Regulatory Impact Statement

Anti-Money Laundering and Countering Financing of Terrorism: Identity Verification Code of Practice

Agency Disclosure Statement

1. This Regulatory Impact Statement has been prepared by the Department of Internal Affairs (the Department), with input from the Reserve Bank of New Zealand and the Financial Markets Authority. It provides analysis of options to facilitate compliance with the standard identity verification requirements of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act).

2. The Act requires reporting entities (including financial institutions, trust and company service providers and casinos) to collect and verify identity information about customers, in order to reduce the opportunities for money laundering and terrorism financing. These statutory obligations impose compliance costs on reporting entities.

3. The Act also empowers the Reserve Bank, the Financial Markets Authority and the Department (the AML/CFT supervisors under the Act) to develop codes of practice, for approval by responsible Ministers. A code of practice is a safe harbour that sets out an acceptable method for reporting entities to comply with specific obligations in the Act.

4. There is no private sector standard or agreed industry best practice for identity verification in New Zealand. Any confusion about how to fulfil the identity verification requirements of the Act will increase compliance costs and be detrimental to compliance. An Identity Verification Code of Practice will help address this issue.

5. There is a Government Evidence of Identity Standard. However, reporting entities consider it to be too strict and costly to implement. The proposed Identity Verification Code of Practice is a pragmatic compromise between the Government Standard and the current reporting entity preference that a minimum of a New Zealand Driver Licence alone be acceptable.

6. Key considerations in the development of the Code of Practice have been to ensure that reporting entities are provided with an acceptable method for complying with the Act that helps minimise compliance costs and that harmonises New Zealand's AML/CFT regime with comparable jurisdictions as much as possible.

7. The proposed Identity Verification Code of Practice is unlikely to impair private property rights, market competition, or the incentives on businesses to innovate and invest; or override fundamental common law principles. The cost of complying with the obligations imposed by the Act is likely to reduce. By contrast, the non-regulatory option (reporting entities being left to develop their own processes to comply with the Act) is likely to increase compliance costs, and is not the approach preferred either by reporting entities or by the AML/CFT supervisors.

…….. / / 2011

Marilyn Little, Acting Chair, Regulatory Impact Analysis Panel
Department of Internal Affairs

Problem Definition

8. The Act requires businesses to verify the identity information of customers. However, there is no private sector standard or agreed industry best practice for identity verification in New Zealand, and there is confusion as to what documents can be used as a basis for identity verification under the Act.

9. The most commonly used form of identification is the New Zealand Driver Licence, which some businesses treat as a de facto identity verification standard. However, the Ministry of Transport has stated that the New Zealand Driver Licence cannot be relied upon as proof of identity for the purposes of meeting the objectives of the Act, as the verification process is not robust enough for this application.

10. This confusion will make it more difficult for reporting entities to comply with the Act when it comes into force on 30 June 2013, increasing compliance costs and reducing the ability to detect, deter and investigate money laundering and terrorism financing.

Status Quo

11. Money laundering and the financing of terrorism are global problems. As New Zealand is a member of the Financial Action Task Force (FATF), there is a strong international expectation for it to implement appropriate anti-money laundering and countering financing of terrorism measures.

12. The Act requires reporting entities to undertake customer due diligence, which includes identity verification, in order to reduce the opportunities for money laundering and terrorist financing. Identity verification should be conducted when a customer begins a business relationship with an entity (e.g. a customer setting up an account with a bank) or enters into a one-time transaction (e.g. monetary transfer by wire service or the exchange of currency). Reporting entities should verify the identity of the customer, ensuring that the customer is who he/she claims to be. This may be done by sighting and comparing identification documents. However, there is no private sector standard or agreed industry best practice for identity verification in New Zealand. As a result, there is confusion as to what documents will be acceptable for identity verification under the Act.

13. The most robust form of identification is generally an official passport. To meet international standards, passports require vigorous identity verification and can generally be relied upon for identity verification purposes. However, it is not practical to require presentation of a passport to prove identity in all circumstances. For example, not all New Zealand citizens have passports, and even those who do, do not necessarily routinely carry them as a form of identification.

14. Consultation with stakeholders indicated that the most common document used for identity verification purposes is the New Zealand Driver Licence. However, the Ministry of Transport has stated that a New Zealand Driver Licence cannot be relied upon as proof of identity for the purposes of meeting the objectives of the Act, as the verification process is not robust enough for this application.

15. This indicates a gap between current practice and the requirements under the Act. Without guidance, reporting entities are left to develop their own processes to comply. This could lead to reporting entities expending resources developing their own identity verification processes. Furthermore, current practice indicates a preference for identity verification that is convenient rather than robust. A lack of guidance on what are acceptable identity verification practices will make it more difficult for reporting entities to comply with the Act, and will increase compliance costs, cause confusion and lessen the ability to detect, deter and investigate money laundering terrorism financing.

Objectives

16. The overall objectives sought are those established by the purpose of the Act, which are to:
    - Detect and deter money laundering and the financing of terrorism;
    - Maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the FATF; and
    - Contribute to public confidence in the financial system.
17. The specific objective is to clarify what documents reporting entities can use to verify the identity of their standard customers, as required under the Act.

Regulatory Impact Analysis

Non-regulatory option

18. The non-regulatory approach is the status quo. Reporting entities would be left to develop their own processes to comply with the Act. However, without guidance, reporting entities may find it difficult to develop suitable processes to ensure compliance with the Act. Some reporting entities may waste resources on ineffective processes, while other reporting entities develop more robust processes.

19. Consultation with reporting entities has indicated a preference for processes that are convenient rather than robust. Without clear instruction on how best to comply with the Act, reporting entities may continue in this practice.

20. This issue could be mitigated by supervising agencies providing guidelines on how to comply with the identity verification requirements of the Act. However, guidelines do not offer a safe harbour in terms of compliance with the Act. Therefore, they will not address the uncertainty in relation to an acceptable method that reporting entities could use to comply with identity verification requirements of the Act. The non-regulatory option is not preferred.

Regulatory Options - regulations

21. One regulatory option would be to set out the requirements for identity verification in regulations. While this would address any confusion as to how to comply with the requirements of the Act, it would stifle innovation and not necessarily reduce compliance costs. Reporting entities would have to follow the regulations, and would be unable to develop other equally effective means to verify their customers' identity that may be better suited to their businesses. This option is not preferred.

Regulatory Options - code of practice

22. Following a code of practice provides a safe harbour – an assurance of compliance with the Act. An Identity Verification Code of Practice is the preferred option. It provides more certainty for reporting entities than a non-regulatory approach and ensures a more robust approach to identity verification. A code of practice is also less restrictive than regulations. Reporting entities can opt out if they develop other equally effective means to ensure compliance[1]. This encourages reporting entities to innovate and develop more efficient processes to ensure compliance.

[1] Section 67 Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

23. The Act specifically allows for codes of practice and AML/CFT supervisors are required to develop a code of practice if directed to do so by their Ministers. A code of practice was also specifically requested by reporting entities during consultation on the development of regulations in February 2010.

24. The AML/CFT supervisors consider the Code of Practice appropriate and necessary given the current lack of robust identity verification processes in the industry. Without this guidance, reporting entities may not fully understand their obligations under the Act, adversely affecting compliance, or they may develop overly complex, inefficient processes in order to over-compensate for the uncertainty.

25. The Code of Practice will cover the verification of the name and date of birth for documentary identity verification of customers who are natural persons, assessed as low to medium risk for money laundering and terrorism financing. The code will also cover the verification of name, date of birth and address for the electronic verification of customers. That is, the Code of Practice will apply to standard customer due diligence.

26. All reporting entities in all AML/CFT sectors under the Act will be covered by the Code of Practice. The Reserve Bank, Financial Markets Authority and the Department will consider reporting entities who comply with this code of practice to have met their obligations under sections 16, 20, 24 and 28 of the Act.

27. The Code of Practice will cover document identity verification, document certification and electronic identity verification. It recognises the need for a robust identity verification procedure while also preserving the ease of doing business for reporting entities and their customers. It will do this by specifying robust, primary, forms of identification, such as passports, that can be solely relied upon, or other, less robust, but more accessible, secondary forms of identification that can be used in combination with other information.

28. Two examples of the latter are: a New Zealand Driver Licence along with a check that the details on the Driver Licence match the Driver Licence Database; or a New Zealand Driver Licence in combination with a document issued by a registered bank that includes the person's name and signature, such as a credit card.

29. The proposed Code of Practice does not reflect the Government Evidence of Identity Standard, which prescribes stricter requirements. Reporting entities considered that those stricter identity verification requirements would be unduly burdensome, particularly for standard customer due diligence, and substantially increase compliance costs. The fact that the proposed Code of Practice accepts, for example, a New Zealand Driver Licence with supporting information that, at a bare minimum, shows that the licence is not a forgery, therefore represents a pragmatic compromise.

30. The Code of Practice will also provide guidance on how to verify a person's identity when a transaction does not take place face to face. This procedure will include detailing who may certify documents and the electronic verification of information.

Consultation

31. The Department is satisfied that adequate consultation has been undertaken as required under the Act[2]. Reporting entities have been involved since the initial stages of the development of the code of practice. AML/CFT supervisors have also consulted the relevant Government agencies. Consultation has included:

[2] Section 64(1)(b) Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

- Workshops between industry representatives and officials from the Ministry of Justice and supervisors.
- An informal discussion document (February 2010) seeking information from industry and setting out options.
- A Cabinet approved public consultation document (August 2010) setting out the refined proposals and a range of exemptions, and seeking submissions from industry.
- Feedback on the Code and Cabinet paper from Government agencies such as the Ministries of Economic Development, Justice, the Police, New Zealand Transport Agency and the Privacy Commissioner.

Conclusion and Recommendation

32. The Department and the other two supervisors consider the Code of Practice to be the most effective means to minimise compliance costs as much as possible, give certainty to businesses and allow for exceptions and innovation, while still giving effect to the purposes of the regime.

Implementation

33. A Code of Practice is implemented by the responsible Minister by way of publication of a Notice in the *Gazette*. As required under the Act, the notice will either set out the code or detail where copies of the code in hard copy or electronic format may be obtained. The Reserve Bank, Financial Markets Authority and the Department, as the AML/CFT supervisors, will ensure that reporting entities are aware that the Code has been approved.

Monitoring, evaluation and review

34. The AML/CFT supervisors will monitor the effectiveness of the Code of Practice and its effect on the compliance of reporting entities with their obligations under the Act. Reporting Entities will also be encouraged to provide feedback and report issues with the Code of Practice and its effectiveness.