

Implementation of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Regulations and Codes of Practice DISCUSSION DOCUMENT

February 2010



Safer Communities Together Kaupapa whai Oranga mo te iti me te rahi

Table of Contents

Information

Section One – Introduction

- 5.....Purpose of this document
- 6.....The AML/CFT Act
- 7.....Regulatory regime
- 8.....Scope of the regulatory framework
- 9.....Commencement timeframes

Section Two – Exemptions, inclusions and thresholds

- 10.....Exemptions
 - 10.....Temporary exemptions for second phase entities
 - 12.....Exemptions where financial activity on a very limited basis
 - 13.....Exemptions for low risk products and services
- 16.....Inclusions
 - 16.....Bearer negotiable instruments
- 17.....Applicable thresholds
 - 17.....Occasional transaction threshold for financial institutions
 - 17.....Occasional transaction threshold for casinos
 - 18.....Stored value products
 - 19.....Travellers' cheques
 - 20.....Money orders and postal orders
 - 20.....Currency exchange
 - 20.....Beneficial ownership
- 22.....Other partial exemptions and reduced measures
 - 22.....Debt collection
 - 22.....Reduced CDD measures for insurance products
 - 23.....Insurance products closed to new customers
 - 23.....Reduced CDD measures for non-bank deposit takers
 - 23.....Reduced measures for workplace-based superannuation funds
 - 24.....Low value superannuation funds
 - 24.....Overseas pension accounts for certain countries
 - 25.....Special remittance card facility
 - 25.....Exemption from address verification for Casinos
- 26.....Wire transfers

Section Three – Customer due diligence

- 28.....Basis for verification
 - 32.....Documentary identity verification
 - 34.....Electronic identity verification
 - 36.....Other non-face to face identification and verification procedures
- 38.....Standard due diligence
- 39.....Simplified due diligence
- 40.....Enhanced due diligence

Section Four - Third party relationships

- 43.....Reporting entity and customer relationships
- 43.....Reliance on third parties
- 43.....Pooled accounts

Section Five – Institutional arrangements

- 45.....Designated Business Groups
 - 45.....Network agents and sub-agents in the money remittance industry
 - 46.....Conditions for membership
- 47.....Additional factors to be considered in risk assessments
 - 47.....Private banking

Appendix 1 - Timeframes and priorities for regulatory development

Appendix 2 – References

Information

The Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (AML/CFT Act) was passed on 16 October 2009. Regulations and codes of practice need to be developed to support the regime set up by the AML/CFT Act. This public document invites discussion and comment on preliminary policy for the regulatory regime that sits under the AML/CFT Act. This document seeks initial views on proposed requirements for reporting entities. Formal consultation for reporting entity obligations is expected in early May 2010.

Any comment on this information document should be provided to the Ministry of Justice by 5pm Friday 19 March 2010, and should be sent to:

Email: international.crime@justice.govt.nz

Post:

Attention: International Criminal Law team
Ministry of Justice | Tahu o te Ture
PO Box 180
Wellington 6401

Publication of submissions, the Official Information Act and the Privacy Act

The Ministry does not intend to publish comment that it receives on this document. However, any comment will be subject to the Official Information Act 1982 and may, therefore, be released in part or full. The Privacy Act 1993 also applies.

If you do provide comment on the document, please state if you have any objections to the release of any information contained in your submission. If so, please identify which parts of your submission you are requesting to be withheld and the grounds under the Official Information Act 1982 (OIA) for doing so (e.g. that it would be likely to unfairly prejudice the commercial position of the person providing the information). Any grounds for withholding information under the OIA must be related to the information within a document, not to the document itself.

Disclaimer

Views expressed in this information document are the views of the Ministry of Justice and do not reflect Government policy.

Readers are advised to seek specific advice from an appropriately qualified professional before undertaking any action in reliance on the contents of this information document. The Crown does not accept any responsibility whether in contract, tort, equity or otherwise, for any action taken, or reliance placed on, any part, or all, of the information in this document, or for any error or omission from this document.

Acknowledgment

The Ministry would like to thank members of the Government inter-agency working group comprising the Ministry of Economic Development, Ministry of Foreign Affairs and Trade, New Zealand Police, Reserve Bank of New Zealand, Department of Internal Affairs, Securities Commission, and State Services Commission, along with New Zealand Customs Service, that have contributed to the development of this document.

Section one – Introduction

Purpose of this document

1. A Public Information Document setting out preliminary thoughts on the make-up of the regulatory regime was released in tandem with the introduction of the AML/CFT Bill. In addition to receiving feedback on the Public Information Document, representatives from the Ministry of Justice and supervising agencies conducted a series of workshops with representatives of the financial and casino industries in November 2009. Feedback from the Public Information Document and the workshops were used to inform the content of this document. This document has been prepared by the Ministry of Justice in consultation with AML/CFT Supervisors and the Financial Intelligence Unit of the New Zealand Police.

Consultation process on the regulations and codes of practice

2. We are now at a stage to test some initial thinking with industry. This document:
 - 2.1. presents an approach for some regulations and/or codes of practice and invites submissions on the content of the proposal
 - 2.2. presents options for an approach for regulations and/or codes of practice and seeks feedback from industry on the preferred approach
 - 2.3. seeks information from industry on a range of issues to assist the development of further proposals for regulations or codes of practice
3. As well as submissions on this discussion document, we wish to continue engaging with industry representatives over January and February. This process is intended to inform the basis of a package of detailed proposals on regulations and codes of practice.
4. Following this process, we will develop a formal consultation document with near-final proposals which is intended to be provided to industry in May 2010. Following submissions on that document, it is anticipated that the final proposals will be put to Ministers and Cabinet in July 2010 at which stage a decision on implementation timeframes would also be taken and communicated to industry.

Consultation on the national risk assessment and the sectoral risk assessment

5. Supervisory agencies are in the process of surveying industry to assess the money laundering and terrorism financing risks in the sectors under their mandate. Simultaneously, the Financial Intelligence Unit of New Zealand Police (FIU) is developing a draft national risk assessment. The national risk assessment under development will be focussed on money laundering typologies at a high level. Sitting under the national risk assessment will be sectoral risk assessments, issued by Supervisors, which will provide more sector-relevant detail. It is envisaged that the national risk assessment and sectoral risk assessments will assist reporting entities and provide good context for the business level risk assessments. A process for involving industry in the development of the national and sectoral risk assessments is under discussion.

The AML/CFT Act

6. The Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 (the Act) engages the assistance of financial institutions and casinos (reporting entities) in detecting and deterring money laundering and terrorism. The Act builds on the existing obligations on financial institutions to carry out AML/CFT activity under the Financial Transactions Reporting Act 1996 (FTRA). The new legislation brings New Zealand into line with the international standards set out by the Financial Action Task Force (FATF).
7. Under the Act reporting entities will have a range of responsibilities including:
 - 7.1. developing and maintaining a risk assessment and a risk-based AML/CFT programme
 - 7.2. customer identification and verification
 - 7.3. ongoing customer due diligence
 - 7.4. suspicious transaction reporting (STR)
 - 7.5. record keeping
 - 7.6. auditing and annual reporting.

Overarching risk-based approach

8. The FTRA sets out universal AML/CFT measures. A risk-based approach underpins the new Act, the key principle being that businesses are well-placed to make decisions as to how to manage and mitigate money laundering and terrorism financing risks. The Act effects this by requiring reporting entities to formally assess AML/CFT risks in their own business' context and to develop sound programmes in proportion to those risks. Reporting entities will be asked to:
 - 8.1. manage the risks associated with identity fraud and the use of anonymity within complex company and trust structures
 - 8.2. observe the customer's transaction behaviour, focussing on those who are a higher ML/TF risk
 - 8.3. actively report suspicions to the police.
9. AML/CFT activity is an important tool for combating crime. Well-targeted and prioritised AML/CFT activity will be of considerable value in detecting and investigating money laundering and terrorism financing. As well, the intelligence will be used to build investigations to combat financial and drug-related crime, organised crime and terrorism. In broadening the coverage of entities and applying a more targeted and risk-based approach to AML/CFT, we expect that the Police will receive significantly broader and enriched intelligence compared to the existing regime.

Two phases of AML/CFT reform for coverage of entities

10. The application of AML/CFT responsibilities for businesses is being approached in two phases. The first phase largely covers financial institutions and casinos; the second phase will potentially extend coverage to real estate agents, lawyers, accountants, conveyancers, bullion dealers, jewellers and other high value dealers. The original timeframe for considering the coverage of second phase entities was February 2009. Any consideration of coverage of second phase entities has been suspended. The timeframes for coverage of second phase entities will not be considered further until late 2010.

Regulatory regime

Policy criteria for regulatory development

11. The Act sets out the high level responsibilities placed on reporting entities. There are a number of further decisions that need to be taken to complete the regulatory framework. Decision-making for the Act was guided by agreed policy criteria. The same criteria will also be applied to the development of regulations and codes of practice. The criteria are:
 - 11.1. 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
 - 11.2. 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
 - 11.3. compatibility with Australian regulatory requirements where consistent with New Zealand's circumstances and requirements
 - 11.4. 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
 - 11.5. consistent regulation and supervision across sectors where feasible, while at the same time recognising sector differences
 - 11.6. transparent regulation, rules and sector guidance that are accessible and provide certainty to business and Supervisors
 - 11.7. effective and coordinated implementation (including information sharing mechanisms) to achieve the overall objectives of the framework and
 - 11.8. 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.
12. All criteria must be considered when developing proposals, but some criteria will be more or less relevant depending on the circumstances where intervention is desired. The criteria will also be used in determining which level of intervention; regulation, codes of practice or non-binding regulatory guidance is appropriate.

Regulations

13. The AML/CFT Act sets out core minimum standards which are designed to meet the FATF Recommendations. The Act also contains a range of regulation-making powers. In the AML/CFT context, regulatory instruments are useful for dealing with risks that change in the medium term, such as thresholds for different products, new and developing products and changing business delivery channels. Exemptions are key regulations for managing risks that may change over time. Exemptions and thresholds for different entities, products, services and transactions are discussed in this document.

Codes of practice

14. Section 63 provides for 'codes of practice' which are intended to operate as a 'safe harbour' for delivery of different aspects of AML/CFT responsibilities. The Ministers responsible for AML/CFT Supervisors (the Reserve Bank, the Department of Internal Affairs and the Securities Commission) are responsible for developing codes of practice relevant to their respective sectors. Codes of practice may also be used to clarify the extent of coverage of aspects of the legislation.
15. Codes of practice offer flexibility and scope for innovation, in that reporting entities may either comply with the code of practice (i.e. incorporate it into the AML/CFT programme) or opt out of the code of practice (or provisions within the code of practice) and adopt an equally effective method of delivering the same obligation. Reporting entities that choose to opt out of a code of practice must advise the relevant AML/CFT Supervisor. Advising a Supervisor of an intention to 'opt out' of the code of practice, however, does not constitute Supervisor approval of the reporting entity's actions. The requirement is intended to assist Supervisors in focusing their supervisory activity.
16. In determining whether a reporting entity has failed to comply with provisions in the Act, a court must have regard to any code of practice in force.
17. Codes of practice may be applied either universally or on a sector specific basis. Managing consistency between sectors and ensuring that the regime does not create ML/TF vulnerabilities are important considerations. This document discusses codes of practice that are intended to be applied universally.

Guidelines and general guidance

18. Less formal instruments include guidance by AML/CFT Supervisors or the FIU and/or industry-developed guidance. It is envisaged that much of the regime will operate through this less formal means of delivering AML/CFT policy although, as guidance would not be a compulsory part of the regime, it is not detailed here.

Comment sought: *This document sets out proposals and options for the use of different instruments. As you consider the issues at hand, comment is invited on the preferred choice of instrument as well as the content of the instruments.*

Scope of the regulatory framework

19. The next stage in the process is to provide financial institutions and casinos with certainty about the scope and shape of the regime so that business planning may begin. Based on feedback received to date, we understand that clarifying the extent of entities' responsibilities in the following key aspects of the regime are important:
 - 19.1. The intended coverage of the AML/CFT Act via exemptions and inclusions to provide certainty as to which businesses, products, transactions and services do or do not attract AML/CFT responsibilities along with any thresholds and/or conditions for exemptions
 - 19.2. The remaining core elements of the AML/CFT regime that may need to be described in the regulatory framework which include:
 - 19.2.1. clarification of the coverage of the regime with respect to which entities and products the Act applies to and which products and services may be subject to reduced CDD measures

- 19.2.2. determining the basis for identity verification of customers and other relevant CDD provisions
 - 19.2.3. application of provisions relating to reliance on third parties
 - 19.2.4. setting thresholds and limits on the degree to which beneficial ownership must be determined
 - 19.2.5. the eligibility attached to the formation of 'designated business groups' (which allow related groups of entities to share elements of AML/CFT programmes).
20. There is scope for issuing a number of codes of practice on different risk-based responsibilities set out in the Act. So far, officials have received feedback from some sector groups that less regulation and codification is preferred. The scope of the issues set out in this document is premised on this feedback.
21. The table in appendix one sets out all areas of the regime that are being considered for further development. The table describes regulations and/or codes of practice that we understand are:
- 21.1. needed immediately (over the next six months) for business planning purposes
 - 21.2. needed less immediately (over the next 18 months) but which are also required prior to implementation.
22. At this stage it is not proposed to prescribe further requirements beyond the scope described in the table, unless significant issues emerge or it is desired by reporting entities.

Comment sought: *Your feedback is sought on the proposed scope of the regulatory regime; in particular, we are interested in whether there are any other issues that need to be prioritised over the next six months to support planning for implementation.*

Commencement timeframes

23. Cabinet earlier agreed to a commencement timeframe of approximately two years, contingent on further consultation with industry. Government agencies representing Supervisors have also been working towards an approximate two year implementation period as of enactment.
24. Submissions from industry on the AML/CFT Bill provided a wide range of views on an appropriate implementation timeframe. Many submitters considered that the implementation timeframes should be contingent on certainty about the regulatory framework.

Comment sought: *Assuming that the formal consultation will provide sufficient clarity about the shape and scope of the regime, further views on implementation dates are invited.*

Section two – Exemptions and inclusions

Exemptions

Background and context

25. The Act provides for partial and full exemptions from AML/CFT obligations. There are two main types of exemption – exemption by regulation and exemption granted by the Minister responsible for the AML/CFT regime. Under section 154(1)(a) regulations may be made to grant exemptions for transactions, products and services from all or any provisions of the legislation. Section 157 provides for the Minister responsible for the AML/CFT regime (the Minister of Justice) to grant exemptions for entities and classes of entities, or transactions and classes of transactions, from all or any provisions. Under section 157 the Minister may grant exemptions unconditionally or subject to any conditions. This section provides for the Minister, in certain circumstances, to grant reporting entities exemptions on a case by case basis.
26. This document seeks information that will assist the development of regulations that will provide for exemptions from all or part of the regime. This document should not be interpreted as comment on the breadth of coverage of the Act. It is considered that codes of practice or guidance may provide further information in this respect.

Criteria for exemptions

27. To be consistent with FATF standards, exemptions, whether granted by regulation or by the Minister, need to have robust justification. Situations generally considered justifiable against FATF standards are where there is little risk of money laundering or terrorist financing activity occurring. The AML/CFT Act sets out the general criteria that need to be considered for exemptions, including:
 - 27.1. the purposes of this Act and the Financial Transactions Reporting Act 1996
 - 27.2. the risk of money laundering and the financing of terrorism
 - 27.3. the impact on the prevention, detection, investigation, and prosecution of offences
 - 27.4. the level of regulatory burden on a reporting entity
 - 27.5. whether the making of the regulation would create an unfair advantage for a reporting entity or would disadvantage other reporting entities
 - 27.6. the overall impact that making the regulation would have on the integrity of, and compliance with, the AML/CFT regulatory regime.
28. It is also useful to consider the consistency of any exemptions with those of New Zealand's key financial trading partners, Australia, the United Kingdom, and the United States.

Temporary exemptions for second phase entities

Temporary exemptions for entities currently covered under the definition of the Financial Transactions Reporting Act (FTRA)

29. Financial institutions currently covered under the Financial Transactions Reporting Act 1996 (FTRA) that are intended to be moved across in the second phase of coverage need to be temporarily exempted from the AML/CFT Act definition of 'financial institution'. A transitional exemption would apply to:

- 29.1. real estate agents who receive funds for the purpose of settling real estate transactions
- 29.2. the New Zealand Racing Board
- 29.3. lawyers (or an incorporated law firm) who receive funds for the purpose of
 - 29.3.1. deposits or investments
 - 29.3.2. settling real estate transactions
- 29.4. conveyancing practitioners (or incorporated conveyancing firm) who receive funds for the purpose of:
 - 29.4.1. deposits or investments
 - 29.4.2. settling real estate transactions
- 29.5. an accountant who receives funds for the purposes of deposit or investment.

Activities captured by AML/CFT Act which are not captured under the FTRA

- 30. The AML/CFT Act also describes a broader range of financial activity from that expressed in the FTRA. However certain entities, for which these activities attract coverage, are intended to be incorporated into the second phase of reforms. It is proposed that a transitional exemption be applied to this type of unintended capture.

Other retailers, dealers and auctioneers of high value or luxury goods, works of art, cars, and yachts

- 31. Money launderers use high value and luxury items to launder money through a range of mechanisms, commonly including:
 - 31.1. cash payments in large amounts, with the goods being either on sold or returned
 - 31.2. goods being used as payment, e.g. being delivered to a third party address either locally or internationally.
- 32. Businesses and retailers dealing in, and auctioneering, high value or luxury goods including bullion, jewellery, works of art, cars, and yachts will be considered for coverage during the second phase. Some of the activities carried out by retailers or high value dealers, for example when they set up accounts for customers, provide in-store consumer credit and accept deposits may or may not attract coverage under AML/CFT Act definition of 'financial institution'. High value dealers and retailers are intended to be considered during the second phase for AML/CFT coverage.

Temporary exemptions for wholesale market instruments

- 33. Commodities futures trading attracts AML/CFT responsibilities under the AML/CFT Act. Electricity is a commodity that is capable of being bought, sold and traded. Most consumers buy electricity on contract from retailers, who, in turn purchase electricity on the wholesale market. Generators compete in the electricity spot market to generate electricity to satisfy demand. Spot market buyers (i.e. retailers and large industrial users) will typically enter into financial contracts with spot market sellers to hedge their exposure. These financial contracts could be considered a form of futures contract. However, the money laundering risks of such hedging contracts are relatively low.
- 34. Other market instruments with similar low AML/CFT risks may also trigger AML/CFT responsibilities. It is intended that these market instruments are considered for coverage during the second phase of reform. Examples of markets that will be considered for either exclusion or inclusion during the second phase include the:

- 34.1. fishing quota market
- 34.2. emissions trading market.

Businesses that carry out pawnbroking activity

- 35. Pawnbroking activity is regulated under the Second-hand Dealers and Pawnbrokers Act 2004 (SDPA), which operates a licensing regime. Pawnbroking as an activity falls under the definition of 'credit contracts' as set out in the Credit Contracts and Consumer Finance Act 2003 (CCCFA) and falls under the definition of 'financial institution'.
- 36. However, due to potential overlap in regulation of CDD and reporting requirements under the SDPA, it is appropriate to further consider coverage of pawnbroking in the second phase of reform.

Treatment of government agencies covered under the first phase

- 37. A number of government agencies may fall within the definition of financial institutions for reasons of providing central banking or settlement services or through funds management of public monies. These may include:
 - 37.1. the Reserve Bank of New Zealand
 - 37.2. the Treasury
 - 37.3. the Debt Management Office
 - 37.4. ACC
 - 37.5. the Earthquake Commission
 - 37.6. the Guardians of the New Zealand Superannuation.
- 38. This area of exemptions requires considerable policy resource. Priority is being given the aspects of AML/CFT regulatory development that affect the private sector. Exemptions for government agencies will be developed later in 2010, after progress is made on private sector related issues.

Exemptions for financial activity on a very limited basis

- 39. The range of financial activity in the AML/CFT Act extends to a financial activity that is carried out '*in the ordinary course of business*'. Further, section 6 clarifies that the AML/CFT Act applies only to the extent that a business carries out the financial activities described in the definition of 'financial institution'. Many non-financial sector businesses carry out certain activities which are undertaken in the ordinary course of business and which are financial in nature; these activities are often carried out on a very limited basis and/or are otherwise a low ML/TF risk.
- 40. There are two ways of dealing with exemptions for situations involving low risk, low volume financial activity conducted where it is not the main business activity.

Option 1: General exemption for retailers and other non-financial service providers

- 41. The UK regulations provide a general exemption for non-financial institutions from coverage where they engage in financial activity on an occasional or very limited basis. The exemption is for low volume/low value financial activity which is ancillary to the main business as determined by a suite of criteria. Conditions that might be used to exempt entities from the definition of financial institutions in NZ are that:
 - 41.1. the main activity is not that of a 'financial institution or casino'

- 41.2. annual turnover in the 'covered' activity is less than \$120,000 NZ (the UK uses 64,000 pounds)
 - 41.3. the financial activity they engage in is limited to a value of less than \$2000 NZ per customer (in a one off or in a series) (the UK uses 1000 pounds)
 - 41.4. the activity does not exceed 5% of the turnover of their total business
 - 41.5. the activity is not money remittance
 - 41.6. the activity is not company or trust provision services
 - 41.7. the activity is not company or trust formation services
 - 41.8. the activity is not a charitable trust
 - 41.9. the activity is only provided to customers of the business' main activity and is not offered to members of the public who are not in a business relationship with the business (ie purchasing goods or services off the business).
42. This type of general exemption might carve off activities including:
- 42.1. operating a Christmas club
 - 42.2. operating hire purchase agreements within a retail business.
43. We note that a generic exemption may not meet with the level of capture intended by the FATF unless it is tightly constrained and is defensible in terms of assessed risk. Further work would be required in order to justify this approach.

Option 2: Exemptions for entities on a case by case basis

44. The second approach, modelled on the Australian regime, is to apply exemptions on a case by case basis against the exemption criteria. This approach would place an obligation on reporting entities, either by industry-based or individual representation, to put a case to the Minister of Justice setting out the rationale for any exemptions.

Comment sought: *What is your view on the different approaches to exemptions, noting that the two approaches are not necessarily mutually exclusive.*

Exemptions for low risk products and services

45. Some financial products potentially have low enough ML/TF risks to warrant partial or full exemptions from the AML/CFT Act. These are some life insurance risk-based products, funeral insurance products, some securities, the selling of government bonds, corporate treasury functions and some parts of the security industry.

Life insurance

46. Products offered by life insurance companies are primarily aimed at transferring the financial risk of a certain event – such as premature death or outliving savings in retirement - from the insured to the insurer. Customers buy life insurance contracts for which they remit stated payments and are guaranteed a minimum payment as designated at death or some other specified time. A customer may be a natural person, or a legal person, and there could also be beneficial owners involved. The beneficiary of the contract may be the customer or it may be a third party to the relationship between the insurer and the customer.
47. Life insurance policies that can be cashed in could be used for money laundering where they allow “dirty” money to be put in and “clean” money to be taken out in the form of an

insurance company cheque. An alternative typology is to borrow legitimate funds against a life insurance policy that is funded with illicit proceeds.

48. Similarly, annuity contracts allow a money launderer to exchange illicit funds for an immediate or deferred “clean” income stream. Further issues may arise from factors such as (but not limited to) the assignment of the legal right to the benefit of the contract, the provision of a “cooling off” period, various intermediaries, and cross border elements to the relationship. Key insurance products that are attractive to money launderers include term and whole life insurance, and fixed and variable annuities, commonly activated through brokerage channels.
49. There are two main types of insurance which are quite different in ML/TF vulnerability.
 - 49.1. Investment policies - where the main objective is to facilitate the growth of capital by regular or single premiums. Common forms are whole life, universal life and variable life policies. These are potentially higher risk products.
 - 49.2. Risk-based protection policies - designed to provide a benefit in the event of specified event, typically a lump sum payment. These are arguably lower risk products.
50. Examples of life insurance products which might be low ML/TF risk might be those that insure for risk only, such as accidental death benefit entitlements as part of travel insurance.

Preferred approach

51. It is proposed to exclude pure risk-based life insurance products from the types of activity described in the definition of ‘financial institution’; this exemption would ensure that insurance businesses that only offer these products are not obliged to apply AML/CFT measures.

Funeral policies

52. A funeral policy is a life insurance policy, often issued by a friendly society, for the sole purpose of providing funeral benefits to pay for the funeral of the insured person. These policies are a nil to low money laundering/terrorism financing risk.

Preferred approach

53. It is appropriate to exempt such policies from the operation of the AML/CFT Act.

Securities

54. The securities sector is vulnerable to ML/TF in a number of respects, including its speed in executing transactions, its global reach, and its adaptability. Moreover, the securities sector is unique in that it can be used both to launder illicit funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Transactions associated with money laundering and predicate securities offences, including insider trading, market manipulation and securities fraud, are often difficult to distinguish.
55. Conversely, there may be situations in the securities sector which represent much lower or negligible ML/TF risk and could be considered for exemptions.
56. We are seeking feedback on treatment of the issuance of shares by a reporting entity to its employees, the issuance of securities or derivatives, or options for securities or derivatives in government agencies and the treatment of share registries.

Comment sought: Can you provide information of the nature and extent of risk which may be associated with the activities described?

Are there other activities in relation to either the insurance or securities sector that should be considered for exemption or inclusion?

Corporate treasury functions

57. Australia recently consulted industry on exemptions for 'corporate treasury' functions provided within corporate groups to remove the unnecessary financial and administrative burden in cases where a corporate treasury can, in practical terms, be said to be lending to 'itself'. The fact that a corporate group is lending to itself should not necessarily qualify the group for coverage under the AML/CFT Act. An exemption for this type of activity is being considered.

Comment sought: We are interested in hearing about the size and nature of corporate treasury lending in New Zealand, both when they occur within New Zealand and between local and overseas parents or subsidiaries to determine whether this is also appropriate in New Zealand.

Security guards and coverage of transportation of cash by security firms

58. Occupational regulation of security guards is provided for under the Private Investigators and Security Guards Act 1974. The FTRA clarifies that merely because that person carries on business as a security guard within the meaning of section 4 of the Private Investigators and Security Guards Act 1974 does not mean that they are included in the definition of financial institution.

Preferred approach

59. It is intended that this clarification continues through to the AML/CFT Act. However, security firms that transport cash and other bearer negotiable instruments on behalf of customers may still be covered in the first phase of reforms in so far as they fall under the definition of financial institution where they 'transfer money or value for, or on behalf of, a customer'.

Safety deposit boxes in the accommodation industry

60. The accommodation industry commonly provides certain financial services to travellers including the provision of safety deposit boxes. It may be onerous for these businesses to run AML/CFT programmes when these activities are peripheral to the main business activity although ML/TF risks need to be managed and mitigated.
61. Exemptions for safe deposit boxes for traveller accommodation are provided for in Australia. Specifically this exemption applies only if the facility is located either:
- 61.1. in the room of the registered guest and controlled by the registered guest; or
 - 61.2. outside the room of the registered guest but within the place of the traveller accommodation and controlled by the provider of the traveller accommodation.

Preferred approach

62. We consider that use of safety deposit boxes does not present a significant ML risk when assessed against the cost for the industry in complying with the obligations of this

Act. We consider it appropriate to mirror the Australian exemptions for accommodation based safety deposit boxes in New Zealand.

Comment sought: *Are there other products or situations that may present low to negligible risk that attract obligations that will be operationally difficult to manage? Please provide information about the type of products or nature of the situation and rationale for why they should be considered for exemption.*

Inclusions

Bearer negotiable instruments

63. 'Stored value cards' is a generic term for a wide variety of products that can be used to load funds onto and then exchange for goods or services, with many stored value cards allowing the balance to be withdrawn as cash. Stored value cards are ordinarily considered to be a form of bearer negotiable instrument.
64. However, stored value cards are not, at this point, included in the definition of a bearer negotiable instrument (BNI). Consideration should be given to including stored value cards into the definition of BNI.
65. A number of stored value cards are able to be used internationally and can have the cash withdrawn from them at any ATM or financial institution that accepts Visa.
66. Stored value cards present ML/TF risk when they are issued and, if the balance is able to be withdrawn in cash, when someone attempts to 'cash in' a stored value card.
67. The purpose of having an occasional transaction threshold is so that when someone who is not your customer attempts to use your services for a high value cash or BNI transaction, their identity is verified. This way if any suspicious activity is detected, law enforcement can readily obtain the customer's information.
68. Therefore when someone presents a stored value card above the occasional transaction (OT) threshold, it would be beneficial for them to be subject to the same AML/CFT processes as if they have presented the same amount in cash.
69. The Act's definition of BNI is also important to the cross-border transportation of cash declaration system set out in sub-part 6 of Part 2 of the AML/CFT Act.

Preferred approach

70. Given the potentially high ML/TF risks of high value stored value products, and the loophole that inaction on this matter would present for money launderers, we propose that stored value cards are included in the definition of a bearer negotiable instrument through a regulation under section 153(b).

Applicable thresholds

71. A number of aspects of the AML/CFT Act come into force once a transaction is, or a customer uses products or services that are, above an applicable threshold. Thresholds are a form of exemption. The use of thresholds recognises that while a particular product may be vulnerable to ML/TF, applying the full suite of AML/CFT requirements would carry compliance costs that are not commensurate to risk, particularly for low value products.

Occasional transaction threshold for financial institutions

72. The FATF Recommendations state that the occasional transactions threshold for financial institutions should, at the most, be equivalent to €15,000 or US\$15,000. New Zealand's current occasional transaction threshold is NZ\$10,000 under the FTRA. In Australia, the cash reporting threshold is AUD\$10,000.
73. The level needs to balance compliance costs against the intelligence losses and risks of not detecting and deterring money laundering and other predicate offences. Further work is underway on assessing the intelligence benefits of different thresholds.
74. It should be noted that where an applicable threshold is specified for particular products or services (such as wire transfers or currency exchange) that this would take precedence over the general occasional transaction threshold.

Options

75. One approach is to retain the status quo at the level of the FTRA which is \$10,000, but we are willing to consider a case for a threshold that is similar to the Australian approach (AUD\$10,000 or NZ\$12,500).

Comment sought: *Is your organisation comfortable with an occasional transaction threshold of \$10,000? If not, why not?*

Are you able to describe and/or quantify the business impact of setting the threshold at NZ\$10,000 compared to (for example) NZ\$12,500?

Occasional transaction threshold for casinos

76. Law enforcement and media reports indicate that criminals typically launder money through casinos by exchanging illicit cash for casino chips and then either:
- 76.1. hold the chips for a period of time then cashing them in for a casino cheque or having the casino wire the money elsewhere
 - 76.2. use the chips as currency to purchase drugs, with the drug dealer later cashing in the chips
 - 76.3. use the chips to gamble in hopes of generating certifiable winnings.
77. Criminals also use casinos to launder counterfeit money as well as large currency notes that would be conspicuous and difficult to use elsewhere, and which may be marked by undercover law enforcement officers. Suspicious activities at casinos often involve customers structuring transactions to avoid recordkeeping or reporting thresholds, using agents to cash-out multiple transactions for an anonymous individual, providing false documents or identifying information, or layering transactions to disguise their source.

78. The occasional transaction threshold for casinos needs to balance compliance costs against intelligence benefits and take into account higher money laundering risks. Further work is underway to assess the intelligence benefits of different thresholds.

Preferred approach

79. The FATF Recommendations state that the occasional transactions threshold for casinos should, at the most, be equivalent to US\$3000/€3000. The preferred approach, at this stage, is to apply a threshold consistent with the level recommended by FATF (NZ\$5,000 - \$6,000).

Comment sought: *Please provide evidence of any benefits of applying a higher threshold. What volume of transactions would not be captured by a higher threshold?*

Stored value products

80. Stored value cards are products that are used in place of cash with cash values loaded into them on a pre-pay basis. 'Stored value cards' is a generic term for a wide variety of products that can be used to load funds onto and then exchange for goods or services. There is an ever-widening variety of stored value products including electronic products and traditional financial products. While some of these products are not immune to ML/TF risks, capturing the full range of businesses that supply and redeem them would be too costly and administratively unwieldy.
81. Stored value cards provide a compact, easily transportable, and potentially anonymous way to store and access cash value. Open system cards lower the barrier to the payment system, allowing individuals without a bank account to access illicit cash via ATMs globally. Closed system cards, primarily store gift cards, present more limited opportunities and a correspondingly lower risk as a means to move monetary value out of the country.
82. The experience in other countries is that some stored value products are a significant risk for both money laundering and terrorism financing. In assessing stored value cards there are five essential factors that need to be considered. These are whether:
- 82.1. the product has some level of maximum storage (either at any one point in time or an annual total, or both)
 - 82.2. the card allows for cash or money withdrawals
 - 82.3. the product can be reloaded with funds
 - 82.4. the product can be used internationally
 - 82.5. the degree to which ownership can be transferred.

Non-cash redeemable gift, store, phone and bus cards

83. There are a wide variety of store cards and gift cards. Most are non-redeemable and, in New Zealand, have a maximum loading of \$1000. These products are typically used as a cash replacement system designed, in part, for customer convenience and have a limited number of vendors that they can be used to purchase goods or services. These cards are sold at a wide range of retail outlets.
84. The ownership of these products can, in most situations, be transferred. Some are reloadable, eg Farmers Gift Card and Warehouse Gift Card although they are generally used in closed systems, and are not generally used internationally (Prezzie Card excepted).

85. Non-redeemable, low value store, bus, and phone cards have low ML/TF risks. The high compliance costs associated with attracting AML/CFT responsibilities for a wide range of retail outlets for low value, non-redeemable stored value cards outweigh the ML/TF detection and deterrence benefits.

Cash redeemable cards

86. Redeemable cards such as the Loaded card or Cash Passports carry more significant ML/TF risks. Many can be reloaded, have high value limits (eg NZ\$15,000), can be used internationally and are easily transferable.
87. The re-loadable nature of these products is a ML/TF risk that can be, in part, controlled through the use of a maximum value (typically in conjunction with an annual maximum loading value). However, these cards represent higher ML/TF risks than non-reloadable cards and therefore should have a lower exemption threshold.
88. An applicable threshold for low-value stored value cards is clearly desirable.

Preferred approach

89. The preferred approach is to provide for two thresholds to reflect the different ML/TF risks that non-cash redeemable and cash redeemable cards represent as follows:
- 89.1. One for cards with a maximum value of less than NZ\$2500, on the condition that the balance of the card cannot be withdrawn in cash
- 89.2. Another for stored value cards (re-loadable or not) which do allow cash withdrawals on the condition that the:
- 89.2.1. maximum value of the card, at any one time, is less than NZ\$1000
- 89.2.2. annual maximum value is no more than NZ\$10,000.

Comment sought: *How many stored value cards do you or are you likely to sell? If you don't support this threshold please provide evidence to support this point of view.*

Travellers' cheques

90. Travellers' cheques carry inherent money laundering risks as they can be used internationally and there is no inherent maximum value. However, there are also mitigating features, in that ownership of travellers' cheques cannot be reloaded, and due to the requirement for the recipient to sign them upon redemption they cannot be transferred.
91. We consider that, given the risks associated with travellers' cheques, and the non-transferability and biometric links to the customer, a threshold for the issuing of travellers' cheques would ensure that obligations are targeted at the greatest risk.
92. In New Zealand, travellers' cheques are predominantly sold by businesses that would otherwise be reporting entities under the AML/CFT Act. However, some businesses such as travel agents also sell traveller's cheques to their customers. Any threshold will need to carefully balance managing ML/TF risks with the possibility of unintended capture and increased customer inconvenience.

Preferred approach

93. A threshold of \$5000 would allow for non-reporting entities to still sell travellers' cheques and allow reporting entities to rely on the internal business processes to control ML/TF risk at these low levels.

Money orders and postal orders

94. Money orders and/or postal orders from most countries are generally made out to a payee and are for a fixed amount. Typically, they represent low values. Unlike travellers' cheques, they can be issued by convenience and grocery stores and in post offices.
95. In the United States there is a maximum value of \$1000 for domestic (US) postal money orders, and \$700 for international postal money orders. Any more than this amount and the reporting entity must conduct CDD. In the UK the maximum for a postal order is £250. New Zealand Post offers money orders up to a maximum of NZ\$1000.
96. As with travellers' cheques, money orders and postal orders can be used internationally but generally there is a maximum amount and they cannot be reloaded.
97. While they may be susceptible to structuring to avoid any threshold value we consider that a low applicable threshold when issuing money and postal orders will both adequately disrupt money laundering and terrorism financing, while not unnecessarily impeding on legitimate business.

Preferred approach

98. The preferred approach is to adopt an applicable threshold of NZ\$1000 in relation to money and postal orders.

Currency exchange

99. Currency exchange services are covered under the Act. Currency transactions can be considered reasonably high risk as these transactions involve cash, which is easily transferable. However, currency exchange transactions are common place, and an unduly low threshold would increase compliance costs and create customer inconvenience.

Preferred approach

100. We consider that an applicable threshold of NZ\$1000 for foreign exchange would adequately allow for a high volume of currency exchange in New Zealand whilst balancing ML/TF risks inherent in these types of transactions.

Beneficial ownership

101. The AML/CFT Act requires a reporting entity, as a part of customer due diligence to identify, and take reasonable steps to verify the identity of, a customers' beneficial owner. The Act defines a beneficial owner as someone who either:
 - 101.1. exercises effective control over the customer
 - 101.2. owns a prescribed threshold (set in regulations) of the customer.
102. Section 15 sets out the Act's identity requirements. Reporting entities must obtain the beneficial owner's:
 - 102.1. full name
 - 102.2. date of birth
 - 102.3. address
 - 102.4. source of wealth or source of funds (if the customer or beneficial owner is subject to enhanced customer due diligence).

103. The beneficial ownership threshold needs to reflect the money laundering and financing of terrorism risks that legal entities such as trusts, companies and limited liability partnerships present. Also relevant are other examples of ownership or control thresholds being used in New Zealand law, as well as the international standard applied in AML/CFT regulation.

Option one: 20%

104. A beneficial ownership threshold of 20% would be consistent with the Reserve Bank of New Zealand Act 1989's definition of a 'controlling interest'. In addition, the Takeovers Act sets out that when a shareholder of a company that is publicly listed (or has 50 or more shareholders) tries to hold more than 20% of the shares, then they must initiate a takeover for full control. While the Takeovers Act 1993 does contain processes for not requiring a full takeover, the intent of the Act recognises that once a shareholder in a large company owns more than a 20% stake in the company they are in a powerful position to influence, and exert control over, the company.
105. A threshold of 20% could be appropriate. However when compared to the 25% threshold, it is not likely, at this point in time, to bring meaningful additional financial intelligence to law enforcement agencies, or be of greater assistance to reporting entities in understanding the mind and management of the customer. Put simply, the additional compliance costs of a 20% threshold, when compared to a 25% threshold outweigh the potential benefits.

Option two: 25% (preferred option)

106. Having a 25% threshold would be consistent both with domestic legislation such as the Companies Act 1993, and other comparable international AML/CFT systems.
107. One of the major considerations when setting the beneficial ownership threshold should be taking into account at what ownership level shareholders have the power to influence the direction of the company. Under the Companies Act 1993, when passing a special resolution 75% of a company's owners (ie shareholders who hold 75% of the shares) must agree. Therefore, if a shareholder holds 25.01% of the shares, they can exert control over the company's decision making.
108. Given that both the United Kingdom, and Australia implement a 25% threshold for beneficial ownership, a 25% threshold would also be internationally consistent and build on the AML/CFT Act's goal of trans-Tasman consistency.

Option three: 50%

109. The final option is to set the beneficial ownership threshold at 50%, the level of absolute control. Once an individual owns 50% of, or has 50% of the voting rights in, a legal person then they are clearly in a position to benefit from, and control, that entity.
110. This threshold would be consistent with the threshold that the Financial Service Providers (Registration and Disputes Resolution) Act 2008 sets for controlling interest.
111. We consider that a threshold of 50% would be too high and does not reflect either the ML/TF risks that legal arrangements present in the New Zealand context, nor does it reflect the FATF Recommendations' intent to understand how a company, trust or other legal arrangement works, and who is in a position to exercise effective control (as opposed to absolute control).

Comment sought: Which option do you support and why? Please provide detailed explanation in support of your view.

Other partial exemptions and reduced measures

Debt collection

112. Submitters on the AML/CFT Bill suggested that debt collection activity warranted exemption from certain AML/CFT obligations.
113. In the majority of cases, a debt collector will receive limited customer due diligence information. If customers are not able to conduct customer due diligence in accordance with the Act, then under section 37 it must terminate the business relationship with the customer. Customers are not ordinarily incentivised to give debt collectors their information. Section 37 of the Act reinforces this disincentive to identification. Given that debt collection is not an activity that is strongly associated with money laundering or terrorism financing risk, there is a rationale for a partial exemption from AML/CFT obligations.
114. Australia is also consulting on exemptions for debt collection agencies. The proposed exemption in Australia defines 'debt' in the debt collection context as meaning an amount of money owed, where:
- 114.1. the provider of the money (account provider) has terminated, cancelled, written off or charged off debt, by reason of the customer's default or continuing default in repaying the money
 - 114.2. the account provider has declined the provision of further credit to the customer under the account.
115. 'Debt collector' means a person who collects debt in the course of carrying on a business of collecting debt.
116. In Australia debt collection activity is proposed to be exempt from all obligations except for those associated with STR reporting and investigation of STRs.

Preferred approach

117. It is proposed that debt collectors have a partial exemption from the AML/CFT Act. They would be exempt from all of the obligations within Part 2 of the AML/CFT Act except for the obligation to report suspicious transactions and keep records relating to any suspicious transaction reports.

Reduced CDD measures for insurance products

118. The FATF Recommendations indicate that reduced measures for certain insurance products are permissible provided that ML/TF risks are managed. An exemption in line with those permitted by the FATF may be appropriate, as follows:
- 118.1. Life insurance products are excluded from CDD verification until cash-out when they meet one of the following criteria:
 - 118.1.1. the product is a regular premium policy with premiums not more than \$1500 per annum
 - 118.1.2. the product is a single premium policy where the premium is not more than \$3000
 - 118.1.3. the product is a contract of consumer credit insurance (ie insurance that provides cover if the consumer cannot meet the payments on a loan).

119. We note that the Australian regime provides for exemptions for the above products from their inclusion in AML/CFT programmes more generally. Further work is required to determine whether it is appropriate for New Zealand to provide for reduced CDD measures or a more full exemption.

Comment sought: *We would like your views as to whether you consider the exemption conditions and the thresholds are appropriate for insurance products in New Zealand. How do you rate the ML/TF risks of the proposed exemptions? Does the proposal offer real benefits in terms of reduced compliance costs?*

Insurance products closed to new customers

120. In Australia policies which are closed to new customers or premiums (other than those contractually agreed) are exempt. This applies to existing (or pre-commencement) customers equally.

Comment sought: *Would you propose the same criteria for exempting insurance products closed to new customers and new premiums in New Zealand? How would you rate the ML/TF risks?*

Reduced CDD measures for non-bank deposit takers

121. We consider that the ML/TF risks associated with businesses that are in the process of being wound up are likely to be very low in most cases. We therefore propose that non-bank deposit-takers that are in receivership or which have entered into moratorium agreements with their creditors and are unable to issue new debt securities to the public be exempted from AML/CFT requirements.

Reduced measures for workplace-based superannuation funds

122. The current regime may allow customer due diligence undertaken by employers on specific workplace based superannuation schemes to be relied upon, but do not specify the criteria under which such reliance is acceptable.
123. Workplace superannuation schemes have good checks and balances in place to manage identity risks including requirements for employers to obtain tax numbers for employees, and their names and addresses. Employers usually also hold employee bank account numbers.
124. Superannuation accounts are commonly transferred between financial institutions. To significantly reduce costs and business inefficiencies for certain organisations, provision needs to be made under the AML/CFT Act for reduced CDD measures for establishing and transferring workplace-based superannuation accounts.
125. In exempting superannuation and retirement schemes, factors for AML/CFT consideration are whether the scheme:
- 125.1. is workplace based or individually based
 - 125.2. is statutorily regulated or private market based
 - 125.3. is domestically or internationally based
 - 125.4. has limits and controls on withdrawal of funds
 - 125.5. has limits on employee contributions
 - 125.6. has limits on transferability to other parties
 - 125.7. has controls on the transfer of the funds to and from other countries.

Preferred approach

126. We propose that reduced measures for both new and existing customers are applied to schemes that:
- 126.1. are established under statute
 - 126.2. are workplace based (with or without employer contributions)
 - 126.3. are managed through a registered provider with a physical presence in New Zealand
 - 126.4. can only be withdrawn on achieving retirement age (or earlier upon decease of the customer)
 - 126.5. cannot be transferred to another beneficiary (other than as an estate)
 - 126.6. are only able to be transferred to or from other countries on emigration and to other FATF compliant countries.
127. The reduced measures constitute an exemption from verification of CDD information on the condition that verification of CDD is conducted on any payout.

Low value superannuation funds

128. In addition to the exemption provided for above, any superannuation accounts which have very low values are a low ML/TF risk. The cashing out of superannuation funds open only to individuals and which are low value accounts (less than A\$1000) are exempted from AML/CTF obligations in Australia. It is proposed that a similar exemption is applied in New Zealand.

<p>Comment sought: <i>Are the reduced measures proposed for superannuation funds and schemes appropriate? Are the criteria reasonable, balancing ML/TF risks and compliance costs?</i></p>

Overseas pension accounts for certain countries

129. The Financial Transactions Reporting (Interpretation) Regulations (No 2) 1997 provides an exemption for overseas pensioners' special bank accounts that are opened, administered, and operated under the Social Security (Alternative Arrangement for Overseas Pensions) Regulations 1996. These special bank accounts are used in the offsetting of overseas pensions against New Zealand social security benefits where an overseas pensioner has entered into an alternative arrangement with the Director-General of Social Welfare.
130. The regulations deem overseas pensioners' special bank accounts not to be facilities for the purposes of the Financial Transactions Reporting Act. The practical effect of the regulations is to exempt financial institutions from the customer verification requirements of the FTRA. A bank does not have face to face dealings with a pensioner under an alternative arrangement, and an overseas pensioner's special bank account can be operated only in very limited circumstances. The Director-General of Social Welfare will have verified the identity of the overseas pensioner, and it is considered onerous to apply the verification requirements to financial institutions.

Preferred approach

131. It is proposed that this exemption be continued under the AML/CFT Act.

Special remittance card facility

132. Financial Transactions Reporting (Interpretation) Regulations 2008 provide an exemption for certain remittance card facilities if certain conditions are met. The regulations have the effect of exempting financial institutions from the requirement to verify the identity of the second card holder of the facility. The rationale for the exemption is that a number of other safeguards exist to manage the risks. For example, there is a maximum balance and annual limits on transactions. The principal facility holder must not hold more than one remittance card facility with any single financial institution in any period of 12 consecutive months.

133. The purpose of these regulations is to facilitate lower cost remittances from people in New Zealand to people in other countries, particularly Pacific Island countries. Financial institutions are not exempt from any other requirements of the Financial Transactions Reporting Act 1996.

Preferred approach

134. The special remittance card facility provides an important tool for New Zealanders to send money to relatives and friends in the Pacific. It is proposed that the current exemption is continued (and existing AML safeguards retained) under the AML/CFT Act.

Exemption from address verification for casinos

135. Reporting entities are required to collect and verify a customer's address. For most reporting entities this requirements is achievable. Verification of address can be achieved in multiple ways, and it is not proposed to restrict or further prescribe the method of verification of address at this point. Guidance may be issued by Supervisors if desirable.

136. The majority of transactions in a casino environment are likely to be conducted outside a business relationship. Most customers will engage with the casino on a single occasion. The decision to enter a casino and conduct a transaction is commonly spontaneous, and a proportion of casino customers are likely to be tourists and non-New Zealand residents.

Preferred approach

137. The requirement to verify address may impact disproportionately on casinos compared to other reporting entities. When weighing the operational impact of this requirement against the added risk management benefit, it is considered an exemption from this requirement may be appropriate.

Comment sought: *Are there other situations where you consider verification of address to be problematic? Please justify your view with reference to the nature of engagement with your customers.*

Wire transfers

138. International wire transfers are those that are either sent or received from offshore. Transfers of funds between accounts in New Zealand and overseas accounts are carried out via international funds transfers systems.
139. A domestic wire transfer is one that occurs wholly within New Zealand. As such, all electronic transfers of funds between bank accounts in New Zealand, such as internet banking may be considered domestic wire transfers.
140. FATF Special Recommendation VII (SR VII) relates to wire transfers. It was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator of wire transfers is immediately available to:
- 140.1. appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals
 - 140.2. financial intelligence units for analysing suspicious or unusual activity and disseminating it as necessary
 - 140.3. beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions.

Exemption threshold

141. Under SR VII for wire transfers below US\$1000, countries may decide to not require CDD on the customer or require originator information accompany the wire transfer.

Preferred approach

142. A threshold of NZ\$1000 recognises that low value wire transfers are of sufficiently low ML/TF risk that they can be exempted. We note that, when submitters on previous consultations commented on what an appropriate threshold for wire transfers would be, the recommendation was that a minimum threshold of NZ\$1000 should be established. Therefore this option appears to be preferred by both public and private sector.

Exemption from originator information for domestic wire transfers

143. Section 27(2) of the Act provides for different ‘accompanying information’ requirements for domestic wire transfer transactions compared to the requirements for international wire transfers. Information requirements for domestic wire transfers may include either the originator’s account number or other ‘*identifying information that may be prescribed*’ provided that the information is able to be provided within 3 working days.

Preferred approach

144. The preferred option is to put in place regulations to specify that the transaction itself will be sufficient to constitute identifying information for the provisions of the AML/CFT Act with respect to domestic wire transfers.

Exemption from requirement to maintain originator information for the domestic leg of incoming international wire transfers

145. One international transfer system used by many of the mainstream banks in New Zealand is the SWIFT system. The SWIFT system is operated according to FATF standards in terms of information requirements. CDD information is sent between countries via the SWIFT system.
146. With respect to international wire transfers, section 27(4) of the Act requires intermediary institutions to pass on any information obtained in a wire transfer to any beneficiary institution (ie the institution that holds the account of the person to whom the funds are being transferred). SR VII indicates that in addition to traceability, information as to the origin of funds is important for beneficiary institutions' assessment of customer risk. Knowing that funds are coming in from overseas and identifying the country of origin is important in determining ML/TF risks. SR VII intends that any intermediary institution passes the originator information along to the next institution in the chain so that the ultimate beneficiary institution is aware that the transaction was received from overseas and is able to use originator information to assist in assessing the risk associated with the transaction.

Preferred approach

147. As for domestic wire transfers, for a domestic leg of an incoming international wire transfer, passing on all originator information may be problematic. We are willing to consider that financial institutions, when they are acting as intermediaries, be exempt from the obligation to pass on all originator information for the domestic leg of incoming wire transfers in situations where it is not reasonable to attach the originator information.
148. In such situations, intermediary institutions may be able to simply apply the same measures (above) as for domestic wire transfers. However, to manage the risk associated with beneficiary institutions being unaware of both the nature of the transaction and the country of origin, it may be appropriate for intermediary institutions to apply risk-based policies for managing the risks associated with the exemption.

Section three - Customer due diligence

Basis for verification

Background and context

149. The AML/CFT Act imposes obligations to collect and verify information relating to customers of reporting entities. In addition to specific requirements that relate to politically exposed persons, correspondent banking relationships, wire transfers and new and developing products/technologies that may favour anonymity, there are three broad types of customer due diligence:
- standard due diligence
 - simplified due diligence
 - enhanced due diligence.
150. The Act sets out the circumstances where each type of due diligence must be carried out and prescribes information collection (identity requirements) and information verification (verification requirements) minimum obligations for each.
151. The Act also contains regulation making powers to prescribe additional circumstances and requirements for all types of due diligence. There is also a regulation making power which enables prescription of a basis for information verification.
152. At this stage, the only areas considered for further prescription of requirements are:
- 152.1. basis for verification applying to a specified situation, customer, product, service, business relationship or transaction
 - 152.2. circumstances where standard due diligence applies
 - 152.3. entities or classes of entity to whom simplified due diligence can be applied
 - 152.4. enhanced customer due diligence identity requirements.

Why is 'knowing your customer' important?

153. Reporting entities (and the financial sector) are particularly exposed to money laundering where opportunities for customer anonymity exist. The FATF recognises this in Recommendation 5 (financial institutions should not keep anonymous accounts or accounts in obviously fictitious names) and through its emphasis on customer due diligence and identification of beneficial ownership.
154. Anonymity arises in the following key ways:
- 154.1. the customer is using a false or assumed identity (identity fraud) and/or insufficient identity information is held about the customer accessing the service or conducting the transaction
 - 154.2. the person operating the account or conducting the transaction is not the person controlling or ultimately benefiting from the transaction or access to the service. The beneficial owner's identity is obscured by complex business arrangements and relationships.

Why is intervention necessary?

155. Police statistics show that in the year to June 2008 there were 1100 misuses of identity involving almost 500 fictional and genuine identities - figures Police say are a fraction of

what is really going on. Police believe this represents probably around 5-10% of all cases though this is very difficult to accurately gauge.

156. The New Zealand Crime and Safety Survey (NZCASS), which asks individuals about their experience of being a victim of crime, also provides some useful information about the prevalence of identity fraud and financial crime. Of credit card, bank card or debit card users, 2.3% said that since 1 January 2005 somebody had used a credit, bank or debit card or card number, without permission, to steal from them.
157. Of respondents in NZCASS 2006, 53% said they were very or fairly worried about having a credit card misused.
158. A recent survey of 506 participants conducted by Unisys indicated 22% of people were seriously concerned about the ability of the Government to protect information and 26% were concerned about financial service providers' ability to do so. More than half of participants surveyed fear identity theft. Areas of concerns were other people obtaining credit card or debit card details, unauthorised access to or misuse of personal information, and the security of shopping and banking online.
159. With increasing access to service online, commercial entities are increasingly creating electronic identities for customers to facilitate ongoing and convenient engagement. Once an online identity is created for an individual, that customer may never need to engage face to face with the reporting entity again. As outlined above, every time a credential is issued to a customer, it is an opportunity to link a false identity to a valid credential and thereby legitimise the false identity.
160. It is important that when online identities are created for individuals, that the process for attaining that online identity contain robust identification procedures. Currently common business practice (in some sectors) is to rely (for example) on a driver's licence to establish a customer's identity. There are some concerns with the use of driver's licences as the sole form of identity verification which are discussed later in this document.

What tools exist to address the issue of identity theft/fraud?

161. The Evidence of Identity Standard (EOI Standard) administered by the Department of Internal Affairs (DIA) is probably the most comprehensive guidance around development of identification procedures available.
162. The EOI Standard was designed for use in public sector organisations but the principles, or objectives of identification are equally applicable in a private sector context.
163. The standard describes the five key objectives of establishing identity as:
 - 163.1. determining that the identity exists (objective A)
 - 163.2. determining that the identity is living (objective B)
 - 163.3. determining that the presenting person links to the identity (objective C)
 - 163.4. providing confidence that the presenter is the sole claimant of the identity for the services requested (objective D)
 - 163.5. providing evidence of the presenter's use of identity in the community (objective E).

164. The EOI Standard recommends organisations undertake an assessment to determine the level of identity risk associated with the delivery of each service. The level of risk will correspond to the level of confidence that an organisation will need to have in the identity of their customer. Based on the level of confidence required, an organisation should design an identification process. An identification process could involve:
- 164.1. The customer producing a combination of documents to meet all five objectives outlined above
 - 164.2. The customer producing a document (or documents) supplemented by validation that the identity information presented is reflected in records held by an authoritative source
 - 164.3. Electronic verification methods that use data sources that meet all five objectives outlined above
 - 164.4. Any combinations of the above, as long as all five objectives are met.
165. While the EOI Standard recognises there is no one size fits all identification process, it provides some clear guidance around what are acceptable evidential requirements (verification) for services that require a low, moderate and high level of confidence in identity. The proposals in this paper have been informed by the guidance in the EOI Standard, but in some respects have been modified to take account of operational considerations in a private sector context.
166. The EOI Standard emphasises that objective C (determining that the presenting person links to the identity) is a vital aspect of identity processes. For moderate or higher levels of confidence, at least one photographic (or other biometric) identity document should be supplied.
167. The documents that are defined by the EOI Standard as adequate for meeting objective A (that the identity exists) are below. These documents are commonly referred to as primary identification documents.
- 167.1. New Zealand passport*
 - 167.2. New Zealand Certificate of Identity (issued to non-New Zealand citizens who cannot obtain a passport from their country of origin)*
 - 167.3. New Zealand Certificate of Identity (issued to people who have refugee status)*
 - 167.4. New Zealand Refugee Travel Document (RTD)*
 - 167.5. Emergency Travel Document (ETD)*
 - 167.6. Firearms Licence*
 - 167.7. Overseas passport (with New Zealand immigration visa/permit)*
 - 167.8. New Zealand Full Birth Certificate
 - 167.9. New Zealand Citizenship Certificate
168. Documents defined as adequate for meeting objective E (that the identity is used in the community) are below. These documents are commonly referred to as secondary documents.
- 168.1. New Zealand Driver Licence*
 - 168.2. 18+ Card*
 - 168.3. Community Services Card
 - 168.4. IR Number

168.5. Electoral Roll Record

169. The following list describes some examples of 'supporting' documents/records. The EOI Standard indicates that these documents can be used if secondary documents are not available.

169.1. Credit cards, bank cards and financial accounts

169.2. International Driving Permit*

169.3. Confirmation of Permit Status

169.4. Steps to Freedom Form

169.5. Student Identity Cards* or Employee Identification Cards *

169.6. Utility accounts.

The case to regulate

170. The requirements within the AML/CFT Act are not aimed at managing the business risk for reporting entities, they are aimed at managing the societal risk of money laundering and financing of terrorism. Reporting entities cannot be expected to assume that responsibility independently of clear advice from government. Therefore it is appropriate that government determine what is required to manage those risks.

171. One way of determining the necessity of regulation is to compare current business practices to the best practice advice available. Based on our discussions across sectors, current practice is not consistent with the EOI standard generally.

172. This may reflect the fact that industry has commercial incentives to ensure that the impact of the AML/CFT obligations on customers is minimised. Any departure from current business practice is going to involve costs to industry to implement; benefits are longer term, less tangible (reputational rather than monetary) and are more likely to be in the national (rather than industries') interest. To ensure that a better practice standard is implemented, an enforceable instrument is preferred.

173. Similarly, reporting entities will interpret guidance or any principles-based requirements differently. A universal minimum standard will ensure consistency. It is important that government does not inadvertently create a situation of competitive advantage for one reporting entity or class of reporting entities.

Level of prescription

174. Not all reporting entities will have the same access to resources for undertaking risk assessments, developing and implementing risk based procedures. Small to medium enterprises for example may prefer a list of clear requirements that provide maximum clarity and certainty of compliance. We are interested in hearing your preferences.

175. For these reasons, it is preferred to establish a minimum standard or standards for verification requirements that is reasonably prescribed either in regulations or codes of practice. This will ensure a level playing field as far as possible, and provide maximum clarity and certainty across sectors.

** Document/record contains a photograph of the holder.

Criteria for regulations or codes of practice

176. We acknowledge that sectors have a number of concerns about further government regulation in this area. Key concerns expressed have included customer convenience and compliance costs of raising the standard of identification.
177. Ultimately, we consider a successful regulatory regime or codes of practice should:
- 177.1. provide for an appropriate level of confidence that a customer is who they say they are
 - 177.2. as far as possible ensure a level playing field across all sectors and not create new opportunities for competitive advantage
 - 177.3. be mindful of wider government evidence of identity standards
 - 177.4. achieve compliance as far as possible with Financial Action Task Force Recommendations and other international obligations
 - 177.5. be compatible with the Australian regime where appropriate
 - 177.6. be flexible enough to take into account different business environments and within different environments, the level of risk presented by different customers or products
 - 177.7. be able to be updated relatively easily as the environment changes
 - 177.8. provide reporting entities with certainty about what will be expected of them (or considered compliant) by Supervisors
 - 177.9. assist reporting entities by setting out easily interpretable processes, or safe harbour procedures
 - 177.10. provide for alternatives, or exceptions, in certain circumstances
 - 177.11. minimise the regulatory burden, not only to reporting entities but also to Supervisors
 - 177.12. seek to minimise compliance costs to reporting entities as much as possible, while still giving effect to the purposes of the regime.

Documentary identity verification

Primary identification documents

178. Feedback from industry indicates that the use of the driver's licence as a primary and sole form of identification is prevalent. The driver's licence is primarily a traffic law enforcement tool to enable Police to determine, at the roadside, that the holder of the licence has met the legal standard of knowledge of the road rules and driving competency. The holder of a current licence is therefore legally entitled to drive a motor vehicle on public roads under the terms and conditions specified on the licence. The driver's licence was not designed or intended to be used as a general-purpose identification document.
179. A driver's licence is a useful document in respect of identification objective C because it contains a photograph that can be compared to the presenting individual. It can be used in respect of objective E because an individual (having had their identity established) passing the legal requirements to operate a motor vehicle on public roads in New Zealand can be considered to be evidence of using the identity in the community.

180. However, in accordance with the EOI Standard, it is not a document that is considered suitable to meet objectives A, B or D, in the sense that it is not an authoritative or primary document. Essentially the driver's licence is useful in combination with a primary document but it is considered that the use of the driver's licence alone, or in combination with only secondary or supporting documents may not be effective in achieving the purposes of the regime.

Preferred approach

181. We favour a clear minimum standard that should apply to all customers and sectors. It is acknowledged that limiting the sole reliance on the driver's licence for consistency with the EOI Standard presents a significant departure from current business practice, and may have a significant impact on customer convenience.
182. However it is important to ensure that risks of identity fraud and money laundering are appropriately managed. It is considered a compromised solution may be a safe harbour code of practice for low to moderate risk customers that allows reporting entities to rely the driver's licence, but subject to certain conditions. This should assist reporting entities in minimising impacts on customers.
183. It is proposed that for customers which a reporting entity has identified as moderate or low risk, the following basis for verification of name and date of birth be acceptable:
- 183.1. two information sources:
- 183.1.1. at least one of which is a primary form of identification (either provision of the document itself, or validation of identity information presented on the document with records held by an authoritative source); and
 - 183.1.2. one of which should be photographic; and
 - 183.1.3. at least 1 of which must demonstrate the identity is used by the customer in the community (social footprint); and
- 183.2. a reporting entity must also check the person's details against their customer records, to ensure that no other person has claimed the same identity.
184. In low to moderate customer risk scenarios, a driver's licence may be used as a substitute for a primary form of identification if the following conditions are met:
- 184.1. validation that the information presented on the driver's licence is reflected in the National Register of Driver Licenses; and
 - 184.2. validation that the identity information presented on the document is reflected in records held by an authoritative source (such as DIA or Immigration) or if this is not possible
 - 184.3. an additional form of secondary identification or supporting document is provided (such as a Community Services Card, or credit card).
185. For customers assessed as high risk the driver's licence should not be substituted as a primary form of identification. A reporting entity should request one of the other primary forms of identification described by the EOI standard (listed in paragraph 165).
186. In addition, in all documentary identification scenarios a reporting entity must verify the identity of the customer:
- 186.1. in-person; or
 - 186.2. seek verification by a trusted referee (discussed later in this document).

187. A reporting entity must also consider, according to the level of risk, whether additional documentation is required to verify the customer's identity.

Exception handling

188. It is intended that a safe harbour code of practice will contemplate a number of circumstances where photographic identification, or standard identification cannot be provided for legitimate reasons – this may include customers under a certain age (such as school children), or who have disabilities which mean access to certain types of documents is limited.
189. A code of practice could prescribe methods or exception handling procedures. Alternatively the code of practice could identify some exceptional circumstances but not prescribe specific procedures. Guidelines or general guidance could then be provided to assist reporting entities.

Opting out of codes of practice

190. If it intends to opt out of the code of practice, a reporting entity must be able to comply with the Act by some other equally effective means.
191. Innovative business practices that are considered 'equally effective' by the Supervisor and AML/CFT coordination committee could be considered for incorporation into guidance or used to amend codes of practice.

Comment sought: *We invite comment on this proposal. In particular we are interested to know:*

- *is a code of practice the right vehicle to use, or are regulations preferred?*
- *is the preferred approach manageable in your business environment?*
- *in what specific circumstances might the code of practice present difficulties?*
- *what are the exceptional circumstances that a code of practice should contemplate?*
- *would you prefer the prescription of exception handling procedures or is guidance preferred?*

Please provide information to support the rationale for your comments.

Electronic identity verification

192. In the absence of further prescribed requirements through regulation, the Act only requires verification on the basis of data, documents or information from a reliable and independent source. The Act does not exclude electronic sources of verification provided it meets a reliable and independent test.

Some examples of electronic verification tools

The Data Validation Service (DVS)

193. The DVS is an electronic service that provides an agency with immediate confirmation that identity information presented to that agency is consistent with the identity information held by DIA. For example if a customer presents a birth certificate, the agency can confirm with DIA through the DVS that the information on the document presented is consistent with information held in DIA records.
194. In its current form, the DVS can validate data against the births register, citizenship register, and passport database. The DVS provides a high level of assurance to an

agency that they are not dealing with forged documents, fictitious identities, or incorrect information.

195. An additional advantage of the DVS is that it may be able to supplement document based identification procedures, and may mean that customers have to supply fewer documents. For example, the driver's licence may be able to be used as the sole form of identification document for verification of name and date of birth if the DVS was used to validate that information against birth records held by DIA. The validation of birth certificate information through the DVS would substitute for the provision of a birth certificate in documentary form.
196. The DVS, however, does not and cannot provide assurance that the person is the rightful claimant of the identity. For instance, a person may present another person's valid birth certificate, and the DVS would not be able to determine whether this has happened. A biometric (or a statement by a trusted referee) would still be needed to link the presenter to the claimed identity. Practically speaking, a photographic identity document in combination with a birth certificate check may be acceptable, but the birth certificate check alone may not be. A customer would still have to appear in person to be identified, or appropriate non face-to-face identification procedures implemented.
197. The DVS has been piloted in two public sector organisations. The Department of Internal Affairs is currently investigating the feasibility of making this service available to the private sector.

igovt Identity Verification Service

198. The igovt Identity Verification Service is a way for people to verify their identity to government agencies online and in real time using an igovt ID. This is similar to showing someone their passport to prove who they are, but it happens online using a unique identifier – the igovt ID. To get an igovt ID, an individual will need to pass through an application process with checks generally equivalent to applying for a passport. Once a person has been issued an igovt ID, the service can be used to verify identity to a participating government agency whenever needed, using the Internet.
199. The igovt Identity Verification Service has been built for use by the public and government agencies. The service is currently being piloted for birth, death and marriage products. Following the initial pilot activity, more government services may use the service and the service will be extended to all members of the public (regardless of whether they are New Zealand passport holders or citizens).
200. DIA has been exploring opportunities for extending usage of the igovt Identity Verification Service to the private sector. DIA has initiated the process of seeking approval for the service to be used by the private sector to support identity verification activities in an AML/CFT context.

Safe harbour for electronic verification

201. The Australian electronic identity verification safe harbour procedure (which is deemed acceptable for low to medium risk customers only) requires verification of name, residential address and date of birth from at least two separate data sources; **and** either the customer's date of birth using reliable and independent electronic data from at least one data source; or that the customer has a transaction history for at least the past 3 years.
202. However, in New Zealand, many data sources that may assist reporting entities in meeting the other objectives of establishing identity are not currently electronically available to the private sector (such as the Births, Deaths and Marriages register,

citizenship or passport databases. The electoral roll, while publically available, is not available in electronic form).

203. Essentially any electronic sources of verification must be reliable and independent. There are some commercially available data sources that may assist reporting entities in meeting objective E when identifying and verifying the identity of customers (as long as the Privacy Act and associated codes and regulations are adhered to). However electronic sources, or a combination of sources currently available may not be sufficient to meet all the objectives of identity verification, without reference to an authoritative source of data (or document) also.
204. We intend to monitor the types of electronic verification products that become available for use by the private sector, with a view to developing a safe harbour code of practice that sets out both criteria for 'reliable and independent' electronic verification, and the number and nature of checks that should be carried out.

Comment sought: *Does your organisation offer, or is your organisation considering the development of electronic verification tools? If so please provide information on the intended nature and operation of the tool and the sources of data it utilises.*

Other non- face to face identification and verification procedures

205. Reporting entities that operate services solely or primarily through online channels may not have physical branches where face to face identification of customers is possible.
206. For example, some online banking organisations offer high interest savings accounts that are linked to nominated accounts held with other institutions. Access to account funds is only through transfer into the nominated bank account. To be eligible for one of these accounts, a customer must hold an account with another institution. The online bank relies on the customer identification carried out by the other institutions. Essentially they trust the customer because another bank trusts the customer.
207. The Act does permit the reliance of one reporting entity on another, where the reporting entity meets all of the following conditions:
- 207.1. relevant identity information is provided before the reporting entity establishes a business relationship or an occasional transaction is conducted
 - 207.2. relevant verification information is provided as soon as practicable, but no later than 5 working days, after the business relationship is established or the occasional transaction is conducted
 - 207.3. the entity consents to conducting the customer due diligence procedures for the reporting entity and to providing all relevant information to the reporting entity.
208. The issue for online banking organisations (and other entities who may provide services in this way) is the need for the consent and cooperation of another reporting entity to obtain appropriate verification information. It is unlikely that reporting entities who offer competing services would consent to reliance.
209. Reporting entities that operate online may be concerned that they will be disproportionately disadvantaged by customer due diligence verification requirements, in particular verification obligations that require obtaining certified copies of identity documents.
210. Concern has been expressed that requiring customers to have documents appropriately certified will have an impact on customer convenience. Customers may

choose to utilise services of institutions that have a branch office in a nearby location rather than obtain certification of documents.

211. Non-face to face identification does present an additional identity fraud risk (and therefore additional money laundering risk). One of the key objectives of a robust identification process is ensuring that the presenter of the identity links to the identity in the documents. This is most effectively achieved through a biometric link, a common form of which is a photograph. When a reporting entity is unable to make a biometric link between a customer and the identity the customer claims, an appropriate level of confidence cannot be achieved. This is a challenge when face to face verification procedures are not possible. In addition, risks of forgery are much higher when a reporting entity is not able to sight an original document.
212. Approaches that mitigate the risks of non-face to face identity verification may include use of data validation services. These services may tell the reporting entity if the document presented is counterfeit, stolen or lost (although not always). It would not however confirm the person presenting the document was the true claimant of the identity that is being asserted.
213. Other electronic verification methods may also mitigate these risks. However a code of practice need to be developed to provide guidance in circumstances where neither electronic verification, nor face to face documentary based identity verification is possible.

Certification of documents

214. Another method of mitigating the risks described above may be through allowing third parties to sight the original documentation on behalf of the reporting entity and certify the authenticity of the copies.
215. Requiring certification of documents may impact on customer convenience. However a code of practice would apply to all reporting entities unable to verify the identity of customers in person. A code of practice should ensure the level of effort required for customers to have documents certified does not exceed the level of effort required for customers to appear in person to be identified (at another bank for example).
216. Customers will also have motivations for choosing the services of a reporting entity other than online account establishment (such as high interest rates, or inability to obtain credit from a larger or mainstream financial institution).
217. On balance, we do not think a requirement to obtain certified copies of documents presents significant competitive disadvantage for organisations that operate primarily through online channels, but are willing to consider further evidence to the contrary.

Preferred approach

218. It is proposed that certification of documents be required for non-face to face identity verification, and that certification is carried out by a trusted referee. The trusted referee would make a statement to the effect that the original identification documents have been sighted and link to the person claiming the identity. We propose certification be required to have been carried out in the three months preceding the presentation of the copied documents.
219. It is proposed a trusted referee not be a relative; be a spouse or partner; or live at the same address. A trusted referee should:
 - 219.1. have known the person for more than 12 months

- 219.2. be known to the reporting entity
- 219.3. hold a particular position of standing within the community (guidance could be provided in this respect)
- 219.4. have an accessible contact address and phone number.
220. It is proposed that these standards for verification of customers through a non-face to face channel be contained in a code of practice. This will allow reporting entities to opt out of the code of practice if they develop alternative or innovative approaches for mitigating the forgery risk of copied documents that are 'equally effective'.
221. Ensuring that the identity presented links to the customer is however a critical element of ensuring a higher level of confidence in a customer's identity. This remains the case, even as electronic verification becomes more widely available. Document certification and trusted referee processes mitigate this risk to some extent, but may not be ideal from an operational or risk management perspective.
222. However, we also understand that the Department of Internal Affairs is initiating a consultation process during January which will include exploration of convenient and efficient ways to meet the objective of ensuring the presenter links to the identity when identification is not being undertaken in person. Interested parties in this consultation process should indicate their interest through email to: identity.assurance@dia.govt.nz.

Comment sought: *How much of your business is carried out in circumstances where identity verification cannot be carried out in person? How is your business currently managing this risk?*

Does certification of documents carried out as described above present any significant challenges in your business environment?

Standard due diligence

223. Currently the Act requires standard due diligence to be applied when:
- 223.1. establishing a business relationship with a new customer
- 223.2. a customer seeks to conduct an occasional transaction through the reporting entity
- 223.3. in relation to an existing customer:
- 223.3.1. there has been a material change in the nature or purpose of the business relationship; and
- 223.3.2. the reporting entity considers that it has insufficient information about the customer.
224. There is one other circumstance that needs to be considered for inclusion in the circumstances where standard due diligence should be applied – existing anonymous accounts.

Existing anonymous accounts

225. Customer anonymity is a significant barrier to the detection and deterrence of illegal activity. The Act prohibits reporting entities from knowingly or recklessly setting up a facility for a customer on the basis of customer anonymity.

226. To trigger CDD on existing (pre-commencement) customers, two tests must be met. There must be both a material change in the nature or purpose of the business relationship and the reporting entity must consider that it has insufficient information about that customer.
227. In relation to existing anonymous accounts, reporting entities will clearly not hold sufficient information. However a material change in the nature and purpose of the business relationship may not occur for any length of time.
228. FATF Recommendations are clear that financial institutions not keep anonymous accounts, and make no distinction between existing and new customers. Customer anonymity presents a high risk of ML/TF and the intention of the Bill in relation to anonymity is clear.

Preferred approach

229. The preference is to use regulations under section 14(d) to specifically require reporting entities to carry out CDD on existing anonymous accounts. It is proposed that the trigger points described in section 12 that relate to existing customers not apply in relation to existing anonymous accounts.

Simplified due diligence

230. Simplified due diligence does not require the identity of the customer to be verified, or beneficial ownership checks on that customer to be carried out.
231. The Act provides that regulations may be issued to expand the list of entities to whom simplified due diligence may be applied. We consider that suitability for simplified due diligence could be predicated on the following key assumptions.
- 231.1. The customer presents an extremely low or negligible risk of ML/TF.
- 231.2. Adequate customer due diligence information is able to be readily obtained from publicly available sources.
- 231.3. Critical information about the customer's 'identity', composition, structure, beneficial ownership and management is transparent, publicly available and subject to public scrutiny (such as the public disclosure requirements of publicly listed companies).
- 231.4. The customer's financial activities are independently and regularly audited.
- 231.5. Transparency and public accountability (through various mechanisms) are required by statute, or by some other instrument that means the level of transparency and accountability has a reasonable degree of longevity.
232. While eligibility for the application of simplified due diligence measures will be considered on a case by case basis, mechanisms of transparency and accountability that may be relevant include (but may not be limited to) the following:
- 232.1. the organisation is subject to audit by the controller and Office of the Auditor general through the Public Audit Act 2001 or other statutory means
- 232.2. an organisation that is subject to and compliant with either the Public Finance Act, and/or the Crown Entities Act
- 232.3. annual reporting that is required to be presented to the House of Representatives and/or published in a public forum
- 232.4. a governance body (such as a Board) that is appointed by government through an appointment process that requires a satisfactory level of financial and

personal probity (such as a process that has been certified as carried in accordance with state services commission guidelines, and/or subject to Cabinet consideration)

232.5. an entity that is subject to performance monitoring by a government agency

232.6. an entity that is directly subject to, and demonstrably compliant with, the provisions of this AML/CFT regime.

233. Consideration must also be given to the effect that allowing simplified due diligence will have on the competitors of entities and/or classes of entities.

Preferred approach

234. At this stage the preferred approach is to consider eligibility on a case by case basis rather than allowing eligibility through a defined list of criteria. Preliminary consideration is being given to the following entities or classes of entities as customers to whom simplified due diligence could be applied:

234.1. Crown entities as defined by section 7(1) of the Crown Entities Act 2004

234.2. Trustees and Statutory Supervisors as defined by section 48 of the Securities Act 1978

234.3. Trustee companies as defined the Trustee Companies Act 1967

234.4. Crown research institutes

234.5. Organisations named in Schedule 4 of the Public Finance Act

234.6. Trusts established in Statute for the purposes of charitable distribution of funds (eg: Community Trusts).

Comment sought: *We invite comment on the proposal, but in particular:*

Would allowing the application of simplified due diligence to the above entities present any challenges to your organisation (competitive issues for example)?

Are there other customers where simplified due diligence may be appropriate in light of the assumptions and/or criteria described above?

Would an approach that set criteria for eligibility (in line with the criteria described above) be preferred? If so why?

Are there any criteria that are not described above that should be included?

Enhanced due diligence

Identity requirements for enhanced customer due diligence

235. For those customers who are sufficiently high risk to apply enhanced due diligence measures, section 23 of the Act currently requires reporting entities to collect the following information.

235.1. Standard due diligence identity requirements:

235.1.1. the person's full name

235.1.2. the person's date of birth

235.1.3. if the person is not the customer, the person's relationship to the customer

- 235.1.4. the person's address or registered office
- 235.1.5. the person's company identifier or registration number.
- 235.1.6. any information prescribed by regulations.

235.2. In addition, the following enhanced requirements under EDD:

- 235.2.1. information relating to the source of the funds or the wealth of the customer
- 235.2.2. any additional information prescribed by regulations.

- 236. Reporting entities are also required to collect information on the nature and purpose of the business relationship.
- 237. Regulation making powers enable the additional specification of information that must be collected. Adding requirements by regulation in section 23 does not necessarily attract a corresponding obligation to verify that information.

Identifying beneficiaries of Trusts

- 238. The FATF methodology defines a beneficial owner as “*the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate, effective control over a legal person or arrangement*”.
- 239. The FATF Recommendations require reporting entities to identify the beneficial owner and take reasonable steps to verify their identity (5.5). Where the customer is a legal person the reporting entity should be required to take reasonable measures to:
 - 239.1. understand the ownership and control structure of the customer
 - 239.2. determine who are the natural persons that ultimately own or control the customer (5.5.2).
- 240. These aspects of FATF Recommendation five are required to be set out in a legal instrument rather than guidance material.
- 241. Under the AML/CFT Act, trusts are subject to enhanced due diligence. Under the Australian AML/CFT regime reporting entities are required to identify beneficiaries of trusts. In the United Kingdom reporting entities must identify beneficiaries who receive more than 25% of the benefit/dispensations from a trust (the UK appears to have applied its 25% beneficial ownership threshold directly to trusts).
- 242. Trusts are internationally recognised as ML/TF risks and New Zealand is no exception. In addition the financial activity of a trust is conducted on behalf, and to the benefit, of the beneficiaries.
- 243. Therefore, we consider that in order to provide adequate scrutiny of trusts, and to continue to provide for trans-Tasman consistency, there is a need for reporting entities to identify, but not necessarily verify the identity of, the beneficiaries of a trust. This requirement would need to be provided for in a regulation, and not a code of practice. This is because a code of practice cannot be used to add obligations, only provide a safe harbour for acting on the AML/CFT Act's obligations.

Large numbers of beneficiaries

- 244. Some New Zealand trusts (for example iwi trusts) can have thousands of beneficiaries. Clearly it is not viable, or desirable, to require reporting entities to identify thousands of

beneficiaries when establishing a business relationship. Therefore any requirement to identify beneficiaries of trusts should incorporate some form of cap on the number of beneficiaries that need to be identified with the remainder of the beneficiaries being identified as totals according to type of beneficiary.

Discretionary trusts

245. Many trusts such as family trusts and charitable trusts do not specify individuals who they give dispensations to. Instead the trust deed gives trustees discretion to choose who should be a beneficiary who receives a disbursement from the trust. This creates practical problems in that reporting entities will not be able to identify the beneficiaries.
246. In the case of trusts who make grants upon application (for example, a charitable trust) it is considered that identifying a class of beneficiaries, or the 'formula' of beneficiaries would be sufficient. The 'formula' is likely to be information about the nature and purpose of the trust and the eligibility criteria for grant distribution.
247. In the case of a family discretionary trust, beneficiaries may be individuals described by the familial relationship (for example; the sons and daughters) intended to capture future children as well as present children. Discretionary trusts structures are also able to determine who will be the beneficiary at any time over the life of the trust. A possible option to manage the identification of these types of beneficiaries may be to require reporting entities to identify beneficiaries at the time the trust makes a disbursement to that beneficiary.

Preferred approach

248. We propose to put in place a regulation under section 23(b) of the AML/CFT Act, requiring reporting entities to identify, but not verify, the name and date of birth of beneficiaries of trusts who are their customers. This regulation would allow for reporting entities to identify 10 beneficiaries and then describe the number and nature (or class) of other beneficiaries where there are a larger number of beneficiaries.
249. In addition, where it is reasonable for the reporting entity to require a discretionary trust to provide it with the identity of a beneficiary it is making a disbursement to, we consider it should do so.

Comment sought: *Does the proposal present significant challenges in your business environment?*

Are there types of trusts that you feel constitute a much lower ML risk? Please provide detailed explanation to support your view.

Section four- Third party relationships

Reporting entity and customer relationships

250. In many reporting entity-customer relationships, third parties are involved. The Act allows for these third parties to play various roles in the business relationship, and for regulations to clarify the various obligations and responsibilities of each party.
251. There are some types of relationships where defining the parties to the business relationship or occasional transaction can be complex. Under the Act, reporting entities have obligations with respect to:
- 251.1. a customer;
 - 251.2. a beneficial owner of a customer; and
 - 251.3. a person acting on behalf of a customer.

Reliance on third parties

252. The Act recognises that it may not always be feasible to obtain CDD information directly from the customer. The Act also recognises that it may be beneficial for reporting entities to involve third parties (for example sharing of AML Programmes in a DBG) and “outsource” certain AML/CFT functions.
253. CDD is an obligation that may be particularly challenging for reporting entities that have little or no contact with underlying customers. CDD involves the collection, handling and storage of sensitive information. Government has a responsibility to ensure that the privacy of individuals is protected, that the information is dealt with appropriately, and risks of money laundering and identity fraud associated with the handling of that information are minimised. The Act does provide for some situations where reporting entities may automatically rely on customer due diligence carried out by third parties to assist in this respect, but attaches conditions to that reliance.
254. It is acknowledged that while the reliance provisions offer some relief to reporting entities there are still operational difficulties in some circumstances where there is no direct interaction with underlying customers.

Pooled accounts

255. An intermediary that stands between an underlying customer and the reporting entity providing a service to that customer may use pooled, nominee or omnibus account structures. As noted above, the Act places obligations on the reporting entity in relation to both the underlying customer and the person acting on behalf of a customer.
256. Complying with AML/CFT obligations such as account monitoring in relation to the underlying customer in these circumstances also presents challenges. If the reporting entity cannot distinguish one underlying customer from another within a pooled account, they cannot effectively monitor transaction behaviour, or reasonably ensure it is consistent with the customer profile.
257. In addition, there may be circumstances in which it may not be commercially desirable for intermediaries to provide customer information to other reporting entities.
258. Some relief for reporting entities in these circumstances may be reasonable and pragmatic. However nominee accounts can also be used as a mechanism for

perpetuating anonymity of underlying customers. We need to ensure that we do not inadvertently encourage the use of nominee accounts for illegitimate purposes.

Preferred approach

259. We propose that a reporting entity that conducts an occasional transaction or has a business relationship with an intermediary, who is acting on behalf of customer(s), through pooled, omnibus or nominee account structures, be exempted from account monitoring and record keeping obligations relating to the underlying customers subject to the following condition.

259.1. The reporting entity must be satisfied that the intermediary is regulated and supervised and has adequate measures in place to comply with the obligations of the AML/CFT Act (or in the case of an overseas person, a regime that contains broadly equivalent obligations) in respect of the customer.

260. For the purposes of this discussion, pooled, omnibus or nominee accounts are those which are not listed in the name of the investor(s), where more than one investor has supplied the funds.

261. Without other AML/CFT obligations, obtaining customer due diligence information about underlying customers has little value for risk management, but is an administrative burden. We further propose that in these circumstances, the reporting entity that is not the intermediary also be exempt from customer due diligence obligations in respect of the underlying customer. This would in essence mean the reporting entity may rely on the intermediary for CDD purposes. Such reliance would need to be subject to the following conditions.

261.1. The reporting entity must be satisfied that the intermediary is regulated and supervised and has adequate measures in place to comply with the obligations of the AML/CFT Act (or in the case of an overseas person, a regime that contains broadly equivalent obligations).

261.2. The reporting entity must obtain written confirmation from the intermediary that CDD has been carried out to the standard required by the AML/CFT Act.

261.3. The reporting entity must have a written agreement with the intermediary to provide customer due diligence information on the relevant customer(s) upon request without delay.

262. We propose that the third condition above could be waived, where the intermediary is able to provide justification of commercial sensitivity to the relevant supervisor.

263. All obligations that relate to the pooled or nominee account itself (held by the intermediary who would be considered a customer of the reporting entity virtue of the fact that they are also a facility holder) still apply. CDD must still be carried out on the intermediary both as a customer and a person acting on behalf of a customer.

Comment sought: *Are there other types of relationships or products that involve intermediaries for which AML/CFT obligations are problematic? Please describe the relationship, which obligations are problematic and explain why they are problematic.*

Would industry like Supervisors to issue guidance which describes who the reporting entities, intermediaries and customers are in specific business relationships and/or transactions, and what obligations apply? If so, which ones?

Section Five – Institutional arrangements

Designated business groups

264. A designated business group (DBG) assists reporting entities within corporate groupings to achieve economies of scale and reduce compliance costs. The AML/CFT Act allows reporting entities within a DBG to share elements of an AML/CFT programme as well as share record keeping, ongoing customer due diligence and account monitoring systems.
265. DBGs also present an opportunity for trans-Tasman harmonisation. The AML/CFT Act's DBG provisions are very similar to the Australian provisions. Given the high rate of trans-Tasman corporatisation, particularly in the banking sector, the Act's provision for cross-jurisdictional DBGs offers opportunity for significant reductions in compliance costs.

Eligibility for membership to a DBG

266. To be eligible to join a DBG a member must be a reporting entity, or a person that is resident in another country with sufficient anti-money laundering and countering the financing of terrorism systems and is supervised or regulated for anti-money laundering and countering the financing of terrorism purposes. The members must also:
- 266.1. be related to each other in terms of corporation law i.e. each member is a holding company, sister-subsiary, or subsidiary of the same holding company, of another member
- 266.2. be party to a joint venture agreement and is providing a financial service (essentially services that are an AML/CFT risk) pursuant to that agreement
- 266.3. be a Government department or State-Owned Enterprise or be involved in the provision of common services or products through a relationship with the Government department of State-Owned Enterprise
- 266.4. be an entity or class of entity prescribed by regulation to be a member of a DGB.

Network agents and sub-agents in the money remittance industry

267. The money remittance industry provides international wire transfer/electronic payments. These services are predominantly provided by agents of organisations such as MoneyGram or Western Union, who in turn provide their services through sub-agents such as corner dairies, ethnic foodmarts, currency exchange providers and some travel agents. Under the AML/CFT Act, each of these sub-agents is a reporting entity. This means they are each responsible for their own AML/CFT programme, CDD, record keeping and so forth.
268. We consider that while this would ensure that each and every remittance service provider was following the Act, there would be merit in allowing agents and sub-agents to join together in a DBG to share account monitoring (thus allowing for multi-site, high frequency transaction monitoring), a central AML/CFT officer (a central point of contact for the AML/CFT supervisor), better training and awareness, and a complex and robust AML/CFT programme.
269. The desirability of money remittance DBGs is increased because the eligibility criteria provide for State-Owned Enterprises and other reporting entities to form a DBG encompassing network agents and sub-agents if they provide common products and

services. This could create a competitive advantage for State-Owned Enterprises over other remittance agents.

Preferred approach

270. We consider that, in light of the potential benefits and in order to address this potential competitive disadvantage, eligibility for membership in a DGB is extended through regulation to encompass private sector network agency and sub-agency relationships in the money remittance industry.

Comment sought: *Would providing for money remittance agents and sub-agents to join in a DBG together affect your business? If so, do you support the preferred option?*

Are there any other business relationships that sit outside the corporate group that you consider would benefit from being eligible for joining a DBG?

If so, please give us your rationale for this and how a DBG structure would bring added benefits for controlling money laundering risks and terrorism financing risks.

Conditions for membership

271. Reporting entities are intended to self-elect into DBGs. The Act provides for regulations to set conditions that must be satisfied in the formation of DBGs. Prior to the formation of DBGs, Supervisors need an understanding of the way in which DBGs intend to manage their AML/CFT programmes across the members and of the proposed oversight for the group.
272. To assist in ongoing supervision of DBGs, it would be useful if DBGs informed Supervisors of any material changes in the financial activities and services that the DBG undertakes or provides, and update them on any material changes to the information that is provided to them when the DBG is approved. This will help AML/CFT Supervisors to maintain up-to-date information on DBGs under their supervision and inform their own supervision policies and schedules.

Preferred approach

273. Our preferred approach would require reporting entities as part of the conditions of DBG membership, to agree to inform its AML/CFT supervisor:
- 273.1. when a DGB is formed
 - 273.2. how the DBG will manage its AML/CFT programmes and functions across the DBG
 - 273.3. how oversight and reporting will be achieved across the DBG
 - 273.4. who the DBG's nominated compliance officer is
 - 273.5. when a reporting entity withdraws from the DBG or the DBG dissolves
 - 273.6. of any material changes in the financial activity of any of the DBG members
 - 273.7. of any material changes in the information provided to Supervisors when the DBG was established.

Comment sought: *Do you think these conditions are appropriate?*

Are there any additional conditions for membership that you think should be applied?

Additional factors to be considered in risk assessments

274. The intention of this Act to adopt, where appropriate in the New Zealand context, Recommendations issued by the Financial Action Task Force is explicit. Effectively, the Recommendations should be adopted unless there is a compelling reason why this is not desirable.
275. FATF refer to a number of situations considered to be high risk, and recommend enhanced measures be applied. Most of those situations have been addressed within the legislation, through specification of types of entities or products to which enhanced due diligence must be applied.

Private banking

276. Our understanding is that private banking is a term for banking, investment and other financial services provided by banks to private individuals investing sizeable assets or high frequency, high value transactions. The term "private" refers to the customer service being rendered on a more personal basis than in mass-market retail banking, usually via dedicated bank advisers. Private banking is typically reserved for customers:
- 276.1. with high levels of wealth
 - 276.2. who conduct high frequency, high value transactions.
277. Private banking may involve increased confidentiality of customer information (the customer's details are only accessible to their personal business manager). The isolation of the relationship between the customer and the business manager from the rest of the organisation means there are additional risks of employee complicity and/or the employee being subject to influence by (often highly valued) customers.
278. When that increased confidentiality is combined with high net wealth or high frequency and high value transaction behaviour, enhanced measures should be applied to ensure that the money laundering risks can be appropriately managed.

Preferred approach

279. While it is possible to regulate to require enhanced due diligence to be applied to private banking situations, requiring a reporting entity to collect information about the source of wealth or funds may not necessarily address all risks associated with this type of service. This is a service that favours anonymity.
280. We are willing to consider that the extent and nature of risks associated with private banking relationships (and referred to by FATF) may not be as significant in the New Zealand context. It is however important for reporting entities who offer this type of service to have policies or controls in place to mitigate the risks that do exist.
281. Under section 58 of the AML/CFT Act, a reporting entity will be required to conduct a risk assessment to understand the money laundering and financing of terrorism risks that it can reasonably expect to face in the course of its business. Section 58(2) sets out a list of factors that a reporting entity must have regard to when conducting its risk assessment, section 58(2)(h) provides for this list to be expanded through regulation.
282. A private banking regulation under section 58(2)(h) would require a reporting entity to explicitly consider the money laundering and financing of terrorism risks that it faces through the provision of private banking (if applicable). This consideration would then need to be accounted for in the reporting entity's AML/CFT programme (under section

57). It is proposed to require a reporting entity to consider private banking as a factor in its risk assessment.

283. Supervisors may choose to issue guidance or a code of practice that discusses the nature of controls that may be appropriate to mitigate the risks associated with this type of financial activity.

Comment sought: *How do you define 'private banking' and does your business offer these services?*

In your view, is private banking a higher risk activity? Please provide evidence that supports your rationale.

Should enhanced due diligence be required?

Is a code of practice desired?

Appendix 1: Timeframes and priorities for regulatory development

	Priority for first six months (to April 2010)	Second round of regulation (May 2010 – December 2010)	Proposed vehicle
Definitions	<ul style="list-style-type: none"> Addition of high value debit cards and other bearer negotiable instruments to the definition 	<ul style="list-style-type: none"> Affiliation of corporations (within the definition of shell banks) 	Regulations
Exemptions	<p><i>Entity exemptions</i></p> <ul style="list-style-type: none"> Second phase entities under FTRA Other second phase entities Exemptions where financial activity is not the main business activity Life insurance exemptions Securities exemptions Corporate treasury functions Security guard exemptions Safe deposit boxes for traveller accommodation <p><i>Reduced measures exemptions</i></p> <ul style="list-style-type: none"> Debt collection exemptions Workplace based superannuation schemes Low value superannuation accounts Overseas pension accounts Insurance products Non-bank deposit-taker products Specific low risk products such as stored value cards Remittance card scheme exemption Verification of address requirement for casinos Wire transfer exemptions <p><i>Threshold exemptions</i></p> <ul style="list-style-type: none"> Occasional transaction <ul style="list-style-type: none"> financial institutions casinos Wire transfers Cross border cash reporting threshold Currency exchange, remittance, travellers cheques and money orders Stored value cards 	<ul style="list-style-type: none"> Government agency exemptions Lotteries Commission Specific case-by case exemptions Consider transitional exemption for some groups from application of 2 year audit to provide for staggering of audits 	Regulations
Customer Due Diligence	<ul style="list-style-type: none"> Basis for verification applying to a specified situation, customer, product, service, business relationship or transaction Circumstances where Standard due diligence applies (anonymous accounts for example) Treatment of specific high risk situations Simplified due diligence – based on public disclosure, accountability and registration factors and 	<ul style="list-style-type: none"> Nothing else planned at this stage 	Regulations or codes of practice or a mix of both

	<p>beneficial ownership checks for specified customers</p> <ul style="list-style-type: none"> Enhanced customer due diligence identity requirements (name of beneficiaries of Trusts for example) Non face-to-face CDD Beneficial ownership requirements including treatment of certain types of trusts and their beneficiaries 		
Third parties	<ul style="list-style-type: none"> Reporting entity and customer relationships Reliance on third parties for carrying out CDD Intermediaries Nominee accounts 	<ul style="list-style-type: none"> Nothing else planned at this stage 	Regulations or codes of practice or a mix of both.
Designated business groups	<ul style="list-style-type: none"> Entity or class of entities prescribed to be a member of a designated business group (network agents and sub-agents) Information that must be provided to Supervisors in terms of oversight arrangements and management and operation of the DBG's AML/CFT responsibilities 	<ul style="list-style-type: none"> Nothing else planned at this stage 	Regulations
Risk assessment and AML/CFT Programmes	<ul style="list-style-type: none"> Factors that reporting entities must have regard to in the risk assessment (eg private banking) National risk assessment (draft) Sectoral risk assessment framework (draft) 	<ul style="list-style-type: none"> Application of the risk based approach generally 	Guidelines or safe harbour codes of practice, or a mixture of both
Record keeping		<ul style="list-style-type: none"> Records that are not required to be kept 	Guidance
Annual reporting		<ul style="list-style-type: none"> Information to be contained in annual reports 	Regulations
Forms	<ul style="list-style-type: none"> STR reporting form Cash border reporting form Designated business group forms 	<ul style="list-style-type: none"> Application form for exemptions Formal warning form Search warrant form 	Regulations

Appendix 2: References

Anti-Money Laundering and Countering Finance of Terrorism Act 2009
Available at www.legislation.govt.nz

Department of Internal Affairs Evidence of Identity Standard
Available at http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index

Ministry of Justice Public Information Document June 2009
Available at: <http://justice.govt.nz/policy-and-consultation/crime/anti-money-laundering-and-countering-the-financing-of-terrorism/fatf>

Financial Action Task Force 40 + 9 Recommendations
Available at: http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html