Privacy Commissioner
Te Mana Matapono Matatapu
Office of the Privacy Commissioner

28 July 2006

File Reference: L2512

FATF Inter-Agency Working Group
c/– Ministry of Justice
PO Box 180
WELLINGTON

Anti-Money Laundering and Countering the Financing of Terrorism: New Zealand's Compliance with Financial Action Task Force Recommendations: Second Discussion Document

1. INTRODUCTION

1.1 The Financial Action Task Force (FATF) issued its 40 Recommendations to combat money laundering in 1990. In response New Zealand, which is a FATF member, enacted the Financial Transactions Reporting Act 1996 (FTRA). Since then FATF has added the countering of terrorist financing to its mission and issued 9 Special Recommendations on Terrorist Financing.

1.2 The Second Discussion Document sets out proposals for a new Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regime. This new regime will extend the coverage and scope of New Zealand's existing regulatory regime in order to meet the new and enhanced FATF standards. The proposed amendments to the FTRA will impose new requirements that are more extensive and more detailed. They will, for example, expand the group of reporting entities and require them to collect more information on a wider group of individuals.

1.3 The Privacy Commissioner acknowledges the need for New Zealand to implement reasonable anti-terrorism measures and to follow through on its commitment to implement the FATF recommendations. However, much of the information at stake here will be personal information about individuals, and must therefore be handled with due regard for the protection of individual and financial privacy. One challenge will be to implement the proposals in a manner that is compliant with the Privacy Act wherever that is possible.

2. IMPORTANCE OF PROPORTIONALITY AND EFFECTIVENESS

2.1 In assessing the privacy implications of the proposals in the Second Discussion Document the Privacy Commissioner has taken an approach that reflects the proportionality test used internationally to analyse state encroachments upon human rights. It is reassuring to note that it is also one of the guiding principles underpinning the proposed legislative framework. If the intrusion on privacy is to be justified the proposed measures must be:

- demonstrably necessary;
- likely to be effective; and
- proportionate to the demonstrated risk.

2.2 In addition, realistic alternatives that are less privacy-invasive should have been considered.

2.3 An important consideration in this assessment is the extent to which the proposals implement or over-reach the FATF recommendations. The Commissioner acknowledges that where New Zealand has accepted international obligations, such as the FATF Recommendations, the government has a restricted set of choices in implantation. However, for proposals going beyond what is strictly required by the FATF, a more stringent case for intrusive requirements should be made out.

2.4 You may be interested in the Commissioner's submission on the Counter Terrorism Bill articulating a suggested approach to be taken to information privacy and anti-terrorism laws (which can be found at http://www.privacy.org.nz/library/counter-terrorism-bill-maintaining-a-proportionate-response-to-terrorism).

3. GENERAL COMMENT ON PROPOSALS IN 2ND DISCUSSION DOCUMENT

Demonstrable justifications needed for limiting privacy

3.1 The proposals to implement the FATF Recommendations involve significant intrusions into personal privacy. They effectively remove, for example, the option to conduct some forms of banking anonymously, and make further inroads into banking confidentiality (between bank and customer). They also require many financial institutions to undertake a form of surveillance of their customers, and to report on these activities to relevant authorities. Non compliance with these investigative and reporting obligations may attract criminal penalties.

3.2 Therefore, in light of these limits to be placed on privacy, those proposing these changes should clearly establish:

- that the perceived risks exist for New Zealand; and
- that the proposed solutions will be both effective and proportionate to those demonstrated risks.

3.3 It is important to ensure that the compliance costs associated with these proposals are measured not just in terms of the costs to business and government, but also in terms of the inconvenience and loss of privacy to individuals. Initiatives that potentially inconvenience many innocent people and diminish their financial privacy need to be justified by clear evidence of an existing problem and of the likely ability of the proposals to combat the problem.

3.4 In addition, there will need to be evidence of a risk, and an explanation of how the proposed changes will combat that specific risk in New Zealand (in addition to being the least privacy intrusive changes realistically possible). A number of submissions to the First Discussion Document commented that New Zealand is a low risk country in terms of money laundering and terrorist financing. This may suggest that a proportionate response should be equally low impact.

3.5 Under the existing law many thousands of suspicious transaction reports are filed with the Police Financial Intelligence Unit every year, but only a small number are actively investigated and few, if any, result in prosecutions.
This suggests that existing reporting requirements may be resulting in sensitive financial information about innocent individuals being disclosed unnecessarily. It may be unhelpful to extend the reporting requirements unless there is clear evidence that such an extension would have a beneficial effect and would justify the additional compliance costs involved.

Adoption of a risk–based compliance regime

3.6 The Commissioner supports a risk-based compliance regime and welcomes the acknowledgement from the FATF Inter-Agency Working Group that it may be possible to aim for less than full compliance in some areas and/or allow for risk-based exemptions or modifications to some requirements. In our view, this amounts to the application of a proportionate approach.

3.7 However, despite this acknowledgement -that it may be possible to aim for less than full compliance and/or allow for risk-based exemptions -we note the following:

1. Most of the proposals focus on full compliance with the relevant Recommendation, even when the Recommendation expressly allows for flexibility and the adoption of less intrusive, risk-based controls. Those

who wish to propose a more proportionate response are invited to make the case in their submission. The preferred approach would be for those who propose privacy-intrusive solutions to provide the justificatory material to demonstrate that full compliance is necessary.

2. In several instances the proposals appear to go beyond the requirements of the Recommendation.

3. The proposals do not address Privacy Act compliance issues, and the proposals do not appear to have been subjected to a Privacy Impact Assessment.

4. SPECIFIC COMMENTS ON THE PROPOSALS TO IMPLEMENT FATF RECOMMENDATIONS

4.1 The following comments relate to the specific proposals for implementation of the FATF Recommendations.

FATF Recommendation 5 – Customer due diligence (Page 24)

4.2 Financial institutions conduct customer due diligence enquiries in the normal course of business. These may well include identifying and verifying the identity of customers and collecting personal information about them. Such activities are compliant with Information Privacy Principle 1 (IPP 1) of the Privacy Act because the collection is necessary for a lawful purpose connected with a function or activity of the agency.

4.3 However the proposals in the Second Discussion Document involve significant increases in the amount of personal information that agencies will be required to collect about their customers and about the beneficial owners of funds. Some of this information will be collected solely for AML/CFT purposes and will not be necessary for the operational purposes of the agency. This presents a Privacy Act compliance problem. The situation is compounded by the requirement to conduct on-going monitoring of all transactions throughout the course of the business relationship on a risk-sensitive basis.

4.4 The Privacy Commissioner, in her submission on the First Discussion Document, acknowledged the obligations imposed by Recommendation 5 but pointed out a number of areas where the proposals appeared to exceed the requirements. A number of these areas have been highlighted in the current Discussion Document, with further feedback sought.

4.5 The proposals seek to reduce or remove certain of the prescribed amounts and designated thresholds in the legislation, and remove limitations on those parties to a trust whose identity needs to be verified. They also seek to remove the exemption from identification for term deposits. From a privacy perspective

the existing limitations are important features. They provide a relatively crude but nonetheless effective means of ensuring that the additional requirements do not disproportionately inconvenience individuals and financial institutions for limited public benefit.

4.6 In situations where the proposals do not appear to be explicitly required by the Recommendations, there needs to be a higher standard of justification. As mentioned earlier, the analysis needs to address whether the proposed changes are:

- demonstrably necessary (the scale of the problem in New Zealand);
- likely to be effective (how the change will solve that problem);
- proportionate to the demonstrated risk (including whether the benefits from the change outweigh any detriment to the interests of individuals (such as loss of privacy) and others (such as compliance costs incurred by financial institutions or customers and liability for breach of the standard).

4.7 In addition, realistic alternatives that are less privacy-invasive should have been considered.

4.8 The Discussion Document also proposes that identity verification procedures and documentation should be made more stringent and be required in a broader range of situations. Identity verification poses a number of privacy risks, particularly electronic verification using third party databases. This issue is dealt with in more detail under Recommendation 8.

FATF Recommendation 6 – Politically exposed persons (Page 34)

4.9 This Recommendation imposes seemingly intrusive requirements in respect of politically exposed persons, on a risk management basis. The proposals will require financial institutions to subject public figures, their families and their close associates to particular monitoring. This includes both foreign and domestic politically exposed persons.

4.10 The implications of this proposal are not entirely clear but it seems likely to have many complexities. For example, defining "politically exposed persons" with clarity and certainty will be a challenge. A broad definition might cause some difficulties for individuals, as well as for financial institutions that may be criminally liable for their actions in relation to this class of person.

4.11 The Discussion Document states that these proposals will not require service providers to breach privacy law or customer confidentiality obligations, which is reassuring. However further explanation of the reference to "private-sector databases that currently provide information about PEPs" would be of value. This reference is not explained and may give rise to concern. There is

insufficient information in the Discussion Document to fully consider what the privacy implications might be.

FATF Recommendation 8 – New technologies and non face-to-face business relationships or transactions (Page 38)

4.12 This Recommendation requires financial institutions to have policies and procedures in place to address any specific risks arising from telephone and internet transactions where hardcopy documents cannot readily be sighted. This would include policies and procedures relating to electronic verification of identity.

4.13 Electronic verification is described in the Discussion Document as "the process by which a customer is identified by cross-checking and verifying unique personal identifiers through either commercial or government databases". This is an unusual definition and seems unrelated to the focus of the Recommendation. In addition, the term 'unique identifier' has a specific meaning under the Privacy Act, and the use of unique identifiers is regulated by the Act.

4.14 Identity verification is an area of considerable significance to privacy. It involves the handling of personal information relating to the identity of individuals and raises issues including: collection purposes and practices; the accuracy and correction of personal information; secondary uses; unauthorised disclosure; retention and deletion of information; and the use of unique identifiers.

4.15 Recommendation 8 does not mention electronic verification. Despite this, a number of submissions were received in response to the First Discussion Document suggesting ways to enhance the accuracy and effectiveness of electronic verification. These included the issuing of national identification cards, and legislating to give electronic verification service providers access to the electoral rolls, vehicle and driver registers, passports and immigration databases and the birth death and marriage registers. Clearly, many of these suggestions raise significant privacy issues, deserving of a thorough analysis and wide consultation.

4.16 Apparently in response, the Second Discussion Document asserts that electronic verification is an integral component of an effective AML/CFT regulatory regime. It encourages appropriate government agencies to establish a dialogue/protocol with electronic identity verification service providers, to ensure that their services meet certain standards of verification and address security and privacy concerns.

4.17 The Privacy Commissioner is firmly of the view that the current FATF initiative is not an appropriate vehicle for creating a regulatory regime concerning the 'electronic identity verification service' area of business.

4.18 Such a regime is outside the scope of the Recommendations, including Recommendation 8. Compliance obligations are established by the Privacy Act and if regulatory change is to be promoted in this area, it must be done on a wider and more principled basis. Such changes would have potential impacts on many other areas, including private sector credit reporting and e-government identity authentication initiatives.

FATF Recommendation 10 – Record keeping (Page 43)

4.19 Recommendation 10 widens the requirements for retention of background files and correspondence relating to transactions as well as copies of official identification documents for at least 5 years after the business relationship has ended.

4.20 Retention of extensive customer records for lengthy periods after the operational need for the information has passed may pose unjustified privacy risks, particularly if they are required to be of a criminal evidential standard. This proposal requires careful scrutiny to ensure that the compliance costs are worth the proven benefits.

FATF Recommendation 15 – AML/CFT policies, practices and programmes (Page 51)

4.21 It is proposed to require financial institutions to have internal policies, procedures and controls – including compliance management arrangements and screening procedures – to ensure high standards when hiring employees. Although this proposal is in line with Recommendation 15, the Interpretative Note does give the New Zealand Government some discretion relating to the implementation of these measures. If it is decided to implement this proposal, then careful consideration will need to be given to the practicalities involved for financial institutions. There will be implementation issues that need to be taken into account, including those relating to the fair handling of personal information and privacy.

FATF Recommendation 25 – Competent authorities to establish guidelines and provide feedback (Page 56)

4.22 The existing "Financial Intelligence Unit Guidelines" on suspicious transaction reporting are issued by the Police Commissioner after consultation with the Privacy Commissioner under section 25 of the FTRA. The Guidelines form part of the FIU's "Best Practice Guidelines for Financial Institutions" and, in their current form, go well beyond the narrow brief given by the statute.

4.23 The changing nature of the FIU's role raises questions about the future purpose and status of the FIU Guidelines and the Privacy Commissioner's statutory consultation role in respect of them. The proposals seem to suggest that in future the wider guidelines will be issued by "the competent authorities" in consultation with industry, while the FIU guidelines will return to their original role. It appears that neither set of guidelines will be legally enforceable. It may therefore be timely to consider the Privacy Commissioner's future role in relation to these proposals.

4.24 Care will need to be exercised to ensure that the guidelines are clear and unambiguous so that agencies are not encouraged to over-report in an abundance of caution, to the potential detriment of innocent individuals.

LEGISLATIVE MODELS

4.25 The Second Discussion Document identifies three possible legislative models and seeks views from submitters on their preferences.

4.26 From a privacy perspective the preferred model is one in which the key components are set out in the Act itself. These are more than just the high level obligations. Intrusive powers should always be set out in the primary legislation. The grounds on which the new powers may be used and the authority to exercise the powers should be expressly stated in legislation.

4.27 Administrative matters may be contained in regulations and rules. The devil is often in the detail and there are dangers in legislating in the broadest terms and allowing potentially privacy damaging requirements to be imposed by deemed regulations, or by mandatory industry guidelines.

5. FURTHER CONTACT

5.1 If you have any comments or queries arising from this submission, or wish to provide further information, please do not hesitate to contact me or my staff. In the first instance please contact Wayne Wilson, Senior Legal and Policy Adviser (tel: 474 7596).

5.2 The Privacy Commissioner anticipates that there will be challenging issues in translating the basic obligations into an effective workable regime and looks forward to being kept informed as these proposals develop.

Yours faithfully

Blair Stewart
Assistant Privacy Commissioner