Australian Government

Office of the Privacy Commissioner

Draft Consolidated Anti-Money Laundering & Counter-Terrorism Financing Rules

Submission to AUSTRAC

March 2007

COMMENTS PROVIDED BY THE OFFICE OF THE PRIVACY COMMISSIONER ON THE DRAFT CONSOLIDATED AML/CTF RULES

1. The Office made four submissions in relation to the development of the Anti-Money Laundering and Counter-Terrorism Financing legislation[1] ('AML/CTF Act') and has also commented on the previous Draft Consolidated AML/CTF Rules ('Rules') for Discussion in a letter to Mr Neil Jensen, Director, AUSTRAC in October 2006.

Privacy of personal information

2. These comments are relevant to those Rules that require an individual to be identified and those that require the collection and subsequent handling of individuals' personal information. This may include individuals in their capacity as ordinary customers, sole traders, partners, trustees and beneficiaries, executive officers of corporations and associations, beneficial owners, agents and so on. In this regard, where personal information is publicly available (such as that held in the ASIC's company registers), individuals may have different expectations regarding how it is collected and handled, compared to information that is not publicly available. It should be noted however, that the *Privacy Act 1988* (Cth) (Privacy Act) and the National Privacy Principles (NPPs) can still apply to publicly available information in certain circumstances.[2]

Customer 'credit history'

3. The Office notes that paragraph 2.2.13(b)(iii) (previously paragraph 2.2.14(b)(iii) in the draft dated 4 July 2006) of the Rules, now requires a reporting entity to verify "that the customer has a transaction history for at least the past three years" rather than a "credit or transaction history" [emphasis added]. The Office believes that the removal of the reference to "credit" in this context addresses the Office's previous concern of opening the credit reporting system to use for purposes unrelated to consumer credit by reporting entities. However, the Office is concerned that although the explicit reference to "credit" has been removed, this clause may prompt reporting entities to access consumer credit reports to obtain transaction history. Such access is currently prohibited by Part IIIA of the Privacy Act. Part IIIA restricts access to the consumer credit reporting system and includes criminal sanctions for non-compliance, including fines of up to $150,000. Furthermore, the Office would suggest that the contents of an individual's consumer credit report will not necessarily contain the required transaction history and so may not be suitable for collection for this purpose.

4. The Office recommends that paragraph 2.2.13 be re-drafted to clearly indicate its intent and effect, and prevent the rule from being interpreted as authorising the disclosure of consumer credit reports in relation to identification of individuals for AML/CTF purposes.[3] Alternatively, a note could be included at the end of the paragraphs under the heading "Collection of information" to prompt reporting entities to consider their obligations under the Privacy Act when collecting information. For example a note could be formulated in the following manner:

---

[1] The OPC's previous submissions on the Bill are available at http://www.privacy.gov.au/publications/index.html under 'Submissions', 2005 and 2006.

[2] See Information Sheet 17 on "Privacy and Personal Information that is Publicly Available", available from the Office's website: http://www.privacy.gov.au/publications/is17_03.html.

[3] Sections 18K and 18N under Part IIIA of the *Privacy Act 1988* regulate when credit reporting agencies and credit providers may disclose consumer credit information.

"Reporting entities should consider their obligations under other legislation, including the Privacy Act 1988 when deciding what information is required to be collected to fulfil the obligations of these Rules."

Clarity and consistency

5. The Office would also draw attention to issues regarding consistency and clarity between the Act and the Rules, most notably on the issue of levels of risk.

6. Paragraphs 2.2.10 to 2.2.13 of the Rules refer to identification procedures where "the relationship with the customer is of medium or lower ML/TF risk" [emphasis added]. However, the Rules do not indicate how the *relationship* risk is determined. The only relevant definition provided is of the term "ML/TF risk", which deals with risk in relation to *designated services*, rather than in the broader context of a relationship. Accordingly, it is not clear whether the term "relationship" refers to something wider than the risk posed by providing a particular "service".[4] The Office suggests that clarity would be promoted by ensuring that there is consistent use of terms between the AML/CTF Act and the Rules.

7. Considering the close relationship between the AML/CTF Act and the Rules in prescribing the extent of the AML/CTF regime, the Office believes mutual consistency and clarity could be aided by cross-referencing relevant clauses of the Act within the Rules (for example, in relation to section 30 of the Act, discussed below).

'Low-risk' services and risk assessment

8. Sections 30 and 31 of the AML/CTF Act operate when a reporting entity provides a service which "under the AML/CTF Rules…is taken to be a low-risk designated service". Section 30 holds that sections 32 and 34 (which stipulate when customer identification procedures are required) "do not apply" to such low-risk services.[5]

9. In the Office's view, by setting aside sections 32 and 34 for services that are considered low-risk "under the AML/CTF Rules", section 30 of the Act recognises that customer identification procedures are unnecessary for such transactions.

10. However, the Rules do not use the term "low-risk designated service" in relation to their dealing with customer identification procedures. Rather, paragraphs 2.2.10 to 2.2.13 only prescribe procedures for services of "medium or lower ML/TF risk". By subjecting low-risk services to the same identification procedures as medium-risk services, the Office believes the Rules do not adequately reflect the Act's expectation that special provisions (involving reduced identification procedures) will apply for the provision of low-risk services.

11. The Office believes this leaves unclear what, if any, identification and reporting procedures the Rules require for a "low-risk designated service". In particular, when and how an individual engaging in a low-risk transaction needs to identify themselves and what information is required to be collected from them.

12. Effective measures to shield low-risk customers from unnecessary privacy interferences would enhance the level of assurance offered to the community that the

[4] AUSTRAC's "Draft Guidance Paper for Discussion – Applicable customer identification procedures" (date unknown) sought comment on defining "continuity of relationship" for the purposes of clauses 27(5) and (6) of the Bill (at para 32), however it appears that these clauses have not been reproduced in the Act.

[5] Sections 32 and 34 of the Act essentially prevent the provision of designated services unless applicable customer identification procedures have been carried out, either before or after the commencement of designated services (respectively).

new AML/CTF regulatory regime will not unnecessarily impact on the privacy of individuals' personal information. In the Office's view, regulatory measures should be taken to protect privacy, and any adverse impact on privacy must be proportionate to the legislation's benefits. As noted in its August 2006 submission:

> "The Office encourages the [Attorney-General's] Department to consider limits to the number and range of transactions to which the requirement for identification is required. These may include eliminating the requirement to provide identification where the individual is only making enquiries, or where the activity involves low value transactions, such as exchanging small amounts of foreign currency." [6]

13. Before the Rules require identifying information to be collected from a wide range of *low*-risk customers (for example, as paragraph 2.2.11 seems to require), it should be seriously considered whether *any* identification of such customers is necessary where the transaction is not considered suspicious.

14. The Office would like to suggest that a sub-heading could be introduced under Part 2.1 such as "Applying Appropriate Risk Based Procedures" which could be used to make it clear that identification procedures are not required for customers seeking low-risk designated services. Alternatively, a note or additional paragraph could be included between paragraphs 2.1.3 and 2.1.4 to the effect of:

> "Pursuant to section 30 of the Act, identification procedures are not required when a reporting entity is providing low-risk designated services to a customer".

15. The Office notes the addition of Part 4.4 "verification of the identity of low-risk service customer" to the 14 February 2007 version of the draft Rules. The Office believes that Part 4.4 goes some way towards making clear the distinction between designated services that are low-risk and those that are medium or lower ML/TF risk. The Office sees a further opportunity at Part 4.4 to address the issues raised in paragraphs 8-13 above by the addition of a note explaining that section 30 of the Act provides for an exemption from the customer identification procedures required by sections 32 and 34 of the Act for low risk designated services.

Increased guidance for reporting entities

16. While it is understood that the Rules are intentionally drafted to be non-prescriptive, the Office sees merit in increasing the amount of guidance provided to reporting entities in several areas. AUSTRAC has previously issued Draft Guidance Papers for Discussion. However, the current status of these Papers (or updated versions) is unknown. The Office would be interested to know if AUSTRAC plans to progress the development of this guidance material. The Office believes further guidance on issues such as determining AML/CTF risk levels, suspicious matter status, and respecting privacy generally, would improve data quality, reduce unnecessary collection of personal information and promote regulatory certainty.

17. Without further guidance, the Rules appear to allow broad discretion for reporting entities, such as in determining how much personal information may be sought from individual customers (see paragraphs 2.2.4 and 2.9.3). This level of discretion may bring with it the prospects of uncertainty and lack of uniformity in the application of the Rules by reporting entities. It may also cause reporting entities, especially those

[6] Office of the Privacy Commissioner, "Consultation on the second exposure draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006 – Submission to the Attorney-General's Department", August 2006.

not accustomed to collecting personal information of this nature, to seek to collect additional personal information "just in case", leading to greater collection of personal information than is warranted and conflicting with the basic premise of NPP 1 that only information which is *necessary* for a particular purpose should be collected.[7] The Office believes it could make a contribution to the effective operation of the Rules through further consultation with AUSTRAC regarding the preparation of additional guidance materials and would welcome the opportunity to collaborate on this matter.

Definition of Know Your Customer (KYC) information and sensitive information collection

18. The amount of personal information listed under the Rules' definition of "KYC information" ('the KYC definition') in Part 1.3 is considerable. The 14 items proposed, together with the significant discretion conferred on reporting entities in determining how much to collect, heighten the Office's concern that significant privacy safeguards be implemented in the Rules. The Office would like to suggest that the KYC definition, or paragraphs within the Rules that refer to the collection of KYC information could include a note referring reporting agencies to their obligations under the Privacy Act in relation to collection of personal information. (See paragraph 4 above.)

19. In particular, the Office draws attention to part (e) of the KYC definition as it relates to individuals. The customer's place of birth is potentially "sensitive information" for the purposes of the Privacy Act, as it may indicate an individual's racial or ethnic origin.[8] The Privacy Act acknowledges that sensitive information should be handled with a higher degree of privacy protection than other information. Reporting entities that are bound by the Privacy Act may only collect sensitive information in accordance with NPP 10.

20. NPP 10.1 provides that an organisation must not collect sensitive information unless in accordance with conditions set out in NPP 10. These conditions mean that in most cases an organisation must obtain the individual's consent, or the collection must be required by law.[9] By requiring *some* KYC information to be collected, while giving reporting entities wide discretion to determine how much, it is uncertain whether part (e) of the KYC definition would *require* sensitive information to be collected *by law*. If not, reporting entities within the Privacy Act's jurisdiction would need to seek consent for the collection. In the Office's view, the refusal to grant such consent should not be considered "reasonable grounds" for suspicion under the AML/CTF Act or Rules. It is also unclear how consent would be sought if the Rules allowed sensitive information to be collected from third parties.[10]

21. For reporting entities that fall outside the Privacy Act's jurisdiction, the inclusion of "place of birth" as optional KYC information may allow sensitive information to be collected without the expected higher standards of privacy protection. Given these potential issues, the Office suggests that AUSTRAC re-consider whether a customers' place of birth is relevant and necessary for collection by reporting entities; the implications under NPP 10 for the collection of such information; and what the impact of removing part (e) from the KYC definition might be.

---

[7] See National Privacy Principle (NPP) 1.1 under the *Privacy Act 1988*.
[8] See the definition of 'sensitive information' under s 6 of the *Privacy Act 1988*.
[9] NPP10.1(a) and (b) respectively.
[10] For example, collection of sensitive information from third parties may be envisaged under Chapter 4 (re-verification) of the Rules.

Employee information and the 'employee records exemption'

22. The Office notes that some rules may expand the range of personal information collected that falls within the Privacy Act's "employee records exemption" (section 7B(3)). This may include information about customer representatives or agents who are employees (as in Part 2.11 of the Rules) and employee screening information (Part 8.3). The result could be more collection, less scrutiny, and no right to access or correct information held about individuals in their capacity as employees.

23. Part 8.3 of the Rules confers particularly large discretion on employers as to "what manner" of employee screening is conducted. This could potentially involve checking criminal records, which are also considered sensitive information under the Privacy Act. This raises similar collection issues to those noted in paragraphs 19-20.

24. To prevent the expansion of personal information held without recourse or regulation under privacy laws, the Rules could provide that any employee information collected should be handled consistently with the NPPs. Such advice could also be provided in any guidance materials.

Third party collection and handling of personal information

25. Under the Privacy Act, NPP 1.4 requires that personal information be collected only from the individual concerned where reasonable and practicable. However, many of the Rules require or authorise the collection of personal information from third-party sources rather than the individual. For example, such collection may occur in relation to partners, trustees and trust beneficiaries, executives of companies and associations, and customers' agents.

26. If it is not reasonable and practicable to collect personal information from the individual themselves, NPP 1.5, in general terms, requires that where an organisation collects personal information from a third-party it must take reasonable steps to ensure the individual is aware of the matters listed in NPP 1.3. Other parts of the Rules anticipate the *disclosure* of personal information to third-party organisations (for example, Parts 2.11, 5.2 and 8.6), which may require notice or consent under NPPs 1.3 or 2 respectively.

27. It is important that the Rules do not conflict with, diminish or undermine reporting entities' NPP 1 obligations. Such obligations keep individuals informed and in control of their personal information. They also ensure a relationship of trust between individuals and the organisations and government agencies which hold personal information. As with employee information discussed above, the Rules could expressly acknowledge, perhaps in a footnote, that reporting entities covered by the Privacy Act must uphold their NPP 1 obligations in the context of third party collection and disclosure. (See paragraph 4 above.)

Access and correction and complaint handling

28. The Office is concerned about how reporting entities will comply with their NPP 6 obligations in relation to their AML/CTF activities. NPP 6 gives an individual the right to access the personal information that an organisation holds about them. There are some exemptions to NPP 6, which include, at NPP 6.1(h), where denial of access is required or authorised by law. The Office acknowledges that there will be times when a reporting entity may have to deny an individual access to the personal information held about them to ensure compliance with the AML/CTF Act and the

Rules. The Office has published guidelines[11] and an information sheet[12] dealing with the application of NPP 6.

29. The Office is particularly concerned about cases in which the AML/CTF Act and the Rules do not prevent reporting entities from providing individuals with access to the information held about them for the purposes of complying with AML/CTF Rules. The Office fears that due to the nature of that information collected and the implications it could have for the commercial relationship between the reporting entity and its clients, a reporting entity may be less motivated to comply with NPP 6 provisions, or may have difficulty determining how to comply with this provision in the context of its AML/CTF activities. The Office believes that this is an area where guidance material would be particularly useful to reporting entities which may encounter difficulties and increased numbers of complaints in relation to NPP 6 issues. The Office would welcome the opportunity to collaborate with AUSTRAC to develop such guidance material.

Privacy training within AML/CTF Programs

30. Considering the amount of information to be collected, used and disclosed by reporting entities as discussed above, and the serious implications of reporting foreshadowed by the AML/CTF Act and Rules, the Office encourages a greater emphasis on privacy considerations within AML/CTF training programs required by Chapter 8 of the Rules. For example, it is suggested that an express requirement for privacy awareness training be inserted into Paragraph 8.2.3, as a crucial element of a reporting entity's AML/CTF Risk Awareness Training.

31. This approach would help to ensure that organisations covered by the Privacy Act remain conscious of their NPP obligations, including those outlined above, when handling personal information for the purpose of AML/CTF regulation.

Definition of "primary photographic identification document"

32. This definition in Chapter 1 of the Rules appears to narrowly restrict photographic identification to drivers' licences and passports. The Office recommends the addition of state government-issued photographic identity cards as suitable primary documentation. [13] Such cards would seem suitable alternatives to the extent that they require evidence of identity equivalent to that for obtaining a driver's licence.

Anti Money Laundering and Counter Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006

33. The Office suggests that the AML/CTF Rules also include a note in a prominent place to advise small businesses that are usually exempt from the Privacy Act of the effect of the *Anti Money Laundering and Counter Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006.* The effect of this legislation is that if a small business is a reporting entity for the purposes of the Act, the *Privacy Act 1988* will apply to the activities they carry out for the purpose of compliance with the Act or AML/CTF Rules as if the small business operator were an organisation. For example, the note could be formulated in the following manner:

---

[11] Guidelines to the National Privacy Principles September 2001 at http://www.privacy.gov.au/publications/nppgl_01.html#npp6.

[12] Information Sheet 4 - 2001: Access and Correction at http://www.privacy.gov.au/publications/IS4_01.html

[13] This would include New South Wales RTA Photocards and other state equivalents (see http://www.rta.nsw.gov.au/licensing/photocard.html).

"Reporting entities should note that the activities they carry out to comply with these Rules are also subject to the provisions of the *Privacy Act 1988*, even if the reporting entity is generally exempt from coverage by the *Privacy Act 1988*."