

A photograph of several stacks of silver coins, likely Euro coins, arranged in a row. The coins are stacked to varying heights, and their metallic surfaces are highly reflective, showing bright highlights and deep shadows. The background is a plain, light color.

**BELL GULLY**

# Anti-Money Laundering and Countering Financing of Terrorism Bill

---

**A practical guide with commentary from our experts**

JULY 2009

---

## THE GUIDE'S PURPOSE

The Anti-Money Laundering and Countering Financing of Terrorism Bill was introduced to Parliament in June 2009, following an extended period of consultation.

This new legislation upgrades the Financial Transactions Reporting Act 1996 (**FTRA 1996**) and will have significant implications for many businesses in New Zealand. As is to be expected, many aspects of the Bill are aligned with the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

We have prepared this practical Guide to assist you to understand the Bill and, in particular, to:

- (a) Assist you to consider submissions during the Select Committee process.
- (b) Assist you in your compliance planning.

We start by providing a brief overview of the Bill and then provide answers and commentary on various key areas of the Bill. A number of the issues that arise were identified from the Consultation Draft of the Bill, but it is timely to review these now that the Bill has been introduced to Parliament.

Please note that the Guide does not seek to comprehensively cover every aspect of the Bill. Rather, it seeks to provide an overview of many of the main areas from a practical perspective.

We trust that you find this Guide useful in understanding and assessing this significant legislation.

Sincerely,

**Bell Gully**

### **Copyright and disclaimer**

Copyright in this document is owned by Bell Gully. This document may not be copied in whole or in part without the prior written approval of Bell Gully. Bell Gully accepts no liability for, and does not guarantee the accuracy of, information or opinion contained in this document. This document provides an overview only and is not intended to be a comprehensive study, nor is it intended to provide legal advice. It should not be treated as a substitute for specific advice on individual circumstances.

© 2009

**OUR EXPERTS**



**Mark Todd**

PARTNER

DDI 64 9 916 8963 MOB 021 614 537

*mark.todd@bellgully.com*



**David Craig**

PARTNER

DDI 64 4 915 6839 MOB 021 674 851

*david.craig@bellgully.com*



**Haydn Wong**

PARTNER

DDI 64 9 916 8918 MOB 021 606 267

*haydn.wong@bellgully.com*



**Jonathan Ross**

PARTNER

DDI 64 9 916 8811 MOB 021 650 734

*jonathan.ross@bellgully.com*



**Murray King**

PARTNER

DDI 64 9 916 8971 MOB 021 684 573

*murray.king@bellgully.com*

Our experts have provided advice on AML/CFT matters since the inception of the Financial Transactions Reporting Act 1996. This advice has covered numerous industry sectors, including financial services, funds management, insurance and others. We look forward to assisting businesses to meet the requirements of the new legislation. In doing so, we have relationships that will enable us to draw upon relevant experience and practice from Australia and other jurisdictions.

## CONTENTS

The Guide’s purpose .....	1
Our experts.....	2
<b>PART 1: OVERVIEW OF THE BILL.....</b>	<b>6</b>
<b>PART 2: PRELIMINARY MATTERS – TIMING, TRANSITION, SELECT COMMITTEE SUBMISSIONS ETC.....</b>	<b>7</b>
Q.1 When will the legislation come into force?.....	7
Q.2 Is there an opportunity to make submissions? .....	7
Q.3 Does the Bill set out all of the applicable requirements?.....	8
Q.4 How is the Financial Transactions Reporting Act 1996 affected?.....	9
<b>PART 3: THRESHOLD ISSUE – WHO DOES THE LEGISLATION APPLY TO?.....</b>	<b>10</b>
Q.5 Who is covered by the legislation? .....	10
Q.6 Does the legislation apply to overseas entities?.....	13
Q.7 Are exemptions available under the legislation? .....	14
<b>PART 4: CUSTOMER DUE DILIGENCE – GENERAL MATTERS .....</b>	<b>15</b>
Q.8 What are the levels of CDD? .....	15
Q.9 Who must be “CDDed”?.....	16
Q.10 What happens if a Reporting Entity is unable to conduct CDD in accordance with the legislation? .....	17
Q.11 A number of the CDD requirements are dependent on the “ <i>level of risk involved</i> ”. How will this operate in practice? .....	17
Q.12 What is the timing for identity verification?.....	18
Q.13 Does the legislation distinguish between new customers and customers accepted under the FTRA 1996 (and previously)? .....	18
Q.14 How does the legislation deal with certain special situations recognised by the FTRA 1996 and other legislation? .....	19
<b>PART 5: STANDARD CDD .....</b>	<b>20</b>
Q.15 When is standard CDD required? .....	20
Q.16 What identity information must be obtained in relation to standard CDD?.....	21
Q.17 What further information must be obtained? .....	22
Q.18 What identity verification requirements apply under standard CDD?.....	23

Q.19	What basis must be applied for verifying identity? .....	23
<b>PART 6: SIMPLIFIED CUSTOMER DUE DILIGENCE .....</b>		<b>24</b>
Q.20	When is simplified CDD available?.....	24
Q.21	What identity information must be obtained in relation to simplified CDD?.....	25
Q.22	What further information must be obtained under simplified CDD?.....	26
Q.23	What identity verification requirements apply under simplified CDD? .....	26
<b>PART 7: ENHANCED CDD .....</b>		<b>27</b>
Q.24	When is enhanced CDD required?.....	27
Q.25	What identity information must be obtained in relation to enhanced CDD?.....	28
Q.26	What identity verification requirements apply under enhanced CDD? .....	29
Q.27	What additional specific requirements apply to particular categories of enhanced CDD?.....	30
<b>PART 8: ONGOING CDD AND ACCOUNT MONITORING .....</b>		<b>31</b>
Q.28	When is ongoing CDD and account monitoring required?.....	31
Q.29	What is required when undertaking ongoing CDD and account monitoring? .....	32
<b>PART 9: RELIANCE ON THIRD PARTIES TO CONDUCT CUSTOMER DUE DILIGENCE .....</b>		<b>33</b>
Q.30	When can a Reporting Entity rely on third parties to conduct CDD?.....	33
Q.31	How do designated business groups work? .....	34
Q.32	When can a Reporting Entity rely on another Reporting Entity or equivalent overseas entity that is neither a member of its DBG or an agent?.....	36
Q.33	When may a Reporting Entity rely on an agent to conduct CDD? .....	37
<b>PART 10: RISK ASSESSMENTS/COMPLIANCE PROGRAMMES ETC.....</b>		<b>38</b>
Q.34	What are the key AML/CFT compliance requirements? .....	38
Q.35	What specific requirements apply in respect of the risk assessment?.....	39
Q.36	What matters need to be covered by a Reporting Entity's AML/CFT compliance programme? .....	40
<b>PART 11: SUSPICIOUS TRANSACTION REPORTS.....</b>		<b>42</b>
Q.37	When is a suspicious transaction report required?.....	42
Q.38	What is the timing for suspicious transaction reports? .....	42
Q.39	Who is the report made to? .....	43
Q.40	What is the form of the report? .....	43

Q.41	What other provisions apply in relation to suspicious transaction reports? .....	43
<b>PART 12: RETENTION OF RECORDS .....</b>		<b>44</b>
Q.42	What records must be kept in relation to transactions? .....	44
Q.43	What records must be kept in relation to identity and identity verification? .....	45
Q.44	What other records must be kept? .....	45
Q.45	How long must records be kept for? .....	46
Q.46	How must records be kept? .....	46
Q.47	What other provisions are there relating to record keeping? .....	46
<b>PART 13: MISCELLANEOUS MATTERS .....</b>		<b>47</b>
Q.48	What general prohibitions apply to Reporting Entities? .....	47
Q.49	What other things does the legislation cover? .....	47
Q.50	Who will be the AML/CFT supervisors? .....	48

## **PART 1: OVERVIEW OF THE BILL**

As expected, the legislation will upgrade New Zealand's AML/CFT regime by:

1. Requiring upgraded customer due diligence (**CDD**) measures, including:
  - (a) Standard due diligence.
  - (b) Simplified due diligence.
  - (c) Enhanced due diligence.
  - (d) Ongoing due diligence.
2. Requiring businesses to produce, implement and maintain a detailed written AML/CFT risk assessment.
3. Requiring businesses to produce, implement and maintain a detailed written AML/CFT compliance programme.
4. Requiring businesses to appoint an AML/CFT compliance officer.
5. Enhancing the requirements relating to suspicious transactions.
6. Enhancing the requirements relating to record keeping.
7. Enhancing the requirements relating to cross-border transportation of cash.
8. Prohibiting facilities involving anonymity or false customer names.
9. Prohibiting relationships with "shell banks".
10. Appointing AML/CFT supervisors and requiring them to prepare Codes of Practice.
11. Imposing significant civil and criminal penalties for non-compliance on businesses and their directors and senior managers.

Importantly for Australasian businesses, the Bill has substantial alignment with the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006. However, there are also a number of areas of divergence between the two countries.

## **PART 2: PRELIMINARY MATTERS - TIMING, TRANSITION, SELECT COMMITTEE SUBMISSIONS ETC.**

### **Q.1 When will the legislation come into force?**

It is currently contemplated that the legislation will be passed into law in the third quarter of 2009. There will then be a two year transitional period before the new regime comes into effect, to provide time for:

- (a) Supervisors to gear up.
- (b) Regulations and guidance materials to be produced.
- (c) Businesses to develop compliance systems.

### **Q.2 Is there an opportunity to make submissions?**

There will be an opportunity to make submissions during the Select Committee process. The closing date for submissions is Thursday 6 August 2009. The relevant Select Committee is the Foreign Affairs, Defence and Trade Committee.

#### **COMMENT:**

Relevant entities will need to identify areas of the Bill that are of particular concern to them. However, matters of potential general concern include:

- (a) As a general proposition, seeking to minimise the areas of divergence between the Bill and the equivalent Australian legislation.
- (b) Clarifying the application of the legislation to equity issuances (see Q.5).
- (c) Seeking an express provision setting out the territorial scope of the legislation (see Q.6).
- (d) Clarifying whether the requirements of the legislation only apply to customers who establish a facility or undertake an occasional transaction, i.e. not to customers more generally (see Q.9).
- (e) Clarifying the application of the “*beneficial owner*” concept to individuals and trusts (see Q.9 and Q.24).
- (f) If considered appropriate, seeking that certain reliefs contained in the FTRA 1996 are carried through into the new legislation (see Q.14).
- (g) Clarifying whether the requirements of the legislation only apply to customers who have a business relationship with the Reporting Entity that involves a relevant class of activity (see Q.15).
- (h) Seeking an amendment so that occasional transactions conducted through an existing facility do not trigger the requirements of the legislation (see Q.15).

- (i) Seeking an amendment to allow simplified CDD in relation to a person acting on behalf of a customer who has been “CDDed” under the FTRA 1996 (see Q.20).
- (j) Seeking to limit the broad definition of “*politically exposed person*” due to the practical issues in identifying such persons (see Q.20).
- (k) Clarifying the identity information that must be obtained from certain customers under simplified CDD (see Q.21).
- (l) Clarifying whether it is necessary to obtain “*information on the nature and purpose of the proposed business relationship between the customer and the Reporting Entity*” under enhanced CDD (see Q.25).
- (m) Clarifying the scope of the requirement to obtain senior management approval in relation to business relationships and occasional transactions involving politically exposed persons (see Q.27).
- (n) Clarifying the scope of ongoing CDD in relation to Existing Customers (see Q.29).
- (o) Seeking an amendment to ensure that the privacy constraints relating to information provided to a Reporting Entity by third parties do not unduly interrupt business operations (see Q.30).
- (p) Seeking to ensure that workable “due diligence” defences are included in the legislation from the perspective of potentially liable directors and senior managers (see Q.49).
- (q) Seeking an ability for corporate groups to be supervised by a single AML/CFT supervisor (see Q.50).

### **Q.3 Does the Bill set out all of the applicable requirements?**

No. Legal requirements will also be contained in:

- (a) Regulations issued under the legislation (clauses 147 and 148 of the Bill).
- (b) Guidance material issued by AML/CFT supervisors (clause 129).
- (c) Codes of Practice prepared by AML/CFT supervisors, after consultation with relevant persons (clauses 60-64).

#### **COMMENTS:**

1. A very significant amount of the relevant detail will be contained in regulations, guidance material and Codes of Practice. Accordingly, Reporting Entities will need to carefully monitor the development of these.

2. In some cases, compliance with a Code of Practice will be deemed to be sufficient to comply with the requirements of the legislation. However, subject to various conditions, it will be open to Reporting Entities to comply with the legislation in another manner. This may be particularly relevant for Reporting Entities that are part of multi-national groups that may have practices and procedures imposed by head office that do not completely align with relevant Codes of Practice.

**Q.4 How is the Financial Transactions Reporting Act 1996 affected?**

The FTRA 1996 will continue to apply until the end of the two year transitional period. After that, the enhanced requirements of the new legislation will replace the requirements of the FTRA 1996 for financial institutions (as defined – see Q.5) and casinos. The enhanced requirements are likely to be rolled out to other relevant entities at a later date under a second phase of reform.

## PART 3: THRESHOLD ISSUE – WHO DOES THE LEGISLATION APPLY TO?

### Q.5 Who is covered by the legislation?

1. The legislation applies to “*Reporting Entities*”. These are defined as:
  - (a) “*Financial institutions*”, as defined.
  - (b) Casinos.
  - (c) Any other person required by any other Act to comply with the legislation.  
(clause 4)
2. A “*financial institution*” is defined to mean a person who, in the ordinary course of business, carries on one or more of the following financial activities:
  - (a) Accepting deposits or other repayable funds from the public.
  - (b) Lending to or for a customer, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions (including forfeiting).
  - (c) Financial leasing (excluding financial leasing arrangements in relation to consumer products).
  - (d) Transferring money or value for, or on behalf of, a customer.
  - (e) Issuing or managing the means of payment (for example, credit or debit cards, cheques, traveller’s cheques, money orders, bankers’ drafts, or electronic money).
  - (f) Undertaking financial guarantees and commitments.
  - (g) Trading for the person’s own account or for the accounts of customers in any of the following:
    - (i) Money market instruments (for example, cheques, bills, certificates of deposit, or derivatives).
    - (ii) Foreign exchange.
    - (iii) Exchange, interest rate, or index instruments.
    - (iv) Transferable securities.
    - (v) Commodity futures trading.
  - (h) Participating in securities issues and the provision of financial services related to those issues.
  - (i) Managing individual or collective portfolios.
  - (j) Safe keeping or administering of cash or liquid securities on behalf of other persons.
  - (k) Investing, administering, or managing funds or money on behalf of other persons.
  - (l) Underwriting or placement of life insurance or other investment related insurance.

(m) Money or currency changing.

(clause 4)

## COMMENTS:

1. Unlike the FTRA 1996, the Bill focuses on activities rather than the nature of the entity. For many businesses that fall squarely within the regime – such as banks, fund managers and life insurers – this is unlikely to be significant.
2. However, the change in approach has the potential to cause businesses not caught by the FTRA 1996 regime to fall within the regime. A number of businesses will therefore need to carefully consider their activities to determine whether they conduct the specified activities. For example:
  - (a) General insurers will need to consider whether they fall within the regime by virtue of activities such as premium lending, providing financial guarantees or commitments or writing small amounts of life insurance.
  - (b) The scope of the reference to “*participating in securities issues and the provision of financial services related to those issues*” is unclear. This reference could potentially be interpreted to apply to issues of listed equity securities.
  - (c) Under the FTRA 1996 certain activities were only caught in relation to persons whose “*business or a principal part of whose business*” consisted of those activities. These activities included:
    - Borrowing or lending or investing money.
    - Administering or managing funds on behalf of other persons.
    - Acting as trustee in respect of funds of other persons.
    - Dealing in life insurance policies.
    - Providing financial services that involve the transfer or exchange of funds, including payment services, foreign exchange services or risk management services (such as the provision of forward foreign exchange contracts); but not including the provision of financial services that consist solely of the provision of financial advice.

The Bill does not contain an equivalent requirement, i.e. a requirement that the business or a principal part of the business consist of these activities. Accordingly, conducting a specified class of activity as a peripheral part of a business may be sufficient to cause the regime to apply.

3. Unlike the FTRA 1996, the Bill requires the relevant activity to be undertaken “*in the ordinary course of business*”. The scope and meaning of this requirement may be relevant to some entities. For example, this may arguably exclude one-off extraordinary transactions and non-business activities from the scope of the regime.
4. The approach of the Bill seems to be to “cast the net wide”, but to provide a broad exemption power (see Q.7). This is similar to the approach of the Securities Act 1978. Businesses that are caught by the legislation, but who engage in low risk activities, may wish to consider seeking an exemption from the legislation.
5. The Bill does not apply to certain types of entity that are currently caught by the FTRA 1996 (unless they carry out a specified activity), such as lawyers, conveyancing practitioners and accountants. As mentioned, it is contemplated that the enhanced requirements will be applied to such entities as part of a Phase two roll out.

**Q.6 Does the legislation apply to overseas entities?**

The Bill does not contain a provision expressly stating the territorial scope of the legislation.

**COMMENTS:**

1. The lack of an express provision relating to territorial scope is capable of creating uncertainty for overseas entities that have some involvement with New Zealand. This uncertainty existed under the FTRA 1996.
2. The position can be contrasted with recent legislation relating to the financial sector such as the Financial Service Providers (Registration and Dispute Resolution) Act 2008 and the Financial Advisers Act 2008, both of which contain express provisions relating to territorial scope.

The Financial Service Providers (Registration and Dispute Resolution) Act 2008 states that:

*“This Act applies to the provision in New Zealand of a financial service by a person who is in New Zealand, regardless of where the financial service provider is resident, is incorporated, or carries on business.”*

The Financial Advisers Act 2008 states that:

*“This Act applies to a financial adviser service performed in New Zealand regardless of where the person performing the financial adviser service is resident, is incorporated or carries on business.”*

3. Businesses may wish to consider making a submission that the territorial scope of the legislation should be clarified. This should remove uncertainty on this matter and also enable questions of competitive neutrality to be expressly considered and relevant requirements established.

**Q.7 Are exemptions available under the legislation?**

1. Yes. The legislation contains broad powers of exemption. An exemption granted under regulations or by the Minister may, for example, exempt:
  - (a) A Reporting Entity or class of Reporting Entities.
  - (b) A transaction or class of transactions, from any or all of the provisions of the legislation.  
(clauses 148 and 151)
2. In granting exemptions, the Minister must have regard to:
  - (a) The intent and purposes of the legislation.
  - (b) The AML/CFT risk.
  - (c) The impacts on the prevention, detection, investigation and prosecution of offences.
  - (d) The level of regulatory burden on a Reporting Entity.
  - (e) Whether the exemption would create an unfair advantage for the Reporting Entity or disadvantage third party Reporting Entities.
  - (f) The overall impact that the exemption would have on the integrity of, and compliance with, the AML/CFT regulatory regime.  
(clauses 148 and 151)

**COMMENT:**

Industries and Reporting Entities should carefully consider aspects of their business that may justify an exemption, taking account of the factors outlined above. We expect that exemptions will particularly be available in respect of activities with a low AML/CFT risk, where the burden of compliance will outweigh the benefits.

**PART 4: CUSTOMER DUE DILIGENCE - GENERAL MATTERS****Q.8 What are the levels of CDD?**

The legislation contemplates three levels of initial CDD:

- (a) Standard CDD.
- (b) Simplified CDD.
- (c) Enhanced CDD.

The legislation also contemplates ongoing CDD.

**COMMENTS:**

1. The three levels of initial CDD, and the requirement for ongoing CDD, are new. The FTRA 1996 only contemplates initial CDD and simply requires the financial institution to verify the identity of the person. The provisions of the new legislation are much more detailed and complex.
2. Simplified CDD is only available in relatively limited circumstances (see Q.20 below). Enhanced CDD is required in prescribed circumstances and businesses will need to establish systems to identify those circumstances (see Q.24 to Q.27 below).

## Q.9 Who must be “CDDed”?

1. When the relevant trigger requirements are met (see Q.15), a Reporting Entity must conduct CDD on:
  - (a) A customer.
  - (b) Any “*beneficial owner*” of a customer.
  - (c) Any person acting on behalf of a customer.
 (clause 9)
  
2. A “*customer*” is defined to mean:
  - (a) A New Customer or an Existing Customer (see Q.13).
  - (b) To include:
    - A facility holder (as defined).
    - A person conducting or seeking to conduct an occasional transaction (as defined).
    - A junket organiser as defined in section 4(1) of the Gambling Act 2003.
  - (c) To include any person deemed by regulations to be a customer and to exclude any person deemed by regulations not to be a customer.
 (clause 4)
  
3. A “*beneficial owner*” of a customer is defined to mean the individual who “*has effective control of a customer or person on whose behalf a transaction is conducted*” or “*owns a prescribed amount of the customer or person on whose behalf a transaction is conducted*” (clause 4).

### COMMENTS:

1. A “*customer*” is defined to include, but does not appear to be limited to, a facility holder or a person conducting an occasional transaction. This potentially extends the identity verification requirements to include individuals who are not establishing a facility or conducting an occasional transaction.
2. The definition of “*beneficial owner*” is likely to give rise to significant interpretational and implementation issues. These are likely to be exacerbated by the fact that the Bill seems to contemplate that customers who are individuals may be “*beneficially owned*” by someone else – see clause 9(2) of the Bill.
3. The FTRA 1996 contains specific provisions requiring the verification of other persons where the financial institution has reasonable grounds to believe that a person is acting on behalf of those other persons. This concept has not been expressly carried through into the Bill, but is

perhaps intended to be captured within the “*beneficial owner*” construct.

4. A difficult issue arises in relation to trusts. Enhanced CDD is required for “*a trust or another vehicle for holding personal assets*” (see Q.24). It is not clear how the “*beneficial owner*” concept might apply to a trust where, as is common, the beneficiaries are discretionary beneficiaries. Note that the Cabinet Papers underpinning the Bill contemplate that Reporting Entities will take reasonable steps to identify the beneficial owner of trust assets.

**Q.10 What happens if a Reporting Entity is unable to conduct CDD in accordance with the legislation?**

In these circumstances, a Reporting Entity:

- (a) Must not establish a business relationship with the customer.
- (b) Must terminate any existing business relationship.
- (c) Must not carry out a transaction with or for the customer.
- (d) Must consider whether to make a suspicious transaction report.

(clause 34)

**Q.11 A number of the CDD requirements are dependent on the “*level of risk involved*”. How will this operate in practice?**

Reporting Entities will be required to conduct initial and ongoing AML/CFT risk assessments. These risk assessments will identify the risks specific to the business and will influence the operation of these CDD requirements (clause 10).

## Q.12 What is the timing for identity verification?

1. A Reporting Entity must carry out the verification of identity before establishing a business relationship or conducting an occasional transaction, unless the exception below applies (clauses 14 and 22).
2. The exception applies where all of the following apply:
  - (a) Delayed verification is essential not to interrupt normal business practice.
  - (b) AML/CFT risks are effectively managed through procedures of transaction limitations and account monitoring.
  - (c) Verification is completed within five days.
 (clauses 14 and 22)

### COMMENT:

This exception is narrower than the exception contained in the FTRA 1996. Under the FTRA 1996, delayed verification is permitted where, broadly speaking, the financial institution does not have face-to-face dealings with the person and it is impracticable to undertake prior verification.

## Q.13 Does the legislation distinguish between new customers and customers accepted under the FTRA 1996 (and previously)?

1. Yes.
 

The Bill defines “*Existing Customers*” to be persons in a business relationship with the relevant Reporting Entity as at the date the main requirements under the new legislation come into force.

There is no definition of “*New Customers*” but the term is used in the Bill – presumably to refer to persons who were not in a business relationship with the relevant Reporting Entity at that time.

 (clause 4)
2. As a general proposition, the initial CDD requirements will not apply to Existing Customers. However, there are a number of circumstances that can cause those requirements to apply to Existing Customers (see Q.15 below).
3. The ongoing CDD requirements apply to both Existing Customers and New Customers.

**Q.14 How does the legislation deal with certain special situations recognised by the FTRA 1996 and other legislation?**

1. The FTRA 1996 recognises a number of special situations relating to CDD. These include:
  - (a) Provisions allowing a financial institution to rely on evidence used on an earlier occasion to verify a person's identity.
  - (b) Provisions reducing the verification requirements in relation to a facility where transactions may be conducted by means of an existing facility provided by another financial institution. This provision is often relied on where a facility is initially established by way of a cheque deposit.
  - (c) Provisions allowing financial institutions associated with employer-sponsored superannuation schemes to rely on identify verification by the employer.
  - (d) Provisions allowing verification of the "*principal facility holder*" where there are three or more facility holders in relation to a facility.
2. Section 204 of the KiwiSaver Act 2006, and Regulations 17 and 18 of the KiwiSaver Regulations 2006, provide AML/CFT relief in relation to default KiwiSaver Schemes.
3. These provisions do not appear to have been carried through into the Bill. In particular, the consequential amendments do not alter the KiwiSaver legislation as would be required to enable the relief to continue to apply.

**COMMENT:**

It may be that some of these provisions will be replicated through regulations and exemptions under the new legislation.

**PART 5: STANDARD CDD**

**Q.15 When is standard CDD required?**

1. Standard CDD is required in the following circumstances (unless simplified CDD is permitted or enhanced CDD is required):
  - (a) If the Reporting Entity establishes a “*business relationship*” with a New Customer (see Q.13 for the meaning of “*New Customer*”).
  - (b) If any customer seeks to conduct an “*occasional transaction*” through the Reporting Entity.
  - (c) If, in relation to any customer, the Reporting Entity suspects that money laundering or financing of terrorism may be involved.
  - (d) If the Reporting Entity suspects on reasonable grounds that any customer is not who he or she claims to be.
  - (e) In relation to an Existing Customer (see Q.13 for a definition of “*Existing Customer*”):
    - If there has been a change in the nature or purpose of the business relationship between the Reporting Entity and the Existing Customer.
    - If doubt arises as to the adequacy or veracity of documents, data or information previously obtained in relation to the Existing Customer.
    - If the Reporting Entity considers that, according to the level of risk involved, it has insufficient information about the Existing Customer.

(clause 12)
2. A “*business relationship*” is defined to mean 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 (clause 4).
3. An “*occasional transaction*” is defined to mean a “*transaction*” (which includes a deposit, withdrawal, exchange or transfer of funds) that is over the threshold value prescribed in regulations (whether the transaction is carried out in a single operation or several operations that appear to be linked). Cheque deposits are excluded. A full definition of “*occasional transaction*” and “*transaction*” is contained in clause 4 of the Bill.

**COMMENTS:**

1. If an entity is a “*financial institution*” then it would appear that the requirements relating to CDD will apply in respect of any customer who enters into a “*business relationship*” regardless of whether the relationship with the customer involves establishing a facility or conducting an

occasional transaction. Further, the requirements would appear to apply whether or not the relationship relates to a relevant activity.

2. Unlike the FTRA 1996, there is no exclusion in the definition of “*occasional transaction*” for transactions conducted through an existing facility. It would therefore appear that the CDD requirements will be triggered where a customer with an existing facility conducts an occasional transaction through that facility. It is not clear to what extent the Reporting Entity may rely on previous CDD.
3. Unlike the FTRA 1996, the definition of “*occasional transaction*” is not limited to transactions involving cash.
4. Procedures will need to be established to identify when there is a change in the nature or purpose of the business relationship with an Existing Customer. There are likely to be grey areas as to when such a change has occurred.

#### **Q.16 What identity information must be obtained in relation to standard CDD?**

A Reporting Entity conducting standard CDD must obtain the following information:

- (a) The person’s full name.
- (b) The person’s date of birth.
- (c) If the person is not the customer, the person’s relationship to the customer.
- (d) The person’s address or registered office.
- (e) The person’s company identifier or registration number.
- (f) Any information prescribed by regulations.
- (g) Any other information that, according to the level of risk involved, could reasonably be obtained.

(clause 13)

#### **COMMENT:**

This is much more prescriptive than the FTRA 1996. These requirements will presumably be met through application forms in relation to facilities and instruction forms in relation to occasional transactions.

**Q.17 What further information must be obtained?**

A Reporting Entity must also obtain:

- (a) Information on the nature and purpose of the proposed business relationship between the customer and Reporting Entity.
  - (b) Sufficient information to determine whether the customer should be subject to enhanced CDD.
- (clause 15)

**COMMENTS:**

1. The practical implementation of the “*nature and purpose*” requirement will need consideration. For example, to what extent can the Reporting Entity provide a pro forma description relating to this matter in an application form? This requirement keys into the requirement under ongoing CDD to monitor accounts to ensure that transactions are consistent with the Reporting Entity’s knowledge about the customer (see Q.29).
2. The requirement relating to enhanced CDD is also capable of giving rise to significant practical issues. Enhanced CDD is considered in further detail in Q.24 to Q.27.

**Q.18 What identity verification requirements apply under standard CDD?**

The Reporting Entity must, according to the level of risk involved:

- (a) Take all reasonable steps to satisfy itself that the identity information provided is current and correct.
- (b) Take all reasonable steps to verify any beneficial owner's identity so that the Reporting Entity is satisfied that it knows who the beneficial owner is.
- (c) If a person is acting on behalf of the customer, verify both the customer's and the person's identity and that person's authority to act on behalf of the customer so that the Reporting Entity is satisfied that it knows who the person is and that the person has authority to act on behalf of the customer.
- (d) Verify any other information prescribed by regulations.

(clause 14)

**COMMENT:**

This is an area where the Codes of Practice produced by AML/CFT supervisors are likely to be particularly relevant.

**Q.19 What basis must be applied for verifying identity?**

Verification of identity must be done on:

- (a) The basis of documents, data or information obtained from a reliable and independent source.
- (b) Any other basis prescribed by regulations.

(clause 11)

## **PART 6: SIMPLIFIED CUSTOMER DUE DILIGENCE**

### **Q.20 When is simplified CDD available?**

Simplified CDD is available in two circumstances:

- (a) Where the Reporting Entity is dealing with certain specified entities including certain listed companies, certain government organisations and entities specified in regulations.
- (b) In relation to a person who purports to act on behalf of a customer when:
  - The Reporting Entity already has a business relationship with the customer.
  - The Reporting Entity has conducted CDD on the customer in accordance with the legislation.

(clause 16)

#### **COMMENTS:**

1. On this basis, the availability of simplified CDD is relatively limited.
2. It would appear that simplified CDD is not available in relation to persons acting on behalf of a customer, unless the customer has been subject to CDD under the new legislation, i.e. would not be available in relation to an Existing Customer who has not needed to be subject to CDD under the legislation.

**Q.21 What identity information must be obtained in relation to simplified CDD?**

1. 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.
    - (b) The person's date of birth.
    - (c) The person's relationship to the customer.
    - (d) Any information prescribed by regulations.
    - (e) Any other information that, according to the level of risk involved, could reasonably be obtained.
- (clause 17)

**COMMENTS:**

1. These identity information requirements are not significantly different to the requirements under standard CDD – see Q.16.
2. The Bill sets out the identity information that must be obtained in relation to a person acting on behalf of a customer but not the information that must be obtained in relation to the specified types of entity (as referred to in (a) under Q.20). We are uncertain whether this means that no identity information must be obtained in relation to those entities or whether the required information will be specified in regulations.

**Q.22 What further information must be obtained under simplified CDD?**

The same requirements apply as for standard CDD (clause 19). See Q.17.

**COMMENT:**

This requirement appears to apply to both persons acting on behalf of a customer and the specified entities.

**Q.23 What identity verification requirements apply under simplified CDD?**

1. A Reporting Entity must, according to the level of risk involved, verify the identity of the person acting on behalf of the customer and the 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 (clause 18).
2. In relation to a person's authority to act, a Reporting Entity may rely on an authority provided in an application form or other document provided to the Reporting Entity that shows the person's authority to act or transact on an account (clause 18).

**COMMENTS:**

1. Again, the identity verification requirement appears to apply in respect of persons acting on behalf of a customer and not in relation to specified entities.
2. The provision relating to the reliance on an application form or other document does not apply in respect of standard CDD.

## **PART 7: ENHANCED CDD**

### **Q.24 When is enhanced CDD required?**

1. A Reporting Entity must conduct enhanced CDD where it establishes a business relationship with a customer or the customer seeks to conduct an occasional transaction and the customer is:
  - (a) A trust or another vehicle for holding personal assets.
  - (b) A non-resident customer from a country that has insufficient AML/CFT systems or measures in place.
  - (c) A company with nominee shareholders or shares in bearer form.
  - (d) A politically exposed person. This is defined in clause 4 of the Bill to include specified office-holders in New Zealand and elsewhere, and their immediate relations and certain related entities.
  - (e) Undertaking a transaction that involves new or developing technologies and products that favour anonymity.

(clause 20)
2. A Reporting Entity must also conduct enhanced CDD:
  - (a) If a customer seeks to conduct a complex, unusually large transaction or unusual patterns of transactions that have no apparent or visible or economic or lawful purpose.
  - (b) When the Reporting Entity considers that the level of risk involved is such that enhanced CDD should apply to a particular situation.
  - (c) If it is an ordering institution, an intermediary institution or a beneficiary institution in relation to a wire transfer (as those terms are defined).
  - (d) If it has, or proposes to have, a correspondent banking relationship (as defined).
  - (e) In any other circumstance specified in regulations.

(clause 20)

**COMMENT:**

One of the most significant challenges for Reporting Entities under the new legislation will be designing and implementing systems to identify circumstances where enhanced CDD is required. This will particularly be the case in relation to politically exposed persons, given the broad definition of that term.

**Q.25 What identity information must be obtained in relation to enhanced CDD?**

1. Subject to the specific requirements referred to in 2 below, a Reporting Entity conducting enhanced CDD must obtain the following information:
  - (a) The information required for standard CDD (see Q.16).
  - (b) Information relating to the source of the funds or the wealth of the customer.
  - (c) Other information prescribed by regulations in relation to enhanced CDD.(clause 21)
2. These requirements do not apply in respect of wire transfers and correspondent banking relationships, which are governed by the specific requirements contained in clauses 24 to 26 of the Bill.

**COMMENT:**

The provisions relating to enhanced CDD do not appear to expressly require the Reporting Entity to obtain “*information on the nature and purpose of the proposed business relationship between the customer and the Reporting Entity*”. Given that this is a requirement of standard CDD (see Q.17), this may be a drafting error.

**Q.26 What identity verification requirements apply under enhanced CDD?**

1. Subject to the specific requirements referred to in 2 below, a Reporting Entity must according to the level of risk involved:
  - (a) Undertake the identity verification requirements applicable under standard CDD (see Q.18).
  - (b) Take all reasonable steps to verify the source of wealth or funds of the customer.
  - (c) Verify any other information prescribed by regulations or required by Codes of Practice in relation to enhanced CDD.

(clause 22)
2. These requirements do not apply in respect of wire transfers and correspondent banking relationships, which are governed by the specific requirements contained in clauses 24 to 26 of the Bill.

**Q.27 What additional specific requirements apply to particular categories of enhanced CDD?**

The following additional specific requirements apply:

- (a) Specific requirements apply in relation to wire transfers and correspondent banking relationships (clauses 24 to 26 of the Bill).
- (b) Before a Reporting Entity establishes a business relationship or conducts an occasional transaction that involves a customer or a beneficial owner who is a politically exposed person the Reporting Entity must:
- Have approval from its senior management.
  - Meet any other applicable requirements prescribed by regulations.
- (clause 23)
- (c) Before a Reporting Entity establishes a business relationship or conducts an occasional transaction that involves new or developing technologies and products that might favour anonymity the Reporting Entity must:
- Take any additional measures that may be needed to prevent the technology or products from being used in the commission of money-laundering or for the financing of terrorism.
  - Meet any other applicable requirements prescribed by regulations.
- (clause 27)

**COMMENT:**

The practicalities of obtaining senior management approval in relation to politically exposed persons will need to be explored. It is unclear from the current drafting of the Bill, whether this requires the approval of each member of senior management or whether this role can be delegated to a single member or committee of senior management personnel.

**PART 8: ONGOING CDD AND ACCOUNT MONITORING****Q.28 When is ongoing CDD and account monitoring required?**

Ongoing CDD is required where there is a business relationship (as defined - see Q.15) between the Reporting Entity and a customer. It is not required in relation to a one-off occasional transaction where there is no business relationship (clause 28).

**COMMENT:**

Ongoing CDD is required in relation to both Existing Customers and New Customers.

**Q.29 What is required when undertaking ongoing CDD and account monitoring?**

1. A Reporting Entity must undertake these activities in order to:
  - (a) Ensure that the business relationship and transactions are consistent with the Reporting Entity's knowledge about the customer and the customer's business and risk profile.
  - (b) Identify any grounds for reporting a suspicious transaction.(clause 28)
2. The Reporting Entity must have regard to:
  - (a) The type of CDD conducted when the business relationship with the customer was established.
  - (b) The level of risk involved.(clause 28)
3. The minimum level of activity is:
  - (a) Regularly reviewing the customer's account activity and transaction behaviour.
  - (b) Regularly reviewing any customer information obtained under the legislation or, in relation to an Existing Customer, any customer information held about the customer.
  - (c) Any other matter prescribed by regulations.(clause 28)

**COMMENTS:**

1. As with enhanced CDD, designing and implementing systems to achieve ongoing CDD and account monitoring is likely to be a very significant challenge for Reporting Entities. This is an area where Codes of Practice produced by AML/CFT supervisors are likely to be particularly relevant.
2. In relation to New Customers, the requirement is to review the customer information obtained under the legislation. In relation to Existing Customers, the requirement relates to any customer information held by the Reporting Entity and appears to potentially be wider than for New Customers. The implications of this need to be considered.

## **PART 9: RELIANCE ON THIRD PARTIES TO CONDUCT CUSTOMER DUE DILIGENCE**

### **Q.30 When can a Reporting Entity rely on third parties to conduct CDD?**

The legislation explicitly contemplates that a Reporting Entity may rely on third parties to conduct CDD in three circumstances:

- (a) A Reporting Entity may rely on another member of a “*designated business group*” (**DBG**).
- (b) A Reporting Entity may rely on another Reporting Entity or an equivalent overseas entity that is neither a member of its DBG or an agent.
- (c) A Reporting Entity may rely on an agent.

Various conditions and requirements apply. Each type of arrangement is considered in further detail in the following questions.

#### **COMMENTS:**

1. There are a number of scenarios in which Reporting Entities may wish to rely on third parties to conduct CDD. Reporting Entities who may wish to do so should carefully consider the permitted arrangements to ensure that they can meet the relevant conditions and to understand how they will operate in practice. Some Reporting Entities are likely to implement more than one of the three types of arrangement.
2. In relation to DBGs only, the reliance may extend beyond CDD and apply also to other requirements under the legislation. See Q.31.
3. The legislation places constraints on the manner in which information received by a Reporting Entity from a third party conducting CDD may be used. Clause 32 states that information may only be used for the purposes of complying with the legislation and regulations. We believe that this may constrain the normal business operations of Reporting Entities and potentially discourage them from establishing third party arrangements. In particular, the constraints on the use of information should not apply where the customer has expressly authorised a wider use of the information.

**Q.31 How do designated business groups work?**

1. The definition of a DBG is detailed and complex, and will need to be carefully analysed by any party wishing to form a DBG. However, key features include the following:
  - (a) A DBG may consist of two or more persons, each of whom has elected to be a member of the DBG.
  - (b) A person may only be a member of one DBG.
  - (c) At least one member of the DBG must be a Reporting Entity.
  - (d) Each member of the DBG must be:
    - Related to each other member of the DBG within the meaning of section 2(3) of the Companies Act 1993 and either a Reporting Entity resident in New Zealand or an equivalent overseas entity; or
    - Providing a service under a joint venture agreement, to which each member of the DBG is a party; or
    - A specified government department or related person.

(clause 4)
2. Where a member of a DBG relies on another member to conduct CDD, there are provisions requiring that other member to provide it with identity and verification information within specified timeframes (clause 29).
3. As well as relying on another member of its DBG to conduct CDD, a member of a DBG may:
  - (a) Adopt that part of the other member's AML/CFT programme that relates to recordkeeping, account monitoring and annual reporting, subject to any conditions prescribed in regulations.
  - (b) Use another member of the group's risk assessment if that risk assessment is relevant to the member.
  - (c) Make a suspicious transaction report on behalf of another member.

(clause 29)

**COMMENTS:**

1. This type of arrangement is clearly of most relevance to corporate groups containing more than one Reporting Entity. It may be of particular use to avoid duplicated CDD where a customer establishes a business relationship with more than one Reporting Entity within the group at the same time.
2. The DBG arrangement would not appear to impact on the substantive CDD requirements that

apply. It is conceivable that a customer may simultaneously enter into a relationship with two Reporting Entities within a DBG in circumstances where the substantive CDD requirements differ for each Reporting Entity (for example, because one relationship has a higher level of risk than the other). In these circumstances, the Reporting Entity conducting the CDD would presumably need to apply the higher CDD standard.

3. It is not clear whether the DBG arrangement is predicated on the Reporting Entity who is undertaking the CDD needing to, or having previously, conducted CDD on the customer in its own right. If this is not required, then the DBG can operate in a manner akin to an agency arrangement.
4. It is also unclear how the DBG arrangement operates where a customer has entered into a business relationship, and been “CDDed”, by one Reporting Entity within the DBG and then at a later date enters into such a relationship with another Reporting Entity within the DBG. To what extent can the second DBG rely on the CDD undertaken at the earlier date?
5. There is nothing to prevent members of the same corporate group from utilising one of the other third party reliance arrangements that are permitted. Corporate groups may therefore wish to consider the relative merits of each type of arrangement.
6. In circumstances where one member of a DBG has relied on another to conduct CDD, and non-compliance occurs, it is unclear which member will have liability for the non-compliance. Unlike for the arrangement referred to in Q.32 below, the provisions relating to DBGs do not expressly specify which Reporting Entity is responsible for ensuring compliance with the CDD requirements.

**Q.32 When can a Reporting Entity rely on another Reporting Entity or equivalent overseas entity that is neither a member of its DBG or an agent?**

1. A Reporting Entity may rely on a third party who is not a member of its DBG or an agent to conduct CDD where all of the following apply:
  - (a) The third party is either a Reporting Entity or an equivalent overseas entity.
  - (b) The third party has a business relationship with the customer concerned.
  - (c) The third party has conducted CDD to at least the standard required by the legislation and provides relevant identity and verification information to the Reporting Entity.
  - (d) The third party has consented to conducting the CDD for the Reporting Entity.
  - (e) Any conditions prescribed in regulations are complied with.

(clause 30)
2. In these circumstances the Reporting Entity, and not the third party, is responsible for ensuring that CDD is carried out in accordance with the legislation (clause 30).

**COMMENTS:**

1. This type of arrangement would appear to be of most relevance where, for example:
  - (a) The relationship between the Reporting Entity and the third party is such that customers of the third party regularly become customers of the Reporting Entity. This may occur, for example, where the products of one Reporting Entity are distributed to the customers of another Reporting Entity.
  - (b) The Reporting Entity and the third party both have CDD obligations in respect of the same arrangement e.g. the trustee and manager of a KiwiSaver Scheme.
2. Unlike in relation to the DBG arrangements, there is no restriction on the number of arrangements that a Reporting Entity may enter into. Accordingly, where considered appropriate from a business perspective, a Reporting Entity may consent to conduct CDD for any number of other Reporting Entities.
3. Although this is not expressly stated, it appears that this type of arrangement is predicated on the third party having conducted CDD in its own right in relation to the relevant customer. In other words, the Reporting Entity is relying on CDD undertaken by the third party for its own purposes, rather than CDD undertaken by the third party solely for the benefit of the Reporting Entity.
4. This potentially gives rise to issues if the standard of CDD required to be undertaken by the third party differs from the standard applicable to the Reporting Entity (for example, because

one relationship has a higher level of risk than the other). Although the Bill is not explicit on this matter, in these circumstances it would appear that the Reporting Entity may not rely on the CDD conducted by the third party.

5. This type of arrangement presumably accommodates a situation where the customer's relationship with the third party is established prior to the establishment of the customer's relationship with the Reporting Entity. It is unclear whether the third party is required to specifically update the CDD procedures as at the point in time when the second relationship is established.
6. This type of arrangement has some similarity to the exemption under the FTRA 1996 under which a financial institution need not verify identity where a transaction is conducted through a facility provided by another financial institution. However, the conditions applicable under the new legislation are much more onerous.
7. The legislation specifically provides that the Reporting Entity will be responsible for the CDD carried out by the third party. This may mean that Reporting Entities who rely on third parties will require undertakings from those third parties to the effect that the CDD procedures comply with the legislation. This may impact on the willingness of third parties to conduct CDD on behalf of Reporting Entities under this type of arrangement.

### **Q.33 When may a Reporting Entity rely on an agent to conduct CDD?**

Subject to any conditions prescribed by regulations, a Reporting Entity may authorise a person to be its agent and rely on that agent to conduct CDD (clause 31).

#### **COMMENTS:**

1. There are no restrictions on the number of agents that may be appointed by a Reporting Entity or the persons who may act as agent.
2. Under this type of arrangement, the agent will be conducting CDD on behalf of the Reporting Entity as the principal. Accordingly, all substantive requirements applicable to the principal will apply and the Reporting Entity will have responsibility for compliance with the legislation.

**PART 10: RISK ASSESSMENTS/COMPLIANCE PROGRAMMES ETC.****Q.34 What are the key AML/CFT compliance requirements?**

The key AML/CFT compliance requirements are as follows:

- (a) Before conducting CDD or establishing an AML/CFT compliance programme, a Reporting Entity must undertake an assessment of the AML/CFT risks that it may reasonably expect to face in the course of its business (clause 55).
- (b) A Reporting Entity must establish, implement and maintain an AML/CFT compliance programme (clause 53).
- (c) A Reporting Entity must designate an employee as an AML/CFT compliance officer to administer and maintain its AML/CFT programme. The compliance officer must report to a senior manager of the Reporting Entity (clause 53).
- (d) The Reporting Entity must conduct a review of its risk assessment and AML/CFT programme in accordance with the requirements of the legislation (clause 56). The legislation does not specify how often this review must be conducted.
- (e) A Reporting Entity must prepare an annual report on its risk assessment and AML/CFT programme, and provide that annual report to its AML/CFT supervisor (clause 57).
- (f) A Reporting Entity must ensure its risk assessment and AML/CFT programme are audited by an independent auditor, in accordance with the legislation, at least every two years. The auditor is not required to be a chartered accountant or a person qualified to undertake financial audits. The Reporting Entity must provide a copy of the audit to its AML/CFT supervisor as soon as practicable after conducting the audit (clause 56).
- (g) Specific obligations apply in respect of the branches and subsidiaries of a Reporting Entity that are in a foreign country (clause 58).

**COMMENT:**

These are new and onerous requirements. The risk management assessment and AML/CFT compliance programme will need to be completed during the two-year transitional period.

**Q.35 What specific requirements apply in respect of the risk assessment?**

1. In assessing the AML/CFT risk, the Reporting Entity must have regard to the following:
  - (a) The nature, size and complexity of its business.
  - (b) The products and services it offers.
  - (c) The methods by which it delivers products and services to its customers.
  - (d) The types of customers it deals with.
  - (e) The countries it deals with.
  - (f) The institutions it deals with.
  - (g) Any applicable guidance material produced by AML/CFT supervisors or the Commissioner relating to risk assessments.
  - (h) Any other factors that may be prescribed in regulations.(clause 55)
2. The risk assessment must be in writing and:
  - (a) Identify the risks faced by the Reporting Entity in the course of its business.
  - (b) Describe how the Reporting Entity will ensure that the assessment remains current.
  - (c) Enable the Reporting Entity to determine the level of risk involved in relation to relevant obligations under this Act and the regulations.(clause 55)

**COMMENT:**

To meaningfully assess risks, businesses will need to understand the objectives and techniques used in laundering money and financing terrorism. This will include new and innovative techniques as they develop. AML/CFT supervisors will have a role in educating businesses and keeping them apprised of new developments.

**Q.36 What matters need to be covered by a Reporting Entity's AML/CFT compliance programme?**

A Reporting Entity's AML/CFT programme must include adequate and effective procedures, policies, and controls for:

- (a) Vetting:
  - Senior managers.
  - The AML/CFT compliance officer.
  - Any other employee that is engaged in AML/CFT related duties.
- (b) Training on AML/CFT matters for the following employees:
  - Senior managers.
  - The AML/CFT compliance officer.
  - Any other employee that is engaged in AML/CFT related duties.
- (c) Complying with CDD requirements (including ongoing CDD).
- (d) Reporting suspicious transactions.
- (e) Record keeping.
- (f) Setting out what the Reporting Entity needs to do, or continue to do, to manage and mitigate AML/CFT risks.
- (g) Account monitoring.
- (h) Examining, and keeping written findings relating to:
  - Complex or unusually large transactions.
  - Unusual patterns of transactions that have no apparent economic or visible lawful purpose.
  - 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.
- (i) Monitoring, examining, and keeping written findings relating to business relationships and transactions from or in countries that do not have, or have insufficient, AML/CFT systems in place and have additional measures for dealing with or restricting dealings with such countries.
- (j) 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.
- (k) Determining when enhanced CDD is required and when simplified CDD might be permitted.
- (l) Providing when a person who is not the Reporting Entity may, and setting out the procedures for the person to, conduct the relevant CDD on behalf of the Reporting Entity.

- (m) Monitoring and managing compliance with, and the internal communication of and training in, those procedures, policies, and controls.
- (n) Any other matters prescribed by regulations.
- (o) Any other matters that may be provided for in the guidance produced by the AML/CFT supervisor for the Reporting Entity or by the Commissioner.

(clause 54)

**COMMENTS:**

1. These requirements do not arise under the FTRA 1996 and are therefore new. They are likely to be onerous and require significant resources to establish and maintain.
2. Reporting Entities will be looking for substantial guidance from their AML/CFT supervisors in relation to these requirements.

## **PART 11: SUSPICIOUS TRANSACTION REPORTS**

### **Q.37 When is a suspicious transaction report required?**

Subject to certain exceptions, a suspicious transaction report is required where a person conducts or seeks to conduct a transaction through a Reporting Entity and the Reporting Entity has reasonable grounds to suspect that the transaction is or may be:

- (a) Relevant to the investigation or prosecution of any person for a money-laundering offence.
- (b) Relevant to the enforcement of the Misuse of Drugs Act 1975.
- (c) Relevant to the enforcement of the Terrorism Suppression Act 2002.
- (d) Relevant to the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009.

(clause 37)

**COMMENT:**

The FTRA 1996 does not cover the Misuse of Drugs Act 1975, the Terrorism Suppression Act 2002 or the Criminal Proceeds (Recovery) Act 2009. In these respects, the new legislation extends the suspicious transaction reporting regime.

### **Q.38 What is the timing for suspicious transaction reports?**

The Reporting Entity must, as soon as practicable, but no later than three working days after forming its suspicion, report the transaction or proposed transaction (clause 37).

**COMMENT:**

The FTRA requires reporting as soon as reasonably practicable. It does not contain the three working day maximum period.

**Q.39 Who is the report made to?**

The report is made to the Commissioner of Police (clause 37). The report must be forwarded by way of secure electronic transmission by a means specified or provided by the Commissioner or by another means agreed between the Commissioner and the Reporting Entity (clause 38). Urgent reports may be made orally to a Police employee authorised by the Commissioner (clause 38).

**Q.40 What is the form of the report?**

A suspicious transaction report must:

- (a) Be in the form prescribed by regulations.
- (b) Contain the details prescribed by regulations.
- (c) Contain a statement of the grounds on which the Reporting Entity holds the suspicion.
- (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).

(clause 38)

**Q.41 What other provisions apply in relation to suspicious transaction reports?**

The legislation also contains the following provisions relating to suspicious transaction reports:

- (a) Provisions creating an exception for privileged communications and arrangements to which section 44(4) of the Terrorism Suppression Act 2002 relates (clause 37).
- (b) Provisions permitting auditors to report suspicious transactions (clause 40).
- (c) Provisions for the protection of persons reporting suspicious transactions (clause 41).
- (d) Provisions limiting the disclosure of information relating to suspicious transaction reports (clause 43).

**PART 12: RETENTION OF RECORDS****Q.42 What records must be kept in relation to transactions?**

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 (clause 46).
2. Without limiting the general proposition, the 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, employee or agent of the Reporting Entity who handled the transaction if that officer, employee or agent:
    - Has face-to-face dealings in respect of the transaction with any of the parties to the transaction.
    - Has formed a suspicion about the transaction.
  - (g) Any other information prescribed by regulations.(clause 46)

**COMMENT:**

These requirements are equivalent to those contained in the FTRA 1996.

**Q.43 What records must be kept in relation to identity and identity verification?**

1. In respect of each case where a Reporting Entity is required under the legislation 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 (clause 47).
2. Without limiting the general proposition, these records may comprise:
  - (a) A copy of the evidence used.
  - (b) If it is not practicable to retain that evidence, any information as is reasonably necessary to enable that evidence to be obtained.(clause 47)

**COMMENT:**

These requirements are equivalent to those contained in the FTRA 1996.

**Q.44 What other records must be kept?**

A Reporting Entity must also keep:

- (a) Records that are relevant to the establishment of any business relationship.
- (b) 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.

(clause 48)

**COMMENT:**

This is a new requirement that is not contained in FTRA 1996. It is potentially broad and guidance under Codes of Practice will assist to understand its scope.

**Q.45 How long must records be kept for?**

Records must be kept as follows:

1. Transaction records must be kept for a period of at least five years after completion of the transaction or such longer period as the AML/CFT supervisor or the Commissioner of Police specifies (clause 46).
2. Identity verification records relating to the establishment of a business relationship must be kept for a period of at least five years after the end of that relationship (clause 47).
3. Identity verification records relating to an occasional transaction must be kept for a period of at least five years after the completion of the occasional transaction (clause 47).
4. Specific requirements apply to identify verification records relating to wire transfers (clause 47).
5. Records under Q.44 must be kept for a period of at least five years after the end of the relevant business relationship (clause 48).

**Q.46 How must records be kept?**

Records must be kept:

- (a) 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.
- (b) In such manner as is prescribed by regulations.

(clause 49)

**Q.47 What other provisions are there relating to record keeping?**

The legislation contains provisions relating to:

- (a) The liquidation of a Reporting Entity (clause 50).
- (b) The requirement to destroy records as soon as practicable after the expiry of the retention period (subject to certain exceptions) (clause 51).

**PART 13: MISCELLANEOUS MATTERS****Q.48 What general prohibitions apply to Reporting Entities?**

1. Subject to certain exceptions, a Reporting Entity must not knowingly or recklessly:
  - (a) 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.

(clause 35)
2. 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 (as defined).
  - (b) A financial institution that has a correspondent banking relationship (as defined) with a shell bank.

(clause 36)

**Q.49 What other things does the legislation cover?**

1. The legislation contains provisions relating to the cross-border transportation of cash (sub-part 6).
2. The legislation sets out detailed provisions relating to enforcement, including provisions imposing potential liability on directors and senior managers of a Reporting Entity (Part 3).

**COMMENT:**

Reporting Entities will need to establish appropriate procedures to protect themselves, their directors and senior managers from these potential liabilities. Careful analysis of the “due diligence” defences in the legislation is required.

**Q.50 Who will be the AML/CFT supervisors?**

1. The Reserve Bank of New Zealand will supervise:
  - (a) Banks.
  - (b) Life insurers.
  - (c) Non-bank deposit takers.(clause 127)
2. The Securities Commission will supervise:
  - (a) Issuers of securities.
  - (b) Trustee companies.
  - (c) Futures dealers.
  - (d) Collective investment schemes.
  - (e) Financial advisers.(clause 127)
3. The Department of Internal Affairs will supervise:
  - (a) Casinos.
  - (b) Non-deposit-taking lenders.
  - (c) Money changers.
  - (d) Other Reporting Entities.(clause 127)
4. If the products or services provided by a particular Reporting Entity are covered by more than one AML/CFT supervisor, the legislation contains provisions enabling a single AML/CFT supervisor to be appointed for that Reporting Entity (clause 127).

**COMMENTS:**

1. The establishment of three separate AML/CFT supervisors creates the possibility of inconsistent approaches. However, this is mitigated by the establishment of an AML/CFT co-ordination committee. It is common in overseas jurisdictions for a number of supervisors to administer AML/CFT requirements.
2. The legislation recognises the need for a single AML/CFT supervisor in relation to a particular Reporting Entity. However, it does not recognise an equivalent requirement in relation to particular corporate groups.

---

**AUCKLAND** VERO CENTRE, 48 SHORTLAND STREET  
PO BOX 4199, AUCKLAND 1140, NEW ZEALAND, DX CP20509  
TEL 64 9 916 8800 FAX 64 9 916 8801

**WELLINGTON** HP TOWER, 171 FEATHERSTON STREET  
PO BOX 1291, WELLINGTON 6140, NEW ZEALAND, DX SX11164  
TEL 64 4 915 6800 FAX 64 4 915 6810