other person that is required by any enactment to comply with this Act as if it were a reporting entity; but
(c) excludes a person or class of persons declared by regulations not to be a reporting entity for the purposes of this Act

security has the same meaning as in section 2(1) of the New Zealand Security Intelligence Service Act 1969

senior manager (and **senior management** correspondingly) means,—

(a) in relation to a reporting entity that is a company, a director within the meaning of section 126 of the Companies Act 1993; and

(b) in relation to a reporting entity that is not a company, a person who occupies a position comparable to that of a director (for example, a trustee or partner); and

(c) any other person who occupies a position within a reporting entity that allows that person to exercise an influence over the management or administration of the reporting entity (for example, a chief executive or a chief financial officer)

shell bank has the meaning set out in section 39(2)

suspicious property report has the same meaning as in section 4(1) of the Terrorism Suppression Act 2002

suspicious transaction report means a report made under section 40

transaction—

(a) means any deposit, withdrawal, exchange, or transfer of funds (in any denominated currency), whether—

(i) in cash; or

(ii) by cheque, payment order, or other instrument; or

(iii) by electronic or other non-physical means; and

(b) without limiting paragraph (a), includes—

(i) any payment made in satisfaction, in whole or in part, of any contractual or other legal obligation; and

(ii) a transaction or class of transactions declared by regulations to be a transaction for the purposes of this Act; but

(c) excludes the following:

(i) the placing of any bet:

(ii) participation in gambling as defined in section 4(1) of the Gambling Act 2003:

(iii) a transaction or class of transactions declared by regulations not to be a transaction for the purposes of this Act

trustee has the same meaning as in section 2(1) of the Trustee Act 1956

verification information means information obtained under sections 16, 20, 24, and 28

wire transfer—

(a) means a transaction carried out on behalf of a person (the **originator**) through a reporting entity by electronic means with a view to making an amount of money available to a beneficiary (who may also be the originator) at another financial institution; and

(b) includes a transfer or transaction, or class of transfers or transactions, declared by regulations to be a wire transfer for the purposes of this Act; but

(c) excludes—

(i) transfers and settlements between financial institutions if both the originator and the beneficiary are financial institutions acting on their own behalf; and

(ii) credit and debit card transactions if the credit or debit card number accompanies the transaction; and

(iii) any other transfer or transaction or class of transfers or transactions declared by regulations not to be a wire transfer for the purposes of this Act.

6 Application of this Act to reporting entities

This Act applies to a reporting entity only to the extent that—

(a) in the case of a reporting entity that is a financial institution, the financial activities undertaken by that entity fall within the activities described in the definition of financial institution; or

(b) a reporting entity, that is not a financial institution, is carrying out activities that may give rise to a risk of money laundering or financing of terrorism.

7 Amounts not in New Zealand currency

(1) This section applies if, for the purposes of this Act, it is necessary to determine whether the amount of any cash (whether alone or together with any other amount of cash)—

(a) exceeds the applicable threshold value; and
(b) is denominated in a currency other than New Zealand currency.

(2) If this section applies, the amount of the cash is taken to be the equivalent in New Zealand currency,—
(a) calculated at the rate of exchange on the date of the determination; or
(b) if there is more than 1 rate of exchange on that date, calculated at the average of those rates.

(3) For the purposes of this section, a written certificate purporting to be signed by an officer of any bank in New Zealand that a specified rate of exchange prevailed between currencies on a specified day, and that at such rate a specified sum in a particular currency is equivalent to a specified sum in terms of the currency of New Zealand, is sufficient evidence of the rate of exchange so prevailing and of the equivalent sums in terms of the respective currencies.

Compare: 1996 No 9 s 4

8 Act binds the Crown

This Act binds the Crown.

Part 2
AML/CFT requirements and compliance

9 Non-compliance not excused by contractual obligations

(1) This Act has effect despite anything to the contrary in any contract or agreement.

(2) No person is excused from compliance with any requirement of this Act or regulations by reason only that compliance with that requirement would constitute breach of any contract or agreement.

Subpart 1—Customer due diligence

10 Definitions

In this subpart, unless the context otherwise requires,—

enhanced customer due diligence means customer due diligence in accordance with the requirements set out in sections 23 to 30 and any other requirements prescribed by regulations

simplified customer due diligence means customer due diligence in accordance with the requirements set out in sections 19 to 21 and any other requirements prescribed by regulations

standard customer due diligence means customer due diligence in accordance with the requirements set out in sections 15 to 17 and any other requirements prescribed by regulations.

11 Customer due diligence

(1) A reporting entity must conduct customer due diligence on—
- (a) a customer:
- (b) any beneficial owner of a customer:
- (c) any person acting on behalf of a customer.

(2) For the purposes of subsection (1)(b), a customer who is an individual and who the reporting entity believes on reasonable grounds is not acting on behalf of another person is to be treated as if he or she were also the beneficial owner unless the reporting entity has reasonable grounds to suspect that that customer is not the beneficial owner.

(3) The type of customer due diligence that must be conducted by a reporting entity is,—
- (a) in the circumstances described in section 14, at least standard customer due diligence:
- (b) in the circumstances described in section 18, at least simplified customer due diligence:
- (c) in the circumstances described in section 22, enhanced customer due diligence.

(4) A reporting entity that is required to conduct customer due diligence in the circumstances described in sections 14, 18, and 22 is not required to obtain or verify any documents, data, or information that it has previously obtained and verified for the purposes of carrying out customer due diligence in accordance with this Act, unless there are reasonable grounds for the reporting entity to doubt the adequacy or veracity of the documents, data, or information previously obtained.

(5) Nothing in subsection (4) affects the obligation to conduct ongoing customer due diligence in accordance with section 31.

12 Reliance on risk assessment when establishing level of risk

When establishing the level of risk involved for the purposes of this subpart, a reporting entity must rely on its AML/CFT programme and its risk assessment undertaken in accordance with section 58.

13 Basis for verifying identity

Verification of identity must be done on—

(a) the basis of documents, data, or information issued by a reliable and independent source; or

(b) any other basis applying to a specified situation, customer, product, service, business relationship, or transaction prescribed by regulations.

Standard customer due diligence

14 Circumstances when standard customer due diligence applies

A reporting entity must conduct standard customer due diligence in the following circumstances:

(a) if the reporting entity establishes a business relationship with a new customer:

(b) if a customer seeks to conduct an occasional transaction through the reporting entity:

(c) if, in relation to an existing customer, and according to the level of risk involved,—

(i) there has been a material change in the nature or purpose of the business relationship; and

(ii) the reporting entity considers that it has insufficient information about the customer:

(d) any other circumstances specified in regulations.

15 Standard customer due diligence: identity requirements

A reporting entity must obtain the following identity information in relation to the persons referred to in section 11(1):

(a) the person's full name; and

(b) the person's date of birth; and
(c) if the person is not the customer, the person's relationship to the customer; and
(d) the person's address or registered office; and
(e) the person's company identifier or registration number; and
(f) any information prescribed by regulations.

16 Standard customer due diligence: verification of identity requirements

(1) A reporting entity must—
(a) take reasonable steps to satisfy itself that the information provided under section 15 is correct; and
(b) according to the level of risk involved, take reasonable steps to verify any beneficial owner's identity so that the reporting entity is satisfied that it knows who the beneficial owner is; and
(c) if a person is acting on behalf of the customer, according to the level of risk involved, take reasonable steps to verify the person's identity and authority to act on behalf of the customer so that the reporting entity is satisfied it knows who the person is and that the person has authority to act on behalf of the customer; and
(d) verify any other information prescribed by regulations.

(2) Except as provided in subsection (3), a reporting entity must carry out verification of identity before establishing a business relationship or conducting an occasional transaction.

(3) Verification of identity may be completed after the business relationship has been established if—
(a) it is essential not to interrupt normal business practice; and
(b) money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring; and
(c) verification of identity is completed as soon as is practicable once the business relationship has been established.

17 Standard customer due diligence: other requirements

A reporting entity must also obtain—

(a) information on the nature and purpose of the proposed business relationship between the customer and the reporting entity; and

(b) sufficient information to determine whether the customer should be subject to enhanced customer due diligence.

Simplified customer due diligence

18 Circumstances when simplified customer due diligence applies

(1) A reporting entity may conduct simplified customer due diligence if—

(a) it establishes a business relationship with one of the customers specified in subsection (2); or

(b) one of the customers specified in subsection (2) conducts an occasional transaction through the reporting entity; or

(c) a customer conducts a transaction or provides a product or service specified in regulations through the reporting entity.

(2) The following are customers for the purposes of subsection (1):

(a) a company that is listed on an exchange registered under Part 2B of the Securities Markets Act 1988:

(b) a government department named in Schedule 1 of the State Sector Act 1988:

(c) a local authority as defined in section 5 of the Local Government Act 2002:

(d) the New Zealand Police:

(e) the New Zealand Security Intelligence Service:

(f) any other entity or class of entities specified in regulations.

(3) A reporting entity may also conduct simplified customer due diligence on a person who purports to act on behalf of a customer when—

(a) the reporting entity already has a business relationship with the customer at the time the person acts on behalf of the customer; and

(b) the reporting entity has conducted one of the specified types of customer due diligence on the customer in accordance with this Act and regulations (if any).

(4) For the avoidance of doubt, nothing in this subpart requires identification or verification of identity of a beneficial owner of a customer in respect of whom a reporting entity may conduct simplified customer due diligence.

19 Simplified customer due diligence: identity requirements

A reporting entity must obtain the following identity information in relation to a person acting on behalf of the customer:

(a) the person's full name; and

(b) the person's date of birth; and

(c) the person's relationship to the customer; and

(d) any information prescribed by regulations.

20 Simplified customer due diligence: verification of identity requirements

(1) A reporting entity must, according to the level of risk involved, verify the identity of a person acting on behalf of a customer and that person's authority to act for the customer so that it is satisfied it knows who the person is and that the person has authority to act on behalf of the customer.

(2) Verification of identity must be carried out before the business relationship is established or the occasional transaction is conducted or the person acts on behalf of the customer.

(3) For the purposes of verifying a person's authority to act in the circumstances described in section 18, a reporting entity may rely on an authority provided in an application form or other document provided to the reporting entity that shows a person's authority to act or transact on an account.

21 Simplified customer due diligence: other requirements

In the circumstances described in section 18(1)(a), a reporting entity must also obtain information on the nature and purpose

of the proposed business relationship between the customer and the reporting entity.

Enhanced customer due diligence

22 Circumstances when enhanced customer due diligence applies

(1) A reporting entity must conduct enhanced customer due diligence in accordance with sections 23 and 24 in the following circumstances:

(a) if the reporting entity establishes a business relationship with a customer that is—

(i) a trust or another vehicle for holding personal assets:

(ii) a non-resident customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place:

(iii) a company with nominee shareholders or shares in bearer form:

(b) if a customer seeks to conduct an occasional transaction through the reporting entity and that customer is—

(i) a trust or another vehicle for holding personal assets:

(ii) a non-resident customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place:

(iii) a company with nominee shareholders or shares in bearer form:

(c) if a customer seeks to conduct, through the reporting entity, a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose:

(d) when a reporting entity considers that the level of risk involved is such that enhanced due diligence should apply to a particular situation:

(e) any other circumstances specified in regulations.

(2) A reporting entity must conduct enhanced customer due diligence in accordance with section 26 if—

(a) it establishes a business relationship with a customer who it has determined is a politically exposed person; or

(b) a customer who it has determined is a politically exposed person seeks to conduct an occasional transaction through the reporting entity.

(3) A reporting entity must conduct enhanced customer due diligence in accordance with sections 27 and 28 if it is an ordering institution, an intermediary institution, or a beneficiary institution in relation to a wire transfer.

(4) A reporting entity must conduct enhanced customer due diligence in accordance with section 29 if it has, or proposes to have, a correspondent banking relationship.

(5) A reporting entity must conduct enhanced due diligence in accordance with section 30 if—

(a) it establishes a business relationship with a customer that involves new or developing technologies, or new or developing products, that might favour anonymity; or

(b) a customer seeks to conduct an occasional transaction through the reporting entity that involves new or developing technologies, or new or developing products, that might favour anonymity.

23 Enhanced customer due diligence: identity requirements

A reporting entity must, in relation to a person referred to in section 11(1), obtain the information required under section 15 and the following additional information:

(a) information relating to the source of the funds or the wealth of the customer; and

(b) any additional information prescribed by regulations.

24 Enhanced customer due diligence: verification of identity requirements

(1) A reporting entity must—

(a) conduct the verification of identity requirements for standard customer due diligence set out in section 16; and

(b) according to the level of risk involved, take reasonable steps to verify the information obtained under section 23(a); and

(c) verify any other information prescribed by regulations.

(2) Except as provided in subsection (3), a reporting entity must carry out verification of identity before establishing a business relationship or conducting an occasional transaction.

(3) Verification of identity may be completed after the business relationship has been established if—

(a) it is essential not to interrupt normal business practice; and

(b) money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring; and

(c) verification of identity is completed as soon as is practicable once the business relationship has been established.

25 Enhanced customer due diligence: other requirements

In the circumstances described in section 22(1)(a), 22(2)(a), and 22(5)(a), a reporting entity must also obtain information on the nature and purpose of the proposed business relationship between the customer and the reporting entity.

26 Politically exposed person

(1) The reporting entity must, as soon as practicable after establishing a business relationship or conducting an occasional transaction, take reasonable steps to determine whether the customer or any beneficial owner is a politically exposed person.

(2) If a reporting entity determines that a customer or beneficial owner with whom it has established a business relationship is a politically exposed person, then—

(a) the reporting entity must have senior management approval for continuing the business relationship; and

(b) the reporting entity must obtain information about the source of wealth or funds of the customer or beneficial owner and take reasonable steps to verify the source of that wealth or those funds.

(3) If a reporting entity determines that a customer or beneficial owner with whom it has conducted an occasional transaction is a politically exposed person, then the reporting entity must, as soon as practicable after conducting that transaction, take reasonable steps to obtain information about the source of wealth or funds of the customer or beneficial owner and verify the source of that wealth or those funds.

27 Wire transfers: identity requirements

(1) A reporting entity that is an ordering institution must identify the originator of a wire transfer that is over the applicable threshold value by obtaining the following information:
- (a) the originator's full name; and
- (b) the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator; and
- (c) one of the following:
  - (i) the originator's address:
  - (ii) the originator's national identity number:
  - (iii) the originator's customer identification number:
  - (iv) the originator's place and date of birth; and
- (d) any information prescribed by regulations.

(2) However, if the wire transfer is a domestic wire transfer, a reporting entity that is an ordering institution may identify the originator by obtaining the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator if the reporting entity that is the ordering institution is able to provide the information specified in subsection (1)(a), (c), and (d) within 3 working days of a request being made by the beneficiary institution.

(3) Regulations may be made under section 154(1)(c) exempting the reporting entity from the obligation to obtain some or all of the information set out in subsection (1) in relation to a specified transfer or transaction.

(4) The information obtained by the reporting entity (the ordering institution under subsection (1) or (2), as the case may be) must accompany the wire transfer.

(5) A reporting entity that is a beneficiary institution must—

(a) use effective risk-based procedures for handling wire transfers that are not accompanied by all the information specified in subsection (1); and

(b) consider whether the wire transfers constitute a suspicious transaction.

(6) Any information obtained by a reporting entity that is an intermediary institution must be maintained by that reporting entity with the wire transfer accompanying the information.

(7) For the purposes of this section, a **domestic wire transfer** is a wire transfer where the ordering institution, the intermediary institution, and the beneficiary institution are all in New Zealand.

28 Wire transfers: verification of identity requirements

(1) The ordering institution must, according to the level of risk involved,—

(a) verify the originator's identity so that the reporting entity is satisfied that the information provided under section 27 is current and correct; and

(b) verify any other information prescribed by regulations.

(2) Verification of the originator's identity must be carried out before the wire transfer is ordered.

29 Correspondent banking relationships

(1) A financial institution (the **correspondent**) that has, or proposes to have, a correspondent banking relationship with a respondent financial institution (the **respondent**) must, according to the level of risk involved, conduct enhanced customer due diligence as set out in subsection (2) in relation to correspondent accounts that are used, or are proposed to be used, for payments to, or receipts from, foreign financial institutions.

(2) The correspondent must—

(a) gather enough information about the respondent to understand fully the nature of the respondent's business; and

(b) determine from publicly available information the reputation of the respondent and whether and to what extent the respondent is supervised for AML/CFT purposes,

including whether the respondent has been subject to a money laundering or financing of terrorism investigation or regulatory action; and

(c) assess the respondent's anti-money laundering and countering financing of terrorism controls to ascertain that those controls are adequate and effective; and

(d) have approval from its senior management before establishing a new correspondent banking relationship; and

(e) document the respective AML/CFT responsibilities of the correspondent and the respondent; and

(f) be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent—

(i) has verified the identity of, and conducts ongoing monitoring in respect of, those customers; and

(ii) is able to provide to the correspondent, on request, the documents, data, or information obtained when conducting the relevant customer due diligence and ongoing customer due diligence; and

(g) meet any other requirements prescribed by regulations and that apply to correspondent banking relationships.

(3) For the purposes of this Act, a **correspondent banking relationship** means a relationship that involves the provision of banking services by a financial institution (the **correspondent**) to another financial institution (the **respondent**) if—

(a) the correspondent carries on an activity or business at or through a permanent establishment of the correspondent in a particular country; and

(b) the respondent carries on an activity or business at or through a permanent establishment of the respondent in another country; and

(c) the correspondent banking relationship relates, in whole or in part, to those permanent establishments; and

(d) the relationship is not of a kind specified in regulations; and

(e) the banking services are not of a kind specified in regulations.

30 New or developing technologies, or products, that might favour anonymity

Before a reporting entity establishes a business relationship or conducts an occasional transaction that involves new or developing technologies, or new or developing products, that might favour anonymity, the reporting entity must, in addition to the requirements in sections 15 and 16,—

(a) take any additional measures that may be needed to mitigate and manage the risk of new or developing technologies, or new or developing products, that might favour anonymity from being used in the commission of a money laundering offence or for the financing of terrorism; and

(b) meet any other requirements prescribed by regulations and that apply to the particular technology or product.

Ongoing customer due diligence and account monitoring

31 Ongoing customer due diligence and account monitoring

(1) This section applies to a business relationship between a reporting entity and a customer.

(2) A reporting entity must conduct ongoing customer due diligence and undertake account monitoring in order to—

(a) ensure that the business relationship and the transactions relating to that business relationship are consistent with the reporting entity's knowledge about the customer and the customer's business and risk profile; and

(b) identify any grounds for reporting a suspicious transaction under section 40(1)(b).

(3) When conducting ongoing customer due diligence and undertaking account monitoring, the reporting entity must have regard to—

(a) the type of customer due diligence conducted when the business relationship with the customer was established; and

(b) the level of risk involved.

(4) When conducting ongoing customer due diligence and undertaking account monitoring, a reporting entity must do at least the following:

(a) regularly review the customer's account activity and transaction behaviour; and

(b) regularly review any customer information obtained under sections 15, 17, 19, 21, 23, 25, 26, 27, 29, and 30, or, in relation to an existing customer, any customer information the reporting entity holds about the customer; and

(c) anything prescribed by regulations.

Reliance on third parties

32 Reliance on member of designated business group

(1) A reporting entity (**member A**) that is a member of a designated business group may—

(a) rely on another member of the group (**member B**) to conduct any customer due diligence procedures required for customer due diligence under this Act or regulations as long as—

(i) any identity information is given to member A by member B before member A establishes a business relationship or an occasional transaction is conducted; and

(ii) any verification information is given to member A by member B as soon as practicable, but no later than 5 working days, after the business relationship is established or the occasional transaction is conducted:

(b) adopt that part of an AML/CFT programme of another member of the group that relates to record keeping, account monitoring, ongoing customer due diligence, and annual reporting and share and use the procedures, policies, and controls relating to those parts of the programme subject to any conditions prescribed by regulations:

(c) use another member of the group's risk assessment if that risk assessment is relevant to member A's business:

(d) make a suspicious transaction report on behalf of any other member or all members of the designated business group.

(2) Despite subsection (1), a reporting entity, and not the member of the designated business group relied on by the reporting entity, is responsible for ensuring that it is complying with this Act and regulations.

(3) An AML/CFT supervisor for a reporting entity that is part of a designated business group may require the reporting entity to undertake its own risk assessment or develop its own AML/CFT programme if the AML/CFT supervisor is of the view that the risk assessment or AML/CFT programme being, or proposed to be, relied on by the reporting entity is not appropriate for that entity.

(4) This section is subject to section 36, which relates to the protection of personal information.

Compare: Anti-Money Laundering and Counter-Terrorism Financing Act 2006 s 36(4) (Aust)

33 Reliance on other reporting entities or persons in another country

(1) Subject to the conditions in subsection (2), a reporting entity may rely on another person (who is not an agent) to conduct the customer due diligence procedures required for customer due diligence under this Act or regulations.

(2) The conditions are that—

(a) the person being relied on is either—

(i) a reporting entity; or

(ii) a person who is resident in a country with sufficient anti-money laundering and countering financing of terrorism systems and measures in place and who is supervised or regulated for AML/CFT purposes; and

(b) the person has a business relationship with the customer concerned; and

(c) the person has conducted relevant customer due diligence procedures to at least the standard required by this Act and regulations and has provided to the reporting entity—

(i) relevant identity information before the reporting entity establishes a business relationship or an occasional transaction is conducted; and

(ii) relevant verification information as soon as practicable, but no later than 5 working days, after the business relationship is established or the occasional transaction is conducted; and

(d) the person consents to conducting the customer due diligence procedures for the reporting entity and to providing all relevant information to the reporting entity; and

(e) any other conditions prescribed by regulations are complied with.

(3) Despite subsection (1), a reporting entity relying on a third party to conduct the customer due diligence procedure, and not the person carrying out the customer due diligence procedure, is responsible for ensuring that customer due diligence is carried out in accordance with this Act.

34 Reliance on agents

Subject to any conditions that may be prescribed by regulations, a reporting entity may authorise a person to be its agent and rely on that agent to conduct the customer due diligence procedures and obtain any information required for customer due diligence under this Act or regulations.

35 Use of information obtained from third party conducting customer due diligence

Information obtained by a third party conducting customer due diligence under sections 32 to 34 for a reporting entity may only be used by that third party for the purpose of complying with this Act and regulations.

36 Protection of personal information and designated business groups

(1) This section applies to personal information that is either—

(a) identity or verification information received for the purposes of ; or

(b) information received for the purposes of section 32(1)(b).

(2) Any information supplied by any member of a designated business group to another member of that group must be subject to privacy protections at least equivalent to those set out in privacy principles 5 to 11 in section 6 of the Privacy Act 1993.

(3) Each member of the designated business group must agree, in writing, to comply with privacy principles 5 to 11 in section 6 of the Privacy Act 1993 or their equivalent if the member is resident overseas.

(4) The entity that provides information to another member of its designated business group remains responsible for the use or disclosure of that information.

(5) A reporting entity may use or disclose information to which this section applies only as follows:

(a) it may use identity and verification information received for the purposes of in a suspicious transactions report:

(b) it may disclose information for the purposes of section 32(1)(b) to another member of the designated business group unless such disclosure is likely to result in a suspicious transaction report being filed in an overseas jurisdiction by the member to whom the information is disclosed.

Prohibitions

37 Prohibitions if customer due diligence not conducted

If, in relation to a customer, a reporting entity is unable to conduct customer due diligence in accordance with this subpart, the reporting entity—

(a) must not establish a business relationship with the customer; and

(b) must terminate any existing business relationship with the customer; and

(c) must not carry out an occasional transaction with or for the customer; and

(d) must consider whether to make a suspicious transactions report; and

(e) may disclose the possibility of making a suspicious transaction report only to a person referred to in section 46(2).

38 Prohibition on false customer names and customer anonymity

(1) A reporting entity must not,—

(a) knowingly or recklessly, set up a facility for a customer on the basis of customer anonymity:

(b) without lawful justification or reasonable excuse, set up a facility for a customer under a false customer name.

(2) Subsection (1) does not apply to a facility—

(a) that has a number or other identifier allocated to it and the customer or the person who is authorised to act on behalf of the customer in respect of the facility has had their identity verified in accordance with the relevant customer due diligence requirements; or

(b) that has been set up for the Commissioner or for the New Zealand Security Intelligence Service for law enforcement purposes.

39 Prohibition on establishing or continuing business relationship involving shell bank

(1) A reporting entity must not establish or continue a business relationship with, or allow an occasional transaction to be conducted through it by,—

(a) a shell bank; or

(b) a financial institution that has a correspondent banking relationship with a shell bank.

(2) For the purposes of subsection (1), a **shell bank** is a corporation that—

(a) is incorporated in a foreign country; and

(b) is authorised to carry on banking business in its country of incorporation; and

(c) does not have a physical presence in its country of incorporation; and

(d) is not an affiliate of another corporation that—

(i) is incorporated in a particular country; and

(ii) is authorised to carry on banking business in its country of incorporation; and

(iii) is sufficiently supervised and monitored in carrying on its banking business; and

(iv) has a physical presence in its country of incorporation.

(3) For the purposes of paragraph (d) of the definition of **shell bank** in subsection (2), a corporation is affiliated with another corporation only if—

(a) the corporation is a subsidiary of the other corporation; or

(b) both corporations are under common effective control; or

(c) both corporations are declared to be affiliated in accordance with regulations (if any).

(4) For the purposes of the definition of **shell bank** in subsection (2), a corporation has a physical presence in a country if, and only if,—

(a) the corporation carries on banking business at a place in that country; and

(b) banking operations of the corporation are managed and conducted from that place.

Compare: Anti-Money Laundering and Counter-Terrorism Financing Act 2006 ss 15, 95 (Aust)

Subpart 2—Suspicious transaction reports

40 Reporting entities to report suspicious transactions

(1) Despite any other enactment or any rule of law, but subject to section 42 of this Act and to section 44(4) of the Terrorism Suppression Act 2002, this section applies if—

(a) a person conducts or seeks to conduct a transaction through a reporting entity; and

(b) the reporting entity has reasonable grounds to suspect that the transaction or proposed transaction is or may be—

(i) relevant to the investigation or prosecution of any person for a money laundering offence; or

(ii) relevant to the enforcement of the Misuse of Drugs Act 1975; or

(iii) relevant to the enforcement of the Terrorism Suppression Act 2002; or

(iv) relevant to the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009; or

(v) relevant to the investigation or prosecution of a serious offence within the meaning of section 243(1) of the Crimes Act 1961.

(2) If this section applies, the reporting entity must, as soon as practicable, but no later than 3 working days after forming its suspicion, report the transaction or proposed transaction to the Commissioner, in accordance with section 41.

(3) Nothing in subsection (2) requires any lawyer to disclose any privileged communication (as defined in section 42).

Compare: 1996 No 9 ss 15(1), 19(1)

41 Nature of suspicious transaction report

(1) Except as provided in subsection (2), a report under section 40 must—

(a) be in the prescribed form (if any); and

(b) contain the details prescribed by regulations; and

(c) contain a statement of the grounds on which the reporting entity holds the suspicions referred to in section 40(1)(b); and

(d) be signed by a person authorised by the reporting entity to sign suspicious transaction reports (unless the report is forwarded by email or another similar means of communication); and

(e) be forwarded, in writing, to the Commissioner—

(i) by way of secure electronic transmission by a means specified or provided by the Commissioner for this purpose; or

(ii) by another means (including, without limitation, by way of transmission by fax or email) that may be agreed from time to time between the Commissioner and the reporting entity concerned.

(2) However, if the urgency of the situation requires, a suspicious transaction report may be made orally to any Police employee authorised for the purpose by the Commissioner, but in any

such case the reporting entity must, as soon as practicable, but no later than 3 working days, forward to the Commissioner a suspicious transaction report that complies with the requirements in subsection (1).

(3) The Commissioner may confer the authority to receive a suspicious transaction report under subsection (2) on—

(a) any specified Police employee; or

(b) Police employees of any specified rank or class; or

(c) any Police employee or Police employees for the time being holding any specified office or specified class of offices.

Compare: 1996 No 9 s 15(2)–(4)

42 Privileged communication defined

(1) For the purposes of section 40(3), a communication is a **privileged communication** only if—

(a) it is a confidential communication, whether oral or written, passing between—

(i) a lawyer in his or her professional capacity and another lawyer in that capacity:

(ii) a lawyer in his or her professional capacity and his or her client:

(iii) any person described in subparagraph (i) or (ii) and the agent of the other person described in that subparagraph, or between the agents of both the persons described, either directly or indirectly; and

(b) it is made or brought into existence for the purpose of obtaining or giving legal advice or assistance; and

(c) it is not made or brought into existence for the purpose of committing or furthering the commission of some illegal or wrongful act.

(2) However, where the information consists wholly or partly of, or relates wholly or partly to, the receipts, payments, income, expenditure, or financial transactions of a specified person (whether a lawyer, his or her client, or any other person), it is not a privileged communication if it is contained in, or comprises the whole or part of, any book, account, statement, or other record prepared or kept by the lawyer in connection

with a trust account of the lawyer within the meaning of section 6 of the Lawyers and Conveyancers Act 2006.

(3) For the purposes of this section, references to a lawyer include a firm in which he or she is a partner or is held out to be a partner.

Compare: 1996 No 9 s 19(2)–(4)

43 Auditors may report suspicious transactions

(1) Despite any other enactment or any rule of law, this section applies to a person who, in the course of carrying out the duties of that person's occupation as an auditor, has reasonable grounds to suspect, in relation to any transaction, that the transaction is—

- (a) relevant to the investigation or prosecution of any person for a money laundering offence; or
- (b) relevant to the enforcement of the Misuse of Drugs Act 1975; or
- (c) relevant to the enforcement of the Terrorism Suppression Act 2002; or
- (d) relevant to the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009; or
- (e) relevant to the investigation or prosecution of a serious offence within the meaning of section 243(1) of the Crimes Act 1961.

(2) A person may report a transaction referred to in subsection (1) to the Commissioner.

Compare: 1996 No 9 s 16

44 Protection of persons reporting suspicious transactions

(1) Subsection (2) applies to a person who—

- (a) discloses or supplies any information in any suspicious transaction report; or
- (b) supplies any information in connection with any suspicious transaction report, whether at the time the report is made or afterwards.

(2) No civil, criminal, and disciplinary proceedings lie against a person to whom subsection (1) applies—

(a) in respect of the disclosure or supply, or the manner of the disclosure or supply, by that person of the information referred to in that subsection; or

(b) for any consequences that follow from the disclosure or supply of that information.

(3) If any information is reported under section 43 to any Police employee by any person, no civil, criminal, or disciplinary proceedings lie against that person—

(a) in respect of the disclosure or supply, or the manner of the disclosure or supply, of that information by that person; or

(b) for any consequences that follow from the disclosure or supply of that information.

(4) However, subsections (2) and (3) do not apply if the information was disclosed or supplied in bad faith.

(5) Nothing in this section applies in respect of proceedings for an offence under any of sections 92 to 97.

Compare: 1996 No 9 s 17

45 Immunity from liability for disclosure of information relating to money laundering transactions

(1) This section applies if—

(a) a person does any act that would constitute, or the person believes would constitute, an offence against of the Crimes Act 1961; and

(b) in respect of the doing of that act, that person would have, by virtue of of the Crimes Act 1961, a defence to a charge under of that Act; and

(c) that person discloses, to any Police employee, any information relating to a money laundering transaction (within the meaning of section 243(4) of the Crimes Act 1961), being a money laundering transaction that constitutes (in whole or in part), or is connected with or related to, the act referred to in paragraph (a); and

(d) that information is so disclosed, in good faith, for the purpose of, or in connection with, the enforcement or intended enforcement of any enactment or provision referred to in section 244(a) of the Crimes Act 1961; and

(e) that person is otherwise under any obligation (whether arising by virtue of any enactment or any rule of law or any other instrument) to maintain secrecy in relation to, or not to disclose, that information.

(2) If this section applies, then, without limiting section 44 and despite that the disclosure would otherwise constitute a breach of that obligation of secrecy or non-disclosure, the disclosure by that person, to that Police employee, of that information is not a breach of that obligation of secrecy or non-disclosure or (where applicable) of any enactment by which that obligation is imposed.

Compare: 1996 No 9 s 18

46 Disclosure of information relating to suspicious transaction reports

(1) This section and section 47 apply in respect of the following information:

(a) any suspicious transaction report:

(b) any information the disclosure of which will identify, or is reasonably likely to identify, any person—

(i) as a person who, in his or her capacity as an officer or employee of a reporting entity, has handled a transaction in respect of which a suspicious transaction report was made; or

(ii) as a person who has prepared a suspicious transaction report; or

(iii) as a person who has made a suspicious transaction report:

(c) any information that discloses, or is reasonably likely to disclose, the existence of a suspicious transaction report.

(2) A reporting entity must not disclose information to which this section relates to any person except—

(a) a Police employee who is authorised by the Commissioner to receive the information; or

(b) the reporting entity's AML/CFT supervisor; or

(c) an officer or employee of the reporting entity, for any purpose connected with the performance of that person's duties; or

(d) a barrister or solicitor, for the purpose of obtaining legal advice or representation in relation to the matter; or

(e) another member of a designated business group of which the reporting entity is a member to the extent necessary to decide whether to make a suspicious transaction report.

(3) A Police employee may only disclose information to which this section applies for law enforcement purposes.

(4) An AML/CFT supervisor may only disclose information to which this section applies to the Police for law enforcement purposes.

(5) A person to whom a function or power has been delegated under section 134 may disclose information to which this section applies only to the AML/CFT supervisor that made the delegation.

(6) A person (**person A**) referred to in subsection (2)(c) to whom disclosure of any information to which that subsection applies has been made must not disclose that information except to another person of the kind referred to in that subsection for the purpose of—

(a) the performance of person A's duties; or

(b) obtaining legal advice or representation in relation to the matter.

(7) A person referred to in subsection (2)(d) to whom disclosure of any information to which that subsection applies has been made must not disclose that information except to a person of the kind referred to in that subsection for the purpose of giving legal advice or making representations in relation to the matter.

(8) Any other person who has information to which this section applies may only disclose that information to the Police for law enforcement purposes.

Compare: 1996 No 9 s 20

47 Disclosure of information in proceedings

(1) No person may disclose, in any judicial proceeding (within the meaning of section 108 of the Crimes Act 1961), any information to which this section applies unless the Judge or, as the case requires, the person presiding at the proceeding is sat-

isfied that the disclosure of the information is necessary in the interests of justice.

(2) Nothing in this section prohibits the disclosure of any information for the purposes of the prosecution of any offence against section 93 or 94.

Compare: 1996 No 9 s 21

48 Disclosure of personal information relating to employees or senior managers

An AML/CFT supervisor that has, in the performance and exercise of its functions and powers under this Act, obtained personal information about employees or senior managers may disclose that information to another government agency for the following purposes if the AML/CFT supervisor is satisfied that the agency has a proper interest in receiving the information:

(a) law enforcement purposes:

(b) the detection, investigation, and prosecution of any offence under the following Acts:

(i) the Companies Act 1993:

(ii) the Financial Advisers Act 2008:

(iii) the Financial Service Providers (Registration and Dispute Resolution) Act 2008:

(iv) the Gambling Act 2003:

(v) the Reserve Bank of New Zealand Act 1989:

(vi) the Securities Act 1978:

(vii) the Securities Markets Act 1988.

Subpart 3—Record keeping

49 Obligation to keep transaction records

(1) In relation to every transaction that is conducted through a reporting entity, the reporting entity must keep those records that are reasonably necessary to enable that transaction to be readily reconstructed at any time.

(2) Without limiting subsection (1), records must contain the following information:

(a) the nature of the transaction:

(b) the amount of the transaction and the currency in which it was denominated:
(c) the date on which the transaction was conducted:
(d) the parties to the transaction:
(e) if applicable, the facility through which the transaction was conducted, and any other facilities (whether or not provided by the reporting entity) directly involved in the transaction:
(f) the name of the officer or employee or agent of the reporting entity who handled the transaction, if that officer, employee, or agent—
(i) has face-to-face dealings in respect of the transaction with any of the parties to the transaction; and
(ii) has formed a suspicion (of the kind referred to in section 40(1)(b)) about the transaction:
(g) any other information prescribed by regulations.

(3) A reporting entity must retain the records kept by that reporting entity, in accordance with this section, in relation to a transaction for—
(a) a period of at least 5 years after the completion of that transaction; or
(b) any longer period that the AML/CFT supervisor for the reporting entity, or the Commissioner, specifies.

Compare: 1996 No 9 s 29

50 Obligation to keep identity and verification records

(1) In respect of each case in which a reporting entity is required, under subpart 1 of this Part, to identify and verify the identity of a person, the reporting entity must keep those records that are reasonably necessary to enable the nature of the evidence used for the purposes of that identification and verification to be readily identified at any time.

(2) Without limiting subsection (1), those records may comprise—
(a) a copy of the evidence so used; or
(b) if it is not practicable to retain that evidence, any information as is reasonably necessary to enable that evidence to be obtained.

(3) A reporting entity must retain the records kept by that reporting entity for,—

(a) in the case of records relating to the identity and verification of the identity of a person in relation to establishing a business relationship, a period of at least 5 years after the end of that business relationship; or

(b) in the case of records relating to the identity and verification of the identity of a person in relation to conducting an occasional transaction, a period of at least 5 years after the completion of that occasional transaction; or

(c) in the case of records relating to the identity and verification of the identity of an originator in relation to a wire transfer,—

(i) if the wire transfer is conducted by a customer with whom the reporting entity has a business relationship, a period of at least 5 years after the end of that business relationship; or

(ii) if the wire transfer is an occasional transaction, a period of at least 5 years after the completion of the wire transfer.

Compare: 1996 No 9 s 30

51 Obligation to keep other records

(1) A reporting entity must keep the following records in addition to the records referred to in sections 49 and 50:

(a) records that are relevant to the establishment of the business relationship; and

(b) records relating to risk assessments, AML/CFT programmes, and audits; and

(c) any other records (for example, account files, business correspondence, and written findings) relating to, and obtained during the course of, a business relationship that are reasonably necessary to establish the nature and purpose of, and activities relating to, the business relationship.

(2) The records must be kept in accordance with section 52 for a period of at least 5 years after the end of the business relationship.

(3) A reporting entity must make records relating to risk assessments, AML/CFT programmes, and audits available to its AML/CFT supervisor on request.

Compare: 1996 No 9 s 31

52 How records to be kept

Records required by this subpart to be kept by a reporting entity must—

(a) be kept either in written form in the English language, or so as to enable the records to be readily accessible and readily convertible into written form in the English language; and

(b) be kept in the manner prescribed by regulations (if any).

Compare: 1996 No 9 s 32

53 When records need not be kept

(1) Nothing in this subpart requires the retention of any records kept by a reporting entity that has been liquidated and finally dissolved except as provided in subsection (2).

(2) The High Court may, in relation to a reporting entity that is being or has been liquidated, make an order requiring that any or all of the records referred to in sections 50 and 51 be kept for any period it thinks fit.

Compare: 1996 No 9 s 33

54 Destruction of records

(1) Subject to subsection (2), a reporting entity must take all practicable steps to ensure that every record retained by that reporting entity under this subpart, and every copy of that record, is destroyed as soon as practicable after the expiry of the period for which the reporting entity is required to retain that record.

(2) Nothing in this section requires the destruction of any record, or any copy of any record, in any case where there is a lawful reason for retaining that record.

(3) Without limiting subsection (2), there is a lawful reason for retaining a record if the retention of that record is necessary—

(a) in order to comply with the requirements of any other enactment; or

(b) to enable a reporting entity to carry on its business; or
(c) for the purposes of the detection, investigation, or prosecution of any offence.

Compare: 1996 No 9 s 34

55 Other laws not affected

Nothing in this subpart limits or affects any other enactment that requires any reporting entity to keep or retain a record.

Compare: 1996 No 9 s 35

Subpart 4—Compliance with AML/CFT requirements

56 Reporting entity must have AML/CFT programme and AML/CFT compliance officer

(1) A reporting entity must establish, implement, and maintain a compliance programme (an **AML/CFT programme**) that includes internal procedures, policies, and controls to—
(a) detect money laundering and the financing of terrorism; and
(b) manage and mitigate the risk of money laundering and financing of terrorism.

(2) A reporting entity must designate an employee as an AML/CFT compliance officer to administer and maintain its AML/CFT programme.

(3) In the case of a reporting entity that does not have employees, the reporting entity must appoint a person to act as its AML/CFT compliance officer.

(4) The AML/CFT compliance officer must report to a senior manager of the reporting entity.

57 Minimum requirements for AML/CFT programmes

A reporting entity's AML/CFT programme must be based on the risk assessment undertaken in accordance with section 58 and include adequate and effective procedures, policies, and controls for—
(a) vetting—
(i) senior managers:
(ii) the AML/CFT compliance officer:

(iii) any other employee that is engaged in AML/CFT related duties; and

(b) training on AML/CFT matters for the following employees:
  (i) senior managers:
  (ii) the AML/CFT compliance officer:
  (iii) any other employee that is engaged in AML/CFT related duties; and

(c) complying with customer due diligence requirements (including ongoing customer due diligence and account monitoring); and

(d) reporting suspicious transactions; and

(e) record keeping; and

(f) setting out what the reporting entity needs to do, or continue to do, to manage and mitigate the risks of money laundering and the financing of terrorism; and

(g) examining, and keeping written findings relating to,—
  (i) complex or unusually large transactions; and
  (ii) unusual patterns of transactions that have no apparent economic or visible lawful purpose; and
  (iii) any other activity that the reporting entity regards as being particularly likely by its nature to be related to money laundering or the financing of terrorism; and

(h) monitoring, examining, and keeping written findings relating to business relationships and transactions from or in countries that do not have or have insufficient anti-money laundering or countering financing of terrorism systems in place and have additional measures for dealing with or restricting dealings with such countries; and

(i) preventing the use, for money laundering or the financing of terrorism, of products (for example, the misuse of technology) and transactions (for example, non-face-to-face business relationships or transactions) that might favour anonymity; and

(j) determining when enhanced customer due diligence is required and when simplified customer due diligence might be permitted; and

(k) providing when a person who is not the reporting entity may, and setting out the procedures for the person to, conduct the relevant customer due diligence on behalf of the reporting entity; and

(l) monitoring and managing compliance with, and the internal communication of and training in, those procedures, policies, and controls.

58 Risk assessment

(1) Before conducting customer due diligence or establishing an AML/CFT programme, a reporting entity must first undertake an assessment of the risk of money laundering and the financing of terrorism (a **risk assessment**) that it may reasonably expect to face in the course of its business.

(2) In assessing the risk, the reporting entity must have regard to the following:

(a) the nature, size, and complexity of its business; and

(b) the products and services it offers; and

(c) the methods by which it delivers products and services to its customers; and

(d) the types of customers it deals with; and

(e) the countries it deals with; and

(f) the institutions it deals with; and

(g) any applicable guidance material produced by AML/CFT supervisors or the Commissioner relating to risk assessments; and

(h) any other factors that may be provided for in regulations.

(3) The risk assessment must be in writing and—

(a) identify the risks faced by the reporting entity in the course of its business; and

(b) describe how the reporting entity will ensure that the assessment remains current; and

(c) enable the reporting entity to determine the level of risk involved in relation to relevant obligations under this Act and regulations.

59 Review and audit of risk assessment and AML/CFT programme

(1) A reporting entity must review its risk assessment and AML/CFT programme to—

(a) ensure the risk assessment and AML/CFT programme remain current; and

(b) identify any deficiencies in the effectiveness of the risk assessment and the AML/CFT programme; and

(c) make any changes to the risk assessment or AML/CFT programme identified as being necessary under paragraph (b).

(2) A reporting entity must ensure its risk assessment and AML/CFT programme are audited every 2 years or at any other time at the request of the relevant AML/CFT supervisor.

(3) The audit must be carried out by an independent person appointed by the reporting entity who is appropriately qualified to conduct the audit.

(4) A person appointed to conduct an audit is not required to be—

(a) a chartered accountant within the meaning of section 19 of the Institute of Chartered Accountants of New Zealand Act 1996; or

(b) qualified to undertake financial audits.

(5) A person appointed to conduct an audit must not have been involved in—

(a) the establishment, implementation, or maintenance of the reporting entity's AML/CFT programme:

(b) the undertaking of the reporting entity's risk assessment.

(6) The audit of the risk assessment is limited to an audit of whether the reporting entity's risk assessment fulfils the requirements in section 58(3).

(7) A reporting entity must provide a copy of any audit to its AML/CFT supervisor on request.

60 Annual AML/CFT report

(1) The reporting entity must prepare an annual report on its risk assessment and AML/CFT programme.

(2) An annual report must—

(a) be in the prescribed form; and
(b) take into account the results and implications of the audit required by section 59(2); and
(c) contain any information prescribed by regulations.

(3) The reporting entity must provide the annual report to its AML/CFT supervisor at a time appointed by the AML/CFT supervisor.

(4) The AML/CFT supervisor must give the reporting entity reasonable notice of the requirement to provide the annual report.

61 Reporting entities to ensure that branches and subsidiaries comply with AML/CFT requirements

(1) A reporting entity must ensure that its branches and subsidiaries that are in a foreign country apply, to the extent permitted by the law of that country, measures broadly equivalent to those set out in this Act and regulations with regard to the requirements for customer due diligence (including ongoing customer due diligence), risk assessments, AML/CFT programmes, and record keeping.

(2) If the law of the foreign country does not permit the application of those equivalent measures by the branch or the subsidiary located in that country, the reporting entity must—
(a) inform its AML/CFT supervisor accordingly; and
(b) take additional measures to effectively handle the risk of a money laundering offence and the financing of terrorism.

(3) A reporting entity must communicate (where relevant) the policies, procedures, and controls that it establishes, implements, and maintains in accordance with this subpart to its branches and subsidiaries that are outside New Zealand.

Subpart 5—Codes of practice

62 Interpretation

In this Part, unless the context otherwise requires,—

code of practice means a code of practice approved by the responsible Minister under section 64, as amended from time to time

proposed code of practice means a document prepared under section 63(1).

63 AML/CFT supervisors to prepare codes of practice for relevant sectors

(1) An AML/CFT supervisor must, if directed to do so by the Minister responsible for that AML/CFT supervisor (the **responsible Minister**), prepare—

(a) 1 or more codes of practice for the sector of activity of the reporting entities for which it is the supervisor under section 130 or in respect of different reporting entities specified by the responsible Minister:

(b) an instrument that amends a code of practice or revokes the whole or any provision of a code of practice prepared under paragraph (a).

(2) The purpose of a code of practice is to provide a statement of practice that assists reporting entities to comply with their obligations under this Act and regulations.

(3) A direction under subsection (1) may (without limitation)—

(a) relate generally to the obligations imposed on the relevant reporting entities by or under this Act or regulations or specify particular aspects of those obligations that are to be covered by the code of practice:

(b) specify the amendments to be made or their intended effect, and specify the extent of the revocation to be made:

(c) indicate the date by which the responsible Minister wishes the code of practice to be provided to him or her:

(d) include details about the recommendation that the AML/CFT supervisor is required to provide under section 64(1)(a).

(4) An AML/CFT supervisor must comply with a direction under subsection (1) as soon as practicable.

(5) No code of practice has legal effect until approved by the responsible Minister under section 64(6).

64 Procedure for approval and publication of codes of practice

(1) The responsible Minister must not approve a code of practice prepared by an AML/CFT supervisor unless—

(a) the AML/CFT supervisor has made a recommendation that the Minister should approve the code of practice; and

(b) the AML/CFT supervisor has consulted the persons and organisations that the Minister thinks appropriate, having regard to the subject matter of the proposed code of practice.

(2) In consulting under subsection (1)(b), the AML/CFT supervisor must ensure that—

(a) a copy of the proposed code of practice or a summary of its contents, in hard copy or electronic format, is provided to the persons and organisations being consulted; and

(b) the persons and organisations being consulted have at least 20 working days to make submissions or representations about the proposed code of practice.

(3) The responsible Minister may direct the AML/CFT supervisor to reconsider any aspect of the proposed code of practice and to make any amendments that the Minister considers necessary.

(4) Despite subsection (3),—

(a) if the AML/CFT supervisor does not amend the proposed code of practice as directed by the Minister or within the time specified by the Minister, the Minister may make those amendments:

(b) the Minister may, after consultation with the AML/CFT supervisor, make any further amendments to the proposed code of practice that he or she considers necessary.

(5) The responsible Minister must—

(a) approve the proposed code of practice as prepared by the AML/CFT supervisor; or

(b) approve the proposed code of practice as amended by the AML/CFT supervisor; or

(c) approve the proposed code of practice as amended by the Minister after consultation with the AML/CFT supervisor.

(6) The responsible Minister approves a code of practice by notice in the *Gazette*, and the notice—

(a) must either set out the code of practice or state where copies of the code of practice in hard copy or electronic format may be obtained or viewed:

(b) is not a regulation for the purposes of the Acts and Regulations Publication Act 1989, but is a regulation for the purposes of the Regulations (Disallowance) Act 1989.

65 Amendment and revocation of codes of practice

(1) A code of practice may be amended or revoked in the same manner as that in which it was made.

(2) Sections 63, 64, 66, and 67 apply with the necessary modifications to the amendment or revocation of a code of practice.

66 Proof of codes of practice

Publication in the *Gazette* of a notice under section 64(6) is conclusive evidence that the requirements of sections 64(1) to (5) and 65 have been complied with in respect of the approval specified in the notice.

67 Legal effect of codes of practice

(1) A reporting entity complies with an obligation imposed on it by or under this Act or regulations by—

(a) complying with those provisions of a code of practice that state a means of satisfying the obligation; or

(b) complying with the obligation by some other equally effective means.

(2) However, a reporting entity may not rely on subsection (1)(b) as a defence to an act or omission on its part unless it has, by notice in writing given before the act or omission occurred, advised the AML/CFT supervisor that it has opted out of compliance with the code of practice and intends to satisfy its obligations by some other equally effective means.

(3) If a person is charged with an offence in respect of a failure to comply with any provision of this Act, a court must, in determining whether that person has failed to comply with the provision, have regard to any code of practice in force under section 64(6) at the time of the alleged failure relating to matters of the kind to which the provision relates.

(4) If an application for an injunction against a person has been made under this Act, a court must, in determining whether to grant the injunction, have regard to any code of practice in force under section 64(6).

(5) If an application for a pecuniary penalty against a person has been made under this Act, a court must, in determining whether to impose a pecuniary penalty, have regard to any code of practice in force under section 64(6) at the time the person engaged in conduct that constituted the relevant civil liability act.

Subpart 6—Cross-border transportation of cash

68 Reports about movement of cash into or out of New Zealand

(1) A person must not move cash into or out of New Zealand if—

(a) the total amount of the cash is more than the applicable threshold value; and

(b) the person has not given a report in respect of the movement of that cash in accordance with this subpart; and

(c) the movement of that cash is not exempted under this Act or regulations (if any).

(2) For the purposes of this Act, a person moves cash into New Zealand if the person brings or sends the cash into New Zealand.

(3) For the purposes of this Act, a person moves cash out of New Zealand if the person takes or sends the cash out of New Zealand.

Compare: Anti-Money Laundering and Counter-Terrorism Financing Act 2006 ss 53(3), 57(2), 58 (Aust)

69 Reports about receipt of cash from outside New Zealand

A person must not receive cash moved to the person from outside New Zealand if—

(a) the total amount of the cash is more than the applicable threshold value; and

(b) the person has not given a report in respect of the movement of that cash in accordance with this subpart; and

(c) the movement of that cash is not exempted under this Act or regulations (if any).

Compare: Anti-Money Laundering and Counter-Terrorism Financing Act 2006 s 55(3) (Aust)

70 Reporting requirements

A report under this subpart must—

(a) be in writing in the prescribed form; and

(b) contain the prescribed information; and

(c) be completed in accordance with regulations (if any); and

(d) be provided to a Customs officer,—

(i) in the case of accompanied cash, at the same time as a departure card is presented in accordance with section 126(2) of the Immigration Act 1987:

(ii) in the case of unaccompanied cash, before the cash leaves New Zealand.

Compare: 1996 No 9 s 37; Anti-Money Laundering and Counter-Terrorism Financing Act 2006 s 55(5) (Aust)

71 Information to be forwarded to Commissioner

(1) If a report is made to a Customs officer under this subpart, that officer must, as soon as practicable, forward the report to the Commissioner.

(2) If, in the course of conducting a search under this Act, a Customs officer discovers any cash in respect of which a report is required to be made under this subpart but has not been made, that officer must, as soon as practicable, report the details of the search, and of the cash, to the Commissioner.

(3) Every report made under subsection (2) must be in the form that the Commissioner may determine after consultation with the chief executive of the New Zealand Customs Service.

(4) The chief executive of the New Zealand Customs Service must—

(a) cause a record to be made and kept of—

(i) each occasion on which a cash report is made to a Customs officer; and

(ii) the details of the identity of the person making the cash report; and

(iii) the date on which the cash report is made; and

(b) ensure that the record is retained for a period of not less than 1 year after the date on which the cash report is made.

Compare: 1996 No 9 s 42

Part 3
Enforcement

Subpart 1—General provisions relating to Part

Proceedings for civil penalties

72 When and how civil penalty proceedings brought

(1) An application for a civil penalty under this Part may be made no later than 6 years after the conduct giving rise to the liability to pay the civil penalty occurred.

(2) In proceedings for a civil penalty under this Part,—

(a) the standard of proof is the standard of proof that applies in civil proceedings; and

(b) the relevant AML/CFT supervisor may, by order of the court, obtain discovery and administer interrogatories.

Relationship between civil penalty and criminal proceedings

73 Relationship between concurrent civil penalty proceedings and criminal proceedings

(1) Criminal proceedings for an offence under this Part may be commenced against a person in relation to particular conduct whether or not proceedings for a civil penalty under this Part have been commenced against the person in relation to the same or substantially the same conduct.

(2) Proceedings under this Part for a civil penalty against a person in relation to particular conduct are stayed if criminal proceedings against the person are or have been commenced for an offence under this Part in relation to the same or substantially the same conduct.

(3) After the criminal proceedings referred to in subsection (2) have been completed or withdrawn, a person may apply to have the stay lifted on the civil penalty proceedings referred to in that subsection.

74 One penalty only rule

(1) If civil penalty or criminal proceedings under this Part are brought against a person in relation to particular conduct, a court may not impose a penalty (whether civil or criminal) on the person if a court has already imposed a penalty under this Part in proceedings relating to the same or substantially the same conduct.

(2) If a person is or may be liable to more than 1 civil penalty under this Part in respect of the same or substantially the same conduct, civil penalty proceedings may be brought against the person for more than 1 civil penalty, but the person may not be required to pay more than 1 civil penalty in respect of the same or substantially the same conduct.

75 Restriction on use of evidence given in civil penalty proceedings

(1) Evidence of information given, or evidence of production of documents, by a person is not admissible in criminal proceedings against the person for an offence under this Part or any other enactment if—

(a) the person previously gave the evidence or produced the documents in civil penalty proceedings under this Part against him or her, whether or not a civil penalty was imposed; and

(b) the proceedings for the civil penalty related to conduct that was the same or substantially the same as the conduct constituting the offence.

(2) This section does not apply to criminal proceedings in respect of the falsity of the evidence given by the person in the proceedings for the civil penalty.

Immunities

76 Protection for AML/CFT supervisors

No civil or criminal proceedings may be brought against an AML/CFT supervisor or a person who is or has been an officer, employee, member of, or member of the board of, an AML/CFT supervisor for anything done or omitted to be done in the course of the performance or exercise of the AML/CFT supervisor's functions or powers under this Act unless it is shown that the AML/CFT supervisor or the person concerned acted in bad faith.

77 Protection for reporting entities, officers, etc, acting in compliance with this Act

No reporting entity, or person who is, or has been, an officer, an employee, or a member of the governing body of the reporting entity, or person appointed under section 56(3) is criminally or civilly liable for any action taken in order to comply with this Act or regulations if the action—

(a) was taken in good faith; and

(b) was reasonable in the circumstances.

Subpart 2—Civil liability

78 Meaning of civil liability act

In this Part, a **civil liability act** occurs when a reporting entity fails to comply with any of the AML/CFT requirements, including, without limitation, when the reporting entity—

(a) fails to conduct customer due diligence as required by subpart 1 of Part 2:

(b) fails to adequately monitor accounts and transactions:

(c) enters into or continues a business relationship with a person who does not produce or provide satisfactory evidence of the person's identity:

(d) enters into or continues a correspondent banking relationship with a shell bank:

(e) fails to keep records in accordance with the requirements of subpart 3 of Part 2:
(f) fails to establish, implement, or maintain an AML/CFT programme:
(g) fails to ensure that its branches and subsidiaries comply with the relevant AML/CFT requirements.

79 Possible responses to civil liability act

If a civil liability act is alleged to have occurred, the relevant AML/CFT supervisor may do 1 or more of the following:

(a) issue a formal warning under section 80:
(b) accept an enforceable undertaking under section 81 and seek an order in the court for breach of that undertaking under section 82:
(c) seek an injunction from the High Court under section 85 or 87:
(d) apply to the court for a pecuniary penalty under section 90.

Formal warnings

80 Formal warnings

(1) The relevant AML/CFT supervisor may issue 1 or more formal warnings to a person if the AML/CFT supervisor has reasonable grounds to believe that that person has engaged in conduct that constituted a civil liability act.

(2) A formal warning must be—
(a) in the prescribed form; and
(b) issued in the manner specified in regulations (if any).

Enforceable undertakings

81 Enforceable undertakings

(1) The relevant AML/CFT supervisor may accept a written undertaking given by a person in connection with compliance with this Act or regulations (if any).

(2) The person may withdraw or vary the undertaking at any time, but only with the consent of the relevant AML/CFT supervisor.

82 Enforcement of undertakings

(1) If the relevant AML/CFT supervisor considers that a person who gave an undertaking under section 81 has breached 1 or more of its terms, the relevant AML/CFT supervisor may apply to the court for an order under subsection (2).

(2) If the court is satisfied that the person has breached 1 or more of the terms of the undertaking, the court may make any or all of the following orders:

(a) an order directing the person to comply with any of the terms of the undertaking:

(b) an order directing the person to pay to the AML/CFT supervisor an amount up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach:

(c) any order that the court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach.

83 Assessment of compensation for breach of undertakings

For the purposes of section 82(2)(c), in determining whether another person (**person A**) has suffered loss or damage as a result of the breach, and in assessing the amount of compensation payable, the court may have regard to the following:

(a) the extent to which any expenses incurred by person A are attributable to dealing with the breach:

(b) the effect of the breach on person A's ability to carry on business or other activities:

(c) any damage to the reputation of person A's business that is attributable to dealing with the breach:

(d) any loss of business opportunities suffered by person A as a result of dealing with the breach:

(e) any other matters that the court considers relevant.

Injunctions

84 Powers of High Court not affected

The powers in sections 85 to 89 are in addition to, and do not derogate from, any other powers of the High Court relating to the granting of injunctions.

85 Performance injunctions

(1) The High Court may, on the application of the relevant AML/CFT supervisor, grant an injunction requiring a person to do an act or thing if—

(a) that person has refused or failed, or is refusing or failing, or is proposing to refuse or fail, to do that act or thing; and

(b) the refusal or failure was, is, or would be a civil liability act.

(2) The court may rescind or vary an injunction granted under this section.

86 When High Court may grant performance injunctions

(1) The High Court may grant an injunction requiring a person to do an act or thing if—

(a) it is satisfied that the person has refused or failed to do that act or thing; or

(b) it appears to the court that, if an injunction is not granted, it is likely that the person will refuse or fail to do that act or thing.

(2) Subsection (1)(a) applies whether or not it appears to the court that the person intends to refuse or fail again, or to continue to refuse or fail, to do that act or thing.

(3) Subsection (1)(b) applies—

(a) whether or not the person has previously refused or failed to do that act or thing; or

(b) where there is an imminent danger of substantial damage to any other person if that person refuses or fails to do that act or thing.

87 Restraining injunctions

(1) The High Court may, on the application of the relevant AML/CFT supervisor, grant an injunction restraining a person from engaging in conduct that constitutes or would constitute a contravention of a provision of this Act.

(2) The court may rescind or vary an injunction granted under this section.

88 When High Court may grant restraining injunctions and interim injunctions

(1) The High Court may grant an injunction restraining a person from engaging in conduct of a particular kind if—

(a) it is satisfied that the person has engaged in conduct of that kind; or

(b) it appears to the court that, if an injunction is not granted, it is likely that the person will engage in conduct of that kind.

(2) The court may grant an interim injunction restraining a person from engaging in conduct of a particular kind if, in its opinion, it is desirable to do so.

(3) Subsections (1)(a) and (2) apply whether or not it appears to the court that the person intends to engage again, or to continue to engage, in conduct of that kind.

(4) Subsections (1)(b) and (2) apply—

(a) whether or not the person has previously engaged in conduct of that kind; or

(b) where there is an imminent danger of substantial damage to any other person if that person engages in conduct of that kind.

89 Undertaking as to damages not required by AML/CFT supervisor

(1) If the relevant AML/CFT supervisor applies to the High Court for the grant of an interim injunction under this subpart, the court must not, as a condition of granting an interim injunction, require the AML/CFT supervisor to give an undertaking as to damages.

(2) However, in determining the AML/CFT supervisor's application for the grant of an interim injunction, the court must not take into account that the AML/CFT supervisor is not required to give an undertaking as to damages.

Pecuniary penalties

90 Pecuniary penalties for civil liability act

(1) On the application of the relevant AML/CFT supervisor, the High Court may order a person to pay a pecuniary penalty to

the Crown, or to any other person specified by the court, if the court is satisfied that that person has engaged in conduct that constituted a civil liability act.

(2) For a civil liability act specified in section 78(b), (c), (d), or (g), the maximum amount of a pecuniary penalty under this Act is,—

(a) in the case of an individual, $100,000; and

(b) in the case of a body corporate, $1 million.

(3) For a civil liability act specified in section 78(a), (e), or (f), the maximum amount of a pecuniary penalty under this Act is,—

(a) in the case of an individual, $200,000; and

(b) in the case of a body corporate, $2 million.

(4) In determining an appropriate pecuniary penalty, the court must have regard to all relevant matters, including—

(a) the nature and extent of the civil liability act; and

(b) the likelihood, nature, and extent of any damage to the integrity or reputation of New Zealand's financial system because of the civil liability act; and

(c) the circumstances in which the civil liability act occurred; and

(d) whether the person has previously been found by the court in proceedings under this Act to have engaged in any similar conduct.

Subpart 3—Offences

Offence and penalties relating to civil liability act

91 Offence and penalties for civil liability act

A reporting entity that engages in conduct constituting a civil liability act commits an offence if the reporting entity engages in that conduct knowingly or recklessly.

Offences relating to suspicious transaction reports

92 Failing to report suspicious transaction

A reporting entity commits an offence if—

(a) a transaction is conducted or is sought to be conducted through the reporting entity; and

(b) the reporting entity has reasonable grounds to suspect that the transaction or the proposed transaction is or may be—

(i) relevant to the investigation or prosecution of any person for a money laundering offence; or

(ii) relevant to the enforcement of the Misuse of Drugs Act 1975; or

(iii) relevant to the enforcement of the Terrorism Suppression Act 2002; or

(iv) relevant to the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009; and

(v) relevant to the investigation or prosecution of a serious offence within the meaning of section 243(1) of the Crimes Act 1961; and

(c) the reporting entity fails to report the transaction or the proposed transaction to the Commissioner as soon as practicable, but no later than 3 working days, after forming that suspicion.

Compare: 1996 No 9 s 22(1)

93 Providing false or misleading information in connection with suspicious transaction report

A person commits an offence who, in making a suspicious transaction report or in supplying information in connection with that report,—

(a) makes any statement that the person knows is false or misleading in a material particular; or

(b) omits from any statement any matter or thing without which the person knows that the statement is false or misleading in a material particular.

Compare: 1996 No 9 s 22(3)

94 Unlawful disclosure of suspicious transaction report

(1) A person commits an offence who contravenes section 46—

(a) for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person; or

(b) with intent to prejudice any investigation into—

(i) the commission or possible commission of a money laundering offence; or

(ii) the financing of terrorism or the possible financing of terrorism.

(2) A person commits an offence who—

(a) is an officer or employee or a former officer or employee of a reporting entity, a person appointed as an AML/CFT compliance officer under section 56(3), or an auditor for a reporting entity; and

(b) has become aware, or became aware, in the course of that person's duties as such an officer or employee, that any investigation into any transaction or proposed transaction that is the subject of a suspicious transaction report is being, or may be, conducted by the Police; and

(c) knows that he or she is not legally authorised to disclose the information; and

(d) discloses that information to any other person—

(i) for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person; or

(ii) with intent to prejudice any investigation into—

(A) the commission or possible commission of a money laundering offence; or

(B) the financing of terrorism or the possible financing of terrorism.

Compare: 1996 No 9 s 22(4), (5)

95 Failure to keep or retain adequate records relating to suspicious transaction

A reporting entity commits an offence if the reporting entity fails to keep or retain adequate records relating to a suspicious transaction.

96 Obstruction of investigation relating to suspicious transaction report

A person commits an offence if the person obstructs any investigation relating to any suspicious transaction report without lawful justification or excuse.

97 Contravention of section 47(1)

A person commits an offence if the person acts in contravention of section 47(1) without lawful justification or excuse.

Compare: 1996 No 9 s 22(8)

98 Defence

(1) It is a defence to a charge against a person in relation to a contravention of, or a failure to comply with, Part 2 if the defendant proves that—

(a) the defendant took all reasonable steps to ensure that the defendant complied with that Part; or

(b) in the circumstances of the particular case, the defendant could not reasonably have been expected to ensure that the defendant complied with that Part.

(2) In determining, for the purposes of subsection (1)(a), whether or not a defendant took all reasonable steps to comply with Part 2, the court must have regard to—

(a) the nature of the reporting entity and the activities in which it engages; and

(b) the existence and adequacy of any procedures established by the reporting entity to ensure compliance with that Part.

(3) Except as provided in subsection (4), subsection (1) does not apply unless, within 21 days after the service of the summons, or within such further time as the court may allow, the defendant has delivered to the prosecutor a written notice—

(a) stating that the defendant intends to rely on the defence referred to in subsection (1); and

(b) specifying the reasonable steps that the defendant will claim to have taken.

(4) In any such prosecution, evidence that the defendant took a step not specified in the written notice required by subsection

(3) is not, except with the leave of the court, admissible for the purpose of supporting a defence under subsection (1).

Compare: 1996 No 9 s 23

99 Time limit for prosecution of offences relating to civil liability act and suspicious transaction reports

Despite anything in section 14 of the Summary Proceedings Act 1957, any information in respect of an offence under any of sections 91 to 97 may be laid at any time within 3 years after the time when the matter of the information arose.

100 Penalties

A reporting entity or person who commits an offence under any of sections 91 to 97 is liable, on conviction, to,—

(a) in the case of an individual, either or both of the following:
  (i) a term of imprisonment of not more than 2 years:
  (ii) a fine of up to $300,000; and

(b) in the case of a body corporate, a fine of up to $5 million.

Other offences relating to non-compliance with AML/CFT requirements

101 Structuring transaction to avoid application of AML/CFT requirements

A person commits an offence if the person structures a transaction (other than a transaction that involves the cross-border transportation of cash) to avoid the application of any AML/CFT requirements.

102 Offence to obstruct AML/CFT supervisor

A person commits an offence if the person wilfully obstructs any AML/CFT supervisor in the exercise of any power conferred or the performance of any function imposed on that supervisor by this Act.

103 Offence to provide false or misleading information to AML/CFT supervisor

A person commits an offence if, without reasonable excuse, the person provides information to an AML/CFT supervisor knowing that information to be false or misleading in any material respect.

104 Time limit for prosecution of offences relating to non-compliance with AML/CFT requirements

Despite anything in section 14 of the Summary Proceedings Act 1957, any information in respect of an offence under any of sections 91 to 97 may be laid at any time within 3 years after the time when the matter of the information arose.

105 Penalties

(1) A person who commits an offence under section 101 is liable, on conviction, to,—

(a) in the case of an individual, either or both of the following:

(i) a term of imprisonment of not more than 2 years:

(ii) a fine of up to $300,000; and

(b) in the case of a body corporate, a fine of up to $5 million.

(2) A person who commits an offence under either of sections 102 and 103 is liable, on conviction, to,—

(a) in the case of an individual, either or both of the following:

(i) a term of imprisonment of not more than 3 months:

(ii) a fine of up to $10,000; and

(b) in the case of a body corporate, a fine of up to $50,000.

Offences relating to cross-border transportation of cash

106 Failure to report cash over applicable threshold value moved into or out of New Zealand

A person commits an offence if the person fails, without reasonable excuse, to make or cause to be made a cash report, in accordance with subpart 6 of Part 2, concerning cash over the

applicable threshold value that the person has moved into or out of New Zealand.

107 Failure to report cash over applicable threshold value received by person in New Zealand from overseas

A person commits an offence if the person fails, without reasonable excuse, to make or cause to be made a cash report, in accordance with subpart 6 of Part 2, concerning cash over the applicable threshold value that the person has received in New Zealand from overseas.

108 Structuring cross-border transportation to avoid application of AML/CFT requirements

A person commits an offence if the person structures a cross-border transportation of cash to avoid the application of any AML/CFT requirements.

109 Defence

It is a defence to an offence under section 106 or 107 in relation to a failure to make or cause to be made a cash report to a Customs officer under section 70(d) if the defendant proves that—

(a) the failure was due to some emergency or to any other circumstances outside the reasonable control of the defendant; and

(b) the defendant made or caused to be made a report in respect of that cash as soon as practicable after the obligation to make the report arose.

Compare: 1996 No 9 s 40(3)

110 Providing false or misleading information in connection with cash report

A person commits an offence if, without reasonable excuse, the person makes or causes to be made a cash report knowing it is false or misleading in any material respect.

Compare: 1996 No 9 s 40(1)(b)

111 Offence to obstruct or not to answer questions from Customs officer

(1) A person commits an offence if the person wilfully obstructs any Customs officer in the exercise of any power conferred or performance of any duty imposed on that officer by this Act.

(2) A person commits an offence if, without reasonable excuse, the person fails to answer questions from a Customs officer.

Compare: 1996 No 9 s 40(2)

112 Penalties

A person who commits an offence under any of sections 106, 107, 108, 110, and 111 is liable, on summary conviction, to,—

(a) in the case of an individual, either or both of the following:

(i) a term of imprisonment of not more than 3 months:

(ii) a fine of up to $10,000; and

(b) in the case of a body corporate, a fine of up to $50,000.

113 Chief executive of New Zealand Customs Service may deal with cash reporting offences

(1) This section applies if, in any case to which section 106 or 107 applies, a person admits in writing that he or she has committed the offence and requests that the offence be dealt with summarily by the chief executive of the New Zealand Customs Service.

(2) If this section applies, the chief executive of the New Zealand Customs Service may, at any time before an information has been laid in respect of the offence, accept from that person a sum, not exceeding $500, that the chief executive of the New Zealand Customs Service thinks just in the circumstances of the case, in full satisfaction of any fine to which the person would otherwise be liable under section 112.

(3) If the chief executive of the New Zealand Customs Service accepts any sum under this section, the offender is not liable to be prosecuted for the offence in respect of which the payment was made.

Compare: 1996 No 9 s 41

Relationship with Customs and Excise Act 1996

114 Relationship with Customs and Excise Act 1996

(1) Nothing in this Act limits or affects the Customs and Excise Act 1996.

(2) The movement of cash in breach of any requirement of this Act or any regulations is, for the purposes of the Customs and Excise Act 1996, the importation or exportation of a prohibited good.

(3) It is the duty of every Customs officer to prevent the movement of cash that is in breach of any requirement of this Act or any regulations.

(4) For the purpose of carrying out the duty in subsection (3), a Customs officer may exercise his or her powers under the following sections of the Customs and Excise Act 1996 in relation to uncustomed or prohibited goods:

(a) section 145 (questioning persons about goods and debt):

(b) section 148 (detention of persons questioned about goods or debt):

(c) sections 149, 149A, 149B, 149C(1) and (2), and 149D (which relate to search and seizure):

(d) sections 151 and 152 (which relate to examination of goods):

(e) section 161 (further powers in relation to documents):

(f) section 165 (copying of documents obtained during search):

(g) section 166 (retention of documents and goods obtained during search):

(h) sections 166A to 166F (which relate to seizure and detention of goods suspected to be tainted property):

(i) sections 167 to 172 (which relate to search warrants and use of aids by Customs officers).

Computer searches by Customs officer

115 Duty of persons with knowledge of computer or computer network or other data storage devices to assist access to Customs officer

(1) A Customs officer exercising a search or examination power under section 114(4) may require a specified person to provide

access information and other information or assistance that is reasonable and necessary to allow the Customs officer to access data held in, or accessible from,—

(a) a computer:

(b) any other data storage device.

(2) In this section,—

access information includes access codes, passwords, encryption keys, and any related information that enables access to a computer or other data storage device

specified person is a person who—

(a) is the owner or lessee of the computer or other data storage device, or is in possession or control of the computer or other data storage device, is an employee of any of the above, or is a service provider who provides service to the above and holds access information; and

(b) has relevant knowledge of—

(i) the computer or a computer network of which the computer or other data storage device forms a part; or

(ii) measures applied to protect data held in, or accessible from, the computer or other data storage device.

(3) A specified person may not be required under subsection (1) to give any information tending to incriminate the person.

(4) Subsection (3) does not prevent a Customs officer exercising a search power from requiring a specified person to provide information that—

(a) is reasonable and necessary to allow the person exercising the search power to access data held in, or accessible from, a computer or other storage device that contains or may contain information tending to incriminate the specified person; but

(b) does not itself tend to incriminate the specified person.

(5) Subsection (3) does not prevent a Customs officer exercising a search power from requiring a specified person to provide assistance that is reasonable and necessary to allow the Customs officer exercising the search power to access data held in, or accessible from, a computer or other storage device that con-

tains, or may contain, information tending to incriminate the specified person.

(6) Subsections (1), (4), and (5) are subject to section 162 of the Customs and Excise Act 1996 (which relates to privilege and confidentiality).

Subpart 4—Search and seizure

116 Definitions

In this subpart, unless the context otherwise requires,—

document—

(a) means any record of information; and

(b) includes—

(i) anything on which there is writing or any image; and

(ii) anything on which there are marks, figures, symbols, or perforations that have a meaning for persons qualified to interpret them; and

(iii) anything from which sounds, images, or writing can be reproduced, with or without the aid of anything else

dwellinghouse means a building, or an apartment, a flat, or a unit within a building, that is used as a private residence

enforcement officer means the relevant AML/CFT supervisor or the Commissioner (as the case may require) and includes a person appointed under section 141 by an AML/CFT supervisor

evidential material means any thing that there are reasonable grounds for believing is or may be evidence, or may provide or contain evidence, of—

(a) an offence under this Part; or

(b) an attempt to commit an offence under this Part; or

(c) a civil liability act

occupier, in relation to any place, includes—

(a) a person who is present at the place and is in apparent control of it; and

(b) any person acting on behalf of the occupier

place—

(a) means anywhere on, under, or over any land or water; and

(b) includes all or any part of a building, structure, or conveyance

seize includes to secure against interference

thing includes—

(a) any substance, article, document, container, or equipment; and

(b) anything in electronic or magnetic form.

Search warrants

117 Search warrant

(1) An enforcement officer may apply for a search warrant in respect of a place.

(2) The application must be made in writing, on oath, by an enforcement officer.

(3) A District Court Judge, Justice of the Peace, Community Magistrate, or Registrar may issue a search warrant in respect of a place if satisfied that there are reasonable grounds for believing that there is evidential material at that place.

(4) Every search warrant must be in the form prescribed by regulations and be directed to—

(a) an enforcement officer by name; or

(b) a constable by name; or

(c) every constable.

(5) Despite a warrant being directed to another person under subsection (4), it may be executed by any constable.

(6) The Judge, Justice of the Peace, Community Magistrate, or Registrar issuing the warrant may impose reasonable conditions on its execution.

118 Powers under search warrant

(1) A search warrant issued under section 117 authorises the enforcement officer or constable who is executing it, and any person called on by that officer or constable to assist, to do any of the following:

(a) enter and search the place at any reasonable time, on 1 occasion within 14 days after the date of the warrant being issued:

(b) use reasonable force to—

(i) make entry (for example, by breaking open a door); and

(ii) open any thing at the place that it is reasonable in the circumstances to open:

(c) search for and seize any evidential material at the place:

(d) inspect and copy any document; and for that purpose also do any of the following:

(i) require any person at the place to produce a particular document:

(ii) require any person at the place who has control or knowledge of a document to reproduce, or assist in reproducing, the document in usable form:

(iii) operate any equipment at the place:

(iv) remove a document temporarily to another place in order to copy it:

(e) take into or onto the place whatever equipment and materials the enforcement officer or constable requires for the search:

(f) require the occupier of the place to answer any questions put by the enforcement officer or constable.

(2) An enforcement officer or constable may require the occupier of the place to do the following:

(a) hold any thing at the place in an unaltered state for a specified period of up to 5 working days:

(b) provide a copy of particular documents within a specified period (which must be a period that is reasonable in the circumstances).

(3) Nothing in this section limits or affects the privilege against self-incrimination.

Conduct of entry, search, and seizure

119 Assistance with searches

(1) An enforcement officer or constable may ask any person to assist the enforcement officer or constable with a search under this subpart.

(2) A person who assists an enforcement officer or constable must be under the supervision of an enforcement officer or constable.

120 Enforcement officers to show identity card on request

(1) An enforcement officer must produce his or her identity card (as issued under section 141(2)) for inspection—

(a) on entering a place under this subpart; and

(b) at any later time, on request, during a search under this subpart.

(2) An enforcement officer who fails to comply with subsection (1) ceases to be authorised to enter the place or to exercise any power under this Act or any regulations with respect to the search.

121 Announcement before entry

(1) This section applies whenever an enforcement officer or constable enters a place under this subpart, unless the entry is made by consent.

(2) Before entering the place, the enforcement officer or constable must—

(a) announce that he or she is authorised to enter the place; and

(b) give any person at the place an opportunity to consent to the entry.

(3) However, subsection (2) does not apply if the enforcement officer or constable believes on reasonable grounds that—

(a) announcing entry would frustrate the purpose of the entry; or

(b) immediate entry to the place is required to ensure the safety of any person.

122 Details of warrant to be given to occupier

If a place is being searched under a warrant, the enforcement officer or constable must give a copy of the warrant to the occupier or, if no person is present at the time, must leave a copy of the warrant in a prominent situation, marked for the attention of the occupier.

123 Occupier entitled to be present during search

(1) The occupier of a place that is subject to a search under this subpart, and who is present at any time during the search, is entitled to observe the search as it is being carried out.

(2) The right to observe the search ceases if the person observing impedes the search.

(3) This section does not prevent 2 or more parts of the place being searched at the same time.

124 Use of electronic equipment

(1) If an enforcement officer, a constable, or a person assisting a search operates electronic equipment found at a place during a search, the officer, constable, or person must take all reasonable care not to damage the equipment or corrupt information stored on it.

(2) If, as a result of a failure to take the care required by subsection (1), the owner of the equipment or information, or the occupier of the place that was searched, suffers damage, the owner or occupier may seek damages from the relevant AML/CFT supervisor or the Police (as the case may require) in respect of that damage.

125 Copies of documents seized to be provided

(1) When a document that is capable of being copied is seized from a place, it must (if practicable) be copied before the original is removed, and the copy must be left at the place.

(2) If it is not practicable to copy the document before removing it, it must be copied as soon as practicable after it is removed, and (if practicable) the copy must be promptly delivered to the occupier of the place.

(3) Subsection (1) does not apply—

(a) to documents obtained as a result of operating electronic equipment found at the place if the equipment is not seized and the documents remain stored on it; or

(b) if an order under subsection (4) has been made.

(4) A District Court Judge, Community Magistrate, or Justice of the Peace may make an order waiving the application of subsections (1) and (2) if satisfied that the volume of material to be copied is such that copying it will involve substantial cost and that the cost is not justified.

(5) An order under subsection (4) may be subject to whatever conditions the person making the order thinks are necessary to protect the interests of the person from whom the documents have been seized.

126 Receipts for things seized

(1) A person who seizes any thing during a search under this subpart must provide the occupier with a receipt for the thing seized.

(2) A single receipt may be given for more than 1 thing.

127 Application of sections 198A and 198B of Summary Proceedings Act 1957

(1) Section 198A of the Summary Proceedings Act 1957, so far as applicable and with all necessary modifications, applies in respect of the seizure of any documents under any search warrant as if the search warrant had been issued under section 198 of that Act.

(2) Section 198B of the Summary Proceedings Act 1957, so far as applicable and with all necessary modifications, applies in respect of accessing any documents under any search warrant as if the search warrant had been issued under section 198 of that Act.

Compare: 1996 No 9 s 50

Return and retention of things seized

128 Return and retention of things seized

(1) An enforcement officer or constable must (subject to any order of a court) immediately return any thing seized under this sub-

part to the person from whom it was seized if the reason for the thing's seizure no longer exists or it is decided that the thing is not to be used in evidence.

(2) If a thing has not been returned under subsection (1) within 90 days of its seizure, the enforcement officer or constable must return the thing unless—

(a) proceedings in respect of which the thing may afford evidence were instituted within 90 days of its seizure, and those proceedings (including any appeal) have not been completed, or the time within which an appeal may be lodged in those proceedings has not expired; or

(b) there is an order in force under section 129 in respect of the thing; or

(c) the enforcement officer or constable is otherwise authorised to retain, destroy, or dispose of the thing other than by returning it to the person from whom it was seized; or

(d) the person to whom it is to be returned cannot be found or does not wish to take back the thing.

(3) A thing may be returned conditionally or under such terms and conditions as the relevant AML/CFT supervisor or the Commissioner (as the case may require) thinks fit.

(4) A thing may not be returned if it is, or is liable to be, forfeited to the Crown.

129 Order to retain things seized

(1) If an enforcement officer or constable wishes to retain any thing seized under this subpart for more than 90 days, he or she may apply to a District Court for an order under this section.

(2) A District Court Judge, Community Magistrate, or Justice of the Peace may make an order under this section if he or she is satisfied that retention of the thing is necessary—

(a) for the purpose of investigating an alleged offence or a civil liability act under this Part; or

(b) as evidence of an alleged offence or a civil liability act under this Part; or

(c) to secure evidence of an alleged offence or a civil liability act under this Part.

(3) An order made under this section may be made for any period of up to 4 years.

(4) If made for a shorter period, the order may be renewed at any interval, but the total period of the order, with any renewals, may not exceed 4 years.

(5) Before making an application, the enforcement officer or constable must—

(a) take reasonable steps to discover who has an interest in the thing; and

(b) if practicable, notify each person who the enforcement officer or constable believes has such an interest in the proposed application and any application for a renewal.

Part 4
Institutional arrangements and miscellaneous provisions

Subpart 1—Institutional arrangements

AML/CFT supervisors

130 AML/CFT supervisors

(1) The AML/CFT supervisors are as follows:

(a) for banks, life insurers, and non-bank deposit takers, the Reserve Bank of New Zealand (**Reserve Bank**) is the relevant AML/CFT supervisor:

(b) for issuers of securities, trustee companies, futures dealers, collective investment schemes, brokers, and financial advisers, the Securities Commission is the relevant AML/CFT supervisor:

(c) for casinos, non-deposit-taking lenders, money changers, and other reporting entities that are not covered by paragraph (a) or (b), the Department of Internal Affairs is the relevant AML/CFT supervisor.

(2) If the products or services provided by a particular reporting entity are covered by more than 1 AML/CFT supervisor,—

(a) the AML/CFT supervisors concerned may agree on the relevant AML/CFT supervisor that will be the reporting entity's AML/CFT supervisor for the purposes of this Act; and

(b) the relevant AML/CFT supervisor will notify the reporting entity accordingly.

(3) If a reporting entity is a member of a designated business group and the products and services provided by members of that designated business group are covered by more than 1 AML/CFT supervisor,—

(a) the AML/CFT supervisors concerned may agree on 1 AML/CFT supervisor that will be the AML/CFT supervisor for all the reporting entities that are members of the designated business group for the purposes of this Act; and

(b) that AML/CFT supervisor will notify the reporting entities accordingly.

(4) If the AML/CFT supervisors cannot agree on which AML/CFT supervisor is to be a reporting entity's supervisor under subsection (2) or (3), then the AML/CFT co-ordination committee must appoint the AML/CFT supervisor for that entity.

(5) A reporting entity may have only 1 AML/CFT supervisor.

131 Functions

The functions of an AML/CFT supervisor are to—

(a) monitor and assess the level of risk of money laundering and the financing of terrorism across all of the reporting entities that it supervises:

(b) monitor the reporting entities that it supervises for compliance with this Act and regulations, and for this purpose to develop and implement a supervisory programme:

(c) provide guidance to the reporting entities it supervises in order to assist those entities to comply with this Act and regulations:

(d) investigate the reporting entities it supervises and enforce compliance with this Act and regulations:

(e) co-operate through the AML/CFT co-ordination committee (or any other mechanism that may be appropriate) with domestic and international counterparts to ensure the consistent, effective, and efficient implementation of this Act.

132 Powers

(1) An AML/CFT supervisor has all the powers necessary to carry out its functions under this Act.

(2) Without limiting the power conferred by subsection (1), an AML/CFT supervisor may,—

(a) on notice, require production of, or access to, all records, documents, or information relevant to its supervision and monitoring of reporting entities for compliance with this Act; and

(b) conduct on-site inspections in accordance with section 133; and

(c) provide guidance to the reporting entities it supervises by—

(i) producing guidelines; and

(ii) preparing codes of practice in accordance with section 63; and

(iii) providing feedback on reporting entities' compliance with obligations under this Act and regulations; and

(iv) undertaking any other activities necessary for assisting reporting entities to understand their obligations under this Act and regulations, including how best to achieve compliance with those obligations; and

(d) co-operate and share information in accordance with sections 46, 48, and 137 to 140 by communicating or making arrangements to communicate information obtained by the AML/CFT supervisor in the performance of its functions and the exercise of its powers under this Act; and

(e) in accordance with this Act and any other enactment, initiate and act on requests from any overseas counterparts; and

(f) approve the formation of, and addition of members to, designated business groups.

(3) An AML/CFT supervisor may only use the powers conferred on it under this Act and regulations for the purposes of this Act.

133 Matters relating to conduct of on-site inspections

(1) An AML/CFT supervisor may, at any reasonable time, enter and remain at any place (other than a dwellinghouse or a marae) for the purpose of conducting an on-site inspection of a reporting entity.

(2) During an inspection, an AML/CFT supervisor may require any employee, officer, or agent of the reporting entity to answer questions relating to its records and documents and to provide any other information that the AML/CFT supervisor may reasonably require for the purpose of the inspection.

(3) A person is not required to answer a question asked by an AML/CFT supervisor under this section if the answer would or could incriminate the person.

(4) Before an AML/CFT supervisor requires a person to answer a question, the person must be informed of the right specified in subsection (3).

(5) Nothing in this section requires any lawyer to disclose any privileged communication (as defined in section 42).

134 Delegation of supervisory function and powers

(1) An AML/CFT supervisor may delegate the following function and powers to a person who, by reason of his or her training or experience, is suitably qualified to perform that function and exercise those powers:

- (a) its function under section 131(d) of investigating the reporting entities it supervises:
- (b) its powers under section 132(2)(a) and (b), for the purpose only of performing the function of investigation under section 131(b).

(2) A delegation under subsection (1)—

- (a) must be made by the chief executive of the AML/CFT supervisor in writing; and
- (b) may be made subject to any restrictions and conditions that the AML/CFT supervisor thinks fit; and
- (c) may be revoked at any time by written notice to the delegate.

(3) A person to whom a function or power of the AML/CFT supervisor is delegated under this section—

(a) may, unless the delegation provides otherwise, perform the function or exercise the power in the same manner, and with the same effect, as if the delegate were the AML/CFT supervisor; and

(b) must disclose to the AML/CFT supervisor and manage appropriately any conflict of interest that might arise in relation to the performance of the function or exercise of the power; and

(c) must not disclose any information obtained under subsection (1) other than to the AML/CFT supervisor.

135 Authority to act as delegate

(1) The chief executive of the AML/CFT supervisor must issue a written authorisation to every person to whom a delegation is made under section 134 stating—

(a) the name of the authorised person; and

(b) the function that he or she is authorised to perform; and

(c) the powers that he or she may exercise.

(2) The delegate, when acting in the capacity of a delegate of the AML/CFT supervisor,—

(a) must carry on him or her—

(i) the written authorisation provided under subsection (1); and

(ii) evidence of his or her identity; and

(b) must produce the written authorisation and evidence referred to in paragraph (a), if requested to do so by a reporting entity that is subject to the delegated function or powers being performed or exercised by the delegate.

(3) The delegate must return the written authorisation to the AML/CFT supervisor as soon as his or her delegation is revoked.

136 Effect of delegation

(1) No delegation under section 134—

(a) affects or prevents the performance of any function or the exercise of any power by the AML/CFT supervisor; or

(b) affects the responsibility of the AML/CFT supervisor for the performance of its functions and the exercise of its powers.

(2) Every person to whom a function or power is delegated under section 134 has the same immunities in relation to the performance of that function or the exercise of that power as the AML/CFT supervisor that made the delegation.

Use and disclosure of information

137 Power to use information obtained as AML/CFT supervisor in other capacity and vice versa

(1) This section applies to information other than personal information.

(2) The Reserve Bank may use any information obtained or held by it in the exercise of its powers or the performance of its functions and duties under the Reserve Bank of New Zealand Act 1989 for the purpose of exercising its powers or performing its functions and duties under this Act as an AML/CFT supervisor.

(3) The Reserve Bank may use any information obtained or held by it in the exercise of its powers or the performance of its functions and duties under this Act as an AML/CFT supervisor for the purpose of exercising its powers or performing its functions and duties under the Reserve Bank of New Zealand Act 1989.

(4) The Securities Commission may use any information obtained or held by it in the exercise of its powers or the performance of its functions and duties under the Securities Act 1978, the Securities Markets Act 1988, and the Financial Advisers Act 2008 for the purpose of exercising its powers or performing its functions and duties under this Act as an AML/CFT supervisor.

(5) The Securities Commission may use any information obtained or held by it in the exercise of its powers or the performance of its functions and duties under this Act as an AML/CFT supervisor for the purpose of exercising its powers or performing its functions and duties under the Securities Act 1978, the Securities Markets Act 1988, and the Financial Advisers Act 2008.

(6) The Department of Internal Affairs may use any information obtained or held by it in the exercise of its powers or the performance of its functions and duties under the Gambling Act 2003 for the purpose of exercising its powers or performing its functions and duties under this Act as an AML/CFT supervisor.

(7) The Department of Internal Affairs may use any information obtained or held by it in the exercise of its powers or the performance of its functions and duties under this Act as an AML/CFT supervisor for the purpose of exercising its powers or performing its functions and duties under the Gambling Act 2003.

138 Restriction on power to use information under section 137

An AML/CFT supervisor may only use information obtained under section 137 if the person providing the information was advised of the purpose or purposes for which the information was obtained at the time he or she provided that information.

139 Power to disclose information supplied or obtained as AML/CFT supervisor

The Commissioner, the New Zealand Customs Service, or an AML/CFT supervisor may disclose any information (that is not personal information) supplied or obtained by it in the exercise of its powers or the performance of its functions and duties under this Act to any government agency for law enforcement purposes if it is satisfied that the agency has a proper interest in receiving such information.

140 Power to use and disclose information supplied or obtained under other enactments for AML/CFT purposes

(1) A government agency or an AML/CFT supervisor may disclose to any other AML/CFT supervisor or government agency any information supplied or obtained under an enactment listed in subsection (2) if the disclosure of that information is necessary or desirable for the purpose of ensuring compliance with this Act and regulations.

(2) The enactments referred to in subsection (1) are—

(a) the Companies Act 1993:

(b) the Criminal Proceeds (Recovery) Act 2009:
(c) the Customs and Excise Act 1996:
(d) the Financial Advisers Act 2008:
(e) the Financial Service Providers (Registration and Dispute Resolution) Act 2008:
(f) the Financial Transactions Reporting Act 1996:
(g) the Gambling Act 2003:
(h) the New Zealand Security Intelligence Service Act 1969:
(i) the Proceeds of Crime Act 1991:
(j) the Reserve Bank of New Zealand Act 1989:
(k) the Securities Act 1978:
(l) the Securities Markets Act 1988:
(m) the Terrorism Suppression Act 2002.

141 Enforcement officers

(1) For the purposes of this Act, an AML/CFT supervisor may appoint any employee as an enforcement officer, on a permanent or temporary basis, to exercise the powers conferred on the AML/CFT supervisor by this Act.

(2) An AML/CFT supervisor must issue its enforcement officers with an identity card.

(3) An enforcement officer must—
(a) carry his or her identity card at all times when acting as an enforcement officer under this Act or regulations; and
(b) return his or her identity card to the relevant AML/CFT supervisor immediately upon ceasing to be an enforcement officer.

Financial intelligence functions of Commissioner

142 Financial intelligence functions of Commissioner

The financial intelligence functions of the Commissioner are to—
(a) receive suspicious transaction reports:
(b) produce guidance material, including—

(i) typologies of money laundering and financing of terrorism transactions:

(ii) information for reporting entities on their obligations to report suspicious transactions and how to meet those obligations:

(c) provide feedback to reporting entities on the quality and timeliness of their suspicious transaction reporting:

(d) enforce requirements to provide suspicious transaction reports:

(e) analyse suspicious transaction reports to assess whether any should be referred to investigative branches of the New Zealand Police and to other law enforcement agencies for criminal investigation:

(f) access, directly or indirectly, on a timely basis the financial, administrative, and law enforcement information that the Commissioner requires to properly undertake his or her financial intelligence functions, including the analysis of suspicious transaction reports:

(g) refer to investigative branches of the New Zealand Police and to other law enforcement agencies any suspicious transaction reports that, in the view of the Commissioner, indicate grounds for criminal investigation:

(h) refer suspicious transaction reports and feedback provided to reporting entities on any suspicious transaction reports to AML/CFT supervisors:

(i) receive, analyse, and (if appropriate) refer to law enforcement agencies any cash reports:

(j) receive, analyse, and (if appropriate) refer to law enforcement agencies any suspicious property reports:

(k) produce risk assessments relating to money laundering offences and the financing of terrorism to be used by the Ministry, the Ministry of Justice, AML/CFT supervisors, and the New Zealand Customs Service:

(l) co-operate with the Ministry, the Ministry of Justice, AML/CFT supervisors, the New Zealand Customs Service, and any other relevant agencies to help ensure the effective implementation of the requirements under this Act and regulations.

143 Powers relating to financial intelligence functions of Commissioner

The Commissioner may—

(a) order production of or access to all records, documents, or information from any reporting entity that is relevant to analysing a suspicious transaction report received by the Commissioner, with or without a court order; and

(b) share suspicious transaction reports, cash reports, suspicious property reports, and other financial information and intelligence with domestic and international authorities for the purposes of this Act and regulations.

144 Delegation of powers of Commissioner

(1) The Commissioner may from time to time in writing, either generally or particularly, delegate to a constable of a level of position not less than inspector the Commissioner's powers under section 143(a).

(2) Where any constable exercises any power conferred under subsection (1), that constable must, within 5 days after the day on which the constable exercises the power, give the Commissioner a written report on the exercise of that power and the circumstances in which it was exercised.

(3) A constable who purports to perform a power under a delegation—

(a) is, in the absence of proof to the contrary, presumed to do so in accordance with the terms of that delegation; and

(b) must produce evidence of his or her authority to do so, if reasonably requested to do so.

(4) Every delegation under this section is revocable at will and does not prevent the exercise of any power by the Commissioner.

145 Guidelines relating to reporting of suspicious transactions

(1) Subject to section 146, the Commissioner must issue, in respect of each kind of reporting entity to which this Act applies, guidelines—

(a) setting out any features of a transaction that may give rise to a suspicion that the transaction is or may be—

(i) relevant to the investigation or prosecution of any person for a money laundering offence; or

(ii) relevant to the enforcement of the Misuse of Drugs Act 1975; or

(iii) relevant to the enforcement of the Terrorism Suppression Act 2002; or

(iv) relevant to the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009; or

(v) relevant to the investigation or prosecution of a serious offence within the meaning of section 243(1) of the Crimes Act 1961; and

(b) setting out any circumstances in which a suspicious transaction report relating to such a transaction may be made orally in accordance with section 41(2), and the procedures for making such an oral report.

(2) Suspicious transaction guidelines must be issued in such manner as the Commissioner from time to time determines.

(3) The Commissioner may issue an amendment or revocation of any suspicious transaction guidelines.

(4) Without limiting subsection (1), suspicious transaction guidelines issued under this section may relate to 1 or more kinds of reporting entities, and such guidelines may make different provision for different kinds of reporting entities and different kinds of transactions.

Compare: 1996 No 9 s 24

146 Consultation on proposed guidelines

(1) The Commissioner must, before issuing any suspicious transaction guidelines,—

(a) consult with, and invite representations from, the Privacy Commissioner under the Privacy Act 1993, and must have regard to any such representations; and

(b) give public notice of the Commissioner's intention to issue the guidelines, which notice must contain a statement—

(i) indicating the Commissioner's intention to issue the guidelines; and

(ii) inviting reporting entities that are likely to be affected by the proposed guidelines, and industry organisations that are representative of those reporting entities, to express to the Commissioner, within any reasonable period that is specified in the notice, their interest in being consulted in the course of the development of the guidelines; and

(c) consult with, and invite representations from, those reporting entities and industry organisations who express such an interest, and must have regard to any such representations.

(2) Nothing in subsection (1) prevents the Commissioner from adopting any additional means of publicising the proposal to issue any suspicious transaction guidelines or of consulting with interested parties in relation to such a proposal.

(3) This section applies to any amendment or revocation of any suspicious transaction guidelines.

Compare: 1996 No 9 s 25

147 Availability of guidelines

On a request by any reporting entity in respect of which any suspicious transaction guidelines are for the time being in force, or by any industry organisation that represents the reporting entity, the Commissioner must, without charge,—

(a) make those guidelines, and all amendments to those guidelines, available for inspection by that reporting entity or, as the case requires, that industry organisation at Police National Headquarters; and

(b) provide copies of those guidelines, and all amendments to those guidelines, to that reporting entity or, as the case requires, that industry organisation.

Compare: 1996 No 9 s 26

148 Review of guidelines

(1) The Commissioner must review from time to time any suspicious transaction guidelines for the time being in force.

(2) Sections 145 and 146 apply, with all necessary modifications, in relation to any such review as if the review were a proposal to issue suspicious transaction guidelines.

Compare: 1996 No 9 s 27

Co-ordination

149 Role of Ministry

The Ministry, in consultation with other agencies with AML/CFT roles and functions, is responsible for advising on the overall effectiveness and efficiency of the AML/CFT regulatory system, including—

(a) advising the Minister on outcomes and objectives for AML/CFT regulation and how best to achieve these (including links to other Government initiatives relevant to the purposes of this Act); and

(b) monitoring, evaluating, and advising the Minister on the performance of the AML/CFT regulatory system in achieving the Government's outcomes and objectives for it; and

(c) advising the Minister on any changes necessary to the AML/CFT regulatory system to improve its effectiveness; and

(d) administering the relevant AML/CFT legislation.

150 AML/CFT co-ordination committee

(1) The chief executive must establish an AML/CFT co-ordination committee consisting of—

(a) a representative from the Ministry; and

(b) a representative from the New Zealand Customs Service; and

(c) every AML/CFT supervisor; and

(d) a representative of the Commissioner; and

(e) such other persons as are invited from time to time by the chief executive in accordance with subsection (2).

(2) Any person invited under subsection (1)(e) must be employed in a government agency.

(3) The chair of the AML/CFT co-ordination committee is the chief executive.

151 Role of AML/CFT co-ordination committee

The role of the AML/CFT co-ordination committee is to ensure that the necessary connections between the AML/CFT supervisors, the Commissioner, and other agencies are made in order to ensure the consistent, effective, and efficient operation of the AML/CFT regulatory system.

152 Functions

The functions of the AML/CFT co-ordination committee are to—

(a) facilitate necessary information flows between the AML/CFT supervisors, the Commissioner, and other agencies involved in the operation of the AML/CFT regulatory system:

(b) facilitate the production and dissemination of information on the risks of money-laundering offences and the financing of terrorism in order to give advice and make decisions on AML/CFT requirements and the risk-based implementation of those requirements:

(c) facilitate co-operation amongst AML/CFT supervisors and consultation with other agencies in the development of AML/CFT policies and legislation:

(d) facilitate consistent and co-ordinated approaches to the development and dissemination of AML/CFT guidance materials and training initiatives by AML/CFT supervisors and the Commissioner:

(e) facilitate good practice and consistent approaches to AML/CFT supervision between the AML/CFT supervisors and the Commissioner:

(f) provide a forum for examining any operational or policy issues that have implications for the effectiveness or efficiency of the AML/CFT regulatory system.

Subpart 2—Miscellaneous provisions

Regulations

153 Regulations

The Governor-General may, by Order in Council, make regulations for all or any of the following purposes:

(a) prescribing requirements (generic and sector-specific) for standard, simplified, enhanced, and ongoing customer due diligence and any other AML/CFT requirements, including, but not limited to, the following:
  (i) information to be provided or obtained for the purposes of identification and verification:
  (ii) the circumstances in which a particular type of customer due diligence must be conducted:
  (iii) specifying entities or classes of entities, or products, services, or transactions for which a reporting entity may conduct simplified customer due diligence:
  (iv) the conditions in which third parties may be relied on to conduct customer due diligence:
  (v) the conditions on which a member of a designated business group may adopt an AML/CFT programme of another member of the group and share and use the policies, controls, and procedures of that programme:
  (vi) the circumstances in which corporations are deemed to be affiliated:
  (vii) the factors that a reporting entity must have regard to when assessing risk:

(b) prescribing instruments to be bearer-negotiable instruments for the purposes of this Act:

(c) prescribing the forms of, and the information to be included in, applications, warrants, reports, and other documents required under this Act:

(d) prescribing amounts or thresholds that are required to be prescribed for the purposes of this Act:

(e) prescribing the information to be included in records and the manner in which records are to be kept by reporting entities, or any specified class or classes of reporting entities:

(f) prescribing other identifying information that allows a transaction to be traced back to the originator for the purposes of section 27(1):

(g) prescribing the manner in which any notice, report, or other document required by this Act is to be given or served:

(h) prescribing for the form of a formal warning and the manner in which it must be issued:

(i) specifying Acts for which disclosure of personal information may be made by an AML/CFT supervisor for the purposes of the detection, investigation, and prosecution of offences under the specified Act:

(j) providing for any other matters contemplated by this Act or necessary for its administration or necessary for giving it full effect.

Compare: 1996 No 9 s 56

154 Regulations relating to application of Act

(1) The Governor-General may, by Order in Council on the recommendation of the Minister, make regulations for the following purposes:

(a) exempting or providing for the exemption of any transaction, product, or service or class of transactions, products, or services from all or any of the provisions of this Act:

(b) excluding certain relationships or banking services from the application of section 29 (which relates to correspondent banking relationships):

(c) exempting a reporting entity from its obligation to obtain some or all of the information set out in section 27(1) in relation to a specified transfer or transaction:

(d) exempting certain movements of cash from the application of subpart 6 of Part 2:

(e) prescribing threshold values for the purposes of sections 68 and 69 and the person or class of persons, transaction or class of transactions, financial activity or class of financial activities to which that threshold value applies:

(f) declaring an account or arrangement to be, or not to be, a facility and the circumstances and conditions in which an account or arrangement is to be, or not to be, a facility for the purposes of this Act:

(g) declaring a person or class of persons to be, or not to be, a reporting entity and the circumstances and conditions in which a person or class of persons is to be, or not to be, a reporting entity for the purposes of this Act:

(h) declaring a transaction or class of transactions to be, or not to be, an occasional transaction and the circumstances and conditions in which a transaction or class of transactions is to be, or not to be, an occasional transaction for the purposes of this Act:

(i) declaring a transfer or transaction or a class of transfers or transactions not to be a wire transfer and the circumstances and conditions in which a transfer or transaction or class of transfers or transactions is not a wire transfer for the purposes of this Act:

(j) declaring a person or class of persons to be, or not to be, a customer and the circumstances and conditions in which a person or class of persons is to be, or not to be, a customer for the purposes of this Act:

(k) declaring an entity or class of entities (whether domestic or overseas) to be a member of a specified designated business group:

(l) declaring a person or class of persons to be, or not to be, a financial institution for the purposes of this Act.

(2) The Minister must, before making any recommendation, have regard to—

(a) the purposes of this Act and the Financial Transactions Reporting Act 1996; and

(b) the risk of money laundering and the financing of terrorism; and

(c) the impact on the prevention, detection, investigation, and prosecution of offences; and

(d) the level of regulatory burden on a reporting entity; and

(e) whether the making of the regulation would create an unfair advantage for a reporting entity or would disadvantage other reporting entities; and

(f) the overall impact that making the regulation would have on the integrity of, and compliance with, the AML/CFT regulatory regime.

(3) The Minister must also, before making any recommendation,—

(a) do everything reasonably possible on the Minister's part to advise all persons who in the Minister's opinion will be affected by any regulations made in accordance with the recommendation, or representatives of those persons, of the proposed terms of the recommendation and of the reasons for it; and

(b) give such persons or their representatives a reasonable opportunity to consider the recommendation and to make submissions on it to the Minister, and the Minister must consider those submissions; and

(c) give notice in the *Gazette*, not less than 28 days before making the recommendation, of the Minister's intention to make the recommendation and state in the notice the matters to which the recommendation relates; and

(d) make copies of the recommendation available for inspection by any person who so requests before any regulations are made in accordance with the recommendation.

(4) Failure to comply with subsection (3) does not affect the validity of any regulations made under this section.

(5) Any regulations made under this section expire on the day that is 5 years after the date on which regulations come into force.

155 Regulations relating to countermeasures

(1) The Governor-General may, by Order in Council made on the recommendation of the Minister, make regulations for, or in relation to, prohibiting or regulating the entering into of transactions or business relationships between a reporting entity and any other person.

(2) Regulations made for the purposes of subsection (1)—

(a) may be of general application; or

(b) may be limited by reference to any or all of the following:

(i) a specified transaction:

(ii) a specified party:

(iii) a specified overseas country.

(3) The Governor-General may, by Order in Council, declare a country outside New Zealand to be a prescribed overseas country for the purposes of this section.

(4) Any regulations made under subsection (1) expire on the day that is 5 years after the date on which regulations come into force.

Compare: Anti-Money Laundering and Counter-Terrorism Financing Act 2006 s 102 (Aust)

156 Consultation not required for consolidation of certain regulations and minor amendments

The Minister is not required to comply with section 154(3) in respect of the making of any regulations to the extent that regulations—

(a) revoke any regulations made under section 154 and, at the same time, consolidate the revoked regulations, so that they have the same effect as those revoked regulations; or

(b) make minor amendments to regulations.

Compare: 1996 No 9 s 56A

Ministerial exemptions

157 Minister may grant exemptions

(1) The Minister may, in the prescribed form, exempt any of the following from the requirements of all or any of the provisions of this Act:

(a) a reporting entity or class of reporting entities; or

(b) a transaction or class of transactions.

(2) The Minister may grant the exemption—

(a) unconditionally; or

(b) subject to any conditions the Minister thinks fit.

(3) Before deciding to grant an exemption and whether to attach any conditions to the exemption, the Minister must have regard to the following:

(a) the intent and purposes of the Financial Transactions Reporting Act 1996:

(b) the intent and purpose of this Act and any regulations:

(c) the risk of money laundering and the financing of terrorism associated with the reporting entity, including, where appropriate, the products and services offered by the reporting entity and the circumstances in which the products and services are provided:

(d) the impacts on prevention, detection, investigation, and prosecution of offences:

(e) the level of regulatory burden to which the reporting entity would be subjected in the absence of an exemption:

(f) whether the exemption would create an unfair advantage for the reporting entity or disadvantage third party reporting entities:

(g) the overall impact that the exemption would have on the integrity of, and compliance with, the AML/CFT regulatory regime.

(4) Every exemption made under this section is deemed to be a regulation for the purposes of the Regulations (Disallowance) Act 1989.

158 Minister must consult before granting exemption

Before granting an exemption under section 157, the Minister must consult with—

(a) the Ministers responsible for the AML/CFT supervisors; and

(b) any other persons the Minister considers appropriate having regard to those matters listed in section 157(3).

159 Requirements relating to exemptions

(1) The exemption must include an explanation of the reason for granting the exemption.

(2) The exemption—

(a) must be granted for a period specified by the Minister but that period must not be more than 5 years; and

(b) may, at any time, be varied or revoked by the Minister.

(3) The exemption must be notified in the *Gazette*.

Transitional and savings provisions

160 Transitional and savings provisions

Transitional and savings provisions relating to the coming into force of this Act are set out in Schedule 1.

Consequential amendments, repeals, and revocation

161 Amendments to other enactments

(1) The enactment specified in Part 1 of Schedule 2 is amended in the manner indicated in that part of that schedule (being consequential amendments relating to the bringing into force of provisions relating to cross-border transportation of cash).

(2) The enactments specified in Part 2 of Schedule 2 are amended in the manner indicated in that schedule (being consequential amendments to other enactments).

(3) The regulations specified in Part 3 of Schedule 2 are revoked.

162 Amendment to Financial Transactions Reporting Act 1996 consequential on bringing into force of Part 2

The Financial Transactions Reporting Act 1996 is amended by repealing paragraphs (a) to (f), (h), (i), and (k) of the definition of **financial institution** in section 3(1).

163 Amendment to Financial Transactions Reporting Act 1996 relating to cross-border transportation of cash

The Financial Transactions Reporting Act 1996 is amended by repealing Part 5.

Schedule 1

s 160

Transitional and savings provisions

1 Offences and breaches of Financial Transactions Reporting Act 1996

(1) This clause applies to an offence under, or a breach of, the Financial Transactions Reporting Act 1996 that was committed before the commencement of this Act.

(2) If this clause applies, then for the purpose of doing the things specified in subclause (3), the Financial Transactions Reporting Act 1996 continues to have effect as if this Act had not been enacted.

(3) The things referred to in subclause (2) are as follows:

(a) investigating the offence or breach:

(b) commencing, continuing, or completing proceedings for the offence or breach:

(c) imposing a penalty for the offence or breach (which, for the avoidance of doubt, must be the same as the penalty that applied to the offence or the breach before this Act was enacted).

2 Barred proceedings

Nothing in this Act enables any proceedings to be brought that were barred before the commencement of this Act.

3 Pending proceedings

Any proceedings that have been commenced under the Financial Transactions Reporting Act 1996 before the commencement of this Act may be continued and completed after that commencement as if this Act had not been enacted, and the Financial Transactions Reporting Act 1996 applies accordingly.

Schedule 2
s 161

Consequential amendments

Part 1
Amendments to Financial Transactions Reporting Act 1996 relating to cross-border transportation of cash

Section 2(1)

Definitions of **cash report** and **Customs officer**: repeal.

Definition of **cash**: omit "except in Part 5 of this Act,".

Part 2
Amendments to other enactments

Crimes Act 1961 (1961 No 43)

Section 244: insert after paragraph (b):

> "(ba) the enforcement or intended enforcement of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009; or".

Criminal Proceeds (Recovery) Act 2009 (2009 No 8)

Definition of **financial institution** in section 5(1): repeal and substitute:

> "**financial institution** means either a person within the meaning of financial institution as defined in section 3 of the Financial Transactions Reporting Act 1996 or as defined in section 5 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009".

Customs and Excise Act 1996 (1996 No 27)

Section 166A(b)(ii): repeal and substitute:

> "(ii) subpart 6 of Part 2 and sections 114 and 115 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009; and".

Section 166C(4): insert after paragraph (b):

> "(ba) Anti-Money Laundering and Countering Financing of Terrorism Act 2009:".

Part 2—*continued*

Financial Transactions Reporting Act 1996 (1996 No 9)

Long Title: insert "**the Terrorism Suppression Act 2002 and**" after "**enforcement of**".

Paragraph (b) of the Long Title: repeal.

Section 15(1)(b): insert after subparagraph (i):

"(ia) that the transaction or proposed transaction is or may be relevant to the enforcement of the Terrorism Suppression Act 2002; or".

Section 16: insert after paragraph (a):

"(ab) that the transaction or proposed transaction is or may be relevant to the enforcement of the Terrorism Suppression Act 2002; or".

Section 21(2): insert after paragraph (a):

"(ab) the enforcement of the Terrorism Suppression Act 2002:".

Section 22(1)(b): insert after subparagraph (i):

"(ia) that the transaction or proposed transaction is or may be relevant to the enforcement of the Terrorism Suppression Act 2002; or".

Section 24(1)(a): insert after subparagraph (i):

"(ia) that the transaction or proposed transaction is or may be relevant to the enforcement of the Terrorism Suppression Act 2002; or".

Section 28: insert after paragraph (d):

"(da) the enforcement of the Terrorism Suppression Act 2002:".

Section 56(1)(b): omit "Parts 2 and 5 of this Act" and substitute "Part 2".

Misuse of Drugs Act 1975 (1975 No 116)

Section 12B(6): insert after paragraph (b):

"(ba) the enforcement or intended enforcement of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009; or".

Part 2—*continued*

Mutual Assistance in Criminal Matters Act 1992 (1992 No 86)

Definition of **financial institution** in section 2(1): repeal and substitute:

"**financial institution** means either a person within the meaning of financial institution as defined in section 3 of the Financial Transactions Reporting Act 1996 or as defined in section 5 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009".

Reserve Bank of New Zealand Act 1989 (1989 No 157)

Section 41(1): add "and the Anti-Money Laundering and Countering Financing of Terrorism Act 2009".

Section 41(2): insert ", or the Anti-Money Laundering and Countering Financing of Terrorism Act 2009," after "by this Act".

Section 51(5): insert "or under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009," after "by this Act".

Section 51: add:

"(9) To avoid doubt, the Governor's functions and powers include his or her functions and powers under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009."

Terrorism Suppression Act 2002 (2002 No 34)

Section 44(1)(b): insert "or by a reporting entity" after "by a financial institution".

Section 44(1)(b): insert "or the reporting entity" after "the financial institution".

Section 44(1)(d)(ii): insert "or reporting entity, as the case may be," after "that Commissioner and the financial institution".

Section 44(2): insert "or the reporting entity" after "the financial institution".

Section 44(4): insert "or reporting entity" after "financial institution" in each place where it appears.

Section 44(5): repeal and substitute:

"(5) In this section, section 47, and Schedule 5,—

Part 2—*continued*

Terrorism Suppression Act 2002 (2002 No 34)—*continued*

"(a) in the case of a financial institution to which the Financial Transactions Reporting Act 1996 applies, **facility**, **financial institution**, **suspicious transaction report**, and **transaction** have the meanings given to them in section 2(1) of that Act; and

"(b) in the case of a reporting entity to which the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 applies, **facility**, **reporting entity**, **suspicious transaction report**, and **transaction** have the meanings given to them in section 5 of that Act."

Section 47(1)(b)(i): insert "or reporting entity" after "financial institution".

Section 47A(1)(a): insert after subparagraph (i):

"(ia) subpart 6 of Part 2 and sections 114 and 115 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009; or".

Section 47C(5): insert after paragraph (a):

"(ab) Anti-Money Laundering and Countering Financing of Terrorism Act 2009:".

Schedule 5: insert "or reporting entity" after "financial institution" in each place where it appears.

Part 3
Regulations revoked

Financial Transactions Reporting (Interpretation) Regulations 1997 (SR 1997/48)

Legislative history

25 June 2009	Introduction (Bill 46–1)
30 June 2009	First reading and referral to Foreign Affairs, Defence and Trade Committee
14 September 2009	Reported from Foreign Affairs, Defence and Trade Committee (Bill 46–2)
24 September 2009	Second reading
13 October 2009	Committee of the whole House (Bill 46–3)
15 October 2009	Third reading
16 October 2009	Royal assent

This Act is administered by the Ministry of Justice.

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2009