Regulatory Impact Statement

Identity Information Confirmation Bill

Disclosure Statement

1. This Regulatory Impact Statement has been prepared by the Department of Internal Affairs.

2. It provides an analysis of options to enable the private sector, and more of the public sector, to validate identity information against information held on the Department of Internal Affairs' registers and systems. This will help the private sector to combat identity fraud and to reduce business compliance costs, while protecting the privacy of New Zealanders.

3. The analysis deals with problems in the current legislation. This is supplemented by financial estimates from Deloitte of the compliance cost of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. However, there are no estimates of how much the proposals referred to in this paper will reduce those compliance costs. The fact that a number of banks and other private sector bodies are interested in the proposal would indicate that reduced compliance costs are possible.

4. The proposal outlined in the Statement does not have any effects which the Government has said will require a particularly strong case before regulation is considered. The preferred option will reduce compliance costs on businesses, rather than increase them, and help them to meet other legal requirements.

5. This Regulatory Impact Statement has been prepared by Greg Stephens, Policy Analyst, Identity and General Policy, Department of Internal Affairs.

5 March 2010

Status quo and problem definition

6. The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act) provides that "reporting entities", such as banks and other financial institutions, must undertake customer due diligence in order to verify the identity of their customers. One of the aims of this requirement is to reduce identity fraud which, in turn, will reduce money laundering and the financing of terrorism, as well as other criminal activity. Reporting entities must rely on information, documents, or data provided by an independent and reliable source. There are substantial business compliance costs associated with these requirements. For instance, banks have estimated that they will face an initial $24.4 million cost with $6.4 million in ongoing identity verification costs, whereas Deloitte have estimated that these costs are $4.2 million and $0.8 million respectively.

7. Reporting entities would benefit from checking whether the identity information presented to them is consistent with that held by the most authoritative source of identity information, which is the Department of Internal Affairs for many New Zealanders. Such checks would allow reporting entities to meet their legal obligations, and do so in an easier, and potentially cheaper, manner. This will help to reduce successful identity fraud attempts in the private sector.

8. Access to identity information (i.e. biographical information such as name, and date and place of birth) that the Department of Internal Affairs holds is governed by the Passports Act 1992, the Citizenship Act 1977 (and the associated Citizenship Regulations 2002), and the Births, Deaths, Marriages, and Relationships Registration Act 1995 (the BDMRR Act). These Acts provide differing barriers to allowing businesses to validate identity information in order to meet the requirements of the AML/CFT Act.

9. Under the Passports Act, it may currently be possible to allow passport information to be accessed by private sector companies. This is because the Act allows for disclosure of passport information to "any appropriate agency, body, or person" for the purpose of verifying identity. However, as the Act clearly defines what passport information can be disclosed to agencies, it does not necessarily provide for the validation of information presented to the Secretary. There is also no clear legislative authority to charge fees to recover costs. Further, these provisions were introduced to allow the sharing of passport information with overseas border agencies, not the private sector. There are no comparable provisions in respect of information held on the citizenship registers or the Births, Deaths, and Marriages office's registers.

10. With respect to the Citizenship Act and the Citizenship Regulations, access to the citizenship registers is possible only with the consent of the named individual or on limited other grounds (which would not be applicable to the private sector). The cost of obtaining a copy of an entry in one of the citizenship registers is $26, and copies are provided within a 20 working day timeframe. These costs are too high and the delays are too long for the private sector. No private sector agency currently uses this method on a regular basis.

11. The BDMRR Act provides for public access to the registers of the Births, Deaths, and Marriages office. However, the wording of the Act requires requests to be made to a Registrar (i.e. a real person), rather than providing an automated facility. The Act prescribes that information is generally provided in the form of a printout of the information on the register or on a certificate. These cost $20 and $26 respectively. There is no general provision to allow for the validation of information presented to the Births, Deaths and Marriages office.

12. In summary, the Acts are not designed to allow private sector companies to check whether identity information presented to them is consistent with that held by the Department of Internal Affairs. While the Acts do not necessarily prevent private sector agencies making such checks, getting access to the relevant information is:
    - too slow and too costly (for the Citizenship and BDMRR Acts); and
    - inconsistent with the purpose of the relevant provisions (for the Passports Act).

    This means reporting entities would have to incur substantial compliance costs to undertake these checks to meet their AML/CFT Act requirements, and would likely use other methods to meet their requirements. This may mean customers face burdensome identity verification checks.

Objectives

13. These reforms seek to provide a system for reporting entities (particularly banks), other private sector companies, and parts of the public sector which do not already have information matching provisions, to validate identity information presented to them against that held by the Department of Internal Affairs. The reforms seek to provide a system that—
    - enables reporting entities to combat identity fraud (particularly the use of fictitious identities) effectively; and
    - reduces the length of identity verification processes and potentially the compliance costs for reporting entities.

    These objectives need to be balanced against the need to protect the privacy of New Zealanders.

Regulatory impact analysis

Non-regulatory options

14. There are no non-regulatory options which would achieve these objectives as access to identity information is already highly regulated.

Alternative regulatory options

15. A number of different regulatory measures were considered and discounted as they offered a weak or partial solution. Some options did not adequately balance the different competing policy objectives, while others failed to achieve the desired goal.

16. For instance, one option is to extend the current information matching provisions to the private sector. This would involve each private sector company being added to the schedules in the Citizenship Act and the BDMRR Act. Information matching provisions would need to be inserted into the Passports Act. Further amendments would be needed to the Privacy Act 1993 as well.

17. This option is, however, inconsistent with the current information matching provisions as they only apply to the public sector. It would also create additional legislative burdens on Parliament as, each time a new agency wanted to validate information, Parliament would need to amend the relevant schedules. This would create additional pressures on Parliament's time and resources, while frustrating private sector organisations wanting access to information in order to meet their statutory obligations.

18. A modification on the proposal in paragraph 17, which would reduce the burden on Parliament, is to provide powers to allow the relevant schedules to be amended by an Order in Council. The Legislation Advisory Committee Guidelines (2001) note that such clauses (known as "Henry VIII clauses") should only be used in exceptional circumstances, and should be granted rarely and with strict controls. These strict controls (such as public consultation, sunset clauses, or confirmation by Parliament) would likely create similar frustrations for private sector organisations, and the provisions would still be inconsistent with the current information matching provisions.

19. Using information matching provisions to achieve the objectives could also place additional burdens on the Privacy Commissioner, particularly in reviewing the operation of information matching arrangements. The Privacy Act requires the Privacy Commissioner to report annually on each information matching arrangement, and provides the power for the Privacy Commissioner to obtain a report from each agency (both those imparting and receiving information) from time-to-time. The Office of the Privacy Commissioner has advised that if extended to the private sector, validating information under these provisions would be difficult and resource intensive.

Preferred regulatory option

20. The preferred regulatory option is to enable private sector companies and public sector agencies (who do not already have information matching provisions) to use the Data Validation Service (the DVS) provided by the Department of Internal Affairs. The DVS is an electronic system where agencies supply the identity information presented to them and the system checks whether this information is consistent with that held by the Department of Internal Affairs. Compared to the existing information matching arrangements, the DVS better protects New Zealanders' privacy and provides information that is current when it is needed by an agency.

21. Legislative changes would be required for the DVS to be used by the private sector, and more widely in the public sector. The preferred method is to establish the DVS by statute and thereby enabling the Department to provide an

electronic system for any organisation to check whether the identity information presented to them by members of the public is consistent and up to date with that held on the relevant register(s) or system(s).

22. Any organisation, company, or agency wishing to use the system would first need to enter into an agreement with the chief executive(s) responsible for the Citizenship and Passports Acts and/or the Registrar-General of Births, Deaths, and Marriages. In order to ensure the privacy of New Zealanders is protected, the chief executive and Registrar-General would need to consult with the Privacy Commissioner on generic terms and conditions for these agreements. Before an agency could use the DVS, it would need to obtain the consent of the individual concerned.

23. Overseas experience for similar services indicates that validation services do prevent the use of fictitious identities. The United Kingdom's Passport Validation Service found that one percent of passports presented to user agencies were fraudulent in the two years (to mid-2009) it has operated. A 1999 pilot of the New South Wales Registry of Births, Deaths and Marriages' Certificate Validation Service with *selected* Westpac Bank branches found 13 percent of birth certificates presented to those branches during the four week trial were not consistent with the information held by the Registry. These overseas experiences highlight that identity fraud is a risk faced by many organisations, and using the DVS is an effective tool in identifying fraud. The two pilots run with other government agencies have shown the New Zealand DVS has the potential to combat identity fraud (due to the nature of the two pilots, adverse action could not be taken and figures on identity fraud levels could not be generated).

24. The DVS costs are largely demand driven (higher transactions volumes will allow the per transaction cost to fall) and it is hard to anticipate demand levels. However, it is anticipated that the cost will be lower than $0.50 per transaction (along with set up and monthly costs). This compares well to international services. The United Kingdom's Passport Validation Service operates at £1.77 per transaction for high volume users. The Australian DVS operates from A$0.70 to A$3 per transaction (depending on the volume). It is therefore expected that the DVS will be cost-effective for private sector agencies. The Department is mindful of the need to keep costs low for the DVS to be cost-effective for the private sector.

Consultation

25. The following government agencies have been consulted on the preferred option: the Ministries of Justice, Economic Development, Health, Social Development, Education, Transport, and Foreign Affairs and Trade, the Department of Labour, Inland Revenue, the New Zealand Customs Service, the Treasury, the Police, the Reserve Bank, the Accident Compensation Corporation, the New Zealand Transport Agency, the Securities Commission, and the Office of the Privacy Commissioner. The Department of the Prime Minister and Cabinet has been informed of the proposals.

26. Officials have discussed whether the private sector would use such a service (but not the proposed provisions) with: the Real Estate Agents Authority (a Crown entity), the New Zealand Bankers' Association, the Investment Saving and Insurance Association, seven banks, nine investment and/or insurance companies, and Veda Advantage.

Conclusions and recommendations

27. Of the possible solutions, allowing the private sector to use the DVS, and for it to be used more widely in the public sector, is the recommended option. The DVS provides a way for agencies to be satisfied that the information they are being presented by a member of the public is consistent with that authoritatively held. It also provides agencies subject to the new AML/CFT Act an ability to meet their obligations in an efficient, and potentially cheaper, manner. The DVS achieves this in a manner which protects the privacy of New Zealanders. This is the recommended option.

Implementation

28. The necessary legislative changes will be made by the Identity Information Confirmation Bill. There is no need for transitional provisions.

29. In order for agencies to use the DVS they will need to enter into an agreement with the responsible chief executive and/or the Registrar-General of Births, Deaths, and Marriages. Work to develop these agreements, including the necessary consultation with the Privacy Commissioner, will begin once the legislative changes are made by Parliament. The use of generic agreements would reduce the compliance costs of signing up for agencies.

Monitoring, evaluation and review

30. If any issue is raised with the Act, officials will determine whether there are substantive grounds for a review. The Act will also be subject to regular review by officials.

31. The operations of the DVS will be monitored closely. The proposed amendments will:
    - require the Department of Internal Affairs to report on the operations of the DVS to the Privacy Commissioner when required to do so by the Privacy Commissioner; and
    - allow the Privacy Commissioner to require reviews of the generic terms of agreements.

    Other internal reviews of the operation of the DVS may consider:
    - the rate of uptake;
    - the cost of each transaction; and
    - technological improvements to help user agencies.