ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM BILL

REPORT OF THE MINISTRY OF JUSTICE

Crime Prevention and Criminal Justice Group
Ministry of Justice

26 August 2009
## CONTENTS

<table>
<thead>
<tr>
<th>Part One</th>
<th>Introduction</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part Two</td>
<td>Summary of submissions</td>
<td>6</td>
</tr>
<tr>
<td>Part Three</td>
<td>Summary of Recommendations</td>
<td>16</td>
</tr>
<tr>
<td>Part Four</td>
<td>Clause by clause analysis</td>
<td>24</td>
</tr>
<tr>
<td>Part Five</td>
<td>Issues not relating to specific clauses</td>
<td>88</td>
</tr>
<tr>
<td>Appendix 1</td>
<td>Terminology and abbreviations</td>
<td>93</td>
</tr>
<tr>
<td>Appendix 2</td>
<td>List of submitters</td>
<td>94</td>
</tr>
<tr>
<td>Appendix 3</td>
<td>Minor and technical changes tables</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>- Table one: proposed amendments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Table two: no changes recommended</td>
<td></td>
</tr>
</tbody>
</table>
Part One: Introduction

1. The Anti-Money Laundering and Countering Financing of Terrorism Bill (the Bill) was introduced to Parliament on 25 July 2009. The Bill represents the first phase of comprehensive anti-money laundering and countering financing of terrorism (AML/CFT) reforms since 1996 and will bring New Zealand into line with the international standards for AML/CFT frameworks, as set out by the Financial Action Task Force (the FATF).

2. The New Zealand AML/CFT framework currently falls short against New Zealand’s international obligations in some important areas, including customer due diligence (CDD) and record-keeping standards and in the supervision of AML/CFT activity.

3. Improving New Zealand’s AML/CFT regime will:
   3.1. provide an effective tool for detecting and preventing organised crime and terrorism domestically.
   3.2. contribute to efforts to prevent and reduce organised crime and terrorism internationally.
   3.3. allow New Zealand to meet its international obligations on AML/CFT.

Key elements of the Bill

4. The Bill is intended to reflect the FATF Recommendations. The key elements of the Bill are:
   4.1. a set of obligations (see paragraph 5) for those entities covered by the Bill (subsequently referred to as 'reporting entities').
   4.2. a risk-based approach to allow resources to be allocated to activities in a way that reflects money laundering and terrorism financing risk and minimises compliance costs.
   4.3. an enforcement regime, including new civil and criminal offences.
   4.4. a regime for supervision, monitoring, and enforcement of AML/CFT obligations involving multiple supervisors including the Reserve Bank, the Securities Commission, and the Department of Internal Affairs.

5. Part 1 of the Bill contains preliminary provisions. Part 2 of the Bill requires reporting entities to:
   5.1. establish, implement and maintain an AML/CFT programme.
   5.2. undertake, as a part of a risk-based approach, more rigorous CDD requirements (improving upon those set out in the Financial Transactions Reporting Act 1996 – FTRA).
   5.3. undertake, as a part of a risk-based approach, ongoing CDD and account and transaction monitoring.
5.4. implement enhanced CDD measures relating to customers, business relationships and transactions presenting higher AML/CFT risk.

5.5. maintain adequate records that can be easily reconstructed.

5.6. undertake more robust measures for reporting suspicious transactions to the Financial Intelligence Unit (currently provided for in the FTRA).

6. Parts 3 and 4 of the Bill, which set out enforcement and supervision arrangements, provide for:

6.1. processes for facilitating compliance with, and enforcing, AML/CFT obligations.

6.2. offences and penalties in the event of non-compliance.

6.3. the definition of supervisors.

6.4. powers for supervisors and the Financial Intelligence Unit of the New Zealand Police (FIU).

6.5. arrangements for facilitating consistency through the AML/CFT Coordination Committee.

Criteria used for developing AML/CFT reforms

7. Cabinet agreed to criteria for developing AML/CFT reform [POL Min (08) 17/3 refers]. These are:

7.1. compliance with international obligations relating to anti-money laundering, unless there are very compelling reasons why particular obligations cannot be met at this time or exemptions or lower levels of compliance are warranted.

7.2. a 'best fit' for New Zealand, justified on the basis of a cost, benefit and risk analysis that takes into account costs on government and business that are justified by: likely benefits; the level of money laundering risk in New Zealand; and the likely consequences of non-compliance with FATF Recommendations.

7.3. compatibility with Australian regulatory requirements where consistent with New Zealand’s circumstances and requirements.

7.4. consistency with AML/CFT legislation in other FATF member countries in expressing AML/CFT regulatory requirements to minimise compliance costs for international investors and financial institutions, unless this is inconsistent with New Zealand’s circumstances and requirements.

7.5. consistent regulation and supervision across sectors where feasible, while at the same time recognising sector differences.

7.6. transparent regulation, rules and sector guidance that are accessible and provide certainty to business and supervisors.

7.7. effective and coordinated implementation (including information sharing mechanisms) to achieve the overall objectives of the framework and
7.8. regulation and supervision that go no further than is necessary to achieve the stated objectives and which are implemented in ways that minimise compliance costs on industry to the extent feasible.

Structure of the report

8. This report is set out in five parts, as follows:

8.1. Part 1 provides an introduction and an overview the Bill and the criteria used for policy development.

8.2. Part 2 provides an overview of submissions and highlights key themes.

8.3. Part 3 presents a summary of the key recommendations proposed in the report.

8.4. Part 4 sets out a clause by clause analysis in sequential order.

8.5. Part 5 contains a suite of issues that do not relate to specific clauses but which are important to the purpose of the Bill.

8.6. Appendix 1 contains a glossary of acronyms for common anti-money laundering and terrorism financing terminology.

8.7. Appendix 2 sets out a list of people and organisations that submitted on the Bill.

8.8. Appendix 3 provides a table of proposed minor and technical issues. Table 1 contains issues for which change is recommended. Table 2 sets out issues that were considered during the analysis process but for which no change is recommended.
Part Two: Key themes from public submissions

Public submissions

9. The Committee received 39 public submissions on the Bill. Most submitters were financial service providers or industry bodies based in New Zealand or Australia. There were only two submissions from private individuals and three submissions from advocacy groups.

10. Three key themes have been identified in submissions:

10.1. support for reform

10.2. the application of a risk-based approach; balancing flexibility with prescription

10.3. harmonisation with Australia.

These themes are discussed in more detail in this part of the report.

<table>
<thead>
<tr>
<th>Principal recommendations in response to key themes from submissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Clarify the application of the risk-based approach to identity verification.</td>
</tr>
<tr>
<td>• Reduce the burden of updating CDD for existing customers by raising the thresholds for triggering the relevant obligations.</td>
</tr>
<tr>
<td>• Clarify that the definition of 'occasional transaction' only applies to cash transactions that are carried out other than in a business relationship.</td>
</tr>
<tr>
<td>• Clarify that reporting entities are not expected to carry out customer due diligence again, when it has previously been carried out in accordance with the Bill.</td>
</tr>
<tr>
<td>• Remove the 5-day time constraint for verification reporting entities and allowing an 'as soon as practicable' approach if money laundering and terrorism financing risks are managed appropriately.</td>
</tr>
<tr>
<td>• Remove explicit senior management liability for civil and criminal breaches.</td>
</tr>
</tbody>
</table>

However, it is proposed to:

• Retain the application of enhanced due diligence to trusts.

• Retain the requirement to identify the beneficial owner of a customer who carries out an occasional transaction.
Support for reform and the New Zealand context

11. The overwhelming majority of the submissions supported the need for AML/CFT legislation. However, several expressed concern about costs of implementation and effectiveness in terms of crime reduction, with several submitters expressing the view that there is low money laundering and terrorism financing in New Zealand. A number of submitters commented on the perceived low level of money within their particular industry or aspect of financial services. These submitters considered that efforts to implement FATF compliant AML/CFT systems should be done in a manner which takes into account this low risk.

Comment

12. Indicators for the rate of money laundering are the size and rate of predicate offending\(^1\). Estimating the size of black economies is inherently problematic. The New Zealand Police estimate that the combined profit from methamphetamine and cannabis sales is between NZ$1.4 billion and NZ$2.2 billion per annum. Roughly 18,000 predicate offences are committed in New Zealand every year, a significant proportion of which are financially motivated, including robbery, drug manufacturing, distribution and smuggling, along with tax evasion and fraud. While there is no estimate of size of financial crime and fraud in New Zealand, there is also no convincing evidence to suggest that the size or rate of financial crime is low compared to other countries.

13. Without a robust regime, New Zealand cannot expect to be insulated from international financial crime. As a stable economy and a member of both the OECD and FATF, but with an ageing AML/CFT framework, New Zealand could be viewed as a target for international money laundering. For example:

13.1. Concerns have been expressed to New Zealand about transactions to Vanuatu using New Zealand as a conduit

13.2. New Zealand foreign trusts have been highlighted by overseas consultancies as a preferred offshore method of asset protection for international organisations.

14. Preventative measures need to be systemic to ensure that any gaps cannot be exploited. There are currently gaps in our measures to ensure that anonymity in companies and trusts is not used for criminal purpose. More widely, New Zealand's measures to positively identify customers are insufficient to prevent identity fraud.

15. From a global perspective, New Zealand has some significant shortfalls in its current AML/CFT regime; New Zealand's level of FATF compliance is substantively lower than that of our key financial trading partners.

\(^1\) Money Laundering requires a predicate offence which generated the criminal proceeds for laundering. In New Zealand a predicate offence is any offence where the maximum sentence is more than 5 years (section of the Crimes Act 1961).
16. For any offshore banking activity, the FATF recommendations place obligations on financial institutions worldwide to consider the reputation and quality of AML/CFT supervision of financial institutions in any country that they deal with. If the AML/CFT framework deficiencies remain, New Zealand banks and banking customers can expect additional scrutiny of their offshore relationships and transactions, thus raising the cost of doing business internationally.

17. From a global perspective, the status of FATF compliance can influence perceptions of financial sector integrity more generally, which in turn may result in New Zealand being placed in higher risk categories with respect to borrowing.

18. Finally, continued non-compliance places at risk our political credibility, reputation, and leadership efforts, especially in the Asia Pacific Region.

19. There are significant compliance costs associated with implementing AML/CFT reforms to the international standards. The proposed AML/CFT reform was estimated to involve: a one-off $97 million in start-up costs; and $21 million, year on year, in ongoing costs to industry. The majority of costs will be borne by the banking sector. The costs of not upgrading New Zealand's AML/CFT regime may be similarly significant for that sector. Australian legislation requires foreign-owned subsidiaries to implement robust AML/CFT measures. Over the coming years it is expected that pressure for New Zealand banks to comply with Australian legislation will grow, should New Zealand legislation not be progressed.

20. Given the illicit nature of terrorism financing in New Zealand it would not be appropriate to attempt an estimate of the size and rate of terrorism financing in New Zealand. However, we do consider that the New Zealand presents a low risk relative to other jurisdictions.

21. We also consider that there is enough risk within New Zealand to warrant bringing our AML/CFT systems into line with the FATF Recommendations, which are the international standard for AML/CFT.

Risk-based approach

22. A major theme from the banking sector is a desire to see provision for greater discretion in managing ML/TF risks through a more permissive risk-based approach (RBA). The focus of concern was specifically about to the CDD provisions. The application of the risk-based approach to ongoing due diligence and transaction monitoring did not draw as much comment.

Flexibility vs. prescription in CDD

23. A key theme of the submissions is the question of whether there should be more scope in implementing a risk-based approach to CDD or whether risk management should be achieved through more clarity and assurance on CDD issues through prescription. This tension, for the most part on behalf of the financial sector, reflects a desire to focus resources on areas of higher risk so that reporting entities
can achieve maximum cost effectiveness in achieving the objectives of AML/CFT activity.

24. The Bill places an emphasis on the importance of ‘knowing your customer’ (KYC) as part of customer due diligence (CDD). CDD involves collecting and verifying of identity (and other) information. The requirements of the Bill that carry the greatest compliance costs are likely to be any minimum CDD verification procedures and standards. Submitters, particularly the banking sector, considered that the minimum CDD provisions as set out in the Bill do not sufficiently allow for a reporting entity’s assessment of the extent of CDD for different customers. Several submitters were also of the view that the New Zealand minimum standards are higher than the Australian minimum standards.

Comment

25. A risk-based approach is desirable because reporting entities are well placed to assess many of the risks in their specific business environments. Reporting entities have competing incentives to manage money laundering risk. While there is an incentive to maintain a positive public reputation, financial imperatives for the effective management of money laundering risk are not the same as other types of financial crime that may result in direct losses. The costs of money laundering are largely borne by the public and the State. To ensure effective management of risks, it is important to achieve a balance between discretion and minimum standards.

26. Once the business relationship has been established, the Bill provides flexibility for reporting entities to develop their own approach to the ongoing management of ML/TF risk for each customer. The Bill only requires that reporting entities have regard to the risk information they have obtained through the customer identification process.

27. The Bill sets out the minimum standards required to give reporting entities a satisfactory level of confidence in the identity of their customers. The minimum identification and verification standards are not intended to go beyond the minima set out in either the FATF Recommendations or the Australian regime. The CDD minima in the Bill are essentially the same minima as are applied under Australian law.

28. The key difference between the two regimes is that it is proposed that the New Zealand legislation sets some minimum standards in statute.

29. The rationale for this is two-fold. Firstly, it is evident that some of the more permissive discretionary frameworks, e.g. setting out minimum obligations in non-enforceable guidance material, are not FATF compliant. The reason that this is a concern to the FATF is that in a commercial environment there are competing incentives to carry out CDD. Minimum requirements therefore need to be enforceable. Secondly, prescribing the CDD information requirements assists in managing privacy impacts. Citizens are understandably protective of their personal financial information. Through prescription in statute, the public are able to know,
in a transparent way, the key personal information that they are expected to disclose for AML/CFT purposes, such as disclosing 'source of wealth' for enhanced due diligence.

30. Analysis of submissions has identified some discrete areas where the Bill could be clearer that a risk-based approach to CDD, above certain minimum, is intended. Several amendments are proposed to the Bill to clarify this. These are discussed in the body of the report.

31. Some submitters signalled a desire to use their own assessments of risk to verify identity below the proposed minimum standards. This would not be FATF compliant would also result in standards below those set out in Australian law.

Harmonisation with Australia

32. A key theme of submissions from the banking sector was harmonisation with Australia. The structure of the Australian legislation and the proposed Bill are quite different. The Australian Act sets out high level requirements; most of the prescription is contained in Rules. There is also a substantial Regulatory guide, a series of explanatory notes and leaflets to support reporting entities in their understanding of the Bill. Officials have proposed to put all key requirements into primary legislation. It is proposed to use regulations for some additional elements, codes of practice and guidance to facilitate understanding.

33. While the Bill may seem prescriptive by comparison compared to the Australian Act, officials consider the fundamental requirements of the overall regimes are fairly similar.

34. Submitters highlighted the importance of ensuring that legislative design was sufficiently similar so that the Australian banking sector’s AML/CFT programme structures and systems could be used as a platform for implementing reforms in New Zealand. Submitters have highlighted concerns about some key differences in the approach between New Zealand and Australia. The areas in which the two AML/CFT frameworks differ are:

34.1. the application of enhanced due diligence
34.2. occasional transactions
34.3. risk-based approach to beneficial owners
34.4. a legislated definition of Politically Exposed Persons (PEPs)
34.5. identity verification requirement with respect to name, date of birth and address
34.6. treatment of existing customers
34.7. timing of verification
34.8. verifying authority to act
34.9. civil and criminal penalty system and liability of senior managers.
Enhanced due diligence approach

35. The Bill does take a more prescriptive approach to enhanced due diligence. Key differences are that provisions identify prescribed circumstances or customers to which enhanced due diligence must be applied (such as PEPs and trusts). The Bill would allow reporting entities to apply a risk-based approach to the rest of their customer base. The enhanced measures include a requirement to collect information on the 'source of wealth' of those customers.

36. The Australian regime allows reporting entities to determine which customers and circumstances are high risks, and which, and how much information to collect to mitigate that risk. Australia applies non-enforceable regulatory guidance to outline expectations of customers and circumstances that should be high risk; it also sets detailed KYC information that should consider collecting in these circumstances. It specifically refers to trusts and PEPs.

37. The Bill is aligned with the FATF Recommendations on high-risk circumstances and customers. The EDD customers and circumstances prescribed are inherently high risk, both as described by the FATF and in the New Zealand context.

38. Determining the source of a customer's wealth is fundamental to the detection of money laundering. Collecting information on the 'source of wealth' is also an invasive requirement. To assist in managing privacy impacts, it is preferable for statute to set out, as far as possible, the people who will be required to disclose sensitive personal information and the amount of information to be disclosed. It is expected that reporting entities will be asking a range of other questions about their customers and this is a critical one. It is important that customers are aware that if they present a high risk, this question could be asked of them.

39. Where the Bill requires enhanced measures at the establishment of a business relationship, the reporting entity (despite a requirements to have regard to that fact), may still apply a risk-based approach to its ongoing relationship with that customer.

40. Where enhanced due diligence must be applied to an occasional transaction, the Bill currently requires reporting entities to take all reasonable steps to satisfy itself that the information collected about that customer is correct. It is proposed to remove the 'all' from the reasonable steps requirements, except for minimum standards, to better provide for a risk-based approach.

Definition of 'occasional transactions'

41. It is important to clarify that the definition of occasional transaction is intended to only capture those cash transactions that are carried out other than in a business relationship. It was initially intended to keep the definition broad and exempt specific types of transactions, but in light of the confusion that this has created, we consider it clearer to state this within the definition in the Bill. The ability to exempt certain types of transactions from the definition will be retained.
Beneficial ownership checks

42. The Australian framework does not apply beneficial ownership checks for all customers carrying out 'occasional transactions' (large cash transactions over $10,000 by a person who is not in a business relationship with the reporting entity).

43. However, in Australia, all large cash transactions are required to be reported directly to the Australian Transactions and Analysis Centre (AUSTRAC). This information is held on a central government database that can be data-mined by government agencies to detect suspicious activity. Through having a central database Australia is able to mitigate the risks of not having requirements to conduct beneficial ownership checks on occasional transactions. The New Zealand Government has not yet considered whether it should establish such a database as part of its AML/CFT measures. In the absence of such controls, it is recommended that the policy to apply beneficial ownership checks for occasional transactions is applied in New Zealand. This is FATF compliant.

44. However, we propose to clarify that reporting entities are not expected to carry out CDD again, where it has previously been carried out in accordance with the Bill.

Risk-based approach to identification of beneficial owners

45. Submitters were concerned that the Bill provides for less scope to apply a risk-based approach to identification and verification of beneficial owners. The Australian Rules require that reporting entities must always identify the beneficial owner of companies and trusts. They must apply a risk-based framework as to the degree to which the beneficial owner (and the company or trust) is verified.

46. The Bill similarly provides that beneficial owners of companies and trusts must be identified and must, according to risk, take 'all reasonable steps' taken to verification. It is proposed to remove the word 'all' from 'all reasonable steps', except for minimum standards, to clarify that a risk-based approach is able to be taken.

47. Also for standard due diligence provision should be made for the possibility of no verification in demonstrably low risk situations. We recommend this.

Definition of PEPs in statute

48. The Bill holds a definition of PEPs. It contains obligations to identify PEPs and to apply enhanced identification measures. In comparison, in Australia reporting entities must 'consider' the risk posed by different customer types, including PEPs. While not defined in the legislation, Australian regulatory guidance defines PEPs in a similar way to the Bill by referencing the FATF definition.

Identity verification difference with respect to address and date of birth

49. The Bill contains requirements to collect and verify both a customer's address and date of birth. The Australian regime requires collection of both, but verification of one or the other. The rationale for verifying date of birth is to give confidence in
identity; verification of address to assist law enforcement officers to investigate criminal activity. It is apparent that there may be some practical difficulties in certain businesses environments in verification of address (for example in casinos). The Bill provides for regulations to exempt reporting entities from the application of address verification where appropriate.

**Treatment of existing customers**

50. The Australian regime requires CDD to be carried out on existing customers only where there is suspicion of money laundering or terrorism financing. As drafted, the Bill would require CDD to be carried out on existing customers at specific times, including where there is a simple change in the nature or purpose of the business relationship.

51. The approach within the Bill is a much lower threshold for triggering due diligence on existing customers compared to Australia. It may be appropriate for New Zealand to employ a lower threshold because New Zealand has not been comprehensively regulated for a longer period. The integrity of the CDD on the existing customer base of reporting entities cannot be assumed.

52. However, it is proposed to reconsider where that threshold should be defined. We propose introducing a higher test of *materiality* to the change in the nature or purpose of the business relationship trigger and linking it with 'doubt about the adequacy and veracity of information held about the customer'. CDD would not be required unless both circumstances arise. It is proposed to delete the two remaining triggers.

**Timing of verification**

53. The FATF Recommendations provide for verification to be carried out after or during the establishment of a business relationship where there are low risks and in controlled circumstances. Clauses 14 and 22 set out the processes for verifying the identity of a customer when conducting standard due diligence and enhanced due diligence. Both clauses also provide for a process for delaying the verification. Verification of identity may be completed after the business relationship has been established or the occasional transaction conducted if it is:

53.1. essential not to interrupt normal business practice

53.2. money laundering and terrorism financing risks are effectively managed, and

53.3. verification is completed within 5 days of the business relationship being established or the occasional transaction being conducted.

54. The Australian legislation provides for a similar regime, but does not place time limits on completion of verification unless a person has begun to transact on an account.
55. We recommend that the 5 day time limit is deleted and reporting entities be required to carry out verification 'as soon as practicable'. Reporting entities will be required to manage money laundering and terrorism financing risks appropriately.

**Verifying authority to act**

56. As with the Bill, in Australia, the legislation sets out that where a person is acting on behalf of a customer, a reporting entity is required to identify the customer, the person acting, and their authority to act on behalf of the customer. Provision is made for companies who wish to have many different people operating on its account through Rules. The Rules are complex, but essentially, they allow for a company to carry out its own identity verification of the people it intends to allow to operate accounts. The approach taken in the Bill is discussed further later in this paper but we consider that it contains enough flexibility for reporting entities to operationally manage their obligation relatively easily.

**Civil and criminal penalty system**

57. The Bill makes a distinction between the civil and criminal penalties regime. The civil penalties are lower than in Australia; the criminal penalties are higher. The difference in penalty regime has no significant impact on operational systems. The FATF requires a range of effective, dissuasive, and proportionate sanctions in order that reporting entities address systemic, deliberate, or inadvertent failures of the entity's compliance framework. The Government approved the introduction of a flexible civil and criminal penalty regime that is proportionate to the nature and scale of the misconduct [CAB Min (09) 14/7 refers]. Offences and penalties are discussed further in the clause by clause analysis. The points of difference relating to the level of penalties do not appear to be a significant barrier to using overseas methodologies to implement AML/CFT obligations in New Zealand.

58. Submitters also expressed concern that senior managers will criminally liable for failures under this Bill. Under the Australian regime, the body corporate is liable in most circumstances. It is proposed to remove senior management liability for civil and criminal breaches.

**Comment**

59. Harmonisation with Australia should be balanced against compliance with FATF Recommendations and the fit with the New Zealand environment. Harmonisation with Australia is desirable in order to minimise compliance costs of the regime for reporting entities with parent or subsidiary organisations based in Australia. This will allow existing systems and compliance solutions to be transferred and used in the New Zealand context. It does not appear necessary for the two countries to have identical policies.

60. A more detailed discussion of these issues is provided in the clause by clause analysis.
Part Three: Summary of Recommendations

61. This part contains a summary of the recommendations for changes to the Bill discussed in this paper.

<table>
<thead>
<tr>
<th>Clause 4 - Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarify that obligations extend to only that part of the business that offers the types of services that qualifies the entity to be a reporting entity.</td>
</tr>
<tr>
<td>Amend the definition of financial institution to not include any person defined as a financial institution in section 3 of the Financial Transactions Reporting Act 1996.</td>
</tr>
<tr>
<td>Amend transitional provisions to also ensure that the relevant sections of the FTRA are removed to ensure that reporting entities are not accidentally exempted from the obligations under the Bill.</td>
</tr>
<tr>
<td>Amend the definition of 'occasional transaction' to clarify that an occasional transaction is a cash transaction that occurs outside of a business relationship.</td>
</tr>
<tr>
<td>Amend the definition of 'beneficial owner' to recognise that for an entity for which simplified due diligence applies under clause 16 (1), the reporting entity will not need to go further in identifying beneficial ownership.</td>
</tr>
<tr>
<td>Clarify that once CDD has been carried out in accordance with the obligations in the Bill, it doesn't have to be done again unless suspicion, or doubt about adequacy or veracity of information arises.</td>
</tr>
<tr>
<td>Amend the definition for Designated Business Group to provide for adding to eligibility to form DBGs through regulations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clause 10 – Reliance on risk assessment when establishing level of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require a reporting entity to rely on its risk assessment and AML/CFT Programme when establishing the level of risk for the purposes of subpart 1 – Customer Due Diligence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clause 11 – Basis for verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace the word 'obtained' with 'issued'.</td>
</tr>
</tbody>
</table>
**Clause 9, 12 and 20 - Customer due diligence**

Remove ‘all’ from ‘all reasonable steps’ as appropriate.

**Clause 12 – Circumstances when standard due diligence applies**

Combine 12 (e) (i) and (ii) so that conditions of materiality and risk must both be satisfied before CDD is triggered for existing customers.

Remove clauses 12 (e) (iii) and 12 (e) (iv).

**Clause 14 Standard due diligence and Clause 22 Enhanced due diligence requirements: verification of identity requirements**

We recommend that the verification requirements within the Bill should facilitate a risk based approach, with a minimum verification standard for customers provided. For standard due diligence (Clause 14(1)) we propose that the Bill require a reporting entity to:

- take ‘all reasonable steps’ to verify the information in clause 13 as is relevant for the customer type (the minimum verification standard)
- ‘according to the level of risk’, take ‘reasonable steps’ to verify the identity of any beneficial owner
- ‘according to the level of risk’, take ‘reasonable steps’ to verify the identity and authority to act for persons acting on behalf of a customer, and
- verify any other information prescribed by regulations, according to the standard provided by regulations.

For enhanced due diligence (Clause 22), we propose that the Bill require a reporting entity to:

- take ‘all reasonable steps’ to verify the minimum identity requirements set out in standard due diligence above
- ‘according to the level of risk’, take ‘reasonable steps’ to verify the identity of any beneficial owner
- ‘according to the level of risk’, take ‘reasonable steps’ to verify the identity and authority to act for persons acting on behalf of a customer
- according to the level of risk, take reasonable steps to verify information obtained about the customers source of wealth or funds (clause 21(a)) and
- any other information prescribed by regulations, according to the standard provided by regulations (21(b)).
Delete the 5 day constraint to allow verification as soon as reasonably practicable.

Remove the ability of reporting entities to delay the verification of identity when conducting occasional transaction.

<table>
<thead>
<tr>
<th>Clause 16: Simplified due diligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amend the regulation making power for simplified due diligence to provide for the inclusion of customers, products, services and transactions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clause 20 – Circumstances when enhanced customer due diligence applies and clause 22 verification requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove ‘all’ from the ‘all reasonable steps’ requirement in clause 22(1)(a).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clause 23 – Politically Exposed Persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require a reporting entity to take reasonable steps to determine whether a customer, or a beneficial owner of a customer, is a PEP.</td>
</tr>
<tr>
<td>Clarify that reporting entities are not required to gain senior management approval when conducting an occasional transaction for a PEP.</td>
</tr>
<tr>
<td>Remove the requirement to gain senior management approval when establishing a business relationship with a domestic PEP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clause 24 and 25 – Wire transfers: identity and verification requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amend clause 24 (5) to read ‘beneficiary institution must adopt effective risk-based procedures for handling wire transfers that are not accompanied by complete originator information, including whether they constitute a suspicious transaction.</td>
</tr>
<tr>
<td>Amend clause 24 (6) to require intermediary institutions in the payment chain for both cross border and domestic wire transfers to maintain the originator information that it received from the previous institution, with the accompanying wire transfer. Delete the reference to information required by subsection (1).</td>
</tr>
</tbody>
</table>
Clause 27 – New or developing technologies and products that might favour anonymity

Amend the Bill to de-couple clause 27 from the enhanced due diligence requirements by removing reference to clauses 21 and 22.

Insert reference to standard due diligence clauses 13 and 14 instead.

Remove cross reference to new or developing technologies from clause 20 in the enhanced due diligence section.

Clause 29 – Reliance on a member of a designated business group

Amend to clarify that despite clause 30(1), it is the reporting entity, and not the DBG member being relied on, responsible for ensuring that it is complying with the obligations in the Bill.

Empower the AML/CFT supervisor, which has responsibility for the DBG members, to require a member to develop its own AML/CFT programme or risk assessment where the AML/CFT supervisor considers the AML/CFT programme or risk assessment of the DBG is not appropriate for the reporting entity that is using it.

Clause 30 - Reliance on another reporting entity

Amend to clarify that a reporting entity can rely on customer due diligence only in the circumstances set out in clauses 29, 30 and 31.

Clause 32 – Prohibitions if customer due diligence not conducted

Amend to provide appropriate protections reporting entities.

Clauses 37, 40 and 139 – Suspicious transaction reports

Amend clauses 37, 40 and 139 to require reporting entities to submit suspicious transaction reports when they have reasonable grounds to suspect that a transaction is, or may be, relevant to the investigation or prosecution of a serious offence (within the meaning of 243(1) of the Crimes Act 1961).
**Clause 43 – Disclosure of Information relating to suspicious transaction reports**

Amend the Bill to provide for information sharing among members of a DBG to the extent that it is strictly necessary during the process of submitting the STR.

**Clause 46 – Record keeping**

Amend clause 46 to ensure that record keeping obligations only apply to business relationships and transactions above the applicable threshold value.

Amend to provide for a court to be able to order a reporting entity to retain records despite liquidation or dissolution.

Amend to provide that reporting entities should take 'all practicable steps' to ensure the destruction of electronic records.

**Clause 54 – Minimum requirements for AML/CFT programmes**

Amend to require reporting entities to keep records of final versions of risk assessments, audits, and AML/CFT programmes for 5 years and that these should be made available to supervisors on request.

**Clause 54: Minimum requirements for AML/CFT programmes, Clause 55: Risk assessment, Clause 64: Legal effect of Codes of Practice**

Add to clause 54 the words 'the AML/CFT programme must be informed by the risk assessment taken in accordance with Clause 55'.

Amend clause 10 to include reference to the 'AML/CFT programme and risk assessment undertaken in accordance with relevant parts of clauses 54 and 55'.

**Clause 56 – Review and audit of risk assessments and AML/CFT programme**

State that a reporting entity must provide a copy of any audit conducted under clause 56 when requested by the relevant AML/CFT supervisor.
### Clause 56 – Review and audit of risk assessment and AML/CFT Programme; clause 57 – Annual AML/CFT report

Amend clause 56(1) to require reporting entities to review (delete 'conduct a review of') its risk assessment and AML/CFT Programme.

Amend section 57 (2)(b) to delete 'of the review required by section 56(1).

Provide for supervisors to request, on notice, a reporting entity’s annual AML/CFT report.

### Clause 58 – Branches and subsidiaries in other countries

Amend to require reporting entities to ensure that all branches and subsidiaries apply ‘broadly equivalent’ measures to New Zealand.

### Clause 73, 74 and 75 – Criminal and civil penalties

Delete clause 73, clause 74 and clause 75 of the Bill.

### Clause 89 – Offence and Penalties for civil liability act

Delete the defence provisions within clause 89(2).

### Clauses 93-95 – Strict liability offences

Clarify that offences in clauses 93 and 94 are strict liability offences by removing 'without lawful justification or excuse'.

### Clause 96 – Defence

Widen the defence within clause 96 to all criminal offences in Part 2 of the Bill.

No change is recommended to the defence or penalties in relation to civil liability acts.
### Clause 127 – AML/CFT supervisors

State that a reporting entity can have only one AML/CFT supervisor.

Amend clause 127 to allow reporting entities to apply to change supervisors for the purpose of electing to join a DBG.

### Clause 147 – Regulation making powers

Remove the regulation making powers in clauses:
- 23(b) and 147(j) for additional requirements relating to PEPs.
- 54(n) and 54(o) and 147(a)(vi) for additional requirements in AML/CFT Programmes.
- 147(n) for prescribing offences and fines.

### Clause 148, 151, 152 and 153 – Exemptions provisions

Relocate regulation making powers set out in clause 147(b), (g) and (i) into clause 148 to ensure they are subject to the same controls as other exemptions regulations.

Amend to make the Ministerial exemptions, as provided for in clauses 151-153, subject to the Regulations (Disallowance) Act 1989.

### Overview clause

Amend to include an overview clause.

### Defence against civil and criminal action

Provide reporting entities with a defence against civil or criminal proceedings where the civil or criminal breach resulted from a reporting entity operating, as a reasonable person, in good faith with the provisions of the Bill.

### Freezing transactions or accounts

No change.
Defence against civil and criminal action for AML/CFT supervisors

Provide appropriate protection from liability for AML/CFT supervisors (and any authorised delegate) when acting in the course of their duties in the Bill.

Search provisions for Customs officers

Amend the Bill to enable Customs officers to effectively carry out their duties in relation to cross border movement of cash.

Amend to insert a complementary provision to establish a duty on persons with knowledge of a computer, computer network, or other storage device to assist with access if required.

Outsourcing of supervisory powers

Amend to allow supervisors to use a 'suitably qualified' third party to:

- require information from a reporting entity, with notice.
- carry out inspections of reporting entities for compliance with the legislation with or without notice.
- assist in investigations.

These delegations should be subject to the following safeguards and conditions:

- any decisions arising from outsourced activities rest with the supervisor.
- any conflicts of interest to be declared and managed.
- all delegations should be made in writing, by the Chief Executive of the supervisory agency.
- proof of identity and authorisation must be provided when carrying out delegated functions.

Prohibit the use and disclosure, of any information collected on delegated authority, except to the supervising agency. The Bill should establish associated offences and penalties for tipping off and other unlawful disclosure by persons with delegated authority.
Part Four: Clause-by-clause analysis

62. Submitters provided substantial comments on the Bill. This section sets out the submitter’s comments and our analysis, including recommendations for amendments clause by clause in numerical order.

Clause 2 – Commencement

63. Clause 2 is the commencement clause. It provides for the Bill, and different provisions within the Bill, to be brought into force by Order in Council.

Submissions

64. Views on the commencement date for the reforms varied significantly. The New Zealand Bankers’ Association (NZBA) indicated that two years after the regulations framework is completed would be manageable, although individual submissions from the banking sector ranged from 18 months to four years after the regulations framework is completed. Key planning issues for implementation were the significant changes in policies, procedures and systems requirements that are needed to implement the reform.

65. Most submitters expressed a preference for bringing in all obligations on a single commencement date, noting that phased implementation, in which different provision might be staggered, would increase uncertainty.

66. One submitter considered that the commencement date for should be in the Bill, and not according to Order in Council.

Comment

67. Based on feedback from previous submissions during the development of AML/CFT reforms, the explanatory note of the Bill signals a 2-year implementation time frame.

68. The Bill provides for implementation through Order in Council. While, for certainty, it is desirable for the Bill to state clearly the commencement dates for obligations, it is preferable to retain flexibility in this case. The regulations framework needs to be finalised, and industry has signalled that there are interdependencies between the timing of the development of regulations and their ability to prepare for implementation. Suggestions will be considered and an implementation date will be proposed to Government once there is certainty about the scope and timing of regulations.

Commencement for obligations for government agencies and cash reporting

69. There are some provisions of the Bill than will need to be brought into effect on enactment to assist reporting entities and smooth implementation. The early commencement of these provisions will not result in an increase in compliance
costs to reporting entities. It will assist reporting entities in their preparations for compliance with AML/CFT Bill when it comes into full force.

**Regulation and exemption making powers**

70. Regulations and exemptions will need to be developed and promulgated well in advance of AML/CFT obligations coming into force to give reporting entities plenty of time to adequately prepare. Consultation on regulations is intended to commence as soon as practicable following enactment. It is therefore proposed that the regulation-making and exemption provisions commence as soon as the AML/CFT Bill is enacted.

**Cross border transportation of cash**

71. It is appropriate that the cross border cash reporting requirements in the Bill come into effect earlier than the obligations for reporting entities, as the changes to Customs’ current regime is minor. There are prescribed forms that need to be in place prior to implementation of these provisions, so immediate commencement is not feasible. We propose the provisions relating to cross border transportation of cash come into force 12 months after enactment.

**Financial intelligence functions and powers**

72. To ensure smooth implementation, it is proposed to allow immediate commencement of provisions which relate to the Financial Intelligence functions of the Police Commissioner. In particular, the Financial Intelligence Unit will need to be able to produce, consult, make available and review guidance material, typologies of money laundering and financing of terrorism transactions, and produce information for reporting entities on how to meet their obligations relating to STRs.

73. The power to produce, consult and review guidelines is particularly important to bring into force upon enactment, as reporting entities will need guidance as early as possible if they are to analyse risks and develop their responses for when their obligations commence.

**AML/CFT supervisors' powers and functions**

74. For successful implementation it will also be necessary to bring some of the powers and functions of supervisors into force early. It is proposed that the following provisions, which relate to the powers and functions of supervisors, commence upon enactment.

74.1. The power to:

- 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
- produce guidelines
- prepare Codes of Practice
- provide feedback on reporting entities' compliance with obligations under this Act and the regulations
- undertake any other activities necessary for assisting reporting entities to understand their obligations under this Act and the regulations, including how best to achieve compliance with those obligations
- co-operate and share information 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
- in accordance with this Act and any other enactment, initiate and act on requests from any overseas counterparts
- approve the formation of, and addition of members to, designated business groups.

74.2. Powers to use and disclose information obtained as an AML/CFT supervisor in other capacity and vice versa, and related restrictions on these powers.

74.3. Powers to use and disclose information supplied or obtained under other enactments for AML/CFT purposes.

74.4. Provisions that allow the appointment of enforcement officers, require the issuing of an identity card, require an enforcement officer to carry an identity card while acting as an enforcement officer, and requiring the return of the identity card upon ceasing to be an officer.

**AML/CFT coordination committee**

75. The AML/CFT Coordination Committee should be brought into effect upon enactment as the AML/CFT Coordination Committee will manage the Bill's implementation, and the promulgation of regulations and Codes of Practice.

### Recommendation

Provide for commencement dates through Order in Council with the following exceptions:

- Provisions that relate to the Financial Intelligence functions of the Commissioner to come into force upon enactment.
- Provisions that relate to the definition, functions and powers of AML/CFT supervisors to come into force upon enactment.
- Provisions that relate to the establishment and operation of the AML/CFT Coordination Committee to come into force upon enactment.
- Provisions that activate regulation and exemption making powers to come into force upon enactment.
Clause 4 – Interpretation

Definition for establishing scope of coverage of financial institutions

76. The definition of ‘financial institution’ is set out in the Bill as described in the FATF Recommendations. The definition is broadly activity-based and is inclusive of all types of financial activity which has been identified by the FATF as being at risk of money laundering.

Submissions

77. A small number of submitters suggested establishing coverage of entities under the AML/CFT regime using the same approach as in Australia. Australia establishes coverage through the inclusion of ‘designated services’.

Comment

78. The purpose of a broad, inclusive definition is to capture all parts of the financial sector that may be used for money laundering and terrorism financing. The key difference between the two regimes is that the Bill provides for exclusion-based management of coverage, and the Australian legislation provides for inclusion-based coverage. Both approaches require detailed consideration of either exclusion or inclusion. The New Zealand definition provides coverage by reference to type of reporting entity. Exclusion is through regulatory exemption. This is preferable as it will ensure a more comprehensive coverage and greater responsiveness to changing risks.

Recommendation

No change

Inadvertent capture of part of business that are not related to financial services

79. The Bill defines a reporting entity as a ‘financial institution’ or a ‘casino’ or another person that is required by enactment to comply with this Act as if it were a reporting entity.

Submissions

80. Several submitters identified that the current drafting of the definition of ‘reporting entity’ would impose AML/CFT obligations on their non-financial sector-related aspects of their business.
Comment

81. The Bill as presently drafted would require a reporting entity to extend AML/CFT obligations to all parts of a reporting entity's business, even where it may have no financial component. This is because the obligations are directed at the 'reporting entity' which is defined as a person who offers certain services. This is not the intention of the Bill.

Recommendation

Clarify that obligations extend to only that part of the business that offers the types of services that qualifies the entity to be a reporting entity.

Inclusion of life insurance in the definition of ‘financial institution’

82. Life insurance is included in the definition of ‘financial institution’ through the wording 'underwriting or placement of life insurance or other investment related insurance'.

Submissions

83. The majority of the concerns of the insurance sector related to the unintended capture of risk-based insurance products, rather than investment-related insurance products and those with a 'surrender value', the latter of which entails money laundering risks.

Comment

84. Pure risk-based products, including re-insurance, accidental death and incidental life insurance, and consumer credit insurance are zero to low money laundering risk. Generally, insurance products with a surrender value are those that could be used for money laundering.

85. Consideration was given to excluding insurance products with no surrender value in the statutory definition of ‘financial institution’. We note that the Securities Act 1978 describes life insurance products with a surrender value. The definition under that Act is held in regulations. For consistency, it is preferable that any definition of life insurance for AML/CFT purposes is similarly held in regulation.

86. We recommend ensuring that pure risk-based life insurance products with no surrender value are exempted from the operation of the legislation by regulation.

Recommendation

No change.
**Potential inclusion of ‘consumer credit’ in the definition of ‘financial institution’**

87. The definition of ‘financial institution’ includes ‘lending to or for a customer, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions (including forfeiting)’.

**Submissions**

88. One submitter considered that the inclusion of consumer credit in the definition of ‘financial institution’ was not appropriate particularly for high volume, low value retail products.

**Comment**

89. Consumer credit is covered by the FATF Recommendations. In New Zealand, it is intended that consideration is given to the inclusion of non-financial institutions which provide consumer credit, including the retail sector, during the second phase of reform. Financial institutions that provide consumer credit as their core business are covered in the first phase. Exemption to coverage by regulation could address this issue.

**Recommendation**

No change.

---

**Inclusion of securities registries in the definition of ‘financial Institution’**

90. The definition of ‘financial institution’ is inclusive of share registries.

**Submissions**

91. Securities sector submitters considered that securities registries should be excluded from the definition of ‘financial institution’ on the basis that they are involved primarily in the transfer of ownership and the information received by registries will not be sufficient to comply with the CDD requirements.

**Comment**

92. Exclusions from the definition of ‘financial institution’ are a matter for regulations.

**Recommendation**

No change.
Generality in the definition of 'financial institution'

93. The definition of 'financial institution' uses general language to describe the types of financial activity that are to be covered.

Submissions

94. A small number of submitters noted that language such as 'forfeiting, other repayable funds' and inconsistency in the use of the words 'lending' and credit' may lead to uncertainty as to intent.

Comment

95. Unintended coverage should be left to regulations. Further clarity about coverage can be provided in guidance.

**Recommendation**

No change.

Coverage of second phase entities in the definition of 'financial institution'

96. At present, the consequential amendment within the transitional arrangements removes first phase financial institutions and casinos from the operation of the FTRA. However, entities intended to be covered during the second phase of AML/CFT reform are still subject to the application of the Bill. This is not intended. It is recommended that the definition of financial institution is amended to ensure that second phase entities are not captured.

**Recommendation**

Amend the definition of financial institution to not include any person defined as a financial institution in section 3 of the Financial Transactions Reporting Act 1996.

Amend transitional provisions to also ensure that the relevant sections of the FTRA are removed to ensure that reporting entities are not accidentally exempted from the obligations under the Bill.

Interplay between 'applicable threshold value', 'business relationship', 'occasional transaction' and 'wire transfer'

97. The definition of 'applicable threshold value' is a value that is to be set in regulations. It applies to 'occasional transactions' below which CDD obligations are not required.
Submissions

98. In the casino industry few customers have business relationships. The casino industry submitted that coverage should only extend to those in business relationships and not those who are casual.

99. Many submitters put forward proposals for a level of applicable threshold value that would apply to occasional transactions and wire transfers.

100. There were calls from the banking sector to raise the applicable threshold value for occasional transactions from the current rate of $10,000 to between $15,000 and $32,000.

101. The casino industry submitted that the applicable threshold for occasional transactions should be $10,000 in line with Australia.

102. Remittance agencies submitted that there should be a minimum threshold of $1,000 for wire transfers, with reduced CDD verification measures applying for monetary amounts between $1,000 and $10,000 and that full CDD should only apply above $10,000.

Comment

103. The definition of 'occasional transaction' carries with it an applicable threshold value. Under the FTRA the threshold is currently NZ$10,000. A threshold for occasional transactions for casinos is yet to be set. Similarly, there is no value set for wire transfers, although it should be noted that the FATF recommends a wire transfer threshold of USD/EUR1,000.

104. With respect to the casino sector, the money laundering risks in the casino environment are high. It is appropriate for casual casino customers who make large cash transactions to be required to undergo CDD. The applicable threshold value for casino customers will be consulted on and determined through regulations.

Recommendation:

No change.

Definition of ‘customer’ in relation to junket organisers

105. The definition of ‘customer’ includes a ‘junket organiser’ as defined in section 4(1) of the Gambling Act 2003.

Submissions

106. The casino industry considered that it was not appropriate to include a ‘junket organiser’ in the definition of ‘customer’.

30
Comment

107. There is a business relationship between a casino and a junket organiser, rather than between the casino and the junket participants. In this situation, the customer is the junket organiser and we would expect full CDD on the junket organiser to be carried out in accordance with the Bill.

108. The junket players are the beneficial owners of the junket organiser as they exercise control over the customer (organiser). They will also need to be identified in accordance with the Act.

109. Junket organisers are independent operators (paid by junket participants) who approach Casinos with a business proposal. Junket organisers also control the coordination of the junket funds. Winnings are paid into a junket account and disbursed back to junket participants by the junket organiser. It is appropriate that they are subject to adequate CDD measures.

Recommendation

No change.

Definition of ‘occasional transaction’

110. The definition of “occasional transaction” is a transaction over an applicable threshold value (whether the transaction is carried out in a single operation or several operations that appear to be linked). It is intended to capture ‘one-off’ transactions by customers who do not have a ‘business relationship’ with a reporting entity. A ‘business relationship’ is expected to have an element of duration.

Submissions

111. Some submitters noted that it would be useful to clarify that an ‘occasional transaction’ is a transaction that is conducted outside a business relationship. Another submitter expressed concern that the ‘aggregation’ of transactions might be captured by the inclusion of ‘operations that appear to be linked’.

Comment

112. Clarifying that the definitions of ‘occasional transaction’ and ‘business relationship’ are mutually exclusive would ensure that reporting entities are not required to conduct CDD on their own customers if they present with large cash transactions. If CDD was done when the business relationship was established, then there is no need for CDD to be re-conducted for further transactions (unless suspicion, doubt about adequacy or veracity of information or other circumstances provided for in clause 12(e) arise).
113. As discussed earlier in this paper, it is intended to clarify that the definition of occasional transaction is only intended to capture cash transactions that are carried out other than in a business relationship. It was initially intended to keep the definition broad and exempt specific types of transactions, but in light of the confusion that this has created, we consider it would be clearer to state this within the definition in the Bill. The ability to exempt certain types of transactions from the definition will be retained.

114. It is considered that 'aggregation' of transactions would be captured by the inclusion of 'operations that appear to be linked'. However it is not considered that this is materially different from the reference to 'structuring' of transactions in the FTRA, although it is acknowledged the obligations this type of transaction triggers are different. Operations that appear to be linked are specifically referred to for inclusion by FATF Recommendations. If appropriate there is ability to exempt types of transactions from the definition. Alternatively a Code of Practice or guidance material could clarify this issue.

**Recommendation**

Amend the definition of 'occasional transaction' to clarify that an occasional transaction is a cash transaction that occurs outside of a business relationship.

Clarity that once CDD has been carried out in accordance with the obligations in the Bill, it doesn't have be done again unless the circumstances in clause 12(e) arise.

**Definition of 'beneficial owner'**

115. A beneficial owner means an individual who:

115.1. has effective control of a customer or person on whose behalf a transaction is conducted; or

115.2. owns a prescribed threshold of the customer or person on whose behalf the transaction is conducted.

116. The Bill provides that CDD must be carried out on a customer, a beneficial owner of a customer, or any person acting on behalf of a customer. Beneficial ownership must identify and take 'reasonable steps' to verify the beneficial owner. Beneficial owners must be identified when conducting occasional transactions and when establishing a business relationship.

**Submissions**

117. One submitter considered that the definition of beneficial owner should be amended to accommodate beneficial owners who are not individuals, for example when the beneficial owner of a customer is a publicly listed company or government department.
118. Some submitters noted that there is no threshold for determining the degree to which a beneficial owner exhibits 'effective control' of a customer.

119. Some submitters were concerned about the determination of effective control and thresholds for certain types of products and trusts such as discretionary trusts and pooled accounts.

Comment

120. A beneficial owner will ultimately be an individual or individuals. Every corporate structure has a natural person or persons that will ultimately own or effectively control the structure. If beneficial ownership consists of more than one or multiple individuals than it is expected that a reporting entity will identify all individuals.

121. The Bill provides for simplified CDD in certain cases. For example, where the beneficial ownership is transparent because the customer is a publicly listed company. FATF envisages that beneficial owners will ultimately be a natural person. An exception to this is where a beneficial owner is identified that is an entity to which simplified due diligence may be applied. In these circumstances it is not expected that reporting entities delve further into beneficial ownership as the information is likely to be publicly available. This could be more explicit in the Bill.

122. The threshold for determining beneficial ownership will be set in regulations. There is a recognised need to provide Codes of Practice and guidance material about different products and trusts.

**Recommendation**

Amend the definition of ‘beneficial owner’ to recognise that for an entity for which simplified due diligence applies under clause 16 (1), the reporting entity will not need to go further in identifying beneficial ownership.

**Definition of Designated Business Group**

123. Clause 4 contains a definition for a designated business group (DBG). A DBG is an arrangement that allows certain, related, groups of reporting entities to join their resources together and share some aspects of their AML/CFT programme and their CDD obligations.

**Submissions**

124. Two submitters, from the money remittance industry, highlighted that the definition of DBG does not include agents and sub-agent relationships if not a State Owned Enterprise (SOE). These submitters contended that, therefore, the definition of DGB creates a market disadvantage to those money remitters that are not in an agent and sub-agent relationship with an SOE.
125. The submitters recommended that the definition for DBG be expanded to include any group where two or more persons have elected to be a part of the group. The submitters specifically requested that principal and network agents should be able to join together in a DBG.

Comment

126. The FATF Recommendations do not explicitly envisage that groups of entities will perform some or all of the AML/CFT obligations on behalf of each other.

127. The DBG arrangements are constructed in line with the Australian AML/CFT legislation. Reflecting DBG arrangements in the Bill is a key aspect of cross-Tasman AML/CFT harmonisation. As in Australia, eligibility to form DBGs is based on the relationships between entities. At present, the Bill permits related companies under the Companies Act, State Owned Enterprises and their franchisees. There is reasonable incentive for related companies, joint ventures, and SOEs and their franchisees to ensure that each member carries out its AML/CFT obligations well because there is either a financial or significant reputational dependency between the parties.

128. A cautious approach is taken to determining the eligibility to form DBGs because the NZ definition, with the exception of SOEs and their franchisees, is identical to that of the Australian legislation. This is especially important given that the FATF have not assessed the compliance of the Australian DBG model.

129. Government has agreed to amend the definition of a DBG to allow other businesses relationships to be allowed to apply for membership in a DBG through regulations. DBGs of the nature suggested by the submitters would be best addressed through this regulation making power within the DBG clause.

Recommendation:

Amend the definition for Designated Business Group to provide for adding to eligibility to form DBGs through regulations.

Definition of a Politically Exposed Person

130. Clause 4 contains the definition of a politically exposed person (PEP). A PEP is an individual who holds in New Zealand the prominent public function of:

130.1. Prime Minister; or
130.2. Minister of the Crown; or
130.3. Judge of the Supreme Court; or
130.4. Governor of the Reserve Bank of New Zealand; or
130.5. Ambassador or High Commissioner; or
130.6. Chief of Defence Force; or
130.7. Board Chair, Chief Executive, or Chief Financial Officer of any State owned enterprise as defined by the State Owned Enterprises Act 1986.

131. As well, a PEP may be an individual who in any other country holds the prominent public function of:

131.1. Head of State or head of a country or government;
131.2. government minister or equivalent senior politician
131.3. Supreme Court Judge or equivalent senior Judge;
131.4. governor of a central bank or any other position that has comparable influence to the Governor of the Reserve Bank of New Zealand; or
131.5. senior foreign representative, Ambassador, or
131.6. High Commissioner; or
131.7. high ranking member of the armed forces; or Board Chair, Chief Executive, or Chief Financial Officer of, or any other position that has comparable influence in, any State enterprise; and

131.7.1. an immediate family member of a person referred to in above including
131.7.2. a spouse; or
131.7.3. a partner, being a person who is considered by the relevant national law as equivalent to a spouse; or
131.7.4. a child and the child's spouse or partner; or
131.7.5. a parent; and
131.7.6. having regard to information that is public or readily available any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close relationship, with a PEP or any individual who has sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of a PEP.

Submissions

132. Three submitters, none of whom are financial institutions or casinos, stated that the definition of a PEP is too narrow and should be expanded. One submitter recommend that the definition be broadened to include:

132.1. all Members of Parliament
132.2. CEO and CFO of government departments, Crown Entities, State Owned Enterprises, Crown Research Institutes and statutory entities
132.3. all judges
132.4. all elected local government representatives and the CEOs and Chief Financial Officers of all local government bodies.
133. Another submitter recommended that, at the least, the definition should include the:

133.1. Commissioner of Police
133.2. Head of the Organised and Financial Crime Agency of New Zealand
133.3. Director of Serious Fraud Office
133.4. Comptroller of Customs
133.5. the Chief Executive of Inland Revenue
133.6. CEOs of all government departments.

134. Three submissions, all of which were from industry representatives, considered the definition too broad. These submitters stated that they were concerned about how reporting entities were expected to identify 'secondary PEPs' (family and close business associates of a PEP). These submitters considered that this would be very difficult if they did not have a business relationship with the primary PEP. One of these submitters recommended that the definition goes beyond the FATF Recommendations and should be narrowed to exclude “de facto partners”.

Comment

135. The PEP definition within the Bill is an attempt to adequately meet the requirements of the United Nations Convention Against Corruption and is in line with other international definitions of PEPs, including the FATF definition. The FATF definition of PEPs is:

"individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves."

136. The definition of a PEP within the Bill represents, in the New Zealand context, those positions that could, if corrupted, represent the greatest harm to New Zealand's economy and interests. The list is in no way a reflection of the individuals within these roles, it merely represents the systemic risks associated with these public positions.

137. Any additions to this list would need to be justified against New Zealand's internationally recognised low level of corruption. The definition of PEP adequately reflects risks in New Zealand, and is sufficiently contained so that reporting entities will be able to manage the identification of these individuals.

Recommendation:

No change.
Publicly available information about PEPs

Submissions

138. Some submitters suggested that the requirement for reporting entities to be able to rely on publicly available information about PEPs would be difficult given that there was likely to be no publicly available information about some PEPs.

139. Many submitters suggested that Government maintain an accessible database of domestic PEPs. This issue is dealt with the Part Four of this report.

Comment

140. The FATF definition specifically refers to the risks associated with close family members and business associates. The reliance on publicly available information relates specifically to close business associates of PEPs. One possible avenue to discover publicly available information of this type is the Companies Register.

141. For family members of PEPs, the expectation is that reporting entities will ask questions to identify these individuals.

Recommendation:

No change.

Clause 10 – Reliance on risk assessment when establishing level of risk

142. Clause 10 requires a reporting entity to rely on its risk assessment to determine the level of risk that attracts CDD provisions.

Submissions

143. One submitter felt this provision should be amended to clarify that when establishing the level of risk involved, a reporting entity must also take into account its AML/CFT Programme, and have reasonable belief as to the level of risk associated with that customer.

Comment

144. We agree that this provision should include a reference to the AML/CFT Programme.

145. With respect to the level of risk associated with the customer, we consider that this is already provided for through the obligation to conduct a risk assessment under clause 55. This is a matter for guidance.

146. The ‘according to the level of risk’ qualification that appears in clause 10 (and elsewhere in the Bill) is intended to capture both a situational risk at the front line
and risk as set out in a reporting entity's AML/CFT Programme and risk assessment.

**Recommendation**

We recommend that the Bill is amended to require a reporting entity to rely on its risk assessment and AML/CFT Programme when establishing the 'level of risk' for the purposes of subpart 1 – Customer Due Diligence.

**Clause 11 – Basis for verifying identity**

*Issuance of reliable and independent information*

147. Clause 11 provides that verification must be done on the basis of documents, data, or information obtained from a reliable and independent source.

**Submissions**

148. Several submitters have suggested that the term 'obtained' in clause 11 may be interpreted as meaning that the reliable and independent source must necessarily be the customer.

**Comment**

149. This clause is intended to require entities to ensure that information is collected from a variety of sources and authorities independent of the customer of beneficial owner. The wording should reflect this.

**Recommendation**

Replace the word 'obtained' with 'issued'.

*Exceptions for where there is no reliable and independent information*

150. Clause 11 provides that verification must be done on the basis of information obtained from a reliable and independent source.

**Submissions**

151. One submitter noted that there may be situations in which there is no reliable or independent source for verifying customer and beneficial owner information.
Comment

152. For extreme genuine situations (such as a person of no fixed abode and/or in situations where there is a lack of identifying documents) exemptions regulations are provided for in the Bill. FATF is explicit that the test for verification must be a reliable and independent source. The interpretation of this test is broad enough to account for a variety of approaches to verification, and further clarity will be provided in regulations. If identity is unable to be verified reliably and independently the reporting entity should not be engaging in business or transacting with that customer. The fundamental intention of CDD is that reporting entities know their customers are who they purport to be.

Recommendation

No change.

Clause 9, 12 and 20 - Customer due diligence

Beneficial ownership checks

153. The Bill provides that CDD must be carried out on a customer, a beneficial owner of a customer, or any person acting on behalf of a customer. Reporting entities must identify and take ‘all reasonable steps’ to verify the beneficial owner. Beneficial owners must be identified when conducting occasional transactions and when establishing a business relationship.

Submissions

154. Several submitters were concerned about the potential for situations in which the beneficial ownership measures would be onerous, including those in which complex company and trust structures could make it difficult to identify a beneficial owner.

155. The general flavour of submission was that the obligation to take reasonable steps to verify the beneficial owner’s identity is not necessarily commensurate with the risk. Doing beneficial ownership checks in all instances is excessive and would be disproportionate to the risk. Some submitters suggested that beneficial ownership checks should not be subject to minimum requirements and that a lesser standard should be applied at the discretion of the reporting entity through their AML/CFT programmes. A proposal for a discretionary framework would include that beneficial ownership should only be required where:

155.1. the customer is an overseas entity
155.2. customer operates in a “high risk area” (as defined in regulations)
155.3. customer is a corporate entity
155.4. reporting entity has suspicion of ML or TF
155.5. customer undertakes a suspicious transaction.

156. Another suggestion was to provide for high risk circumstances in AML/CFT programmes.

157. One submitter commented that the cost of complying with beneficial ownership requirements would involve upgrading systems and redesigning of application forms.

158. One submitter considered that beneficial ownership checks should not be required when conducting occasional transactions.

Comment

159. It is acknowledged that identifying and verifying beneficial owners is one of the most challenging aspects of an AML/CFT regime. The lack of obligation on reporting entities to establish and verify the identity of beneficial owners is a key gap in the New Zealand AML/CFT regime. The high level of anonymity with which the current regime allows is a money laundering and terrorism financing risk. It is important to conduct beneficial ownership checks when both establishing a business relationship and when conducting an occasional transaction.

160. Once “all” is removed, the obligation to take reasonable steps to verify a beneficial owner’s identity is able to be done on a risk basis. The implication here is that even if the risk is very low, some effort should be made – the extent of that effort will be more or less reasonable based on the risk.

161. While the suggestion about a discretionary framework is not a bad one, it assumes that reporting entities will know in advance what situations and scenarios are likely to constitute higher risk. It will not always be that clear cut. Risk can arise based on a combination of factors that culminate in a specific situation. The submitter’s suggestion will not obligate reporting entities to consider taking reasonable steps unless the situation is one identified in the AML programme.

Recommendation

Amend to remove ‘all’ from ‘all reasonable steps’ where appropriate.

Electronic verification

162. The Bill currently provides for verification of identity to be done on the basis of documents, data or information obtained from a reliable and independent source.

Submissions

163. Several submitters wanted to ensure that the Bill provided for electronic verification of identity.
164. One submitter wanted a provision that state verifying identity information for AML/CFT purposes is a law enforcement function, so that reporting entities could be provided access to government registers – with proper restrictions on the use of this information.

165. Three submitters wanted transactional history, credit information or other social footprint information to be included as an alternative to date of birth. Submitters wanted amendments to the credit reporting codes (in the Privacy Act) should be amended to allow for electronic verification.

166. One submitter suggested that Bill should explicitly allow for the Electoral Roll to be accessed for the purpose of verifying CDD information.

167. Five submitters wanted an express provision in the Bill to allow for the use of public agency register information and electronic verification tools (like the IVS) to facilitate electronic verification.

Comment

168. The Bill does provide for electronic verification of identity information. Clause 11 explicitly states that verification can be done on the basis of data or information as well as documents. This would permit electronic verification as long as the source was reliable and independent.

169. Subclause (b) provides for further requirements relating to the basis for verification to be set out in regulations. Regulations are the appropriate place to consider the appropriateness of credit reporting information, transaction history, social footprint, and electoral roll information as a basis for verification. It is important to note however, that a customer's date of birth is a fundamental aspect of establishing that an identity is unique. Regardless of the basis of the verification, the minimum information collection requirements set out in the customer identification sections of the Bill must still be met.

170. Amendments to other Acts to enable information matching and other verification techniques are outside the scope of this Bill.

Recommendation

No change.

Clarification of types of documents sufficient for verifying CDD on existing customers

171. Clause 11 provides that verification must be done on the basis of documents, data, or information obtained from a reliable and independent source.

Submissions
172. Some submitters called for further clarity on the types of documents that could be used to satisfy the standard due diligence requirements with respect to existing customers.

Comment

173. It is expected that at a minimum, reporting entities would ensure that they had enough information about a customer to accurately identify that customer. This is the intent of the FATF Recommendations. The CDD identity minimum information requirements are set out in the Bill.

174. The basis for verification, such as the types of documents or electronic verification that are appropriate for establishing identity would be best described in regulations.

175. Assuming the amendments indicated to clause 12 (e) (above) it is important to note these measures would only apply to existing customers when there is a material change in the nature or purpose of the business relationship and doubt arises as to the adequacy or veracity of the data documents or information previously obtained for the purposes of identification or verification.

Recommendation

No change.

Clause 12: Circumstances when standard due diligence applies

Triggers for updating existing customer CDD

176. The AML/CFT Bill’s CDD provisions for existing customers (clause 12(e)) states that reporting entities must conduct CDD on an existing customer if, in relation to an existing customer:

176.1. there has been a change in the nature or purpose of the business relationship (12(e)(i)); or

176.2. doubt arises as to the adequacy or veracity of documents, data, or information previously obtained for the purposes of identification or verification of the customer, the beneficial owner, or the person who is acting, or who has acted, on behalf of the customer (12(e)(ii)); or

176.3. the reporting entity suspects that a transaction the customer is seeking to conduct may involve money laundering or the financing of terrorism (12(e)(iii)); or

176.4. the reporting entity considers that, according to the level of risk involved, it has insufficient information about the customer (12(e)(iv)); or

176.5. in any other circumstances provided for in regulation (12(f)).
Submissions

177. There was significant concern from the banking sector about the feasibility of updating existing customer CDD as set out in the Bill. The key concern is the low threshold for triggering CDD as set out in the 'change in the nature or purpose of the business relationship' provision. A second concern is the obligation to update CDD information if there is, according to the level of risk, insufficient information. For reporting entities, this potentially would require updating all customers who have beneficial owners. Some submitters signalled a preference for a greater reliance on reporting entities' perceptions of risk for their pool of existing customers.

Comment

178. The FATF expects that existing customers are moved across onto enhanced regimes on the basis of materiality and risk. Presently there is some ambiguity with clause 12(e). In particular it is not clear what a "change in the nature or purpose of the business relationship" means. The test for triggering CDD on existing customers may be too low.

179. Other jurisdictions appear to have interpreted the FATF Recommendations to mean that the threshold should meet tests of both materiality and risk, rather than materiality or risk as is currently outlined in the Bill.

180. In addition, the requirements to update CDD based on whether there is sufficient information is arguably already expressed in provision 12(e)(ii) which requires updated CDD 'where doubt arises as to the adequacy or veracity of CDD information. The trigger for CDD when suspicion arises is also covered elsewhere in the Bill.

181. It is not intended that these provisions go further than is required to meet FATF standards. We propose introducing a test of materiality to the change in the nature or purpose of the business relationship trigger and linking it with doubt about the adequacy and veracity of information held about the customer. This would mean that CDD is not required unless both circumstances arise. It is proposed to delete the two remaining triggers.

Recommendation

Amend to combine 12(e)(i) and (ii) so that conditions of materiality and risk must both be satisfied before CDD is triggered for existing customers.

Remove clauses 12(e)(iii) and 12(e)(iv)
Doubt about the adequacy or veracity of existing information in relation to addresses

182. The trigger for updating CDD on existing customer includes a test of doubt as to the veracity of existing customer information.

Submitters

183. One submitter was concerned that returned mail would signal incorrect information. Given that it is common for New Zealanders change their address, the trigger for updating customer CDD would be set too low. The submitter proposes that the provisions should make it clear that incorrect address information should not require full CDD to be (re)done.

Comment

184. The obligation to 'reverify' information only applies to the information which is thought to be inadequate. A reporting entity would hold existing information on a customer and filling in important gaps is a common sense approach. It is not intended that each time a piece of mail is returned to the bank that customers are required to provide evidence that verifies a change of address. This is likely to require the customer to come into the branch and this is not practical. A full CDD process is not required under the Bill.

185. Receipt of an address change notification from a customer is sufficient as long as it resulted in mail no longer being returned. Banks would be obliged to contact customers (by telephone or electronic channels) if mail has been returned (as is current common practice). In addition we consider it good practice for customers to be required to bring in evidence of address when they next come into the branch.

186. In light of proposed changes to the provision for existing customers, these matters can all be addressed through Codes of Practice or guidance.

Recommendation

No change.

Clarity about coverage of electronic transactions and occasional transactions

187. Clause 12(b) requires CDD for occasional transactions.

Submissions

188. One submitter noted that the requirement to conduct CDD on occasional transactions could potentially cover a wide range of business as usual transactions.
189. Also, clarity as to how occasional CCD obligations work with electronic transactions.

Comment
190. There will be a threshold set in regulation that determines what an occasional transaction is. Transactions under the threshold will not attract CDD provisions.

191. There are two types of occasional electronic transactions envisaged. Wire transfers are dealt with separately in the Bill. Other electronic transactions will be from an account holder to another account holder and therefore CCD on those business relationships will have been carried out.

192. The occasional transaction definition will clarify that CDD does not have to be carried out on a customer when it has already been carried out – even in occasional transactions – unless the circumstances described in 12(e) (that trigger CDD on existing customers) apply.

Proposal to retain the FTRA provisions for CDD for occasional transactions
193. Clause 12(b) requires CDD for occasional transactions.

Submitters
194. One submitter proposed that the FTRA provisions for occasional transactions be retained.

Comment
195. The CDD requirements within the Financial Transaction Reporting Act 1996 are no longer FATF compliant as it does not require reporting entities to identify beneficial owners.

196. Occasional transactions represent an unknown person using the services of a reporting entity and seeking to do so with an amount of cash / BNI that is above the threshold (eg $10,000).

197. Occasional transactions are a high money laundering risk. Standard due diligence is the appropriate minimum standard for KYC in these situations.

Recommendation
No change.
Clause 14 Standard due diligence and Clause 22 Enhanced due diligence requirements: verification of identity requirements

CDD – verification, “all reasonable steps” and the risk-based approach

198. Clauses 14 and 22 establish the process and standard for verifying the identity of a customer when conducting standard due diligence (clause 14) and enhanced due diligence (clause 22).

Submitters

199. Submitters commented that the identity verification requirements do not provide for practical application of a risk-based approach. This is because the wording ‘must take all reasonable steps’ does not provide for such steps to be varied according the level of risk of different situation.

Comment

200. The verification of identity provisions are fundamental to complying with FATF, and effectively managing money laundering and terrorism financing risk. At a minimum, sufficient information about a customer’s identity needs to be verified so that a reporting entity is satisfied that the customer is who they purport to be. The risk-based approach is intended to apply in respect of information obtained above that minimum standard, including in relation to ‘beneficial ownership’ and ‘acting on behalf’ considerations.

Standard due diligence

201. Currently the requirements within clause 14(1)(a) may be interpreted as going further than is required by requiring all information obtained according to Clause 13 to be verified.

202. An appropriate minimum standard for a natural person, similar to the approach taken by Australia, would be for the customer’s name, date of birth and address to be verified (it is noted however that Australia takes an ‘either/or’ approach to the verification of date of birth and address). Additional information obtained would be verified by taking reasonable steps according to the level of risk presented by the particular situation – the risk-based approach.

203. It is appropriate that the information collected about ‘beneficial ownership’ and persons ‘acting on behalf’ should be verified ‘according to the level of risk’ as is currently provided for beneficial ownership. The use of the word ‘all’ before reasonable steps arguably takes some away discretion away from reporting entities. This discretion is important for the risk-based approach. Therefore the word ‘all’ should be removed from the reasonable steps approach to verifying the identity of ‘beneficial owners’.

204. The requirements in the Bill to verify the identity of a person acting on behalf of a customer and the authorisation to act currently are permissive of a risk-based approach that would enable a decision by a reporting entity to choose not to verify
identity at all if the risk was perceived to be low. This is not desirable. To avoid this scenario it is proposed to take a similar approach to the beneficial owner verification requirements and insert a 'reasonable steps' test.

**Enhanced due diligence**

205. The intent of the enhanced customer due diligence verification of identity requirements is essentially that it is standard due diligence verification, but also requires a reporting entity to collect and take reasonable steps to verify one additional element of information – the source of wealth or funds. There is an ability to specify additional requirements in regulations.

206. As currently drafted, Clause 22(1) requires all information obtained to be verified. Submitters argue that this does not adequately facilitate a risk-based approach.

207. It is appropriate that the enhanced CDD verification of identity requirements rely on the standard due diligence verification provisions to set out a minimum standard of verification.

208. Certain situations will require a more robust set of information, and it is expected that reporting entities consider collecting more information and whether to verify that information. We agree that this latter consideration should be for the reporting entity to determine according to their assessment of the risk presented in relation to their risk assessment and AML/CFT programme.

209. In summary, to better facilitate a risk-based approach to verification of identity, clauses 14 and 22 should clearly state a minimum level of verification that is required, and then make all other verification requirements subject to a "reasonable steps", according to the level of risk, test.

**Recommendation**

We recommend that the verification requirements within the Bill should facilitate a risk-based approach, with a minimum verification standard for customers provided. For standard due diligence (Clause 14(1)) we propose that the Bill require a reporting entity to:

- take all reasonable steps to verify the information in clause 13 as is relevant for the customer type (the minimum verification standard)
- according to the level of risk, take reasonable steps to verify the identity of any beneficial owner
- according to the level of risk, take reasonable steps to verify the identity and authority to act for persons acting on behalf of a customer
- verify any other information prescribed by regulations, according to the standard provided by regulations

For enhanced due diligence (Clause 22), we propose that the Bill require a reporting entity to:
Removing the obligation to verify customer information from statute

210. As outlined above, clause 14 (1) (a) requires reporting entities to take all reasonable steps to satisfy itself that the prescribed minimum information, including name, date of birth and address, is correct.

Submitters

211. A submitter has suggested that clause 14(1)(a) should be amended to make the obligation to verify information collected under clause 13 as prescribed by regulations. This would create greater flexibility for verification and should be in line with Australia (either DOB or address).

Comment

212. Identification is a core component of the AML/CFT regime and critical to effectively detect and deter ML/TF. Verification is a key element of identification. These requirements are best placed in legislation to ensure maximum certainty, clarity and scrutiny for reporting entities.

213. The collection of identity information is of limited value unless that information can be verified. At a minimum, the customers full name, and date of birth must be verified to give reporting entities a degree of confidence in the identity of their customer.

214. While we acknowledge that in situations verification of address may impact upon customer convenience, we think this can be managed through the interpretation of verification provisions that provide for ‘reasonable steps’ to be taken to verify, according to the level of risk. This could be a matter discussed in Codes of Practice tailored to specific sectors or by exemption regulations if necessary.

215. It is desirable for reporting entities (in particular, banks) to hold accurate address information about their customers. Accurate address information is essential to assist the investigation and apprehension of offenders. While it is acknowledged...
that address verification may be problematic in specific business environments, exemptions regulations are able to be employed.

**Recommendation**

No change

**Clause 14 and 18 requirements to verify the authority to act**

216. Standard due diligence clause 14(1)(a) and simplified due diligence clause 18(1) both require a reporting entity to, according to the level of risk, verify authority to act of a person acting on behalf of a customer.

**Submissions**

217. Submitters expressed concern about this requirement, suggesting it should be risk-based.

**Comment**

218. The need to ascertain authority is a FATF requirement. As outlined in the preceding section, it is intended that the Bill provide for a risk-based approach to this requirement.

219. For standard due diligence, the reporting entity will be required to 'according to the level of risk' take reasonable steps to verify the identity of the person acting on behalf of the customer, and the authority to act. The test is for the reporting entity to be satisfied that the person has authority to act on behalf of the customer.

220. In simplified due diligence, the requirement to verify the identity and the authority to act are both able to be determined by the reporting entity according to the level of risk. There is no 'reasonable steps' requirement.

221. Simplified due diligence is able to be applied to prescribed types of customers. Clause 16(2) also provides that simplified due diligence may apply to a person who purports to act on behalf of a customer, when the reporting entity has a business relationship with the customer, and has previously carried out appropriate CDD on that customer as required by the Bill.

222. It is considered that this requirement may be relatively easy to manage operationally. For example, an acceptable procedure would be for customers to provide a list of authorised employees or delegates to the reporting entity. When the employee or delegate attempted to operate the account, they would be identified (and identity verified) and authorisation could be verified with reference to the list provided by the customer. Where simplified due diligence applies verification can also be carried out according to risk.
223. Clause 14 (1) (b) sets out that all reasonable steps to verify any beneficial owner’s identity to the extent that the reporting entity is satisfied that the person is who they say they are.

Submissions

224. Submitters suggest that reporting entities should only be obligated to verify beneficial owners where they suspect the person is not who they say they are. The suggestion was to redraft clause 14 (1) (b) to read ‘where it suspects that a person has provided incorrect information as to their identity.’

Comment

225. FATF is clear that reporting entities should undertake CDD including identifying beneficial owners. This reflects that in reality the beneficial owners control and benefit from the customer.

226. In most circumstances it is through the process of verification that a reporting entity could determine that the information is incorrect.

CDD – timing of verification

227. Clauses 14 and 22 set out the processes for verifying the identity of a customer when conducting standard due diligence and enhanced due diligence. Both clauses also provide for a process for delaying the verification process in certain circumstances. Verification of identity may be completed after the business relationship has been established or the occasional transaction conducted if it is:

227.1. essential not to interrupt normal business practice

227.2. money laundering and terrorism financing risks are effectively managed and

227.3. verification is completed within 5 days of the business relationship being established or the occasional transaction being conducted.
Submissions

228. Verification should be completed 'as soon as reasonably practicable' rather than have a five-day limitation, as this is too rigid and may unnecessarily instigate the closure of an account, thus causing inconveniences and perhaps costs to customers and additional compliance costs for reporting entities.

229. It is suggested that timeframes should managed through limitations and an ability to transact or on an account until verification is complete. In this way, customers are incentivised to assist reporting entities to complete verification rather than being externally motivated by legislation.

230. This manages the money laundering risk and is consistent with the risk-based approach envisaged by the FATF.

Comment

231. The five day requirement was proposed as an incentive for reporting entities to carry out verification promptly. It is acknowledged that there are practical difficulties associated with a five day constraint around timing, especially when a reporting entity is required to cease transacting and end a business relationship with a customer.

232. The key concern is that money laundering and terrorism financing risks are managed. If there is an explicit requirement (as provided in clauses 14(3)(b) and 22(3)(b)) for reporting entities to take measures to manage those risks, it is considered that the five-day constraint could be amended to allow verification as soon as reasonably practicable.

Recommendation
Delete the five-day constraint to allow verification as soon as reasonably practicable.

Delay in verification of identity for occasional transactions

233. As discussed above, clauses 14 and 22 currently provide for reporting entities to take up to five days to complete verification of identity, both when commencing a business relationship or conducting an occasional transaction, subject to specific criteria.

Comment

234. It is proposed to remove the five day constraint and allow reporting entities to undertake verification as soon as reasonably practicable, in line with FATF recommendations. However, it is proposed that for occasional transactions, verification must still take place before the transaction is carried out. The nature of an occasional transaction is that it is one-off and the customer departs after the
transaction is complete. Verification after the fact is essentially meaningless. If it is determined through verification that the customer is high risk or provided false identity information the transaction has already taken place and the damage is done.

235. FATF Recommendations clearly seek to prevent those who would use the financial system for ML/TF from transacting. Where the FATF Recommendations do provide a degree of flexibility in the timing of CDD, it is clear this applies only to business relationships.

**Recommendation**

Remove the ability of reporting entities to delay the verification of identity when conducting occasional transaction.

Clause 15 - Standard due diligence: other requirements

**Risk assessment of need to collect and verify information beyond standard due diligence**

236. Clause 15 provides for additional information that a reporting entity must obtain for standard due diligence. It places an obligation on a reporting entity to obtain information on the nature and purpose of the business relationship and sufficient information to determine whether customer should be subject to EDD.

**Submissions**

237. Submitters requested that the requirement to obtain other CDD information, including the 'nature and purpose of the business relationship', should be conducted according to the level of risk.

**Comment**

238. FATF Recommendation 5.6 states that 'financial institutions should be required to obtain information on the purpose and intended nature of the business relationship.' This FATF recommendation does not envisage that a risk-based approach applies to obtaining this information. It is fundamental to determining whether enhanced due diligence needs to be applied. In addition, it is prescribed so that privacy impacts are better managed.

239. The Bill requires reporting entities to question customers on matters identified in their risk assessment. The risk assessment will need to contain a range of questions that need to be asked in different situations depending on risk. The range of questions will need to be sufficient to determine whether a particular situation constitutes a high risk (such as PEP status, and residency status). If they are not obliged to obtain this information they will have no mechanism to determine when EDD will be applied.
Clause 16: Simplified due diligence

Addition of low-risk products, services to the simplified due diligence category

240. Clause 16 sets out the circumstances in which a reporting entity may conduct simplified due diligence. The Bill sets out entities for whom simplified due diligence may be conducted and provides for regulations to add entities to the simplified due diligence category.

Submitters

241. One submitter considered that Bill should provide for a mechanism to add products, transactions, customer types and services to the simplified due diligence category. Three submitters considered that reporting entities should be able to add to the category through an AMU/CFT programme.

Comment

242. Simplified due diligence is, in effect, a customer exemption from CDD (and FATF) requirements. The FATF intends that countries allow reporting entities to implement lesser standards of CDD where there are demonstrated and controlled low, or negligible money laundering and terrorism financing risks and information about beneficial owners is otherwise available.

243. It is agreed that provision should be made to add to the list of situations in which simplified due diligence is appropriate. It is proposed that this is achieved through a regulation making power that is broadened to include products, services, customers and transactions.

Recommendation

Amend the regulation making power for simplified due diligence to provide for the inclusion of customers, products, services and transactions.

Proposal to add State Owned Enterprises and Crown entities to the simplified due diligence category

Submitters

244. One submitter suggested including State Owned Enterprises and Crown Entities to the list of entities for which simplified due diligence is permitted.
Comment

245. Adding to the list within clause 16(1) can be achieved through regulations. This is appropriate as it will involve robust consideration of the customer type against a set of objective criteria.

246. Consideration of adding Crown Entities and State-Owned Enterprises to clause 16(1) would be made when developing regulations for simplified due diligence.

Recommendation

No change.

Clause 20 – Circumstances when enhanced customer due diligence applies and clause 22 verification requirements

247. A reporting entity must conduct enhanced due diligence in certain circumstances. The types of circumstances listed are those that involve customers or situations that, by their nature, are considered to have a high risk of money laundering or the financing of terrorism. This includes customers who are trusts, are not resident in New Zealand and come from countries that have insufficient AML/CFT systems, companies with nominee shareholders or shares in bearer form, or politically exposed persons.

248. In addition to standard due diligence, enhanced measures must be taken, including identifying the source of wealth of the customer.

Submitters

249. Many submitters were concerned that enhanced due diligence is required in prescribed situations noting that there is no ability to remove customers or situations from the EDD information and verification requirements into the standard category. This is different from Australian legislation and rules, which allows reporting entities to decide whether EDD information and verification should apply in addition to standard levels.

Comment

250. The Bill provides for EDD to be conducted in specific situations, identified by FATF as being inherently high risk.

251. Reporting entities are only required to collect the minimum information set out in the Bill. For enhanced due diligence, the only additional information collection requirement is the customer’s source of wealth. All other information to be collected is at the reporting entity’s discretion as guided by AML/CFT programmes and risk assessments. The Bill is prescriptive with respect to the requirement to collect information on the source of wealth. The rationale is that clearly stating to
252. Requesting information on source of wealth is not onerous. It is however acknowledged that verification of this information may be operationally difficult. To mitigate this, a lesser verification standard (the reporting entity must only be satisfied that the information is correct) is applied. It is further proposed to reduce the requirement to take "all reasonable steps" to just "reasonable steps". This will allow reporting entities to apply a more discretionary approach according to the level of risk.

**Recommendation**

Remove 'all' from the 'all reasonable steps' requirement in clause 22(1)(a).

**Clause 23 – Politically Exposed Persons**

253. Clause 23 places an obligation on reporting entities to conduct enhanced CDD on politically exposed persons (PEPs) who are seeking to either establish a business relationship or an occasional transaction. Clause 23 also sets out additional obligations of:

253.1. getting senior management approval before establishing a business relationship with a PEP

253.2. any other requirements prescribed by regulations that apply to PEPs.

**Identifying Politically Exposed Persons**

254. The Bill does not set out a process which reporting entities must follow to identify PEPs.

**Submissions**

255. One submitter commented that the process for identifying PEPs is onerous and that reporting entities must establish multiple issues concerning the identification of PEPs before it may establish a business relationship or conduct an occasional transaction. The submitter recommended that the Bill be amended to allow reporting entities to rely on appropriate declaration forms as an accepted way of identifying PEPs.

**Comment**

256. The enhanced due diligence requirements for PEPs are a reflection of the minimum requirements within the FATF Recommendations and other international obligations. The Bill does not prevent reporting entities from using declaration forms to manage the identification of PEPs.
Enhanced Due Diligence on PEPs for occasional transactions

257. The Bill requires reporting entities to conducted enhanced due diligence when a customer (or a beneficial owner) is a PEP and is seeking to conduct an occasional transaction.

Submissions

258. Three submitters from the banking sector recommended either:

258.1. that the requirement to conduct enhanced due diligence on PEPs who conduct occasional transactions should be removed (two submitters), or

258.2. that reporting entities should only be obligated to identify and verify the identity of PEPs conducting an occasional transaction when suspicion arises (one submitter).

Comment

259. EDD on occasional transactions where the customer or the beneficial owner is a PEP, is a minimum requirement of the FATF Recommendations.

260. An objective of the effective AML/CFT controls is the prevention of transactions that are used to launder funds. If a suspicion arises following an occasional transaction and appropriate CDD has not been undertaken, there will be insufficient information available for law enforcement officers for investigative purposes and the funds will be difficult to recover. Also, if there is a request from an overseas counterpart in relation to a foreign PEP, relevant CDD information needs to be available in order to assist in global anti-corruption efforts and investigations.

Recommendation

No change.

Knowingly commencing a business relationship, or conducting an occasional transaction for a PEP

261. The Bill requires reporting entities to conduct EDD on all customers who are PEPs, or have beneficial owners who are PEPs.
Submissions

262. The casino industry considered that clause 23 should be amended to only require reporting entities to conduct the enhanced due diligence requirements on PEPs where the entity 'knowingly' establishes a business relationship with, or conducts an occasional transaction for, a PEP.

Comment

263. 'Knowingly' is a very high standard to prove and does not require reporting entities to make sure that their customer is, or is not, a PEP. The FATF Recommendations do not provide, or promote such an approach. The expectation within the FATF Recommendations and UNCAC is that PEPs are identified and that they are subject to enhanced due diligence.

264. The submitter's underlying concern appears to be that the PEP requirements are absolute and do not take account of reasonable steps, or knowledge, by the reporting entity is valid. It would be appropriate to amend clause 23 to clarify that a reporting entity is obligated to undertake 'reasonable steps'. What constitutes reasonable steps could be set out in a Code of Practice.

Recommendation

Require a reporting entity to take reasonable steps to determine whether a customer or a beneficial owner of a customer is a PEP.

Requiring senior management approval when offering services to PEPs

Submissions

265. Three submitters contended that a requirement to gain senior management approval for conducting an occasional transaction for PEPs was onerous and should be removed.

266. One submitter recommended that the requirement for senior management approval for business relationships with foreign PEPs should be removed, or at least allow for delegation of authority.

Comment

267. Senior management approval for occasional transactions for PEPs is onerous and is not a requirement by the FATF Recommendations. Clause 23 does not require reporting entities to gain senior management approval when conducting an occasional transaction for a PEP, only when establishing a business relationship with a PEP (refer clause 23(a)).
268. However, as three submitters, have incorrectly interpreted this clause, officials consider it appropriate to amend the clause to clarify this matter.

269. Officials also note that it is not strictly required by the FATF Recommendations to gain senior management approval when establishing a business relationship with a domestic PEP. Therefore, in appreciation of the compliance costs, we recommend that the Bill be amended to remove the requirement to gain senior management approval when establishing a business relationship with a domestic PEP.

270. However, the requirement for senior management approval when establishing a business relationship is a FATF minimum for foreign PEPs. In part, the intent of the requirement to gain senior management approval is to protect more junior staff from undue influence in the course of establishing the business relationship.

**Recommendation**

Clarify that reporting entities are not required to gain senior management approval when conducting an occasional transaction for a PEP.

Remove the requirement to gain senior management approval when establishing a business relationship with a domestic PEP.

---

**Domestic PEP database**

**Submissions**

271. Eight submitters recommended that the Commissioner of Police, or a government department, provide a freely accessible database that lists domestic PEPs. One submitter suggested that not having a government sponsored list or database would be inefficient and require resources beyond those assessed in the Deloitte Report².

272. One of the submitters recommended that if the government was not prepared to maintain a PEP database then a government agency should be responsible for certifying which privately provided databases are appropriate for this purpose.

**Comment**

273. The creation of a database listing domestic PEPs is an operational decision and does not require statutory provisions within the Bill. Certification of appropriate databases is also an issue that could be considered, but does not need to be addressed in the Bill.

---

Clause 24 and 25 – Wire transfers: identity and verification requirements

274. The Bill as currently drafted requires ordering institutions to collect specified information and ensure it is attached to a wire transfer. Intermediary institutions must ensure that the wire transfer has the same full set of originator information attached when they pass the transfer on. Beneficiary institutions are also obligated to take all practicable steps to ensure the full originator information accompanies the wire transfer when it is sent. The implication is that at each step of the process institutions must manually intervene in the wire transfer to proactively determine if the full set of originator information set out in subsection (1) is attached. If it is not, they are required to take steps to remedy the situation.

Submissions

275. Submitters expressed concerns about the requirement for reporting entities to take ‘all practicable steps’ to ensure that originator information accompanies the wire transfer. While it is possible to confirm that all electronic fields for attaching information are populated, there is a practical difficulty in checking that the information attached to a wire transfer is correct.

276. The requirement to transfer the full originator information to an offshore institution is particularly problematic in clause 24(6) (an intermediary must transfer full originator information to the next reporting entity in the chain) if the full originator information was not received from the ordering institution. These requirements would mean that the transaction will not be able to be completed unless the intermediary proactively seeks the full information from the ordering institution.

Comment

277. It is acknowledged that manual intervention to check that the originator information attached to the wire transfer is correct would be onerous. It is proposed to clarify that a reporting entity will only be required to confirm that the originator information is attached. This could be done through a Code of Practice or guidance.

278. Further, placing an obligation on a beneficiary institution to ensure the complete originator information accompanies a wire transfer may be unduly onerous. This obligation is best placed on ordering institutions. It is proposed to amend the Bill to adopt the FATF recommended risk-based policies and procedures approach, for handling wire transfers that are received without full originator information.

279. Clause 24 (6) will also need to be amended to allow intermediary institutions to simply pass on the information they receive, rather than requiring them to go back in the process to obtain information that may be missing.
Clause 26 – Correspondent banking

Currently the Bill requires a correspondent institution in a correspondent banking relationship to conduct enhanced due diligence on a respondent institution. There is a prescribed range of information that must be collected, including a requirement to determine from publicly available information about 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 money laundering or financing of terrorism investigation or regulatory action.

Submissions

Submissions from the banking sector have suggested there should be a timeframe within which regulatory action should be considered relevant (5 years is suggested).

Comment

Ultimately this is a subjective test and it is up to reporting entities to determine what level of risk historical regulatory action represents within their own context. It is not proposed to amend the Bill to include a timeframe, but if reporting entities are concerned guidance can be provided on this matter.

Recommendation

No change.

Clause 27 – New or developing technologies and products that might favour anonymity

Currently the Bill requires that before establishing a business relationship or conducting an occasional transaction that involves new or developing technologies or products that might favour anonymity, reporting entities must (in addition to the requirements of enhanced due diligence) take additional measures that may be
needed to prevent the use of such technologies and products from being used in the commission of a money laundering or financing of terrorism offence.

Submissions

284. One submitter expressed a preference for new or developing technologies and existing technologies to be treated in the same manner. The underlying concern is that imposing a higher burden of CDD in respect of new or developing technologies may retard useful innovation in the financial sector.

285. It was suggested that the provisions should be deleted, or at least reworded to ‘take any additional measures, appropriate to the level of risk involved and likely cost, to prevent new or developing technologies and products from being used in the commission of a money laundering offence’.

Comment

286. Anonymity is a risk factor, and therefore enhanced measures to manage that risk is appropriate. The extent of measures is able to be determined by reporting entities on a risk sensitive basis. Types of measures that might be appropriate can be set out in guidance.

287. However on balance we consider that the requirements to identify the source of funds or wealth of the customer may not be necessary and as such we consider that standard due diligence in conjunction with other, appropriate controls to prevent this new technology being used for ML or TF would be sufficient to meet the FATF standard. It is proposed to remove the link between clauses 27 and 21 and 22 that require enhanced due diligence to be carried out as well.

Recommendation

Amend the Bill to de-couple clause 27 from the enhanced due diligence requirements by removing reference to clauses 21 and 22.

Insert reference to standard due diligence clauses 13 and 14 instead.

Remove cross reference to new or developing technologies from clause 20 in the enhanced due diligence section.

Clause 28 – Ongoing customer due diligence and account monitoring

Detecting suspicious transactions

288. Clause 28 requires reporting entities to continue to conduct due diligence and to monitor accounts. It sets out the minimum requirements for ongoing CDD. This includes a review of customer account activity and transaction behaviour and customer information held by a reporting entity.
Submissions

289. One financial sector representative body submitted that ongoing CDD should focus on detecting suspicious activity and not on reviewing CDD information.

Comment

290. Ongoing CDD is about both account monitoring and reviewing CDD information so that suspicious activity can be more easily detected. Reporting entities need accurate information about customers so that they can ensure that transactions being conducted are consistent with the reporting entities knowledge of that customer and the customer profile. When suspicion is found through account monitoring, customer information also needs to be accurate for law enforcement purposes. FATF discuss the importance of reviewing customer information in Recommendation 5. The Bill allows reporting entities to take a risk-based approach to focus attention on higher risk customers.

Recommendation

No change.

Clause 29 – Reliance on a member of a designated business group

Responsibility for CDD within a designated business group

291. Clause 29 allows one member of a DGB to rely on another member of that group to perform certain aspects of the AML/CFT requirements. In particular, one member of the group may rely on another member to conduct CDD procedures if certain conditions are met.

292. FATF are clear that when relying on third parties to conduct CDD, the responsibility for making sure this is done adequately must remain with the reporting entity.

293. It is intended that this is also the case for members of a DBG, it has been queried whether this is clearly expressed in the Bill. We propose to clarify that this is the intention.

Recommendation

Amend to clarify that despite clause 30(1), it is the reporting entity, and not the DBG member being relied on, responsible for ensuring that it is complying with the obligations in the Bill.
Shared AML/CFT programmes within a DBG

294. To ensure that reporting entities within a DBG manage ML/TF risks in a way that takes account of individual risk variations in their business environment, supervisors should be able to require that an individual member of a DBG establishes its own risk assessment and AML/CFT programme if this is considered appropriate in the circumstances.

Recommendation

Empower the AML/CFT supervisor, which has responsibility for the DBG members, to require a member to develop its own AML/CFT programme or risk assessment where the AML/CFT supervisor considers the AML/CFT programme or risk assessment of the DBG is not appropriate for the reporting entity that is using it.

Clauses 29, 30 and 31 - Reliance on third parties

Requirement to collect verification information when relying on third party CDD

295. Clause 30 allows a reporting entity to rely on the CDD of another reporting entity with certain conditions attached. One of the conditions is that, within 5 days, the relevant verification information is provided to the reporting entity as soon as practicable, but no later than 5 days after the business relationship is established or the occasional transaction conducted.

Submissions

296. Two submissions considered that collecting verification information from the third party is too onerous.

Comment

297. Reporting entities are required to ensure that CDD information provided to them is accurate and available should law enforcement authorities need to reconstruct the identity of their customer, or the transaction. FATF are clear that a reporting entity relying upon a third party to carry out CDD should immediately obtain the necessary information.

Recommendation

No change.

Request to transfer liability for CDD to third party and guarantee stamps

298. As with DBGs, clause 30 allows a reporting entity to rely on the CDD of another reporting entity with certain conditions attached. One of those conditions is that
the reporting entity in receipt of CDD information remains responsible for ensuring that the CDD is carried out in accordance with the obligations in the Bill.

Submissions

299. Some submitters considered that the liability imposed on reporting entities by the Bill should be transferred onto the third party rather than the reporting entity receiving the CDD verification information. As an alternative, it was suggested that there could be provision for a defence, mitigation or relief where the reporting entity has appropriate agreements, policies, procedures that have been followed through contractual arrangements with a third party.

300. Submitters in the securities sector considered that provision should be made for reliance on third parties for off-market paper based transfer when it is authenticated through a ‘guarantee stamp’ as this would reduce money laundering risks and would ensure that securities registries are able to be exempted from obligations to conduct CDD.

Comment

301. The FATF expects reporting entities to conduct CDD on customers and that responsibility and liability rest with the reporting entity. Also, in some cases, particularly where the third party is overseas, it is not possible for the Bill to provide that liability is transferred to a third party. Contractual arrangements between reporting entities and third parties, while providing reporting entities with a mechanism to take action against a third party for failure, do not provide sufficient incentives for ensuring obligations are met.

302. The proposal for exemption of securities registries from CDD upon reliance on a guarantee stamp would need to be examined to ensure that the conditions outlined in the Bill could be met. If it is appropriate, there is the possibility that guarantee stamps could be provided for through an exemptions regulation.

Recommendation

No change.

Business relationships incidental to another business relationship

303. Verification of standard due diligence sets out minimum standards. Clause 30 allows reporting entities to rely on the CDD of another reporting entity with certain conditions. Relying on CDD obtained from another reporting entity or third party (third hand CDD) is not permissible under the AML/CFT Bill.

Submissions
304. One submitter requested an exemption from the requirement to rely only on third hand CDD in certain situations. For example, where there is a manager and a trustee of a unit trust, and where the manager has relied on the CDD of a bank, the Bill would prevent the trustee from being able to rely on the CDD of the manager.

305. The proposed remedy is that there is an allowance for reliance on third hand CDD requirements for reporting entities where the business relationship is incidental to another business relationship for which CDD has already been completed.

Comment

306. The rationale for preventing reliance on CDD third hand is that reporting entities must be in a position to evaluate the CDD capabilities of the party they are relying on. This is not always possible, particularly if a third party is in an overseas jurisdiction. CDD information is sensitive and the passing on of this information must be tightly controlled. There is always a possibility of exemptions regulations to apply to very specific situations where is considered that the risks outlined above can be managed.

Recommendation

No change

Reliance is limited to the third parties described in the Bill.

307. Subject to specific conditions, clauses 29, 30 and 31 provide for reliance on:
- members of DBGs
- other reporting entities or persons in another country
- agents.

Comment

308. The Bill should specify that these people are the only groups that reporting entities may have reliance on. The concern is that if this is not made specific then there is nothing preventing them from relying on other agents under an outsourcing/contractual arrangement which would not be subject to the conditions outlined in the Bill.

309. The policy on reliance on third parties needs to be clarified, because the ML/TF risks of outsourcing, particularly to other jurisdictions, is high. It is recommended that the Bill reflects that the reliance provisions are limited to those specified in clauses 29, 30 and 31.
Clause 32 – Use of information obtained from third party conducting customer due diligence

Use of personal information by third party

310. Clause 32 provides that the information obtained from a third party conducting CDD procedures for a reporting entity may only be used by that entity for the purposes of complying with the Bill and the regulations.

Submissions

311. One submitter considered that CDD information collected by an agent for a reporting entity should not be prevented from using that information if the customer consents to the information being used for other, commercially appropriate purposes other than those aligned with the Bill and its regulations.

Comment

312. It is reasonable for a reporting entity to use CDD information obtained from a third party, or for the third party to use that information, for other purposes if the customer has consented to its use for purposes other than complying with the Bill and its regulations. However no change to the Bill is necessary to provide for this, it is provided for under the Privacy Act 1993.

Recommendation

No change.

Clause 32 – Prohibitions if customer due diligence not conducted

Relationship between existing legal and contractual obligations to terminate

313. Clauses 34 and 36 contain prohibitions on establishing or continuing a business relationship in certain circumstances or in relation to certain transactions.

Submissions

314. The obligation to terminate existing business relationships with the customer if CDD is not carried out could be difficult due to conflicting statutory laws or conflicting common law obligations preventing unilateral termination of business relationships. For example, life insurance practice generally permits only the insurer to terminate in limited circumstances. The obligation may also result in 'tipping-off' a customer.
315. It should be noted that termination of a business relationship is required upon failure to carry out adequate CDD, not on formation of a suspicion. This element of the Bill is about managing risk, by knowing who the customer is, before services are provided, so that if a suspicious matter does arise, the reporting entity has enough accurate information to issue an STR and assist law enforcement officers in investigation. If reporting entities are unable to identify customers, it is argued that they should not be entering business relationships with them. The obligation to terminate the business relationship is recommended by FATF.

316. Where there are conflicting statutory obligations, it is a matter for a court to weigh up which obligation is superseded.

317. However, the concern raised by the submitter is legitimate. We propose to provide appropriate protection for reporting entities in carrying out their obligations described in this Bill.

**Recommendation**

Amend to provide appropriate protections reporting entities.

**Clauses 37, 40 and 139 – Suspicious transaction reports**

**Suspicious transaction reports to relate to all serious crime**

318. Clause 37 deals with the reporting of suspicious transactions by reporting entities to the Commissioner of Police. The Bill provides for reporting entities to submit an STR where they have reasonable grounds to suspect that a transaction, or proposed transaction, is relevant to a money laundering investigation, the enforcement of the Misuse of Drugs Act 1975, the Terrorism Suppression Act 2002 or the Criminal Proceeds (Recovery) Act 2009.

**Comment**

319. Given that the New Zealand definition of money laundering is contingent on a serious offence having taken place to generate the proceeds it is appropriate reporting entities to submit STRs where they have reasonable grounds to suspect that the transaction is, or may be, relevant to the investigation or prosecution of any serious offence.

**Recommendation**
Clause 43 – Disclosure of Information relating to suspicious transaction reports

Sharing of STR information between principal and sub-agents

320. Clause 43 provides that reporting entities are only able to share STR information with:
   320.1. a Police employee who is authorised by the Commissioner to receive the information; or
   320.2. the reporting entity's AML/CFT supervisor; or
   320.3. an officer or employee of the reporting entity, for any purpose connected with the performance of that person's duties; or
   320.4. a barrister or solicitor, for the purpose of obtaining legal advice or representation in relation to the matter.

Submissions

321. One submitter has sought an exemption to allow subagents to share STR info with principal agents. Principal agents that conduct transaction monitoring across multiple subagents may be able to identify patterns of transaction which lead to a suspicion being formed. The submitter would like the ability to be able to share information with the subagent where the suspicious transaction was conducted and also the compliance department of the parent company.

Comment

322. STRs contain highly sensitive information that needs to be managed carefully to protect both the customer's privacy and to prevent tipping off customers. For this reason the FATF expects that reporting entities will be solely responsible for the management of STR matters. It is not considered that an exemption from information sharing restrictions is appropriate.

323. It is however intended that reporting entities be able to share information within a DBG to the extent that it is strictly necessary during the process of submitting of an STR. In situations like the one described by this submitter, this may assist reporting entities in identifying suspicious patterns of transactions and trigger an STR.

324. In the Bill as currently drafted, a principal agent and a sub-agent would not be able to form a designated business group. However it is proposed to amend the
interpretation clause to provide for additions to the definition of DBG through regulation.

325. If the definition was expanded to cover a principal agent and a sub agent relationship, information relating to an STR could be shared. Information sharing would only be permitted prior to the submission of the STR, to the extent that it was strictly necessary to determine whether an STR should be submitted. Sharing of STR information with the compliance department of the parent company would still be prohibited. Officials will consider amendments to the definition of DBG by regulation.

Recommendation

Amend the Bill to provide for information sharing among members of a DBG to the extent that it is strictly necessary during the process of submitting the STR.

Seeking advice from the FIU and supervisors on submission of STRs

326. Currently there is nothing in the Bill that prevents a reporting entity from seeking advice from the FIU or their AML/CFT supervisor about whether to submit an STR.

Submissions

327. Submitters have requested the Bill be amended to prescribe an information sharing safe harbour so that reporting entities can discuss and share information with the Financial Intelligence Unit and supervisors to establish whether or not to submit an STR.

Comment

328. It is not intended to permit a reporting entity to discuss whether or not to submit an STR with a supervisor or the FIU. Forming a suspicion is a subjective judgement that should be made by the reporting entity alone. They are best placed to weigh up the context, and other relevant factors to determine if the behaviour is unusual. Reference to the supervisor or FIU might encourage unduly cautious behaviour and result in over reporting.

329. In addition, high levels of reporting (thousands of STRs are received a year) it is not feasible for the FIU to be able to comment on specific instances of STR reporting. To assist reporting entities, guidance will be issued by the FIU in relation to forming suspicion and appropriate timing for submitting an STR.

Recommendation

No change
Clause 46 – 52 Record keeping

Obligation to keep transaction records

330. Clause 46 currently obliges reporting entities to retain a full set of records for every transaction that is conducted through a reporting entity including the following information:

330.1. the nature of the transaction
330.2. the amount of the transaction and the currency in which it was denominated
330.3. the date on which the transaction was conducted
330.4. the parties to the transaction
330.5. 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
330.6. the name of the officer or employee or agent of the reporting entity who handled the transaction, if that officer, employee, or agent—
   330.6.1. has face-to-face dealings in respect of the transaction with any of the parties to the transaction; and
   330.6.2. has formed a suspicion about the transaction
330.7. any other information prescribed by regulations.

Submissions

331. Submitters expressed concerns that these requirements appear to apply to all transactions, even those under the applicable value threshold (which is yet to be determined through regulations).

Comment

332. This is an oversight. The intention is that record keeping provisions within clause 46 that relate to the obligation to keep transaction records should only apply to business relationships and transactions above the applicable value threshold. The Bill needs clarification.

Recommendation

Amend clause 46 to ensure that record keeping obligations only apply to business relationships and transactions above the applicable threshold value.
When records need not be kept

333. Clause 50 in the Bill allows a reporting entity to not keep records when they are liquidated and finally dissolved.

Submissions

334. Both officials and submitters have identified that this presents an opportunity for reporting entities to conceal evidence of money laundering through dissolution. This is not desirable; records need to be kept for an appropriate length of time to allow for reconstruction of transactions to aid law enforcement officers in the investigation of suspicious matters.

Comment

335. It is proposed to provide for a court to be able to order the retention of records upon liquidation or dissolution of a reporting entity.

Amend to provide for a court to be able to order a reporting entity to retain records despite liquidation or dissolution

Destruction of records

336. Clause 51(1) requires a reporting entity to ensure that every record and copy of the record retained is destroyed as soon as practicable after the expiry of the period for which that reporting entity is required to retain it.

Submissions

337. Several submitters have commented on the practical difficulty of ensuring that electronic records are destroyed. Some have suggested amending the provision to require a reporting entity to take all practicable steps to ensure the destruction of records.

Comment

338. It is acknowledged that permanent destruction of all electronic records is increasingly difficult. This is a much wider problem that applies to all information stored electronically.

339. It is proposed to amend the requirement for provide that reporting entities should take all practicable steps to ensure the destruction of electronic records.
Clause 54 – Minimum requirements for AML/CFT programmes

Defence against prosecution when following AML/CFT programme

340. Clause 54 sets out the minima that a reporting entity must include in an AML/CFT programme.

Submissions

341. One submitter recommended that the Bill should give reporting entities a defence against prosecution if their AML/CFT programme has been approved by their AML/CFT supervisor.

Comment

342. The Bill does not provide for AML/CFT supervisors to approve a reporting entities AML/CFT programme. The risk-based approach that has been incorporated into the Bill, provides the flexibility for reporting entities to lead the creation, and maintenance of their AML/CFT programme. Where a reporting entity has breached their obligations under their Bill, they should be liable for those breaches.

Recommendation

No change

Keeping records relating to risk assessments

343. Clause 54 sets out minimum requirements for AML/CFT programmes. Subclause (h) requires the keeping of written findings in relation to some transactions and other suspicious activity.

344. It has been queried whether an entity should be required to keep records relating to reviews of risk assessments, audits, and AML/CFT programmes.

Comment

345. With respect to risk assessments, reviews of risk assessments and AML/CFT programmes, we agree that it is important for supervisors to be able to trace the development of risk assessments and AML/CFT programmes of its entities over time so as to assess progress and continuous improvement.
346. Clauses 54 and 55 deal with internal policies and procedures and controls that a reporting entity must have in order to prevent activities related to money laundering and the financing of terrorism. A reporting entity must have an AML/CFT compliance programme. The reporting entity must also undertake a risk assessment of the risk of money laundering and terrorism financing. This risk assessment is used to determine the level of risk when conducting different types of CDD, and ongoing due diligence and account monitoring.

347. The Bill provides for supervisors to develop Codes of Practice. Clause 64 provides for the legal effect of Codes of Practice.

Submissions

348. One submitter commented that there is no explicit link between the CDD provisions and the AML/CFT programme and that the programme should be explicitly referred to in Part 2 of the Bill as the means for achieving compliance.

349. Further clause 54 should be amended to be clear that processes are risk-based.

Comment

350. Early submissions during the third consultation phase, and on the consultation draft Bill sought detail within the AML/CFT programme and CDD provisions.

351. The AML/CFT Programme exists to help reporting entities implement their obligations under the Bill. The programme is not, in and of itself, the primary obligation. The programme should be based on the risk assessment that the reporting entity conducts.

352. We consider that clause 10 ties the CDD obligations through to both the programme and the risk assessment through a direct reference to clause 54. However, for avoidance of doubt this could be made more explicit.
Clause 56 – Review and audit of risk assessments and AML/CFT programme

Submission of audits to AML/CFT supervisors

353. Clause 56 requires reporting entities to review and audit their risk assessment and AML/CFT programme. Sub-clause (7) requires reporting entities to provide a copy of the audit to the relevant AML/CFT supervisor.

354. It has been requested that the Bill should be amended such that the requirement to submit the audit report to the supervisor is not mandatory, but is at the supervisor’s request.

Comment

355. A mandatory requirement to submit an audit report places incentives on reporting entities to enter into the audit process defensively, whereas the purpose of such an audit is to foster continuous improvement.

356. The intent of the regulatory system is to foster voluntary compliance. Therefore it is appropriate that the mandatory requirement for submission of the audit to an AML/CFT supervisor is removed. Instead, the Bill should provide for the audit reports to be submitted to supervisors on request.

Recommendation:

State that a reporting entity must provide a copy of any audit conducted under clause 56 when requested by the relevant AML/CFT supervisor.

Clause 56 – Review and audit of risk assessment and AML/CFT Programme; clause 57 – Annual AML/CFT report

357. The Bill currently requires reporting entities to conduct a review of its risk assessment AML/CFT Programme to:

357.1. ensure the risk assessment and AML/CFT programme remain current; and

357.2. identify any deficiencies in the effectiveness of the risk assessment and the AML/CFT programme; and
357.3. make any changes to the risk assessment or AML/CFT programme identified as being necessary under paragraph (b).

358. A reporting entity must also 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.

359. Clause 57 requires reporting entities to report annually on the risk assessment and AML/CFT Programme and the annual report must take into account the results and implications of the review and audit.

Submissions

360. One submitter commented that reviews of programmes should be annual to tie in with annual reporting requirements. Other submitters seemed confused about the role and frequency of the ‘review’ referred to in clause 56.

Comment

361. The wording ‘conduct a review’ in clause 56 has caused confusion about what is required and how often. Rather than undertake a regular review process, it is intended that reporting entities review the programme and risk assessment to ensure it is still up to date and relevant. The regularity and timing of review is at the discretion of reporting entities to determine.

362. Clause 57 requires the results and implications of the review and audit to be taken into account in the annual report. It is proposed to remove the requirement to take into account the result of ‘the review’ as it is really intended as an internal mechanism for on-going maintenance of the risk assessment and AML/CFT programme. The independent audit is really the mechanism through which any deficiencies will be identified and reporting entities are expected to remedy these and take into account in annual reports.

Recommendation

Amend clause 56(1) to require reporting entities to review (delete ‘conduct a review of’) its risk assessment and AML/CFT Programme.

Amend section 57(2)(b) to delete ‘of the review required by section 56(1)’.

Timing of submission of annual reports

363. Clause 57 requires a reporting entity to provide an annual report on its risk assessment and AML/CFT programme to its AML/CFT supervisor.

364. There is potential for situations to arise when the reporting entity and the supervisor do not agree on timing.
365. The intent behind agreement on timing in this instance is to ensure that both reporting entities and supervisors are able to manage work flows and yearly cycles as far as possible. However, it is acknowledged that there will be times when agreement is not possible.

366. It is proposed that the timing of submission of annual reports should be at the discretion of the supervisor. However, the supervisor must have regard to the planning and business cycle of the reporting entity.

**Recommendation**

Provide for supervisors to request, on notice, a reporting entity’s annual AML/CFT report.

**Clause 58 – Branches and subsidiaries in other countries**

367. Currently the Bill requires reporting entities to ensure that all branches and subsidiaries in a foreign country apply, to the extent permitted by the law of that country, measures at least equivalent to those set out in the Bill.

**Submissions**

368. One submitter requested an amendment to allow subsidiaries in Australia to implement the Australian AML/CFT requirements where they are more permissive than New Zealand.

**Comment**

369. Clause 58 references FATF’s recommendation for subsidiaries and branches to have adequate AML/CFT systems. The policy intention here is to ensure that reporting entities are subject to adequate supervision for ML/TF. It is considered that provision by provision equality is not necessary, but that the overall regime is broadly equivalent and comparable in terms of FATF compliance.

370. We propose amending the Bill to require reporting entities to ensure that all branches and subsidiaries apply ‘broadly equivalent’ measures to New Zealand. Broadly equivalent could be further defined in guidance or a Code of Practice.

**Recommendation**

Amend to require reporting entities to ensure that all branches and subsidiaries apply ‘broadly equivalent’ measures to New Zealand.
Clause 64 - Legal effects of Codes of Practice

371. Clause 64 provides that a reporting entity complies with the obligations of the Bill (or any regulations) by complying with a Code of Practice which state the means of satisfying the obligation or comply by some other equally effective means.

Submissions

372. Submitters expressed a desire to see an explicit reference to the AML/CFT Programme in this provision.

373. Concerns were that the term 'equally effective means' will not promote flexibility. An alternative means that is effective in achieving compliance should be sufficient and an AML/CFT Programme would contain these.

374. The Legislation Advisory Committee (LAC) also felt that clause 64(3) requiring a court to have regard to the Code of Practice, created incentives to always follow the Code of Practice.

Comment

375. The AML/CFT Programme is not a legal instrument. Reporting entities develop Programmes, with reference to any Code of Practice, at their own risk. To allow reporting entities to rely on an AML/CFT Programme as if it were a legal instrument (which is the practical effect of the submitter’s suggestion) would not guard against deficiencies in the Programme. It would not be an efficient use of limited resource for supervisors to approve the AML/CFT Programme of every reporting entity (which is essentially what would be required). This is why Codes of Practice are useful.

376. Other ‘equally effective’ means is designed to accommodate situations where a comparable standard can be achieved through other policies and procedures. ‘Equally effective means’ may include policies and procedures set out in AML/CFT Programmes.

377. Codes won’t necessarily specify detailed procedures or policies (although they may). Codes can be used to establish a standard of practice that should be reached, but the procedures will still be able to be determined by reporting entities.

378. Where codes are procedurally prescriptive, it is still envisaged that an alternative means that is effective in achieving compliance would be acceptable.

Recommendation

No changes.
Clause 73, 74 and 75 – Criminal and civil penalties

Civil and criminal liability for senior managers should be removed

379. Clauses 73 and 74 provide that senior managers of reporting entities are liable for civil and criminal breaches of the obligations in the Bill

379.1. A senior manager of a body corporate commits a criminal offence if:

379.2. the body corporate commits an offence under this Part

379.3. the manager knew that the offence was being or would be committed

379.4. the manager was in a position to influence the conduct of the body corporate in relation to the commission of the offence

379.5. the manager failed to take all reasonable steps to prevent the commission of the offence.

380. A senior manager of a body corporate is liable to a civil penalty if:

380.1. the body corporate engages in conduct that constitutes a civil liability act

380.2. the manager knew that the civil liability act was occurring or would occur

380.3. the manager was in a position to influence the conduct of the body corporate in relation to the civil liability act

380.4. the manager failed to take all reasonable steps to prevent the civil liability act.

Submissions

381. A number of submitters, mostly from the banking sector, recommended that the Bill remove the civil and criminal liability of senior managers. Submitters commented that body corporate should be liable and not senior managers, individuals should only be civilly liable where they have actively sought to induce a civil liability act.

382. Submitters argued that the civil and criminal liability of senior managers within the Bill would be likely to:

382.1. result in defensive suspicious transaction reporting and counter-productive outcomes

382.2. impair the ability of senior managers to implement a risk-based approach when they are facing high consequences of getting it wrong

382.3. make it more difficult for reporting entities to attract talented and capable people to posts where they are exposed to such high penalties.
383. Submitters were also critical of these clauses and their inconsistency with the more limited liability of senior managers within the Australian AML/CFT framework.

Comment

384. The FATF Recommendations provide that sanctions should be available in relation to the directors and senior managers of the legal entity (for example, the body corporate) as well as the reporting entity itself.

385. We consider that the common law currently provides adequate means to hold legal and natural persons, including senior managers, accountable for breaches of the legislation. A senior manager may be found liable as an individual if it can be shown that they committed the act or were responsible for the unlawful actions of another person. Establishing the liability of a senior manager in these circumstances would also go towards establishing the liability of the body corporate.

386. We recognise that although clauses 73 and 74 go towards establishing a culture of compliance within an organisation, they do represent a departure from the current law. It would be more appropriate if such an approach was considered in a broader review of the criminal law.

387. Furthermore, the submissions raise significant concerns about compliance with the regulatory regime. We therefore propose that clauses 73 and 74 be deleted in order to promote active compliance to control money laundering and terrorism financing risks. Clause 75 should also be removed as it relates only to clauses 73 and 74.

Recommendation

Delete clause 73, clause 74 and clause 75.

Clause 76 – Meaning of a civil liability act

Civil liability burden of proof

388. Clause 76 sets out what constitutes a civil liability act. A reporting entity commits a civil liability act when it:

388.1. fails to conduct CDD as required by subpart 1 of Part 2,
388.2. fails to adequately monitor accounts and transactions,
388.3. enters into or continues a business relationship with a person who does not produce or provide satisfactory evidence of the person's identity,
388.4. enters into or continues a correspondent banking relationship with a shell bank.
fails to keep records in accordance with the requirements of subpart 3 of Part 2
fails to establish, implement, or maintain an AML/CFT programme
fails to ensure that its branches and subsidiaries comply with the relevant AML/CFT requirements.

Submissions

389. One submitter from the banking sector suggested that the burden of proof for civil action should be lifted from the balance of probabilities to the criminal burden of beyond reasonable doubt.

Comment

390. If the burden of proof was raised to a criminal burden then all of the civil liability acts would, in effect, be criminal offences without the requirement of mens rea. Changing the burden of proof in civil cases is beyond the scope of the Bill.

Recommendation

No change.

Clause 89 – Offence and Penalties for civil liability act

Knowingly or recklessly committing a civil liability act and the defence of reasonable steps

391. Clause 89 sets out that it is a criminal offence when a reporting entity knowingly, or recklessly, commits a civil liability act.

Submissions

392. One submitter, from the banking industry, suggested that criminal offences for civil liability acts are not appropriate and that criminal offences should be saved for obstruction of supervisors and breaches of STR-related obligations. They recommended that the provisions within clause 89 should be removed from the Bill.

Comment

393. Where a reporting entity knowingly (or recklessly) breaches their obligations, criminal liability is entirely appropriate. The test for criminal liability is very high and the weight of the offence is proportionate.

394. Clause 89(2) provides a reasonable steps defence for reporting entities who have committed an offence.
Arguably a more complete and appropriate defence is provided for in clause 96 and that the defence within clause 89(2) is unnecessary. It should be deleted and instead should cross-reference clause 96.

It is proposed to extend the defence in clause 96 to apply to other criminal offences in Part 2 of the Bill (this is discussed below). In light of the recommendation to extend the defence within clause 96 to all criminal offences relating to Part 2 of the Bill, it is recommended that the defence provisions within clause 89(2) are deleted from the Bill. Therefore, there is no requirement to explicitly cross-reference clause 96 within clause 89.

**Recommendation**

Delete the defence provisions within clause 89(2).

**Clauses 89-94 and 99-103 – Criminal offences**

**Removal of personal responsibility**

Clauses 89 through 94 and 99 through 103 are criminal offences which both natural and legal persons are subject to.

**Submissions**

One industry representative body submitted that personal liability should be removed from all criminal offences. This suggestion was based on the premise that individual action and criminal behaviour are already covered by section 243 of the Crimes Act 1961 which refers to money laundering.

**Comment**

The criminal offences contained with the Bill are separate from the offence of money laundering set out in the Crimes Act 1961. The criminal offences within the Bill relate to:

- knowingly or recklessly committing a civil liability act
- suspicious transaction reports (failure to report, providing false or misleading information in a report, unlawful disclosure of a report)
- failing to keep or retain adequate records
- obstructing an investigation or a supervisor
- structuring transactions or cross-border transportation of cash to avoid AML/CFT obligations (also known as ‘smurfing’)
- providing false or misleading information to a supervisor or Customs officer
- cross-border transportation of cash.
These offences represent either the actions of a natural person seeking to circumvent the purposes of the Bill, or a reporting entity failing in their obligations which most represent a systemic risk to the detection and deterrence of money laundering and financing of terrorism.

Most of the criminal offences relating to cross-border cash and STR reporting are a continuation of FTRA offences.

**Recommendation**

No change.

**Clauses 93-95 – Strict liability offences**

Clauses 93 and 94 set out criminal offences that are strict liability, or that do not contain mens rea.

**Comment**

These clauses are intended to be strict liability offences. However, the inclusion of the words ‘without lawful justification or excuse’ implies that the offences contain a mental, or mens rea, element. These offences should be constructed to make it clear that they are strict liability offences.

**Recommendation**

Offences within clauses 93 and 94 should make it clear that they are strict liability offences by removing ‘without lawful justification or excuse’.

**Clause 96 – Defence**

**Extension of defences to cover civil and criminal breaches**

Clause 96 sets out a defence for reporting entities who have been charged with a criminal offence that relates to the CDD provisions within Subpart 1 of Part 2. This defence is based on taking all reasonable steps to ensure compliance, or that in the particular circumstances it could not reasonably have been expected to ensure compliance.

**Submissions**

Four submitters, including two submissions from industry representatives commented on the defence within clause 96. Submitters recommended that clause 96 should apply to civil liability acts as well as all criminal offences, not just CDD related offences. As a part of broadening this defence submitters recommended that clause 96 be relocated.
Comment

406. Currently the defence in clause 96 applies only to criminal offences relating to CDD. Extending the defence to cover other criminal offences in Part 2 of the Bill is appropriate.

407. Providing for this defence for civil liability acts is not appropriate. Civil liability is a strict liability, and does not require knowledge. If the reporting entity has knowledge that they are committing a civil liability act then, under clause 89, they have committed a criminal offence.

Recommendation

Widen the defence within clause 96 to all criminal offences relating to Part 2 of the Bill.

No change is recommended to the defence or penalties in relation to civil liability acts.

Clause 127 – AML/CFT supervisors

Reporting entities to have one supervisor

408. Clause 127 provides that there will be three AML/CFT supervisors. Clause 127 also provides that when a reporting entity provides services that are covered by more than one AML/CFT supervisor, the supervisors may agree between them who will supervise the reporting entity.

Submissions

409. Two submitters recommended that clause 127 should explicitly state that one reporting entity can only be supervised by one AML/CFT supervisor. These submitters also suggested that this provision should also extend to DBGs.

Comment

410. A reporting entity should have only one AML/CFT supervisor. While clause 127 does provide for AML/CFT supervisor to agree as set out above, it would be reasonable to amend clause 127 to clarify that a reporting entity will only have one AML/CFT supervisor.

411. One of the conditions of joining a DBG is that all of the reporting entities seeking to join the DBG must be all have the same supervisor. This allows reporting entities that are a part of the same corporate group, to be able to jointly pool their resources and share aspects of their AML/CFT programme and have one AML/CFT Compliance Officer.

Recommendation

State that a reporting entity can have only one AML/CFT supervisor.
Reporting entities seeking to join a designated business group

412. Clause 127(2) only allows AML/CFT supervisors to agree to which AML/CFT supervisor will supervise an entity when that reporting entity offers services that come under the remit of more than one AML/CFT supervisor. It does not allow reporting entities to switch AML/CFT supervisors for the purpose of joining a DBG with other reporting entities.

Submissions

413. Two submitters recommended that clause 127 be amended to allow reporting entities within corporate groups, to apply to change supervisors for the purpose of joining a DBG.

Comment

414. In light of the requirement for members of DBGs to have the same supervisor, the submitter’s suggestion is necessary.

415. We consider that the supervisors should be permitted to ‘switch’ a reporting entity from one supervisor to another on the condition that the reporting entity elects to join a DBG and that the supervisor agrees to the reporting entity joining the DBG.

Recommendation

Amend clause 127 to allow reporting entities to apply to change supervisors for the purpose of electing to join a DBG.

Clause 147 – Regulation making powers

416. Clause 147 provides for regulation making powers to

416.1. prescribe matters that apply to PEPs.

416.2. prescribe additional requirements for AML/CFT Programmes.

416.3. prescribe offences and fines in respect of the contravention or non-compliance with the Bill.

Submissions

417. The Legislation Advisory Committee has suggested that because the requirements of AML/CFT programmes are fundamental to the purpose and operation of the legislation that requirements should be subject to appropriate scrutiny and concern has been expressed that the regulation making power may allow these requirements to be expanded beyond the parameters of the legislation and this is not appropriate. The LAC also had concerns about regulation making powers for PEPs and offences and fines.
Comment

418. The minimum requirements for AML/CFT programmes attract significant compliance costs for reporting entities. Requirements should be clear, certain and subject to robust scrutiny. Implications for adding requirements to enhanced due diligence for PEPs also attract significant costs and to mitigate privacy concerns these requirements should be clear transparent and subject to robust scrutiny.

419. Citizens need absolute clarity about what constitutes an offence and what the penalties will be. Officials do not consider it appropriate to be able to create offences (or fines) in regulation. It is proposed to delete all three regulation making powers from clause 147 and the related provisions in the body of the Bill.

Recommendation

Remove the regulation making powers in clauses:

- 23(b) and 147(j) for additional requirements relating to PEPs.
- 54(n) and 54(o) and 147(a)(vi) for additional requirements in AML/CFT Programmes
- 147(n) for prescribing offences and fines.

Clause 148, 151, 152 and 153 – Exemptions provisions

Supervisors granting exemptions

420. Clause 148 provides for exemptions regulations and contains a set of criteria that the Minister responsible for the Bill must consider before recommending that an exemption regulation is issued. Clauses 151, 152 and 153 provide the Minister to grant exemptions, again with a suite of criteria that must be considered before granting the exemption.

Submissions

421. One submitter commented that the use of regulations for exemptions can be time-consuming and arduous. The submitter supported the provision of a Ministerial exemption making power, but recommended that this should be instead given the chief executive of an AML/CFT supervisor, the supervisor pointed to the Australian AML/CTF Act, which confers the CEO of AUSTRAC with an exemption making power.

422. The Legislation Advisory Committee also commented on the Ministerial exemption scheme and suggested that it could, instead, be a Ministerial Rules system. In addition the Legislation Advisory Committee and the Regulations Review Committee recommended that the Ministerial exemptions be subject to the
Regulations (Disallowance) Act 1989, to ensure an appropriate level of parliamentary scrutiny.

423. The Regulations Review Committee also recommended that clauses 147(b), (g) and (i), which are effectively exemptions, be moved into clause 148 to ensure they are subject to the same controls as the other exemptions regulations, including scrutiny by the Regulations Review Committee.

Comment

424. It is not appropriate for chief executives of supervisory agencies, which include an independent crown entity, to be granting exemptions from statutory obligations. This is especially important in a multi-supervisory model as opposed to a single supervisor model. Ministerial rules are highly flexible and quickly instituted instruments. It is considered that Ministerial exemptions arguably provide better scrutiny and transparency. It is considered that there is enough flexibility (through the ability to waive the 28-day rule) to be responsive to changes in the environment.

425. In order to ensure transparency and scrutiny, all exemptions should be subject to the Regulations (Disallowances) Act 1989.

Recommendation

Relocate regulation making powers set out in clause 147(b), (g) and (i) into clause 148 to ensure they are subject to the same controls as other exemptions regulations.

Amend to make the Ministerial exemptions, as provided for in clauses 151-153, subject to the Regulations (Disallowance) Act 1989.
Part Four: Issues not relating to specific clauses

426. Some of the issues and recommendations raised by submitters did not appear to relate to any specific clause in the Bill. These issues are set out below.

Overview clause

427. The Legislation Advisory Committee suggested to officials that the Bill could benefit from an overview clause that sets out, in plain English, the contents of the Bill.

Comment

428. The suggestion to include an overview clause is an excellent one. The Bill, and the obligations within it, are complex and an overview clause is likely to assist readers of the Bill in understanding its contents and structure.

Recommendation

Amend to include an overview clause.

Defence against civil and criminal action

429. Three submitters raised concerns that reporting entities may end up being exposed to civil and criminal liability, for example if reporting entities breach contracts with customers because they are required to terminate a business relationship under the Bill. These submitters recommended that the Bill include a general defence for reporting entities against civil and criminal action, where they have been acting to comply with the obligations within the Bill.

Comment

430. Submitters have raised concerns that when they do (or omit to do) anything in accordance with the Act, a customer or a third party may lay a claim against them.

431. The Act does not presently provide for immunity against such claims, which may realistically arise. For example, if a reporting entity terminates a business relationship due to the provisions of clause 34, an action in contract may lie against a reporting entity.

432. This is not an appropriate outcome, as the Bill should not create impediments to compliance. By not providing for immunity, the management of potential claims could increase compliance costs.

433. However, this has to be balanced against the right of a customer or third party to bring an action where they are justifiably wronged. As such, officials propose...
including a 'good faith' immunity provision, which would have a reasonable belief that the person was complying with the Act, which would provide for protection against civil or criminal proceedings where a reporting entity (or an officer) is complying with the obligations under the Bill.

434. Such immunity would need to exclude any civil or criminal proceedings under the AML/CFT Bill, to ensure that enforcement actions under the Bill itself are still possible.

**Recommendation**

Provide reporting entities with a defence against civil or criminal proceedings where the civil or criminal breach resulted from a reporting entity operating, as a reasonable person, in good faith with the provisions of the Bill.

**Freezing transactions or accounts**

**Submissions**

435. A submission from an advocacy group suggested that the Bill should provide for reporting entities to freeze accounts and transactions for up to 7 days.

436. One submitter would like immunity where it decides, having submitted an STR, to freeze the transaction or account. This is especially important in terms of being liable under the Terrorism Suppression Act 2002 or the Crimes Act 1961 for facilitating ML or TF.

**Comment**

437. The purposes of this Bill are the detection and deterrence of, rather than combating, money laundering, and countering financing of terrorism. The Bill does not deal with the seizure or forfeiture of criminal proceeds. These issues are appropriately dealt with by the Proceeds of Crime Act 1991, the Terrorism Suppression Act 2002 and the Criminal Proceeds (Recovery Act) 2009. The Bill does not provide for reporting entities to freeze accounts and therefore cannot provide immunity to these actions.

438. It should be noted that suspicion of a transaction, and the filing of an STR, does not automatically constitute wrong-doing. To expressly provide for reporting entities to freeze accounts without due process may not be consistent with principles of natural justice.

**Recommendation**

No change.
Defence against civil and criminal action for AML/CFT supervisors

439. The Bill does not provide AML/CFT supervisors, or their officers, protection from civil or criminal action when they have been carrying out their functions in accordance with the Bill. It is considered appropriate for all AML/CFT supervisors to be granted protection from liability to enable them to carry out their functions properly.

440. The State Sector Act 1988 generally provides for protections from liability for public servants; however these protections do not extend to the Reserve Bank or the Securities Commission as they are not Public Service Departments listed in Schedule 1 of the State Sector Act. The Securities Act 1978 provides adequate protection for the Securities Commission, but protections in the Reserve Bank Act 1989 only relate to powers exercised under that statute.

441. It is proposed, to insert provisions into the AML/CFT Bill that ensure all AML/CFT supervisors, and authorised delegates, are given appropriate protection from liability.

Recommendation

Provide appropriate protection from liability for AML/CFT supervisors (and any authorised delegate) when acting in the course of their duties in the Bill.

Search provisions for Customs officers

442. Security encrypted stored value cards and other BNI in electronic form are methods of transporting money across borders. The Bill broadens the existing cross border cash declaration provisions within the FTRA to include BNI and unaccompanied money. The Bill also confers a specific duty on Customs officers to prevent the movement of cash (including BNI) in certain circumstances.

443. Currently neither the Custom’s and Excise Act 1996 nor any other Act contains provisions to require a person to provide to a Customs officer passwords, encryption keys or information to enable access to a data storage device or other such electronic device. This is not desirable.

444. General powers enabling access to electronic information are currently being considered as part of the Search and Surveillance Bill. It would be feasible to effect a consequential amendment to the AML/CFT Bill via that legislation. However, due to the fact that the timing of the passage of that Bill is less certain and its outcomes are unknown, it is appropriate that the AML/CFT Bill provides for the powers necessary for the enforcement of the Bill’s definition of ‘cash’.

445. It is proposed to amend the Bill to enable Customs officers to effectively carry out their duties in relation to cross border movement of cash. It is also proposed to amend the Bill to insert a complementary provision to establish a duty on persons...
with knowledge of a computer, computer network, or other storage device to assist with access if required. This approach is consistent with the proposals contained in the Search and Surveillance Bill.

**Recommendation:**

Amend the Bill to enable Customs officers to effectively carry out their duties in relation to cross border movement of cash.

Amend to insert a complementary provision to establish a duty on persons with knowledge of a computer, computer network, or other storage device to assist with access if required.

**Outsourcing of supervisory powers**

446. There are potential efficiency gains in providing for supervisors to outsource certain functions to the private sector. Currently the AML/CFT Bill does not provide for this. It is proposed that Bill be amended to enable outsourcing, subject to appropriate safeguards and conditions.

**Comment**

447. To ensure the integrity of the regulatory framework it is appropriate to limit the types of supervisory powers to those that are operational in nature or where the private sector can provide specific skill sets more effectively than the public sector.

448. There are three supervisory functions considered suitable for outsourcing.

448.1. Requiring information from a reporting entity, with notice.

448.2. Carrying out inspections of reporting entities for compliance with the legislation with or without notice.

448.3. Using a qualified third party to assist in investigations.

449. To ensure the consistent application of the legislative framework and the management of AML/CFT risks, and the appropriate collection, use and disclosure of information by third parties, it is proposed that the following safeguards and conditions are put in place:

449.1. Legislation needs to ensure that any decisions arising from outsourced activities rest with the supervisor.

449.2. To ensure that any delegation is carried out transparently, it is appropriate for the legislation to require any conflicts of interest to be declared and managed. It is reasonable to expect that in New Zealand, there will be a scarcity of skilled resources in AML/CFT activity. Many agencies in the private sector may be either reporting entities in their own right as defined under the AML/CFT Bill, or may be contracted to reporting entities in an advisory or audit capacity.
449.3. To ensure transparency and accountability in the exercise of delegated functions, all delegations should be made in writing by the Chief Executive of the supervisory agency. Proof of identity and authorisation must be provided when carrying out delegated functions.

449.4. To ensure that delegated functions are carried out competently it is considered desirable to explicitly require that supervisors are permitted to outsource only to 'suitably qualified' persons.

449.5. To ensure that sensitive information is protected, it is appropriate for the AML/CFT Bill to provide for a prohibition on use and disclosure of any information except to a supervising agency, and associated offences and penalties for tipping off and other unlawful disclosure. The AML/CFT Bill allows supervisors to share personal information and information related to reporting entities. This information is highly sensitive and could include suspicious transactions reports on customers, or employment-related information on employees and managers of reporting entities.

449.6. In addition, the supervisors' protections as set out in the AML/CFT Bill would need to apply to authorised persons insofar as they relate to the powers being delegated (for example, immunity and protections for good faith reporting of STRs).

**Recommendation:**

Amend to allow supervisors to use a 'suitably qualified' third party to:

- require information from a reporting entity, with notice;
- carry out inspections of reporting entities for compliance with the legislation with or without notice;
- assist in investigations.

These delegations should be subject to the following safeguards and conditions:

- any decisions arising from outsourced activities rest with the supervisor;
- any conflicts of interest to be declared and managed;
- all delegations should be made in writing by the Chief Executive of the supervisory agency;
- proof of identity and authorisation must be provided when carrying out delegated functions.

Prohibit the use and disclosure, of any information collected on delegated authority, except to the supervising agency. The Bill should establish associated offences and penalties for tipping off and other unlawful disclosure by persons with delegated authority.
## Appendix One  Terminology and abbreviations

<table>
<thead>
<tr>
<th>Abbreviation / Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti-money laundering and countering financing of terrorism</td>
</tr>
<tr>
<td>AUSTRAC</td>
<td>Australian Transaction Reports and Analysis Centre (this Australian authority is both the Financial Intelligence Unit and supervisor for AML/CFT)</td>
</tr>
<tr>
<td>BNI</td>
<td>BNI are non-cash monetary instruments which may contain the instruction 'pay to the bearer.' The bearer is the person in possession of the BNI. Common examples of BNIs are cheques, promissory notes, traveller's cheques, bearer bonds, money orders and postal orders.</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>DGB</td>
<td>A Designated Business Group</td>
</tr>
<tr>
<td>DIA</td>
<td>The Department of Internal Affairs</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Customer Due Diligence</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FATF Recommendations</td>
<td>The FATF 40 Recommendations on Money Laundering and the 9 Special Recommendations on the Financing of Terrorism</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit. The FIU is a part of the New Zealand Police National Intelligence Centre.</td>
</tr>
<tr>
<td>FTRA</td>
<td>Financial Transactions Reporting Act 1996</td>
</tr>
<tr>
<td>Junket</td>
<td>A junket is where gamblers are flown to the casino, typically from an overseas jurisdiction.</td>
</tr>
<tr>
<td>KYC</td>
<td>Know your customer, this is another term for customer due diligence</td>
</tr>
<tr>
<td>ML</td>
<td>Money laundering</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development. The FATF is administratively attached to the OECD and is housed within the OECD headquarters in Paris, France.</td>
</tr>
<tr>
<td>Predicate Offence</td>
<td>A predicate offence is an offence which generates the criminal proceeds that are laundered. In New Zealand a predicate offence is any offence where the maximum sentence is more than 5 years, commonly referred to as a 'serious offence' (section of the Crimes Act 1961)</td>
</tr>
<tr>
<td>RBNZ</td>
<td>The Reserve Bank of New Zealand</td>
</tr>
<tr>
<td>Reporting Entity</td>
<td>The Bill applies to &quot;reporting entities&quot;, which are financial institutions and casinos.</td>
</tr>
<tr>
<td>SDD</td>
<td>Simplified Customer Due Diligence</td>
</tr>
<tr>
<td>Sec Com</td>
<td>The Securities Commission, which is an independent crown entity.</td>
</tr>
<tr>
<td>STR</td>
<td>A Suspicious Transaction Report, which is submitted by reporting entities to the Financial Intelligence Unit</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorism financing</td>
</tr>
</tbody>
</table>
Appendix Two: List of Submitters

450. The Committee received 39 submissions on the Bill from the following individuals or groups/agencies: The submissions notated (OP) made oral submissions in person before the Committee.

<table>
<thead>
<tr>
<th>No.</th>
<th>Submitters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Nicola Vryenhoek</td>
</tr>
<tr>
<td>2.</td>
<td>Phil Divett</td>
</tr>
<tr>
<td>3.</td>
<td>Anonymous (Private Evidence) (OP)</td>
</tr>
<tr>
<td>4.</td>
<td>Anonymous (Private Evidence) (OP)</td>
</tr>
<tr>
<td>5.</td>
<td>Atu Enua Kuki Airani</td>
</tr>
<tr>
<td>6.</td>
<td>Trustee Corporations Association of New Zealand</td>
</tr>
<tr>
<td>7.</td>
<td>Securities Industry Association (OP)</td>
</tr>
<tr>
<td>8.</td>
<td>AA Insurance (OP)</td>
</tr>
<tr>
<td>9.</td>
<td>Farmers Mutual Group (OP)</td>
</tr>
<tr>
<td>10.</td>
<td>Transparency International (OP)</td>
</tr>
<tr>
<td>11.</td>
<td>New Zealand Retailers Association</td>
</tr>
<tr>
<td>12.</td>
<td>Veda Advantage (OP)</td>
</tr>
<tr>
<td>13.</td>
<td>Munichre NZ Services</td>
</tr>
<tr>
<td>14.</td>
<td>SkyCity Entertainment Group (OP)</td>
</tr>
<tr>
<td>15.</td>
<td>GE Money</td>
</tr>
<tr>
<td>16.</td>
<td>Dun and Bradstreet</td>
</tr>
<tr>
<td>17.</td>
<td>Kiwibank (OP)</td>
</tr>
<tr>
<td>18.</td>
<td>ACE Insurance</td>
</tr>
<tr>
<td>19.</td>
<td>ASB Group (OP)</td>
</tr>
<tr>
<td>20.</td>
<td>Institute of Financial Advisors</td>
</tr>
<tr>
<td>21.</td>
<td>Link Market Services</td>
</tr>
<tr>
<td>22.</td>
<td>Real Estate Institute of New Zealand (REINZ)</td>
</tr>
<tr>
<td>23.</td>
<td>ING</td>
</tr>
<tr>
<td>24.</td>
<td>Westpac New Zealand (OP)</td>
</tr>
<tr>
<td>25.</td>
<td>Australian Bankers’ Association</td>
</tr>
<tr>
<td>26.</td>
<td>IAG</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>27.</td>
<td>Financial Services Federation</td>
</tr>
<tr>
<td>28.</td>
<td>New Zealand Association of Credit Unions</td>
</tr>
<tr>
<td>29.</td>
<td>Investment Saving and Insurance Association</td>
</tr>
<tr>
<td>30.</td>
<td>Anonymous (Private Evidence) (OP)</td>
</tr>
<tr>
<td>31.</td>
<td>Australian Finance Conference</td>
</tr>
<tr>
<td>32.</td>
<td>New Zealand Bankers Association</td>
</tr>
<tr>
<td>33.</td>
<td>New Zealand Institute of Chartered Accountants</td>
</tr>
<tr>
<td>34.</td>
<td>Investment &amp; Financial Services Associate</td>
</tr>
<tr>
<td>35.</td>
<td>Anonymous (Private Evidence)</td>
</tr>
<tr>
<td>36.</td>
<td>Chapman Tripp</td>
</tr>
<tr>
<td>37.</td>
<td>Australian Financial Markets Association</td>
</tr>
<tr>
<td>38.</td>
<td>Insurance Council of New Zealand</td>
</tr>
<tr>
<td>39.</td>
<td>National Council of Women of New Zealand</td>
</tr>
</tbody>
</table>
### APPENDIX 3 – MINOR AND TECHNICAL CHANGES

**TABLE 1 – PROPOSED AMENDMENTS**

All proposed amendments will be subject to Parliamentary Counsel Office drafting.

<table>
<thead>
<tr>
<th>Concern / Points</th>
<th>Submitter</th>
<th>Policy consideration</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definitions and preliminary provisions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Cross references to definitions should be inserted into CLAUSE 4.</td>
<td>Submitter 36</td>
<td>Technical drafting issue for clarity. For example suggestion is to insert into clause 4 cross references like: <strong>code of practice has the meaning set out in section 59</strong></td>
<td>Insert definition cross references into clause 4 for clarity.</td>
</tr>
<tr>
<td>2. Defined terms are not used consistently throughout the Bill – a list should be inserted at the end of each section as per the Income Tax Act in order to clarify meaning.</td>
<td>Submitter 36</td>
<td>Agree that consistency of language is desirable.</td>
<td>Ensure that language is consistent.</td>
</tr>
<tr>
<td>3. Definition of ‘beneficiary institution’ should refer to ‘wire transfers’ instead of ‘electronic transfer of funds’ and ‘beneficiary’ instead of ‘payee’ so that it the Bill is internally consistent.</td>
<td>Submitter 36</td>
<td>Agree the Bill should have consistency of terminology.</td>
<td>Ensure terminology is consistent.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>5.</td>
<td>The term money-laundering is not defined in the Bill, or alternatively the term money-laundering offence should be used.</td>
<td>Submitter 36&lt;br&gt;Submitter 32</td>
<td>Drafting omission</td>
</tr>
<tr>
<td>6.</td>
<td>The element of duration in the definition of business relationship needs careful drafting to ensure that there is clarity about what is expected.</td>
<td>Submitter 29</td>
<td>Officials believe that the clarity provided in this definition is enough to allow reporting entities to determine for themselves, in their business context what types of interactions should constitute a business relationship, and which will not. Guidance will provide further clarification if needed.</td>
</tr>
<tr>
<td>7.</td>
<td>It is not clear that it is the agency receiving information that retains responsibility under the reliance provisions.</td>
<td>Submitter 36</td>
<td>Agreed.</td>
</tr>
</tbody>
</table>

**Standard CDD**
<table>
<thead>
<tr>
<th>8.</th>
<th>Clause 30(5) requires reporting entities to gain <strong>prior</strong> consent before relying on the CDD carried out by another reporting entity. This will result in financial advisors/planners having to enter into multiple agreements with reporting entities to gain consent before conducting CDD on customers. Requirement 30(3) states that it is the reporting entity who is responsible for ensuring that CDD is carried out in accordance with the Act. This is going to mean reporting entities are going to want to have agreements with each adviser/planner to protect their legal position. <strong>CLAUSE 30</strong></th>
<th>Submitter 33</th>
<th>It is not intended to require financial advisors to gain consent from reporting entities in advance of carrying out CDD. FATF is clear that the reporting entity who uses the CDD must remain responsible for ensuring it is done correctly. However an agreement between reporting entities and 3rd parties could assist reporting entities to take action where deficiencies or failures have led to a breach.</th>
<th>Amend clause 30(5) to ensure that consent does not have to be obtained <strong>prior</strong> to a third party reporting entity carrying out CDD.</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Clause 13(g) should be deleted. It is not reasonable to require reporting entities to collect other information that ‘could be reasonably obtained’, as it is unreasonable to require entities to collect unspecified information. <strong>CLAUSE 13</strong></td>
<td>Submitter 32</td>
<td>Agreed. Reporting entities should be able to, as a part of their risk-based approach, ask for additional information as is considered appropriate through their AML/CFT programme.</td>
<td>Amend the Bill by removing 13(g).</td>
</tr>
<tr>
<td>10.</td>
<td>Information verification requirements should be framed as “issued by” not</td>
<td>Submitter 29</td>
<td>Agreed. The policy intent is that verification should be from issued, not obtained</td>
<td>Amend Bill to “issued by”, not “obtained from”.</td>
</tr>
</tbody>
</table>
obtained from" as most documentation will be obtained from customers.

CLAUSE 11

The verification provisions should use consistent wording with the identity provisions (replace use of the word provided with obtained) in order to minimise doubt.

Verification wording for persons acting on behalf of a customer in clause 18(1) simplified DD, should also be consistent with the wording in 14(1) standard DD and 22(1) enhanced DD

For example, SDD allows for information to be prescribed by regulations, and EDD allows it by regulations or codes of practice.

CLAUSE 14, 18 and 22

---

### CDD of Existing Customers/remediation

| 11. The verification provisions should use consistent wording with the identity provisions (replace use of the word provided with obtained) in order to minimise doubt. Verification wording for persons acting on behalf of a customer in clause 18(1) simplified DD, should also be consistent with the wording in 14(1) standard DD and 22(1) enhanced DD For example, SDD allows for information to be prescribed by regulations, and EDD allows it by regulations or codes of practice. | Submitter 36 | Identification and verification requirements should be consistent within and across the three levels of CDD. It is intended that EDD provisions only refer to further prescription by regulation, not by a code of practice. | Ensure consistent wording within identity and verification provisions and with SDD and EDD provisions. Delete reference to codes of practice from clause 22. |

---

### Simplified Due Diligence

<p>| 12. Reference to the New Zealand Security Intelligence Service Act 1969 as a customer is an error. | Submitter 36 | Drafting error, this should reference the New Zealand Security Intelligence Service, not the Act listed. | Delete the words 'Act 1969' from clause 16(1)(c). |</p>
<table>
<thead>
<tr>
<th></th>
<th>Enhanced Due Diligence</th>
<th>Correspondent banking</th>
<th>Shell banks</th>
<th>Trusts</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>Enhanced CDD does not seem to require reporting entities to obtain information on the nature and purpose of the relationship.</td>
<td>CLAUSE 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submitter 7</td>
<td>Drafting omission. EDD should include requiring information about the nature and purpose of the business relationship.</td>
<td>Amend clause 21 to refer to clause 13 and 15(a).</td>
</tr>
<tr>
<td>13.</td>
<td></td>
<td>Submitter 36</td>
<td>Drafting omission. EDD should include requiring information about the nature and purpose of the business relationship.</td>
<td>Amend clause 21 to refer to clause 13 and 15(a).</td>
</tr>
<tr>
<td>14.</td>
<td>Correspondent banking provisions are unclear.</td>
<td>CLAUSE 20</td>
<td></td>
<td>Replace &quot;manager or conducted&quot; with &quot;managed and conducted&quot;.</td>
</tr>
<tr>
<td></td>
<td>EDD is not defined for correspondent accounts that are proposed to be used for payments to, or receipts from, foreign financial institutions. The words ‘are used’ limit application to only those existing relationships.</td>
<td>Submitter 36</td>
<td>Drafting omission. Provision should read ‘are used, or proposed to be used’.</td>
<td>Replace &quot;manager or conducted&quot; with &quot;managed and conducted&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Amend to read ‘are used, or proposed to be used’.</td>
<td>Replace &quot;manager or conducted&quot; with &quot;managed and conducted&quot;.</td>
</tr>
<tr>
<td>15.</td>
<td>In relation to the defining whether a 'shell bank' has a physical presence, the current description of 'managed or conducted' inadvertently captures entities which may not be shell banks.</td>
<td>CLAUSE 36</td>
<td>Drafting issue. It needs to be clear that the intent is that there is physical presence where banking services are managed and conducted.</td>
<td>Remove ambiguity from title of clause 27.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Officials</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>Clause 27 requirements should apply to either or both of new or developing technologies or products</td>
<td>Submitter 36</td>
<td>Requirements in clause 27 apply to new and developing technologies or products</td>
<td>Remove ambiguity from title of clause 27.</td>
</tr>
</tbody>
</table>
technologies and products that favour anonymity. Wording implies that both conditions must be met.

New / developing technologies obligations should be re-worded to cover those that actually create or support customer anonymity, rather than simply “favour”. It could be argued that electronic banking transactions may “favour” anonymity.

CLAUSE 27

Submitter 30

that favour anonymity. The condition that must be met is anonymity.

The policy intent is to require reporting entities to mitigate risks associated with anonymity.

Guidance will be developed to support understanding about favouring anonymity.

Amend the definition of a DBG to require relation to only one of government department, State enterprise or Crown entity

Clause 33 (4) be amended by deleting the reference to ‘the reporting entity’ and replacing it with ‘the entity’.

17. Membership of a Designated Business Group (DBG) should require relation to only one of a government department, State enterprise or Crown entity.

CLAUSE 4

Submitter 36

Drafting error.

Amend the definition of a DBG to require relation to only one of government department, State enterprise or Crown entity.

18. Privacy protection within DBGs should be available to information provided within a designated business group whether or not the entity providing the information is a reporting entity.

CLAUSE 33

Submitter 36

Drafting error.
| 19. | Record keeping of CDD within a DBG should be allowed to be in a central place, as opposed to requiring each member that has that customer to keep the records. This is overly burdensome and costly. Verification information should be able to be held by one member of a DBG. Recommend that the DBG provisions be extended to allow joint compliance reporting. | Submitter 29 Submitter 31 | The DBG arrangements are intended to allow reporting entities within a DBG to share the same ongoing CDD, record keeping, and reporting obligations. Record keeping requirements of the Bill allow a DBG arrangement where one member can keep the CDD records in one location provided that each member who has a business relationship with the customer in question can access those records and can meet their requirements under the Bill. It is intended that joint compliance reporting is provided for under clause 29(1)(b) which allows a reporting entity to adopt a DBG member's AML/CFT Programme (including annual reports). For the avoidance of doubt it is proposed to reword this provision slightly to make it clear that 'adopt' also means do, or use. |
| 20. | Drafting error in privileged communication provisions. Clause 39(1)(a) has inadvertently omitted a reference to one party. | Submitter 36 | Drafting error. In addition the provisions for privileged information should be consistent with the Evidence Act. Amend clause 39 to cross reference section 60 of the Evidence Act. |
refers to confidential communication passing between an agent. It should be between an agent and an agent of a lawyer or client of that lawyer and that lawyer or client should be privileged.

**CLAUSE 39**

21. At present, clause 129 provides for supervisors to co-operate and share information in relation to suspicious transaction reports and information on employees and senior managers. The expectation set out by FATF is that with respect to information-sharing AML/CFT supervisors co-operate domestically and with overseas counterparts more broadly than this.

**CLAUSE 129**

<p>| 22. | Clause 54(c) and (g) should be combined. A distinction does not need to be drawn between CDD and account monitoring in the requirements for AML/CFT Programmes. Account monitoring is part of CDD. | Submitter 36 | Drafting clarification. | Combine 54(c) and (g) so that 54(c) reads 'complying with CDD requirements (including on-going CDD and account monitoring). |
| 23. | There is no provision for entities that | Submitter 36 | A reporting entity who was a natural person | Clarify the designation of an |</p>
<table>
<thead>
<tr>
<th>Clause</th>
<th>Text</th>
<th>Provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>have no employees (e.g. partners and self-employed) to appoint compliance officers other than employees.</td>
<td>(self-employed) could be the compliance officer themselves. An amendment to the designation of an ‘employee’ as a compliance officer to include capture of self employed persons and partners would be useful. ‘employee’ as a compliance officer to include capture of self employed persons and partners.</td>
</tr>
<tr>
<td>34</td>
<td>Termination of business relationship requires refunding balance of account but the Bill prevents this through the prohibition to not transact with the customer. Refund should be permitted with the condition of a STR being filed.</td>
<td>Any transaction required to effect the termination of a business relationship would be acceptable. An STR would not necessarily be required as triggers for terminating a business relationship (such as inability to carry out CDD) will not always constitute a suspicious transaction. Reporting entities will have to consider on a case by case basis whether an STR is required this is required by 34(d). Clause 34(c) should be amended to clarify that the prohibition on carrying out transactions with or for the customer only applies to occasional transactions. Amend the Bill to change the reference to transaction in 34(c) to ‘occasional transaction’.</td>
</tr>
<tr>
<td>25</td>
<td>Court injunctions should be the sole remit of supervisors, the words “any other person” should be deleted.</td>
<td>The provision should not be permissive of any other person as it is only supervisors that are empowered to enforce obligations under this Bill. It is appropriate for other Amend clause 85 to only allow supervisors to seek court injunctions.</td>
</tr>
<tr>
<td>CLAUSE 85</td>
<td>Agencies to work through the supervisor if they are having problems with reporting entities.</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>26.</strong> A problem may arise as a consequence of the requirement in clause 67(d) of the AML Bill (which provides that the report must be provided to a Customs officer “before the cash leaves the control of Customs.”)</td>
<td>The officials need to be informed that the offence of failing to declare cash under section is not committed until the cash is exported. No charges can be laid in respect of cash which is discovered by a Customs officer before a passenger leaves New Zealand because the passenger will be able to argue that he still had an opportunity to make a report and intended to do so, except in the unlikely event that a passenger refuses to make a report when the cash is discovered and then leaves New Zealand with the cash.</td>
<td></td>
</tr>
<tr>
<td><strong>CLAUSE 67</strong></td>
<td><strong>Officials</strong></td>
<td></td>
</tr>
<tr>
<td><strong>27.</strong> Clause 98 incorrectly provides a lower fine and imprisonment term for offences under clause 92.</td>
<td>The penalty should be the same as the other criminal penalties.</td>
<td></td>
</tr>
<tr>
<td><strong>CLAUSE 92</strong></td>
<td><strong>Officials</strong></td>
<td></td>
</tr>
<tr>
<td><strong>28.</strong> Clause 130 (2) empowers supervisors to question people in reporting entities.</td>
<td>An ability to question employees or people representing reporting entities would clarify</td>
<td></td>
</tr>
<tr>
<td>Clause</td>
<td>Description</td>
<td>Recommendation</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>29.</td>
<td>Clause 132 requires supervisors to inform reporting entities of the purposes for which information will be collected. At present, 132 refers to 'purpose' in the singular and this may be too limiting.</td>
<td>Clause 132 is intended to provide transparency and protections for reporting entities with respect to expectations on information collection for AML/CFT purposes and other purposes relating to dual supervisory roles. At present it is unclear as it makes reference to a singular purpose and the intent is that there may be more than one purpose.</td>
</tr>
<tr>
<td>30.</td>
<td>Clause 134 refers to the fact that information collected via the Financial Advisers Act may be relevant for AML/CFT purposes, but is not listed in 134 (2).</td>
<td>Clause 134 seeks to cover regulatory information relevant to AML/CFT supervision. The Financial Advisers Act deals with matters of competence, accountability and supervision of financial advisers, who are generally covered by the AML/CFT definition of 'financial institution'. It is therefore relevant for information-sharing. It is recommended that the FAA is added to the list set out in 134 (2).</td>
</tr>
<tr>
<td>Clause</td>
<td>Description</td>
<td>Issues/Recommendations</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Clause 143</td>
<td>sets out the role of the Ministry responsible for the administration of the Bill. One submitter recommended that the role of the Ministry should be amended. Currently one of the roles of the Ministry is to be responsible for “advising on the overall effectiveness of the AML/CFT regulatory system”. The submitter recommended that this role should be amended to include efficiency because they considered the term “effectiveness” is too narrow and would not include consideration of the cost.</td>
<td>The AML/CFT regulatory system should be effective, efficient and operating at peak. The submitter’s suggestion has merit and clause 143 should be amended accordingly.</td>
</tr>
<tr>
<td>Clause 143 (a)</td>
<td>requires the Ministry responsible for AML/CFT legislation to advise on links to other Ministry initiatives. It has been queried whether this clause should clarify which initiatives are being referred to in the light that the Ministry of Justice may not always be the designated lead in the future. Also, this limitation appears too narrow.</td>
<td>The rationale for the Ministry of Justice being the policy lead on AML/CFT is that essentially the matters at hand relate to the ‘rule of law’. The initiatives that the Bill should refer to are government initiatives. It is recommended that the Bill reflects this.</td>
</tr>
</tbody>
</table>

**CLAUSE 143**
**TABLE TWO – NO CHANGES RECOMMENDED**

<table>
<thead>
<tr>
<th>Concern / Points</th>
<th>Submitter</th>
<th>Policy consideration</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definitions and preliminary provisions</strong></td>
<td></td>
<td></td>
<td>No change recommended.</td>
</tr>
<tr>
<td>1. Definition of Bearer Negotiable Instrument (BNI) and of transaction and how/if it relates to letters of credit in international trade.</td>
<td>Submitter 1</td>
<td>The suggestion is that the definition of BNI should be extended to include letters of credit and bills of lading/airway bills. This is based on the grounds that these documents are evidence of right or title and are easily assigned or transferable. These types of instruments are not legally considered ‘bearer negotiable instruments’. The United States’ ‘Uniform Commercial Code’ governs the issuance and negotiation of negotiable instruments in the United States and is the international standard on BNI. Article 5 specifically excludes letters of credit as BNI and Article 7 excludes bills of lading/airway bills. Letters of credit are not the same type of instrument contemplated by the BNI definition. These are issued between financial institutions as part of international funds transfers. Bills of lading are documents that effect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Definition of Financial Institution should be amended to read &quot;other than a casino who&quot;.</td>
<td>Submitter 14</td>
<td>Casinos do not appear to be covered by the definition unless they offer financial services. Where Casinos do offer financial services, it is appropriate that this aspect of their business is covered by the AML/CFT Bill.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.</td>
<td><strong>CLAUSE 4</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|   | Definition of Financial institution should be reviewed for consistency with other Acts such as the Financial Service Providers (FSP) Act and the Securities Act. Guidance requested as to which entities are intended to be caught by the regime and the definition amended as appropriate. | Submitter 36 | The definition within the Bill is consistent with the FSP Act. Section 5(n) of the FSP Act includes "any other financial service that is prescribed for the purposes of New Zealand complying with the FATF Recommendations, other recommendations by FATF, or other similar international obligations that are consistent with the purpose of this Act."

The definition of Financial institution in the Bill is closely aligned to FATFs. While the definition in the FSP refers to financial services, not institutions it is designed to be consistent with the FATF definition. | No change recommended. |
<p>| 3. | <strong>CLAUSE 4</strong> | | | |
| 4. | It is not clear whether certain trusts are included in phase one or phase two of the reforms. | Submitter 6 | Trusts are covered where they are customers of a reporting entity. | No change recommended. |
| <strong>CLAUSE 4</strong> | | | | |
| 5. | Purpose statement should reflect ‘manage and mitigate’ ML/TF risks rather than ‘detect and deter’ ML/TF. Purpose statement should also be extended to reinforce Trans-Tasman harmonisation objectives. | Submitter 32 | Reporting entities managing and mitigating the risk within their environment will assist in the detection and deterrence of money laundering and terrorism financing at a national level. Cabinet has agreed that Trans-Tasman harmonisation is one of the criteria used to guide decision-making on AML/CFT matters in New Zealand. It is not appropriate to include this in the purpose statement of the AML/CFT legislation, as it is not a purpose of this legislation, and as a criterion for decision-making on AML/CFT matters it is one of many with which it must be balanced. | No change recommended. |
| <strong>CLAUSE 3</strong> | | | | |
| 6. | The Financial Transactions Reporting Act (FTRA) provisions for CDD should be retained and the AML/CFT Bill should be refocused to aim at behaviour and transaction monitoring. | Submitter 17 | The FTRA is no longer FATF compliant; this is a key driver for these reforms. CDD is a critical component in the management of money laundering and terrorism financing risks and central to the | No change recommended. |
| <strong>Standard CDD</strong> | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Bill's objectives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Clause 12(f) requires a reporting entity to conduct CDD in circumstances where the reporting entity suspects that money laundering or terrorist financing may be involved. This needs an &quot;on reasonable grounds&quot; proviso and so does the expression &quot;when doubts arise&quot; in clause 12(e)(ii).</td>
<td>Submitter 34</td>
</tr>
</tbody>
</table>

No change recommended.|

<p>| 8. | It is not clear when a business relationship is &quot;established&quot; for the purposes of this Bill. | Submitter 36 | A common sense approach would be permitted. A business relationship is likely to be established when a customer has | No change recommended. |</p>
<table>
<thead>
<tr>
<th>CLAUSE 12</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td><strong>The Bill and regulations should allow reporting entities to assess risks and put in place the appropriate level of CDD.</strong></td>
</tr>
<tr>
<td></td>
<td>There is concern about the level of prescription that will be put in regulations and how that may circumvent a risk-based approach.</td>
</tr>
<tr>
<td></td>
<td><strong>Submitter 7</strong></td>
</tr>
<tr>
<td></td>
<td>The Bill requires reporting entities to assess risks and take a risk-based approach to due diligence over and above prescribed minimum standards. Some of the detail of those standards could be established through regulations.</td>
</tr>
<tr>
<td></td>
<td>The Bill signals comprehensive consultation on regulations.</td>
</tr>
<tr>
<td></td>
<td>Industry, including representative groups such as Submitter 7, will be consulted on regulations.</td>
</tr>
<tr>
<td>10.</td>
<td><strong>The requirement to conduct CDD on occasional transactions could potentially cover a wide range of business as usual transactions.</strong></td>
</tr>
<tr>
<td></td>
<td>Also, clarity as to how occasional CCD obligations work alongside electronic transactions.</td>
</tr>
<tr>
<td></td>
<td><strong>Several submitters</strong></td>
</tr>
<tr>
<td></td>
<td>There will be a threshold set in regulation that determines what an occasional transaction is. Transactions under the threshold will not attract CDD provisions. There are two types of electronic transactions envisaged. Wire transfers are dealt with separately in the Bill. Other electronic transactions will be from an account holder to another account holder and therefore CCD on those business relationships will have been carried out. The occasional transaction definition will clarify that CDD does not have to be</td>
</tr>
<tr>
<td></td>
<td>No change recommended.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>11.</td>
<td><strong>Clause 12(b) requires CDD for occasional transactions.</strong> One submitter proposed that the FTRA provisions for occasional transactions be retained.</td>
</tr>
<tr>
<td></td>
<td><strong>CLAUSE 12-13 and 29-31</strong></td>
</tr>
<tr>
<td>13.</td>
<td>Request for a unique customer identifier to be made available to reporting entities for identification/verification purposes.</td>
</tr>
<tr>
<td>14.</td>
<td>Reliance on 3rd parties is impractical and will not work in a competitive market environment.</td>
</tr>
<tr>
<td>15.</td>
<td>Clause 13 includes obligations to collect information (such as date of birth) that are not relevant for non-natural persons. Suggest adding in the wording “or”</td>
</tr>
</tbody>
</table>
where that person is not an individual the prescribed information relevant to that type of person" at the end of clause 13(a).

CLAUSE 13

<table>
<thead>
<tr>
<th>CDD of Existing Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>16.</strong> It should be clear that the information required to be obtained under clauses 15 and 19 (information about the nature and purpose of the business relationship) is not required to be verified.</td>
</tr>
<tr>
<td>Submitter 36</td>
</tr>
<tr>
<td>There is no requirement to verify the 'nature and purpose' of a business relationship. Reporting entities are required to regularly review CDD information. There is an express cross reference to clauses 15 and 19 in the obligations under the ongoing due diligence clause.</td>
</tr>
<tr>
<td>No change recommended.</td>
</tr>
<tr>
<td><strong>CLAUSE 15 and 19</strong></td>
</tr>
</tbody>
</table>

<p>| <strong>17.</strong> The requirement to conduct CDD on existing customers (clause 12(e)) is not clear that it only applies to customers with whom the reporting entity had a business relationship before the commencement of Part 2.  |
| Submitter 36  |
| Submitter 34  |
| Submitter 24  |
| The term 'existing' customers is defined in clause 4. The definition of existing customer clearly states that it applies to 'pre-commencement' customers. |
| No change recommended. |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLAUSE 12</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>this is a more accurate term.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLAUSE 29, 30 and 31</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be permitted to rely on other members of the NZX.</td>
<td>Submitter 7</td>
<td>Reliance on NZX members would be permitted in so far as they were reporting entities or otherwise included in the permissions set out in clauses 29, 30 or 31. NZX members are likely to be reporting entities and may be relied upon, provided the requirements of the Bill are met.</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Simplified Due Diligence</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be clear that simplified due diligence means that due diligence is only required to be carried out on the person acting on behalf of the customer and not the customer itself or any beneficial owner.</td>
<td>Submitter 36</td>
<td>The Bill does not contain any requirements to carry out CDD on a customer or beneficial owner of a customer to whom simplified due diligence is permitted to be applied.</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLAUSES 16-19</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Occasional Transactions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clarification is sought about where the Bill allows for a setting of a minimum threshold for wire transfers.</td>
<td>Submitter 4</td>
<td>The definition of occasional transactions provides for applicable threshold values to be set in regulations. It is intended to set an applicable threshold value for wire transfers.</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLAUSE 25</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tourists who are seeking to use money changing services should not have to</td>
<td>Submitter 4</td>
<td>There will be a threshold for occasional transactions set in regulations. Those</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clause 12</td>
<td>Complete CDD for low value transactions.</td>
<td>Transactions under the threshold will not be subject to CDD.</td>
</tr>
</tbody>
</table>

### Beneficial Ownership

| 22. | When a power of attorney changes, full verification of beneficial owners should not be required. | CLAUSE 18 | Submitter 20 | Power of Attorney is an authority to act on a customer's behalf. The person who holds Power of Attorney would qualify for simplified due diligence. Simplified due diligence applies where a person has authority to act and the reporting entity has previously done CDD on the customer (as opposed to the person with authority). Beneficial ownership verification is not required in simplified due diligence obligations. | No change recommended. |

| 23. | Beneficial ownership requirements seem unworkable. Further consultation on the specific requirements should be undertaken. | CLAUSE 9 | Submitter 27 | Beneficial ownership requirements are a core element of the FATF recommendations and the effective management of ML/TF risks. | No change recommended. |

### Enhanced Due Diligence

<p>| 24. | EDD applies to customers from countries that insufficiently apply FATF measures. Reliance on third party CDD is not permitted if the third party is from a country that insufficiently applies | CLAUSE 36 | Submitter 36 | Guidance on countries that are FATF compliant will be developed. | No change recommended. |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>25.</strong></td>
<td>Reporting entities must identify a company with nominee shareholders or shares in bearer form. Nominee shareholding is not disclosed by the share register. It is not possible to know whether shares are in bearer form from company search. Request that circumstances be clarified.</td>
<td>Submitter 36</td>
<td>It is expected that reporting entities will ask customers that are companies to disclose whether they have bearer form, or nominee shareholdings. If the customer confirms this to be the case, the reporting entity is obligated to conduct EDD.</td>
</tr>
<tr>
<td><strong>CLAUSE 20 and 30</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>26.</strong></td>
<td>It is not clear how a reporting entity is to obtain and verify information relating to the source of wealth or funds of a customer. What are benchmarks for complexity and unusual largeness? Guidance is required.</td>
<td>Submitter 36</td>
<td>A reporting entity can obtain the information from the customer. The reporting entity is then required to take reasonable steps to satisfy itself that the information they have obtained as part of enhanced due diligence is correct. This may be able to be done in a variety of ways. Guidance will be provided on this matter. Guidance will also discuss what should be considered when looking for transactions that are unusually large or complex.</td>
</tr>
<tr>
<td><strong>CLAUSE 20</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>27.</strong></td>
<td>With respect to nominee shareholders, 'company' is not defined. The</td>
<td>Submitter 36</td>
<td>The intention is to include overseas registered companies, however it is not</td>
</tr>
</tbody>
</table>
Companies Act definition, would appear to exclude overseas registered companies because they are not in the Companies Act 1993.

CLAUSE 4

considered necessary to include this explicitly as the context makes it apparent that overseas companies are included.

The Bill does not refer to the definition in the Companies Act 1993.

<table>
<thead>
<tr>
<th>28.</th>
<th>How CDD applies to trusts is unclear.</th>
<th>CLAUSE 20</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Upon whom does clause 20(1)(a)(i) impose an obligation to perform CDD as a trust is not a customer, it is a legal entity. It could be settlor, trustee, institutional manager, etc.</td>
<td></td>
</tr>
</tbody>
</table>

Submitter 36

A customer is natural or legal person and therefore can be a legal entity. The customer would be the trust.

CDD information should be obtained about the Trust, from the person who has authority to act on behalf of the trust (e.g. settlor, trustee, institutional manager) or who is establishing the business relationship on behalf of the Trust.

No change recommended.

<table>
<thead>
<tr>
<th>29.</th>
<th>Who is the customer in the context of trusts for the purpose of obtaining information regarding the source of wealth or funds? The source of wealth of the trust is arguably limited to the assets of the trust itself.</th>
<th>CLAUSE 21</th>
</tr>
</thead>
</table>

Submitter 36

The customer is the trust. As described above, the information can be provided by an appropriately authorised officer/delegate of the trust.

What might constitute 'source of wealth' or 'wealth' is a matter dependent on the context and situation.

Further guidance can be provided in codes

No change recommended.
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>30.</strong></td>
<td><strong>It needs to be clarified what 'personal assets' are being referred to in trusts. It is not legally defined.</strong></td>
<td><strong>Submitter 36</strong></td>
</tr>
<tr>
<td><strong>CLAUSE 20</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>31.</strong></td>
<td><strong>Are Unit Trusts' trusts' or 'companies'?</strong></td>
<td><strong>Submitter 36</strong></td>
</tr>
<tr>
<td><strong>CLAUSE 4</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>32.</strong></td>
<td><strong>What constitutes a domestic wire transfer is not clear. The circumstances of an institution being 'in' NZ should be described. Does this mean incorporated or registered?</strong></td>
<td><strong>Submitter 36</strong></td>
</tr>
<tr>
<td><strong>CLAUSE 24</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>33.</strong></td>
<td><strong>$1000 should be the appropriate threshold for occasional transactions for wire transfers; and this threshold should be consistent across all sectors.</strong></td>
<td><strong>Submitter 3</strong></td>
</tr>
<tr>
<td><strong>CLAUSE 4</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# New technologies and products

| 34. | Reporting entities should only have to take all reasonable steps or apply a risk-based approach to prevent new/developing technologies from being used in the commissions of ML or TF. | Submitter 30 | The use of new and developing technologies within a business relationship is, for the most part within the control of reporting entities. It is appropriate that reporting entities should undertake to conduct additional measures to control the use of this technology. This is a core part of FATF Recommendations. | No change recommended. |
|     | Even if measures are taken to prevent the use of new or developing technologies favouring anonymity, if those technologies are subsequently used in the commission of a money laundering offence a reporting entity will not have satisfied the requirement. | Submitter 34 | The extent of such measures will be able to be determined by reporting entities according to the level of risk. | |
|     | As currently written the obligation is absolute and has no consideration of costs or effectiveness. | Submitter 36 | A specific defence in relation to civil liabilities is provided in clause 89. A common law defence of reasonable steps also exists for criminal liability. | |
|     | **CLAUSE 27** | Submitter 27 | | |

# Correspondent banking

<p>| 35. | There needs to be clarity that the definition of correspondent banking does not include non-bank reporting entities. | Submitter 7 | A correspondent banking relationship is defined by the provision of banking services between one financial institution and another. Exemptions from this definition are provided for through regulation if reporting entities are concerned about unintended capture. | No change recommended. |
|     | <strong>CLAUSE 26</strong> | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th>For the purposes of correspondent banking, the 'assessing the adequacy of a respondent bank's controls' in subclause 2(c) is difficult. Regulations are needed to set out the standards and how an assessment can reasonably be performed.</th>
<th>Submitter 7</th>
<th>Guidance will be provided on this matter.</th>
<th>No change recommended.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>CLAUSE 26</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Politically Exposed Persons</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36.</td>
<td>Submitter considers that the customers with relevant criminal histories are high risk. This group of customers has been overlooked in the development of policy on the Bill.</td>
<td>Submitter 2</td>
<td>Recognition of criminal convictions and the risk they present may be best left to reporting entities to ascertain, as a part of their risk assessments and to control for through their AML/CFT Programmes if they deem it necessary. Should this be a significant concern for reporting entities the Bill provides for regulations or codes of practice to address this issue.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37.</td>
<td>Clarify whether senior management approval means multiple or single managers.</td>
<td>Submitter 36</td>
<td>FAFT is silent on this issue. Recommendation 6 only states that reporting entities should obtain 'senior management approval'. It would seem that an appropriate and business sensitive interpretation of this</td>
<td>No change recommended.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CLAUSE 20</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CLAUSE 23</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>would be to require the approval of the most relevant or appropriate senior manager.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ongoing CDD</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39. Ongoing CDD is operationally onerous and inconsistent with a risk-based approach.</td>
<td>Submitter 17</td>
<td>The Bill allows reporting entities to tailor their ongoing CDD methods and interventions according to risk. It provides for regular review of customer CDD. The Bill is silent on the frequency of review (or meaning of regular) as it is intended to be risk-based.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Submitter 29</td>
<td>Clause 28(3) specifically requires reporting entities, when undertaking on-going due diligence and account monitoring, to have regard to the level of risk.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Submitter 15</td>
<td>As part of the AML/CFT Programme reporting entities are also required to have procedures, policies and controls for complying with CDD requirements. This includes on-going CDD and account monitoring and is the appropriate place to determine regularity of these activities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Submitter 34</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Submitter 36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CLAUSE 28</td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40. Recommend clarification on how ongoing CDD impacts on existing customers who are exempted from</td>
<td>Submitter 7</td>
<td>The risk profiles of existing customers, and thus the level of ongoing CDD that is undertaken on them should be ascertained</td>
<td>No change recommended..</td>
<td></td>
</tr>
<tr>
<td>Issue</td>
<td>Recommendation</td>
<td>Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDD.</td>
<td>through a reporting entities risk assessment and AML/CFT Programme. Clause 28(3) specifically requires reporting entities, when undertaking on-going due diligence and account monitoring, to have regard to the level of risk – this applies to all customers.</td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inquiry of the customer could be intrusive.</td>
<td>A reporting entity only needs to contact the customer if they think that the information they hold is no longer relevant or accurate. Account monitoring is essentially a back office function. A ‘review’ of customer information does not require obtaining further information from the customer unless the reporting entity thinks it necessary due to a change in risk profile or, in the case of existing customers, if CDD has not been completed up to the new standard required by the Bill.</td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The use of the terms ongoing due diligence and account monitoring are redundant and are not defined. There is inconsistent language between several clauses in ongoing due diligence</td>
<td>What constitutes ongoing CDD and account monitoring is set out through the requirements as set out in clause 28. The Bill provides for guidance or codes of practice for further clarification if necessary.</td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>43.</strong></td>
<td>Definition is unclear. On one hand, the definition says that at least one member must be a reporting entity, yet it also says that each member must be a reporting entity or a non NZ-resident in a country with AML/CFT supervision.</td>
<td>Submitter 36</td>
<td>The DBG definitions require that each member is either a reporting entity or an overseas reporting entity, and than one member of the DGB is a NZ reporting entity. This is a matter for regulations or codes of practice.</td>
<td></td>
</tr>
<tr>
<td><strong>CLAUSE 4</strong></td>
<td></td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>44.</strong></td>
<td>The Bill should be clear that being part of an overseas DBG is not going to stop reporting entities from joining a DBG.</td>
<td>Submitter 7</td>
<td>The operation of overseas DBGs is not within the control, or scope of the Bill. The Bill does not prevent members of overseas DBG being a member of a New Zealand DBG. The AML/CFT Bill does not have extra-territoriality.</td>
<td></td>
</tr>
<tr>
<td><strong>CLAUSE 29</strong></td>
<td></td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>45.</strong></td>
<td>Verification on buyers should be done on the 'wallet test'; using only those documents which an individual has</td>
<td>Submitter 22</td>
<td>This is a matter for regulations or codes of practice.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Designated Business Groups**

**Electronic Verification for CDD**
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>46.</td>
<td>Are reporting requirements annual?</td>
<td>CLAUSE 57</td>
<td>Submitter 6</td>
</tr>
<tr>
<td></td>
<td>Annual reports are required. The detail of these will be in regulations.</td>
<td>Submitter 6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audits however, must be undertaken every 2 years.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**STR Reporting**

<p>| 47. | STRs should be renamed to Suspicious Activity Reports, Suspicious Matter Reports, Unusual Matter Reports or the like to signal that the scope of suspicious activity is not limited to transactions. | Submitter 32 | STR is a widely recognised term that is used in the FTRA. It has been retained for consistency. |
| 48. | STR reporting should not be required within a prescribed timeframe. Instead this should be “as soon as is practicable”. | Submitter 24 | The provisions within the Bill relating to the timing of STR reporting are consistent with the FTRA and are designed to encourage timely reporting after a suspicion is formed. |
| 49. | Auditors should be allowed to submit STRs, but the auditor should be required to submit the STR to both the reporting entity and FIU. They are not able to do this under the Bill. | Submitter 7 | Auditors are intentionally prohibited from disclosing STR reports to the reporting entity. This is to prevent tipping off should the reporting entity be complicit or negligent in any suspicious matter. |</p>
<table>
<thead>
<tr>
<th><strong>CLAUSE 40</strong></th>
<th><strong>If the STR matter is related to a customer of the reporting entity and not the reporting entity itself, the FIU is able to share the information with the reporting entity where necessary.</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>50.</strong> Currently there is a protection for privileged communications by lawyers in relation to disclosure of STRs.</td>
<td><strong>Submitter 33</strong></td>
<td>STRs can contain highly sensitive information and the risks of tipping off must be carefully controlled. As such reporting entities are not permitted to share STR information with tax advisors. They are only able to share STR information with the FIU (any legal counsel).</td>
</tr>
<tr>
<td><strong>CLAUSE 39</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>51.</strong> An Australian entity operating in NZ should be able to share STR information with members of its DGB.</td>
<td><strong>Submitter 34</strong></td>
<td>Sharing STR information by an Australian reporting entity will depend on information sharing provisions in the Australian regime.</td>
</tr>
<tr>
<td><strong>CLAUSE 33</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Record Keeping</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>52.</strong> Records should be able to be thrown out after a sensible period of time.</td>
<td><strong>Submitter 7</strong></td>
<td>The purpose of record keeping is to assist with investigations and law enforcement. Destruction of documents that are still relevant to a relationship or individual will defeat this purpose.</td>
</tr>
<tr>
<td>Destruction should be allowed where updated replacement documents have been obtained.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLAUSE 46</td>
<td>The record keeping provisions only require retention of verification information that is reasonably necessary to enable reconstruction of the information obtained. Therefore updating of records would be allowed under the Bill as currently drafted. The Bill provides for further guidance through codes of practice and guidelines.</td>
<td></td>
</tr>
<tr>
<td>53.</td>
<td>Bill requires destruction of records as soon as practicable after a period of no less than 5 years. How can as soon as practicable be attached to a timeframe that is not finite?</td>
<td></td>
</tr>
<tr>
<td>Submitter 7</td>
<td>After 5 years have passed reporting entities must adopt an &quot;as soon as is reasonably practicable&quot; approach to record destruction. No change recommended.</td>
<td></td>
</tr>
<tr>
<td>54.</td>
<td>Bill should explicitly allow for electronic record keeping.</td>
<td></td>
</tr>
<tr>
<td>Submitter 15</td>
<td>There is nothing in the Bill to prevent this. No change recommended.</td>
<td></td>
</tr>
<tr>
<td>Submitter 27</td>
<td>The Bill requires that records must be readily convertible into the written form and the English language. If, electronic storage meets this test then it can be used. No change recommended.</td>
<td></td>
</tr>
<tr>
<td>Submitter 31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>55.</td>
<td>If 3rd party verification is allowed then the record keeping requirements should</td>
<td></td>
</tr>
<tr>
<td>Submitter 27</td>
<td>3rd party verification is allowed. No change recommended.</td>
<td></td>
</tr>
<tr>
<td>Page 56.</td>
<td>be modified to require reporting entities to keep record of the verification notice, as opposed to the physical document or form of verification.</td>
<td></td>
</tr>
<tr>
<td>CLAUSE 47</td>
<td>The only requirement is that reporting entities must retain records that are reasonably necessary to enable the nature of the evidence used for identification and verification to be readily identified at any time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clause 47(2)(b) expressly provides that if it is not practicable to retain the actual evidence (such as a passport or photocopy of a passport) the record must contain any information that is reasonably necessary to enable that evidence to be obtained. A customer’s name, date of birth and passport number would be sufficient.</td>
<td></td>
</tr>
<tr>
<td>Page 57.</td>
<td>Record keeping should be risk-based.</td>
<td></td>
</tr>
<tr>
<td>CLAUSE 46</td>
<td>FATF does not envisage a risk-based approach to record keeping. Record keeping is a fundamental aspect of the detection of ML/TF. All records should be kept to facilitate this process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No change recommended.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The intention is to capture the name of the employee who handled the transaction. Employees may be required to assist law enforcement officers in the reconstruction of the transaction and investigation. A suspicious transaction report may not always have been filed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No change recommended.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CLAUSE 46</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>58.</strong> Record keeping requirements are significantly different from tax administration requirements due to the link to an enduring business relationship. Guidance on this should be provided.</td>
<td>Submitter 36</td>
<td>Record keeping requirements have been developed with reference to FATF Recommendations. Guidance material will be provided.</td>
</tr>
<tr>
<td><strong>CLAUSE 46</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Risk assessment and AML/CFT Programme**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>59.</strong> Clauses 53 and 54 should be reworded to be purpose focussed (like the Australian legislation) rather than outcomes focussed.</td>
<td>Submitter 25</td>
<td>These provisions are setting out obligations, not the way in which reporting entities should meet them.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td><strong>CLAUSES 53 and 54</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>60.</strong> The risk assessment should be more prescriptive by making it clearer what factors should be taken into account in determining ‘types of customer’. Recommend a specific amendment to require reporting entities to take into account public, and readily available information pertaining to customers/individuals prior criminal convictions for money laundering or</td>
<td>Submitter 2</td>
<td>The AML/CFT Bill contains high level indications of what is required in the risk assessments and AML/CFT Programmes. The high risk customers currently specified within the Bill are those specifically referred to in the FATF Recommendations (e.g. Trusts, PEPs). How ‘types’ of customer are relevant in risk assessments is a matter that reporting</td>
<td>No change recommended.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>61.</td>
<td>Concerns about the level of the obligations for AML/CFT Programme and risk assessment for retailers operating in low risk environments.</td>
<td>CLAUSE 54 and 55</td>
<td></td>
</tr>
<tr>
<td></td>
<td>entities themselves are best placed to determine within their own context.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Where there is evidence of particularly significant or more universal risks, codes of practice or guidelines will be developed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The national risk assessment and sectoral risk assessments provided by the FIU and supervisors will provide guidance on this point. The risk assessment needs to be flexible to accommodate changing environments and therefore requirements in legislation are not appropriate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>62.</td>
<td>Clause 57 requires each reporting entity to produce an annual report on its risk assessment and AML/CFT Programme. Is this really necessary?</td>
<td>CLAUSE 57</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Retailers will not be covered in phase 1 of reforms.</td>
<td>Submitter 11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Decisions about coverage of entities in phase 2 of reforms will be informed by an assessment of risks conducted by the FIU.</td>
<td>No change recommended.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The annual report will give supervisors information about how reporting entities are implementing the obligations of the Bill in a holistic and meaningful way without requiring reporting entities to submit all three documents.</td>
<td>Submitter 27</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No change recommended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audits should only be every 3 years. Frequency of audit should be left to negotiation between supervisors and reporting entities. <strong>CLAUSE 56</strong></td>
<td>Submitter 30</td>
<td>The FATF Recommendations require reporting entities to “maintain” an independent audit function. 3 yearly audits would be out of step with other international requirements for audit frequency and is unlikely to be FATF compliant. It should be noted that Australia incorporates an internal audit into the annual reporting process. A set requirement for every 2 years provides clarity and certainty to industry and supervisors and meets FATF Recommendations.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>63.</td>
<td></td>
<td>Submitter 29</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64.</td>
<td>For reviews of risk assessments and programmes, it is not clear how frequently reviews should be undertaken. If annual or biennial reviews are envisaged, the legislation should clearly state this. It is hard to know whether a single review is sufficient to meet the term of clause 56. <strong>CLAUSE 56</strong></td>
<td>Submitter 36</td>
<td>Reviews should be undertaken as and when the need arises. This will vary substantially for reporting entities. Some reporting entities may be operating in a static environment and will not need reviews as often as those operating in a dynamic environment. Reporting entities are best placed to make these judgements in consultation with supervisors. The legislation is silent on this. Further guidance on this point can be provided.</td>
</tr>
</tbody>
</table>
| Guidance or criteria needs to be developed to describe what the regulator will be expecting of an audit/review, and who can undertake and audit.  
Sub-clause 56(4) A person appointed to conduct an audit is not required to be a chartered accountant within the meaning of section 19 of the Chartered Accountants of NZ Act or qualified to undertake financial audits. This is confusing/redundant and should be deleted. Institute members should not be singled out.  
CLAUSE 56 | Submitter 33 | Guidance can be provided.  
Sub-clause 54(4) responds to potential concerns that hiring qualified accounts may be cost prohibitive for smaller entities.  
No change recommended. |
|---|---|---|
| Clause 34(b) should be deleted as 34(c) is sufficient.  
Terminating the account could see money going back to the launderer.  
CLAUSE 34 | Submitter 14 | Clause 34(b) refers to the termination of a business relationship; subclause (c) refers to the conducting of occasional transactions which are outside of a business relationship. Both provisions are considered necessary.  
Termination of a business relationship when CDD is not able to be performed adequately is explicitly recommended by FATF.  
No change recommended. |

**Prohibitions**
These obligations are intended to prevent the use of the financial system for money laundering, not to seize illegal funds.

Seizure of illegal funds is carried out through the Criminal Proceeds (Recovery) Act 2009 (which replaces the Proceeds of Crime Act 1991).

### Supervisors and FIU issues

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **67.** | "Supervisors should have a power to recognise equivalence of particular or comprehensive aspects of the Australian regime, or AML/CFT regimes of recognised countries." | "Submitter 32
Supervisors do not need a specific power to promulgate a code of practice or guidance on which countries sufficiently meet with FATF requirements." |
| **CLAUSE 129** |   | No change recommended. |
| **68.** | "Would like a definition of "any reasonable time" for the conducting of on-site inspections for example "usual time of business" or hours of trading." | "Submitter 6
It is not feasible to provide certainty of hours of business for searches within primary legislation, as there are a range of businesses covered under the AML/CFT Bill, with varying opening hours."
|   |   | No change recommended. |
| **CLAUSE 130** |   |   |

It is expected that supervisors will act appropriately and in good faith. It is considered that 'any reasonable time' will be interpreted as during the usual time of business for a given reporting entity.
<table>
<thead>
<tr>
<th></th>
<th>Request strict requirements for enforcement officers when dealing with commercially sensitive / confidential information when conducting on-site visits.</th>
<th>Submitter 6</th>
<th>Supervisors are only empowered to collect and use information during the course of their activity in the ways set out in the Bill. Collection of information above and beyond those purposes would not be lawful.</th>
<th>No change recommended.</th>
</tr>
</thead>
<tbody>
<tr>
<td>70.</td>
<td>Enforcement officers, including supervisors, must produce identity cards if they are to search premises. Request further information about ‘identity cards’, including assurances about a limited number of issuers so that authenticity can be readily and easily confirmed.</td>
<td>Submitter 6</td>
<td>There is a requirement for supervisors and enforcement officers to produce identity cards. The only issuers will be supervisors or the New Zealand Police for their enforcement officers. Supervisors are defined by statute and there are a limited number of them.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td>71.</td>
<td>An occupier is entitled to be present during a search of premises, but loses this right if they impede the search. Request a definition or guidance regarding what may amount to “impede” in clause 120.</td>
<td>Submitter 6</td>
<td>This is a matter that can be addressed through guidance.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td>72.</td>
<td>Request a clause allowing an occupier/reporting entity to have nominated representatives to accompany searchers where a search</td>
<td>Submitter 6</td>
<td>Nothing in the Bill as currently drafted prohibits this. A common sense approach would be permitted. The term occupier could refer to more than one occupier.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td>Clause</td>
<td>Original Text</td>
<td>Comment</td>
<td>Recommended Change</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>---------</td>
<td>--------------------</td>
<td></td>
</tr>
<tr>
<td>73.</td>
<td>The Commissioner of Police receives suspicious transaction reports. The Commissioner's powers may be delegated to a constable. Request for the Bill to be amended to require the Commissioner to advise reporting entities of the employees that are authorised to received STRs.</td>
<td>Submitter 15</td>
<td>The Bill provides that a constable to whom power is delegated is, in the absence of proof to the contrary is presumed to do so in accordance with the delegation. In practice, all STRs are submitted to the Financial Intelligence Unit of the Police. It is expected that general guidance from the Commissioner would clearly state the unit to whom the power has been delegated to.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td>74.</td>
<td>Want guidance regarding the degree of proof required to utilise clause 121(2).</td>
<td>Submitter 6</td>
<td>It would need to be demonstrated that enforcement officers/constables did not take all reasonable care.</td>
<td>No changes recommended.</td>
</tr>
<tr>
<td>75.</td>
<td>Want a process to challenge retention of items that have been seized.</td>
<td>Submitter 6</td>
<td>Items seized have to be returned within 90 days unless they are relevant to proceedings or other actions set out in the Bill. Failure to do so is unlawful.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td>76.</td>
<td>Information-sharing powers are broad and include Income Tax Act. Want assurances about a clear procedure in terms of activating use of clause 131 (power to use information obtained as an AML Supervisor in other capacity)</td>
<td>Submitter 6</td>
<td>Income Tax Act in included due to tax evasion being a predicate offence for money laundering under the Crimes Act 1961. Clause 131 addresses circumstances</td>
<td>No changes recommended.</td>
</tr>
</tbody>
</table>
and vice versa) in light of clause 132 (restriction on power to use information).

CLAUSE 131 and 132

where an AML/CFT supervisor is a regulator under another statute. This clause recognises that information may be relevant for law enforcement purposes in both statutory roles. Clause 132 requires the AML/CFT supervisor to disclose to the person providing the information the purpose for which it will be used.

<table>
<thead>
<tr>
<th>77. AML supervisors should be required to consult on codes of practice.</th>
<th>CLAUSE 61</th>
<th>Submitter 7</th>
<th>This is already provided for through clause 61. No change recommended.</th>
</tr>
</thead>
<tbody>
<tr>
<td>78. The Bill should provide for reporting entities to freeze accounts and transactions for up to 7 days. The Commissioner should be given the power to direct financial institutions to initially freeze accounts for a period of 7 days.</td>
<td></td>
<td>Submitter 10</td>
<td>Any freezing or seizure regime must contain adequate systems for checks and balances in order to preserve natural justice. Freezing and seizure of assets is covered by the Proceeds of Crime Act (soon to be replaced by the Criminal Proceeds (Recovery Act) 2009), and the Terrorism Suppression Act 2002. No change recommended.</td>
</tr>
</tbody>
</table>

<p>| Civil and Criminal Offences and Penalties |
| --- | --- | --- |
| 79. Clause 89(1), which establishes offences and penalties for civil liability | Submitter 14 | In determining whether to bring a criminal prosecution against a reporting entity in No changes recommended. |</p>
<table>
<thead>
<tr>
<th>Acts, should require that the conduct represents a systemic failure and not be immaterial. <strong>CLAUSE 89</strong></th>
<th>relation to knowingly / recklessly committing a civil liability act, supervisors are likely to consider a wide range of tests such as materiality, systemic risk, level of previous engagement.</th>
<th>No change recommended.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLAUSE 90</strong> 90(b) should require actual suspicion, not just ‘reasonable grounds’</td>
<td>If a reporting entity fails to meet what would be expected of a reasonable person involved in the submission of STRs, this appropriately constitutes a breach. There needs to be an objective test (such as reasonable grounds) to guards reporting entities actively not forming suspicions. Reporting entities should be acting in good faith and ensuring that staff have adequate training, knowledge and experience to meet a &quot;reasonable grounds&quot; test.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td><strong>CLAUSE 96</strong> &quot;All reasonable steps&quot; should be removed from clause 96(a). Instead the requirement should be that the individual took reasonable precautions and exercised due diligence.</td>
<td>The test of reasonable steps is used consistently throughout the Bill. The term &quot;exercised due diligence&quot; is not used elsewhere within the Bill. The terminology within the Bill should be consistent.</td>
<td>No change recommended.</td>
</tr>
<tr>
<td><strong>CLAUSE 82</strong> The offence relating to record keeping of STRs should require systemic failure</td>
<td>Clause 89 provides that a criminal offence requires a reporting entity to &quot;knowingly or</td>
<td>No change recommended.</td>
</tr>
<tr>
<td>83.</td>
<td>Offence for structuring transactions to avoid obligations under the Bill should be reworded to a customer or beneficial owner, not a 'person' as this includes both reporting entities/staff and customers.</td>
<td><strong>CLAUSE 99</strong></td>
</tr>
<tr>
<td>84.</td>
<td>In clauses relating to structuring of cross-border transactions to avoid AML/CFT requirements it is not clear what constitutes 'avoidance' for the purposes of clauses 99 and 106. The penalty is too high. The bar should be set at 'evasion' rather than avoidance. Avoidance is not defined.</td>
<td><strong>CLAUSES 99 and 106</strong></td>
</tr>
<tr>
<td>85.</td>
<td>Rather than a prohibition of &quot;setting up a facility for a customer under a false</td>
<td><strong>Submitter 34</strong></td>
</tr>
<tr>
<td>Customer name without reasonable excuse” it would be more feasible to have an offence of providing a reporting entity with false, misleading information or documents. This would be consistent with Australian legislation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely to constitute an offence under the Crimes Act 1961. The offence as currently drafted is intended to incentivise reporting entities to ensure that their customers are not using false information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CLAUSE 35

<table>
<thead>
<tr>
<th>Clause 3 states the purpose of the Bill. Suggestion that the purpose clause should contain an explicit purpose of achieving harmonisation with the Australian AML/CFT framework.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The significance of the interdependency of the New Zealand and Australian financial sectors is reflected in the AML/CFT reforms. The basic framework and risk-based approach adopted in Australia is largely reflected in the Bill. Compatibility with Australia’s AML/CFT regulatory requirements where consistent with New Zealand’s circumstances and requirements is one of eight key criteria for guiding AML/CFT reform. It is not necessary to create a purposive statement on harmonisation in the Bill. No change recommended.</td>
</tr>
</tbody>
</table>

### Other

<table>
<thead>
<tr>
<th>All regulations that can affect the setting or altering of minimum compliance standards should be in clause 148 which sets out the purposes of regulations relating to the application of the Act.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clause 147 and 148 deal with different types of regulations which are subject to different criteria. Regulations covered by clause 148 are subject to a more explicit set of criteria. No change recommended.</td>
</tr>
<tr>
<td>CLAUSE 148</td>
</tr>
<tr>
<td>---</td>
</tr>
</tbody>
</table>
| 88. | Clause 148 should require the Minister to consider "whether the making of the regulation would promote the risk-based approach provided for under the AML/CFT regulatory regime". | This suggestion duplicates the Minister’s obligations as set out in 148 (d), (e) and (f) which require consideration of (among other things):  
- the level of regulatory burden on a reporting entity; and  
- whether the making of the regulation would create an unfair advantage for a reporting entity or would disadvantage other reporting entities; and  
- the overall impact that making the regulation would have on the integrity of, and compliance with, the AML/CFT regulatory regime. | No change recommended. |
| 89. | The Kiwisaver Act (2004) and regulations which relate to coverage under the FTRA should be carried over in the new Act.  
This is because Kiwisaver is an opt-out programme that cannot accommodate CDD before joining. | The FTRA provisions within the Kiwisaver Act and regulations relate only the FTRA.  
An ability to exempt the Kiwisaver scheme exists through regulations under the Bill. | No change recommended. |
<p>| 90. | This submitter gave support to policies that foster flexibility in delivering | The remittance card facility regulations will be considered for continuation under the | No change recommended. |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>financial services products to Pacific Island nations e.g. remittance card facility.</td>
<td>new regime. No comments on this submission as they are all outside of the scope of the AML/CFT Bill.</td>
<td></td>
</tr>
<tr>
<td>Many other recommendations outside the scope of the Bill, relating generally to NZ-Cooks foreign relations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>91.</strong> The National Coordination Committee’s (NCC) role in evaluating the reforms should be focussed on effective and efficient achievement across the whole system including both reporting entities and supervisors.</td>
<td><strong>CLAUSE 144</strong> Consideration of any economic efficiency outcomes arising from the reforms is problematic because its cost and benefits must be measured against a black economy that we are unable to accurately quantify. However, crime reduction outcomes can be assessed through a suite of indicators. Government has directed officials to report back on an evaluation framework for the AML/CFT reforms. The regulatory system needs to consider effectiveness of supervision and delivery by reporting entities. We consider that the Bill covers both. It is intended that mechanisms for reporting entities concerns to be heard or raised with the NCC will be established operationally.</td>
<td><strong>No change recommended.</strong></td>
</tr>
<tr>
<td>At present the provisions appear to relate only to the effectiveness of supervisors.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>