The Senate

Legal and Constitutional Legislation Committee

Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005

April 2006

ISBN 0 642 71634 X

This document was printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra

MEMBERS OF THE LEGISLATION COMMITTEE

Members

Senator Marise Payne, **Chair**, LP, NSW
Senator Patricia Crossin, **Deputy Chair**, ALP, NT
Senator Andrew Bartlett, AD, QLD *
Senator Linda Kirk, ALP, SA
Senator Brett Mason, LP, QLD
Senator Nigel Scullion, CLP, NT

Substitute Members

* Senator Natasha Stott Despoja, AD, SA to replace Senator Andrew Bartlett for matters relating to the Attorney-General's Portfolio

Participating Members

Senator the Hon. Eric Abetz, LP, TAS
Senator Lyn Allison, AD, VIC
Senator G. Barnett, LP, TAS
Senator Mark Bishop, ALP, WA
Senator George Brandis, LP, QLD
Senator Bob Brown, AG, TAS
Senator George Campbell, ALP, NSW
Senator Kim Carr, ALP, VIC
Senator Grant Chapman, LP, SA
Senator the Hon R Colbeck, LP, TAS
Senator Stephen Conroy, ALP, VIC
Senator Alan Eggleston, LP, WA
Senator Christopher Evans, ALP, WA
Senator the Hon. John Faulkner, ALP, NSW
Senator Alan Ferguson, LP, SA
Senator Jeannie Ferris, LP, SA
Senator Steve Fielding, FFP, VIC
Senator Concetta Fierravanti-Wells, LP, NSW
Senator the Hon Bill Heffernan, LP, NSW
Senator John Hogg, ALP, QLD
Senator Gary Humphries, LP, ACT
Senator Annette Hurley, ALP, SA
Senator Barnaby Joyce, NATS, QLD
Senator Ross Lightfoot, LP, WA
Senator Joseph Ludwig, ALP, QLD
Senator Kate Lundy, ALP, ACT
Senator the Hon Ian MacDonald, LP, QLD
Senator Julian McGauran, NPA, VIC
Senator Jan McLucas, ALP, QLD
Senator Christine Milne, AG, TAS
Senator Kerry Nettle, AG, NSW
Senator Stephen Parry, LP, TAS
Senator the Hon Kay Paterson, LP, VIC
Senator Robert Ray, ALP, VIC
Senator the Hon. Nick Sherry, ALP, TAS
Senator Rachel Siewert, AG, WA
Senator Ursula Stephens, ALP, NSW
Senator Russell Trood, LP, QLD
Senator John Watson, LP, TAS

Secretariat

Mr Jonathan Curtis	Secretary
Ms Julie Dennett	Principal Research Officer
Ms Rebecca Manen	Principal Research Officer
Ms Ann Palmer	Senior Research Officer
Ms Marina Seminara	Executive Assistant

Suite S1.61	T: (02) 6277 3560	E: legcon.sen@aph.gov.au
Parliament House	F: (02) 6277 5794	W: www.aph.gov.au/senate_legal

TABLE OF CONTENTS

ABBREVIATIONS

ABA	Australian Bankers' Association
ACA	Australian Casino Association
Allens	Allens Arthur Robinson
AML/CTF	anti-money laundering and counter-terrorism financing
APF	Australian Privacy Foundation
APRA	Australian Prudential Regulation Authority
ASFA	The Association of Superannuation Funds of Australia
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CUIA	Credit Union Industry Association
Department	Attorney-General's Department
Exposure Bill	Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005
EV	electronic verification
FATF	Financial Action Task Force on Money Laundering
FATF Recommendations	FATF Forty Recommendations on AML
FPA	Financial Planning Association of Australia
FSR	Financial Services Reform
FSR Act	*Financial Services Reform Act 2001*
FTR Act	*Financial Transaction Reports Act 1988*
IAG	Insurance Australia Group
ICA	Insurance Council of Australia
IFSA	Investment & Financial Services Association
Minister	Minister for Justice and Customs

NPPs	National Privacy Principles
NSWCCL	NSW Council for Civil Liberties
NSWPC	Office of the NSW Privacy Commissioner
OPC	Office of the Privacy Commissioner
PIA	Privacy Impact Assessment
Platinum	Platinum Asset Management Limited
Privacy Act	*Privacy Act 1988*
SDIA	Securities & Derivatives Industry Association
SMSFs	self-managed superannuation funds
Special Recommendations	FATF Nine Special Recommendations on CTF
UK	United Kingdom
US	United States

CHAPTER 1

INTRODUCTION

Background

1.1 On 9 February 2006, the Senate referred the Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005 (Exposure Bill) to the Legal and Constitutional Legislation Committee for inquiry and report by 13 April 2006.

1.2 The Attorney-General's Department (Department), in conjunction with the Australian Transaction Reports and Analysis Centre (AUSTRAC), is also conducting a public consultation process; comments and submissions to that process close on 13 April 2006. The committee is mindful of advice by the Department and media reports that the Exposure Bill is not a static document and will undergo substantial re-drafting during, and as a result of, the consultation process.[1] However, the committee has necessarily confined itself to examination of the publicly released version of the Exposure Bill for the purposes of this inquiry.

1.3 The Exposure Bill forms part of a package of reforms consisting of legislation, regulation and rules, which is eventually intended to replace Australia's principal anti-money laundering legislation, the *Financial Transaction Reports Act 1988* (FTR Act), and the *Financial Transaction Reports Regulations 1990*. The Exposure Bill will supersede the FTR Act to the extent that the FTR Act applies to financial services.

1.4 The package of reforms is intended to improve and strengthen Australia's current anti-money laundering and counter-terrorism financing (AML/CTF) system, in line with international standards issued by the Financial Action Task Force on Money Laundering (FATF).[2]

1.5 These international standards are contained in the FATF Forty Recommendations on AML, which were revised in June 2003 (FATF Recommendations), and the Nine Special Recommendations on CTF (Special Recommendations) which were adopted following the terrorist attacks in the US on 11 September 2001.

---

1 See, for example, *Committee Hansard*, 14 March 2006, p. 61; E. Colman, 'Dirty money laws stall, face revision', *The Australian*, 17 March 2006.

2 The FATF is an international organisation concerned with strengthening AML provisions in the global financial system, including recommending legislative and enforcement measures for individual countries to implement.

1.6 The FTR Act was last updated in a significant way through the *Proceeds of Crime Act 2002* and, in relation to terrorism, through the *Suppression of the Financing of Terrorism Act 2002*. However, following the revision of the FATF Recommendations in 2003, the Federal Government committed itself to a further overhaul of the FTR Act and associated legislation.[3] In December 2003, the Minister for Justice and Customs (Minister) announced that Australia would be implementing the FATF Recommendations which would require a significant review of Australia's AML regime, including some new measures intended to counter terrorist financing.[4]

1.7 Early consultations with stakeholders resulted in a range of in-principle agreements between the Federal Government and industry on the approach to the proposed reforms, including implementation of the reforms in two tranches. Following the conclusion of these consultations, the Minister announced, in October 2005, that the Federal Government had agreed to proceed with a package of reforms to strengthen Australia's AML/CTF system. The Minister also announced that the next step in the reform process would be the release of the Exposure Bill.[5]

1.8 The Exposure Bill sets out the first tranche of reforms covering a range of services provided by the financial services sector, gambling service providers and bullion dealers. It also covers lawyers and accountants to the extent that the services provided are in direct competition with the financial sector.[6]

1.9 Following the first stage of reforms, the Minister has indicated that there will be a second stage extending AML/CTF obligations to real estate agents, jewellers and professionals, such as accountants and lawyers, when they provide specified non-financial services.[7] The committee understands that there is no settled timeframe for the second stage but that it is likely to be developed during the transition period for the first tranche of reforms. The FTR Act will remain in force, although significantly

---

3 Sue Harris Rimmer, Ann Palmer, Angus Martyn, Jerome Davidson, Roy Jordan and Moira Coombs, Parliamentary Library, Anti-Terrorism Bill (No. 2) 2005, Bills Digest No. 64 2005-06, 18 November 2005, p. 49.

4 Minister for Justice and Customs, Media Release, *Australia endorses global anti-money laundering standards*, 8 December 2003, at http://www.ag.gov.au/agd/www/Justiceministerhome.nsf/Page/RWP448419DCA3156F1BCA256DF5007AC772?OpenDocument (accessed 6 April 2006).

5 See http://www.ag.gov.au/aml

6 Minister for Justice and Customs, Media Release, *Exposure draft of anti-money laundering and counter-terrorist financing Bill released for public comment*, 16 December 2005, at http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/AllDocs/B8D9EAFB4FED18E6CA2570D8007C616D?OpenDocument (accessed 7 February 2006).

7 Minister for Justice and Customs, Media Release, *Exposure draft of anti-money laundering and counter-terrorist financing Bill released for public comment*, 16 December 2005, at http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/AllDocs/B8D9EAFB4FED18E6CA2570D8007C616D?OpenDocument (accessed 7 February 2006).

amended, until the second stage of legislation applying to non-financial services matters, at which point it will be repealed.

1.10 Significantly, Australia's progress in meeting the FATF Recommendations was reported in a FATF country evaluation published in October 2005. The evaluation found that Australia's AML/CTF laws addressed requirements under 31 of the 40 FATF Recommendations. In relation to the Special Recommendations, the evaluation rated Australia as 'partially compliant' with Special Recommendation VI (regulating alternative remittance dealers), Special Recommendation VIII (regulation of charitable and non-profit organisations) and Special Recommendation IX (cash couriers), and 'non-compliant' with Special Recommendation VII (wire transfer funds services). Australia achieved a rating of 'largely compliant' with most of the other Special Recommendations.[8]

1.11 The Anti-Terrorism Bill (No 2) 2005 addressed four of the Special Recommendations. Amendments contained in Schedule 3 of that bill were intended to 'strengthen the existing terrorist financing offences'[9] in the Criminal Code and the FTR Act. Schedule 9 of that bill amended the FTR Act (with consequential amendments to the *Proceeds of Crime Act 2002* and the *Surveillance Devices Act 2004*) to address Special Recommendation VI, Special Recommendation VII and Special Recommendation IX.

1.12 The committee understands that proposed reforms in the Exposure Bill will ensure that Australia complies fully with the remainder of the FATF Recommendations plus the Special Recommendations, excluding Recommendation 12 (designated non-financial businesses and professions – to be covered by the second tranche of reforms), and excluding Special Recommendation 8 (non-profit and charitable organisations – to be dealt with separately[10]). The committee also notes that some aspects of the FATF Recommendations and the Special Recommendations are already covered by other legislation, including the Criminal Code, and mutual legal assistance and extradition legislation.

---

8 Minister for Justice and Customs, Media Release, *Australia fighting money laundering and terrorist financing*, 17 October 2005, at http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/AllDocs/2DCD3F1AC23A43A8CA25709E0027F92E?OpenDocument (accessed 6 April 2006).

9 *Explanatory Memorandum*, p. 12.

10 In September 2005, the Council of Australian Governments (COAG) agreed that the Commonwealth would consult with the states and territories about the enactment of laws to prevent the use of non-profit or charitable organisations for the financing of terrorism: Minister for Justice and Customs, Media Release, *Australia fighting money laundering and terrorist financing*, 17 October 2005, at http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/AllDocs/2DCD3F1AC23A43A8CA25709E0027F92E?OpenDocument (accessed 6 April 2006).

Conduct of the inquiry

1.13 The committee advertised the inquiry in *The Australian* newspaper on 1 March 2006, and invited submissions by 8 March 2006. Details of the inquiry, the Bill, and associated documents were placed on the committee's website. The committee also wrote to over 80 organisations and individuals.

1.14 The committee received 33 submissions which are listed at Appendix 1. Submissions were placed on the committee's website for ease of access by the public.

1.15 The committee held a public hearing in Sydney on 14 March 2006. A list of witnesses who appeared at the hearing is at Appendix 2 and copies of the Hansard transcript are available through the Internet at http://aph.gov.au/hansard.

Acknowledgement

1.16 The committee thanks those organisations and individuals who made submissions and gave evidence at the public hearing.

Note on references

1.17 References in this report are to individual submissions as received by the committee, not to a bound volume. References to the committee Hansard are to the proof Hansard: page numbers may vary between the proof and the official Hansard transcript.

CHAPTER 2

OVERVIEW OF THE BILL

2.1 This chapter briefly outlines the purpose and main provisions of the Exposure Bill.

Purpose of the Exposure Bill

2.2 The Exposure Bill is intended to provide a generic framework enabling individual businesses to manage money laundering and terrorism financing risks specific to their industry sector. The Bill purports to adopt a risk-based – rather than a prescriptive – approach. The general principles set out in the Exposure Bill will be supplemented by legally-binding Rules, and non-binding Guidelines.[1]

2.3 The Rules are intended to establish operational details, including relevant standards and specific requirements for matters such as customer identification procedures, the monitoring of customer activity, reporting suspicious matters, appropriate 'risk-trigger' events, and the development of AML/CTF Programs.

2.4 The Guidelines will provide guidance only and may be issued by AUSTRAC from time-to-time to assist reporting entities to interpret their obligations under the AML/CTF legislative framework.

2.5 AUSTRAC would continue to be Australia's financial intelligence unit and AML/CTF regulator. AUSTRAC would regulate reporting entities covered under the Exposure Bill and continue to collect, retain, analyse and disseminate financial intelligence to designated law enforcement, revenue, national security, social justice and other regulatory agencies. AUSTRAC would also have an enhanced enforcement and monitoring role under the Exposure Bill.[2]

Main provisions of the Exposure Bill

General outline

2.6 Banks and other 'cash dealers' are already subject to AML/CTF measures under the FTR Act. However, the Exposure Bill (as well as the amendments to the

---

1 *Overview of the exposure Anti-Money Laundering and Counter-Terrorism Financing Bill* at http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~OverviewExposureDraftAML.pdf/$file/OverviewExposureDraftAML.pdf (accessed 7 February 2006).

2 *Overview of the exposure Anti-Money Laundering and Counter-Terrorism Financing Bill* at http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~OverviewExposureDraftAML.pdf/$file/OverviewExposureDraftAML.pdf (accessed 7 February 2006).

FTR Act, and other related legislation, made by the Anti-Terrorism Bill (No 2) 2005) extends these measures beyond 'cash dealers' to include a range of other financial service providers.

2.7 AML/CTF obligations under the Exposure Bill will no longer be linked to cash transactions. Instead, an activities-based definition will be introduced under which a person who provides, deals in, or handles a 'financial product'[3] will be subject to customer due diligence and enhanced reporting obligations.

2.8 The Exposure Bill sets out the primary obligations of 'reporting entities' when providing 'designated services'. A 'reporting entity' is a financial institution, or other person. The key obligations for reporting entities under the Exposure Bill include:

- verifying the identity of new customers;
- monitoring customers and their transactions;
- reporting specified transactions and suspicious matters; and
- implementing and maintaining AML/CTF Programs.

2.9 AML/CTF Rules will set out the specific requirements to underpin the broader obligations contained in the Exposure Bill. The Rules will enable the flexible application of the Exposure Bill's broader principles such as customer due diligence. The Rules are being developed by AUSTRAC, in consultation with industry, and will be legally binding.

2.10 The Rules would cover the following types of matters:

- standards and/or procedures that reporting entities should use when verifying the identify of a customer – procedures may apply to different types of customers (for example, individuals, companies and other legal entities);
- the matters that reporting entities should take into account in determining whether a matter is suspicious and should be reported to AUSTRAC;
- the matters that reporting entities should address in their AML/CTF Programs, including:
    - systems to identify and mitigate money laundering and terrorism financing risks;
    - a customer due diligence program; and
    - a staff risk-awareness training program;
- when reporting entities should re-verify the identity of customers;

3 The definition of 'financial product' will correspond to the definition of that term in the *Corporations Act 2001* – although some of the more specific exemptions in the Corporations Act relating to financial services regulation for investor protection and market integrity purposes, which do not accord with AML/CTF objectives, will not apply.

- the details that reporting entities should include in their reports to AUSTRAC of threshold transactions, suspicious matters and funds transfer instructions; and
- the matters that reporting entities should assess when conducting a due diligence assessment of a correspondent banking relationship.[4]

2.11 The Guidelines would not be legally binding. They will be developed by AUSTRAC in consultation with industry.[5]

2.12 The following provides a brief summary of each Part of the Exposure Bill.

Part 1 - Introduction

2.13 Part 1 provides the objects of the Exposure Bill. Definitions are contained in proposed section 5.

2.14 As noted above, a 'reporting entity' is a financial institution, or other person, who provides 'designated services'. Designated services are listed in the tables in proposed section 6. Reporting entities will have customer due diligence, reporting and record-keeping obligations for such designated services. As the tables list services rather than specific service providers, any business that supplies one of the listed services will be covered, for example, lawyers and accountants who provide financial services.

2.15 Whether the person (legal or natural) providing the designated service is a 'reporting entity' will also be determined by whether the service is provided:

- at or through a permanent establishment of the person in Australia;
- by a resident of Australia at or through a permanent establishment of the person in a foreign country (foreign branch); or
- by a subsidiary of a company that is a resident of Australia at or through a permanent establishment of the subsidiary in a foreign country (foreign subsidiary) (proposed subsection 6(4)).

2.16 A service provider that does not have one of these geographical links to Australia is not a 'reporting entity' under the Exposure Bill.

---

4 *Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Rules – Questions and Answers* at http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~QAAMLCTFRules.pdf.pdf/$file/QAAMLCTFRules.pdf.pdf (accessed 10 February 2006)

5 *Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Rules – Questions and Answers* at http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~QAAMLCTFRules.pdf.pdf/$file/QAAMLCTFRules.pdf.pdf (accessed 10 February 2006)

2.17 Reporting entities that are foreign branches or foreign subsidiaries of Australian residents will be required to apply the principles of Australian AML/CTF obligations through their AML/CTF Programs to the extent possible under local law.

Part 2 – Identification procedures

2.18 Part 2 provides customer identification obligations of reporting entities, which form part of their customer due diligence responsibilities. A reporting entity must carry out a procedure to verify a customer's identity before providing a designated service to the customer. However, in special cases, customer identification procedures may be carried out *after* the provision of the designated service. Such special circumstances would involve instances where identifying the customer before the provision of the designated service would disrupt the ordinary course of business, and the service is specified in the AML/CTF Rules, and:

- is not provided on a face-to-face basis; or
- consists of acquiring or disposing of a security or derivative on behalf of a customer; or
- consists of issuing or undertaking liability as the insurer under a life policy or a sinking fund policy.

2.19 Existing customers will not be subject to initial customer identification requirements and will only need to have their identity re-verified where warranted by materiality and risk. However, existing customers would be subject to ongoing due diligence obligations.

2.20 The AML/CTF Rules will set out circumstances in which the identity of all customers will be required to be re-verified. The Rules may vary customer identification procedures for the provision of certain designated services taken to be low-risk services. The Rules will include a mechanism to allow a third party to carry out customer identification procedures on the reporting entity's behalf.

Part 3 – Reporting obligations of reporting entities

2.21 A reporting entity must give AUSTRAC reports about suspicious matters (proposed section 39).

2.22 Issues to be taken into account in determining whether to report a suspicious matter will be set out in the AML/CTF Rules. Relevant issues may include whether a transaction was complex, unusual or large, or whether it involves a resident of a particular foreign country.

2.23 Further, if a reporting entity provides a designated service that involves a threshold transaction ($10,000, unless changed by regulation), the reporting entity must give AUSTRAC a report about the transaction within 10 business days after the day on which the transaction takes place (proposed section 41).

2.24 If a reporting entity provides a designated service that relates to an international funds transfer instruction, the reporting entity must give AUSTRAC a report about the provision of the service within 10 business days after the day on which the service commenced to be provided (proposed section 42).

Part 4 – Reports about cross-border movements of physical currency and bearer negotiable instruments

2.25 Cross-border movements of physical currency must be reported to AUSTRAC, a customs officer or a police officer, if the total value moved is above a threshold of $10,000 (proposed section 49).

2.26 If a bearer negotiable instrument is produced to a police officer or a customs officer by a person leaving or arriving in Australia, the officer may require the person to give a report about the instrument to AUSTRAC, a customs officer or a police officer (proposed section 55).

Part 5 – Funds transfer instructions

2.27 Reporting entities must verify the identity of customers originating a funds transfer and transmit originator information with the funds transfer (proposed sections 58, 60 and 61).

2.28 Where a reporting entity receives two or more incoming funds transfer instructions from an overseas counterpart that do not include appropriate originator information, AUSTRAC may direct the reporting entity to request their overseas counterpart to include appropriate originator information in all future funds transfer instructions (proposed section 59).

Part 6 – Register of providers of designated remittance services

2.29 AUSTRAC must maintain a register of providers of designated remittance services (proposed section 71). Persons who provide designated remittance services must provide business details to AUSTRAC for inclusion on the register (proposed section 70).

Part 7 – Anti-money laundering and counter-terrorism

2.30 Reporting entities must develop, maintain and comply with AML/CTF Programs (proposed section 73).

2.31 An AML/CTF Program is defined in proposed section 74. An AML/CTF Program is a program that is designed to identify and 'materially mitigate' the risk that the provision of a designated service might involve or facilitate a transaction that is connected with the commission of:

- a money laundering offence; or
- a financing of terrorism offence.

2.32 Amongst other things, AML/CTF Programs must require the monitoring by reporting entities of their provision of designated services to each of their customers (monitoring forms part of their ongoing customer due diligence obligations).

Part 8 – Correspondent banking

2.33 Financial institutions must not enter into a correspondent banking relationship with a shell bank or another financial institution that maintains accounts with a shell bank (proposed section 78).

2.34 Before a financial institution enters into a correspondent banking relationship with another financial institution, the financial institution must carry out a due diligence assessment (proposed section 79).

2.35 If a financial institution has entered into a correspondent banking relationship with another financial institution, the financial institution must carry out regular due diligence assessments (proposed section 80).

2.36 A financial institution must not enter into a correspondent banking relationship with another financial institution unless the respective rights, obligations and responsibilities of the parties are set out in a written agreement (proposed subsection 79(5)).

Part 9 – Countermeasures

2.37 Regulations may prohibit or regulate transactions with residents of prescribed foreign countries (proposed section 83).

Part 10 – Record-keeping requirements

2.38 If a reporting entity makes a record of a designated service, the reporting entity must retain the record for a certain number of years (to be agreed after consultation) (proposed section 85).

2.39 If a customer of a reporting entity gives the reporting entity a document relating to the provision of a designated service, the reporting entity must retain the document for a certain number of years (to be agreed after consultation) (proposed section 86).

2.40 A reporting entity must retain a record of an applicable customer identification procedure for a certain number of years (to be agreed after consultation) after the end of the reporting entity's relationship with the relevant customer (proposed section 87).

2.41 A person who carries out an applicable customer identification procedure on behalf of a reporting entity must give a record of the procedure to the reporting entity (proposed section 88). The reporting entity must retain the record for a certain number of years after the end of the reporting entity's relationship with the relevant customer (proposed section 89).

Part 11 – Secrecy and access

2.42 Specified government agencies (the Australian Taxation Office (ATO) and other designated agencies) will be able to access information held by AUSTRAC, under certain conditions. In the case of the ATO, information may be accessed for any purpose relating to facilitation of the administration or enforcement of a taxation law; in the case of other agencies, information may be accessed for the purposes of performing that agency's functions and exercising the agency's powers (proposed sections 98 and 99).

2.43 Reporting entities must not disclose that they have formed an applicable suspicion or have reported information to AUSTRAC under the suspicious matter reporting requirements, or that they have given further information to a law enforcement agency in response to a request (proposed section 95).

Part 12 – Offences

2.44 Part 12 of the Exposure Bill establishes offences for:

- providing false or misleading information or documents (proposed sections 107 and 108);
- forging identity documentation (proposed section 109);
- providing or receiving a designated service anonymously or using a false customer name (proposed sections 110 and 111); or
- structuring a transaction to avoid a reporting obligation (proposed sections 112 and 113).

2.45 Other offences are contained in other Parts of the Exposure Bill for failure to comply with specific requirements set out in those Parts.

Part 13 – Audit

2.46 An 'authorised officer' (a member of the staff of AUSTRAC, appointed in writing by AUSTRAC) may enter any reporting entity business premises by consent or under a monitoring warrant to monitor compliance with obligations under the Exposure Bill (proposed section 117).

2.47 Monitoring powers of authorised officers are contained in proposed sections 118 and 119.

Part 14 – Information gathering powers

2.48 Part 14 enables authorised officers to give a notice requiring the giving of information or the production of documents from a reporting entity or a person suspected of being a reporting entity (proposed section 131).

Part 15 – Enforcement

2.49 Part 15 provides a civil penalty framework as an alternative enforcement mechanism to criminal offence provisions.

2.50 In addition to the criminal offences in Part 12, there are criminal offences in other Parts of the Exposure Bill for failure to comply with requirements set out in those Parts. For many of those offences, the same conduct that constitutes the criminal offence may also be the subject of a civil penalty provision. This creates a two-tier system of penalty provisions, whereby civil penalties would be used in situations where the offending conduct does not warrant criminal prosecution; criminal sanctions would be sought for more serious failures to comply with obligations.

2.51 Pecuniary penalties are payable for contravention of civil penalty provisions (proposed section 140).

2.52 Authorised officers, customs officers and police officers may issue infringement notices where a report that is required for cross-border movements of physical currency or bearer negotiable instruments is not made (proposed sections 149 and 150).

2.53 AUSTRAC is to monitor compliance by reporting entities of their obligations under the Exposure Bill (proposed section 155).

2.54 The Federal Court may grant injunctions in relation to contraventions of the Exposure Bill (proposed sections 156 and 157).

2.55 Customs officers and police officers may exercise powers of questioning, search, seizure and arrest in connection with a cross-border movement of physical currency or bearer negotiable instruments (proposed sections 161, 162 and 163).

Part 16 – Administration

2.56 Part 16 establishes AUSTRAC, its functions and staffing arrangements; and provides that AUSTRAC may issue legislative instruments, known as AML/CTF Rules.

Part 17 – Vicarious liability

2.57 Part 17 establishes a standard of proof for liability in matters involving employees or agents of reporting entities.

Part 18 – Miscellaneous

2.58 Part 18 contains miscellaneous provisions:

- partnerships, trusts and unincorporated associations are to be treated as persons for the purposes of the Exposure Bill (proposed sections 196, 197 and 198);

- the Exposure Bill is not intended to affect the concurrent operation of state and territory laws (proposed section 199);
- the Exposure Bill does not affect the law relating to legal professional privilege (proposed section 201);
- a contravention of the Exposure Bill does not affect the validity of any transaction (proposed section 202);
- provision is made in relation to the making of reports to AUSTRAC (proposed section 203); and
- the Governor-General may make regulations for the purposes of the Exposure Bill (proposed section 205).

CHAPTER 3

KEY CONCERNS FOR INDUSTRY

3.1 Business and industry bodies who participated in the committee's inquiry expressed in-principle support for the need for an effective and efficient framework to prevent money laundering and terrorist financing activity in Australia. However, a range of concerns emerged in submissions and oral evidence in relation to specific aspects of the proposed AML/CTF regime. These included timing issues with respect to consultation and implementation of the new regime.

3.2 This chapter considers the key issues and concerns for industry raised in the course of the committee's inquiry.

Consultation process

3.3 On 16 December 2005, the Minister released the Exposure Bill for public comment for a period of four months, with the aim of introducing the legislation into Parliament in June 2006.[1] As noted in Chapter 1, submissions to that process close on 13 April 2006. However, the committee understands that extensive consultations in relation to the AML/CTF regime have been progressing on an ongoing basis with the financial sector since January 2004.

3.4 Key features of the consultation process aside from the release of the Exposure Bill have included:

- commencing in July 2005, a series of four Ministerial meetings between the Minister, officials from the Department and AUSTRAC, and representatives of the financial sector; and
- the later establishment of a formal consultative framework comprising of:
    - an overarching ministerial advisory group (that is, the Minister and representatives of the peak industry bodies); and
    - a number of joint industry/AUSTRAC technical working groups and sub-working groups.[2]

3.5 The committee understands that there are currently four working groups reporting to the ministerial advisory group, each of which is co-chaired by industry representatives and government. In three cases, the government co-chair is AUSTRAC and in the other case, the co-chair is the Department. These working groups are examining the following areas:

- AML/CTF programs;

---

1 See http://www.ag.gov.au/aml (accessed 7 February 2006)

2 *Committee Hansard*, 14 March 2006, pp 63-65.

- international issues;
- risk principles; and
- identity verification.[3]

Timeframe for consultation

3.6 During the course of the inquiry, the committee learned that most industry groups have been largely satisfied with the extent and nature of their ongoing engagement with the Minister and/or the Department in terms of preliminary discussions and a consultation process.

3.7 However, despite this, all industry groups expressed concern that the four-month consultation period for the Exposure Bill itself, and the associated Rules and Guidelines, is not adequate to thoroughly assess the full impact of the regime.

3.8 The Investment & Financial Services Association (IFSA) argued that this is amplified by the fact that key areas of the regime are yet to be finalised. At the time of IFSA's submission:

> … around half of the consultation period ha[d] passed and much of the detail around critical elements of the package such as an acceptable method for Electronic Verification; acceptable methods for determining P[olitically] E[xposed] P[erson]s; Risk Triggers for re-identification; Continuity of Relationship and Low Risk Designated Services are still outstanding.[4]

3.9 IFSA also pointed out, despite the best efforts and intentions of all parties, adequate consultation on a finalised package in the remaining timeframe is not possible:

> … the range of services covered in the Bill are very broad and in order to effectively regulate those services, the relevant products themselves and the way they operate and are distributed needs to be clearly understood. For this reason, industry believes that effective consultation on the AML/CTF package needs to be iterative (i.e. submissions made by industry, considered by AUSTRAC, AUSTRAC then providing feedback or seeking further clarification from industry or both, and industry responding, etc).[5]

3.10 Mr John Anning from the Financial Planning Association of Australia (FPA) agreed with this assessment:

> Given the scale of the task to create an effective AML CTF regime, it is not an indictment of the effort put in by all parties that much remains to be done before industry can comment definitively on the proposed regime. FPA strongly believes therefore that the government should extend the

---

3 *Committee Hansard*, 14 March 2006, p. 65.

4 *Submission 2*, p. 2.

5 *Submission 2*, p. 2.

> consultation period beyond the current deadline of 13 April in order for comprehensive analysis to be undertaken as to how the components of the regime will work together. The effective implementation of this legislation is too critical to Australia's welfare to be jeopardised by strict adherence to initial time lines.[6]

Staggered release of Rules

3.11 Many submissions and witnesses argued that the timeframe for consultation was particularly inadequate given that the majority of the Rules were not released as part of the consultation process, and particularly since much of the detail forming the basis of the new regime is to be included in the Rules and the Guidelines.

3.12 Many submissions expressed concern that, without the full package of draft legislative instruments, affected bodies are unable to analyse to a sufficient extent the true impact of key areas of the regime, the practicalities of implementation, and whether or not the regime will achieve the desired objective of countering money laundering and terrorist financing.[7]

3.13 As IFSA explained:

> … the staggered release of the draft Rules, which form a fundamental part of the regime, makes it extremely difficult to undertake comprehensive analysis and provide carefully considered comments to Government.[8]

3.14 The ABA argued that the banking industry holds serious doubts that the April deadline can be met at the present pace:

> The consultative framework set up by the Minister is workable but the issues are very complex, there are many uncertainties in the existing drafts, and progress is slower than expected.
>
> …
>
> The industry concern is that if the AML legislative package is pulled together in a rush to meet the current mid-April deadline, issues will not be properly resolved, or will be overlooked, resulting in implementation difficulties and ongoing operational problems.[9]

3.15 The ABA submitted further that at least five or six weeks would be required from the date of delivery of the complete AML/CTF package in order to conduct a complete analysis and to prepare detailed submissions to the Department's consultation process.[10]

---

6 *Committee Hansard*, 14 March 2006, p. 16.

7 For example, IFSA, *Submission 2*, p. 2; ING Direct, *Submission 13*, p. 2.

8 *Submission 2*, p. 2.

9 *Submission 18*, p. 2.

10 *Submission 18*, p. 2.

3.16 In their joint submission, CPA Australia and The Institute of Chartered Accountants in Australia noted that a four month timeframe for comment would normally be adequate but, since 'the majority of the related rules and guidelines, which provide the detail on compliance processes and obligations, have not yet been released' there is simply not enough remaining time.[11]

3.17 Mr John Anning from the FPA made a similar argument:

> At the moment it is impossible to take a definitive position on the draft package, given that so much of it is unknown. Currently, you cannot make sense of the draft bill until you see the subsidiary pieces. If the draft bill contained all the relevant principles—the key one which is missing for us at the moment is appropriate recognition of the risk based approach to implementation—it would be possible to comment properly on the bill itself rather than wait for the rules and guidelines.[12]

3.18 Ms Michelle Mancy from American Express supported this view:

> In view of the fact that the law is not yet complete, the April deadline for completion of the consultation processes is too short. Even if all the missing rules are released in the next two to three weeks, it would not be enough time for organisations to absorb impact and effectiveness before responding in a meaningful way. I will give you an example of how the job has only been half done to date. As you are well aware by now, identification comes in two parts: collection and verification. We have draft rules for collection but nothing for how it is to be verified. This area is one of great financial burden to institutions, and we are 50 per cent incomplete on the information relevant to assess whether we can do it at all and how much it will cost.[13]

3.19 Insurance Australia Group (IAG) submitted that it would be prudent for the consultation period to be reassessed based on industry having access to the complete suite of initiatives contained in the reform package.[14]

3.20 In its submission, The Treasury supported the availability of the complete package of reform proposals:

> Treasury's experience in implementing broad-ranging financial sector reform, such as the *Financial Services Reform Act 2001* (FSR Act), has demonstrated that the availability of a full package of reform proposals is desirable to allow industry to understand the range of requirements under which they are placed and thereby ascertain their compliance costs and necessary system and personnel changes. Given this, it would be desirable for industry to have the opportunity to comment on the full package of

11 *Submission 7*, p. 1.

12 *Committee Hansard*, 14 March 2006, p. 20.

13 *Committee Hansard*, 14 March 2006, p. 48.

14 *Submission 11A*, p. 8.

> AML/CTF measures. To date we note that significant obligations are yet to be specified in rules and provided to industry for their consideration.[15]

Department response

3.21 At the hearing, the Department responded to concerns raised with respect to the consultation process. A representative from the Department told the committee that the consultation period is 'genuine' and, from its perspective, 'a very positive exercise'. He stressed that the Department has taken, and will take, comments and criticisms 'on board'. In particular, he noted that:

> People obviously have to speak about the exposure draft which is out there, but I can guarantee that the final bill, even if nothing else happened from here on, would be different in a whole lot of respects from what we have here. That, of course, is part of the process and makes it a bit difficult for people to comment on, and we have the difficulty in, firstly, making announcements about changes that will be made, because it will be a government decision—it is not up to us as officers to make that call—and, secondly, because the consultation period is not over. It is possible that things will change; people will come up with good ideas that we will be more than happy to take on board. Some of the evidence given this morning was that comments have been made, they have sat on the table and not been reacted to. From our perspective, that is not the way the process is working.[16]

3.22 In relation to concerns about the large number of Rules yet to be released for comment during the consultation process, the representative assured the committee that 'the key rules, the vital rules, the rules needed to make it work'[17] would be released prior to the end of the consultation period. He told the committee that this amounts to 'five sets' of Rules, that is:

- AML/CTF Programs Rules ;
- Identity Verification Rules;
- Suspect Transaction Reports Rules;
- Correspondent Banking Rules; and
- Threshold Reporting Rules.[18]

3.23 He noted that, 'the position is [not] quite as bleak as some of the evidence has suggested', and that, of those sets of Rules:

> AML programs are at a very advanced stage, suspect transaction rules are at a very advanced stage, and I think threshold reporting is too. The real work

15 *Submission 29*, p. 2.

16 *Committee Hansard*, 14 March 2006, p. 61.

17 *Committee Hansard*, 14 March 2006, p. 61.

18 *Committee Hansard*, 14 March 2006, p. 61.

> that has to be done is in ID verification rules and the correspondent banking rules … The current approach being taken in relation to both of those rules is to create a further version of them based on the risk based approach, and that will be presented to industry over the next short period. We hope that we will be able to produce draft ID verification rules in time for the next meeting of the ministerial advisory group on Thursday. I think correspondent banking rules will take a little longer because we are still getting information. They are going to be drafted in consultation with industry.[19]

3.24 AUSTRAC's legal representative advised that there are 'essentially three broad categories of outstanding rules', namely in relation to identification, reporting obligations and 'a miscellaneous category of definitions and the like'. She told the committee that the process with respect to release of these Rules to the working groups is about two weeks behind schedule.[20]

3.25 In relation to the possibility of opportunities for an extended period of consultation or further consultation prior to finalisation of the Exposure Bill and its introduction into Parliament, the departmental representative noted that:

> It is really the minister's call as to whether there is that further period of consultation or further opportunities for industry to examine the bill, so I cannot make any commitment in relation to that. At this stage the minister is still keen to introduce legislation as soon as it can be done. Bearing in mind the length of time that this process has taken, we are very keen to push on. We have now been evaluated by FATF and 12 months after the evaluation we are going to be called upon to explain progress, so there are time pressures which people should not lose track of.[21]

Timeframe for implementation

3.26 Many industry and business entities raised the issue of a timeframe for implementation of the new regime. There was widespread uncertainty about the Federal Government's plans for implementation of the Exposure Bill, particularly given the Exposure Bill's scope and complexity. Many submissions and witnesses noted the extensive obligations imposed by the Exposure Bill and the anticipated costs of administration and compliance, including implementation of appropriate information system changes, which would be particularly burdensome for small- and medium-sized enterprises.[22]

---

19 *Committee Hansard*, 14 March 2006, p. 61.

20 *Committee Hansard*, 14 March 2006, p. 78.

21 *Committee Hansard*, 14 March 2006, p. 61.

22 For example, IFSA, *Submission 2*, p. 2; CPA Australia & The Institute of Chartered Accountants in Australia, *Submission 7*, pp 1 & 4; Insurance Australia Group, *Submission 11A*, p. 8; Suncorp-Metway Limited, *Submission 14*, p. 4, Platinum Asset Management, *Submission 21*, p. 3.

3.27 The majority of industry groups were of the view that a period of two to three years would be necessary for implementation. However, the committee notes that the Minister has indicated that a period of 12 months to comply with the legislation is more likely.[23]

3.28 Mr Tony Burke from the Australian Bankers' Association (ABA) told the committee:

> Once the legislation is ready, we believe that a time of two to three years will be necessary to implement this very complex piece of legislation which has very significant ramifications across our institutions. At this stage we do not have a firm position from government as to what they see the transition period as being, but it is our firm view that regardless of where the drafting ends up, a time of two to three years will be necessary.[24]

3.29 Mr Raj Venga from the Australian Association of Permanent Building Societies agreed:

> Our initial view is that we will need two to three years to properly implement the proposed legislation, given the systems modifications, staff training and processes that need to be undertaken. We note that the FSR provided a transition period of two years, which I thought was a reasonable indication of the time required, because the AML is no less difficult to implement than the FSR.

3.30 IFSA submitted that the AML/CTF regime is 'one of the most significant reforms to the financial services industry in the last twenty years'.[25] It also drew comparisons with the consultation and transition periods relating to the FSR regime, noting that they amounted to a combined total period of six years:

March 1999:	CLERP 6 Consultation Paper released
February 2000:	Draft FSR Bill released
September 2001:	Bill receives the Royal Assent
March 2002:	Legislation commences with 2 year transition period
March 2004:	End of transition period[26]

3.31 Further, and importantly, IFSA pointed out that:

> … despite the extensive consultation … industry and Government are still attempting to overcome a number of practical difficulties with the FSR regime. Indeed, while many of the ongoing difficulties were largely unintentional, IFSA nevertheless believes that the industry's and the

23 S. Patten, 'Laundering laws rinsed off', *Australian Financial Review*, 17 March 2006.

24 *Committee Hansard*, 14 March 2006, p. 2.

25 *Submission 2*, p. 2.

26 *Submission 2*, p. 3.

> Regulator's experience would have been far worse had there not been extensive consultation from the outset.[27]

3.32 Suncorp Metway noted that the FSR legislative package allowed for a two-year transition period 'stated well in advance of the final package reaching Parliament'. It argued that implementation of the FSR should serve as a useful precedent for implementation of the AML/CTF regime.[28]

3.33 The Treasury also supported sufficient lead time for implementation of the AML/CTF regime requirements:

> This is particularly necessary where the measures necessitate substantial changes to information systems and processes, and require training for staff so that they can discharge their obligations under the legislative regime. In supporting this approach we are mindful of the experience in implementing the FSR Act which demonstrated that industry requires a sufficient implementation period to allow it time to understand its new obligations and their implications at a practical level. In addition, industry will often call for guidance as to how it can meet its new obligations and in this regard it is important for policy advisers to remain engaged to ensure that implementation of the measures proceeds in a way that is consistent with the policy intention.[29]

3.34 The Australian Friendly Societies Association submitted that the new regime will require significant changes to systems and processes which cannot be underestimated:

> The AML/CTF package will involve major changes to systems and procedures, potentially requiring new systems, as well as workforce training requirements, which will create significant demands and resourcing issues from both a costs and personnel perspective. Therefore, serious consideration must be given to ensuring that a transition period of as long as possible a duration is provided – we would be suggesting at minimum a 2 year transition period from the date of Royal Assent of the AML/CTF package.[30]

3.35 The ABA pointed out that, since the Exposure Bill extends to a range of financial service providers not currently covered by the FTR Act, the level of change required for these entities will be particularly significant: 'culturally, technologically and procedurally'.[31]

---

27 *Submission 2*, p. 3.

28 *Submission 14*, p. 5.

29 *Submission 29*, p. 2.

30 *Submission 17*, p. 2.

31 *Submission 18*, p. 25.

Purported risk-based approach

3.36 The majority of industry bodies who made submissions to the committee's inquiry argued that, despite the purported risk-based approach, the Exposure Bill is overly prescriptive, expansive and unbalanced. Many noted that there are areas of the Exposure Bill where prescriptive and mandatory requirements have replaced a risk-based approach, with very little scope left for industry guidelines.[32] This is undesirable since it imposes a disproportionate burden on business and is inconsistent with good regulatory practice.[33]

3.37 They argued that, further, since the regime captures a wide range of reporting entities and transactions, a 'one-size-fits-all' framework of prescriptive obligations is undesirable as, arguably, this would have serious flow-on effects on business and the general public in terms of inconvenience and compliance costs. Moreover, it may not provide the optimum means of combating money laundering and terrorist financing in Australia.[34]

3.38 In evidence, Mr Brett Knight from American Express told the committee that initially the Exposure Bill had taken on a risk-based approach and that many of the Rules, as they began to form in some of the consultative working groups, had taken an overarching risk-based approach. However, in his view, the proposed regime has begun to take on a more prescriptive approach as the Exposure Bill and the Rules have undergone development:

> What has happened is that the AUSTRAC working groups have 40 people from 40 different industries putting up examples of how their operations work and this and that. AUSTRAC is trying to take all of this and, instead of creating overarching risk principles, they have started to prescribe in very strict detail what institutions should do. As you can appreciate, a global company like American Express has complied with the USA Patriot Act for years and the last thing we would like to see is legislation come in that is prescriptive and contrary to our requirements in other jurisdictions. It makes us invest millions of dollars where we do not think that is effective.[35]

3.39 Many argued also that the measures in the Exposure Bill go far beyond the FATF Recommendations, further than comparable overseas AML legislation, and beyond the AML and CTF objectives stated by the Federal Government as the rationale for the Exposure Bill.

---

32 For example, CPA Australia & The Institute of Chartered Accountants in Australia, *Submission 7*, p. 2; Australian Bankers' Association, *Submission 18*, p. 2.

33 *Submission 18*, p. 7.

34 For example, Australian Privacy Foundation, *Submission 4*, p. 4; CPA Australia & The Institute of Chartered Accountants in Australia, *Submission 7*, p. 2; Ms Catherine Kennedy, The Institute of Chartered Accountants in Australia, *Committee Hansard*, 14 March 2006, p. 43; ING Direct, *Submission 13*, p. 2.

35 *Committee Hansard*, 14 March 2006, p. 51.

3.40 The following section of the committee's report examines these issues in more detail.

FATF Recommendations

3.41 The Introduction to the FATF Recommendations states that:

> … FATF recognises that countries have diverse legal and financial systems and so all cannot take identical measures to achieve the common objective, especially over matters of detail. The Recommendations therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional frameworks.[36]

3.42 A number of submissions and witnesses argued that the proposed AML/CTF regime, despite being touted as a measure to bring Australia into line with the FATF Recommendations, in fact departs from those recommendations in a number of key respects.

3.43 Liberty Victoria argued that the Exposure Bill extends beyond the FATF Recommendations and the existing regime of the FTR Act 'without apparent justification'.[37] Liberty Victoria pointed to some differences:

> … while the FATF 40 Recommendations and the FTRA focus on financial institutions, the Bill focuses on the provision of certain services. While the FATF 40 Recommendations stipulate a threshold transaction of over A$20,000, the Bill proposes one of A$10,000. The Bill's suspicious reporting requirements go far beyond the FATF 40 Recommendations and even substantially extend the already extensive obligations in the FTRA. The Bill contains novel requirements concerning funds transfers and registration of remittance service providers which are found nowhere in the FATF 40 Recommendations or the FTRA.[38]

3.44 The Australian Privacy Foundation (APF) made a similar argument, noting that:

> The Objects clause (Section 3) focuses almost entirely on the need to meet 'international obligations' in the areas of money-laundering and terrorist financing – specifically the Financial Action Task Force (FATF) Recommendations. Apart from being seriously misleading by omission…this focus is not supported by any rigorous analysis of what is actually required to meet those Recommendations.[39]

---

36 FATF Documents on the Forty Recommendations, p. 3 at http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html#40recs (accessed 10 February 2006)

37 *Submission 26*, p. 2.

38 *Submission 26*, p. 2.

39 *Submission 4*, p. 4.

3.45 The APF also submitted that international comparisons show that 'there is considerable flexibility for signatories to interpret the Recommendations, and not all jurisdictions are putting in place such a comprehensive identification, reporting and monitoring regime'.[40] Therefore, in the APF's view:

> … the Australian Government is being highly selective in using the FATF Recommendations to support its wider policy objectives where it suits, and at the same time being deliberately vague about those aspects of the existing FTR Act, and draft Bill, which go beyond the FATF requirements.[41]

3.46 Mr Tony Burke from the ABA emphasised the point that the FATF recommendations recognise a risk-based approach which is not reflected in the proposed regime:

> As recognised in the FATF recommendations concerning the measures to be taken by financial institutions and agreed by government and industry, the entire approach should reflect a risk based approach in order to ensure that appropriate resources are matched to high-risk activities and functions. The proposed regime is not risk based either at global or structural level, nor in relation to specific obligations. Generally a risk based approach should match the obligations imposed on an entity with the risks faced by that entity in a proportional and balanced way. More demanding obligations should be imposed to manage more serious risks.[42]

3.47 Mr Burke told the committee that the proposed regime's approach 'is inconsistent with what w[as] agreed with the minister and the Department last year at the roundtable meetings, inconsistent with FATF recommendations, and inconsistent with best practice internationally.[43]

Elements of a true risk-based approach

3.48 Many submissions and witnesses to the committee's inquiry maintained that the industry preference is not for prescription but rather for guidance and information from AUSTRAC about AML/CTF risks, and AUSTRAC's expectations about industry's response to those risks. Essentially, they argued that the obligations of reporting entities should be commensurate with self-assessed risk.

3.49 As The Association of Superannuation Funds of Australia (ASFA) submitted:

> A genuinely risk-based approach should set down high-level principles in line with the FATF requirements. Reporting entities would then be able to introduce their own policies and procedures that are appropriate given the

40 *Submission 4*, p. 4.

41 *Submission 4*, p. 4.

42 *Committee Hansard*, 14 March 2006, p. 2.

43 *Committee Hansard*, 14 March 2006, p. 2.

> risks presented by their products and customers as well as the entity's size and capacity.[44]

3.50 The FPA argued that one of the main benefits of principles-based legislation is that it is capable of being applied confidently by businesses in a flexible way to suit their particular needs and clients:

> By being overly prescriptive, whether in standards or legislation, businesses irrespective of size, structure or business model, are unable to determine appropriate ways of incorporating the requirements into their businesses. It should be possible to innovate within the broad bounds of Government policy without having to seek explicit approval from the regulator.[45]

3.51 Mr Tony Burke from the ABA also provided the committee with an industry view of the requirements of a true risk-based approach:

- first, legal obligations should be framed so that the scope of the legal obligations are clear and the entity subject to the obligations is be able to determine what needs to be done to comply;
- second, compliance with the legal obligations should be feasible and practical and the entity subject to the legal obligations should be able to do what is needed to comply; and
- third, appropriate enforcement mechanisms should be in place whereby the entity subject to legal obligation is subject to reasonable and proportionate sanctions in cases of non-compliance.[46]

3.52 With respect to appropriate enforcement mechanisms, Mr Burke submitted that these are most effectively achieved by an overriding object in the interpretation part of the relevant legislation that makes clear that, both qualitatively and quantitatively, each obligation is to be interpreted consistently with a risk-based approach relevant, for example, to the nature, scale, complexity and risk profile of a reporting entity's business. As part of this overriding part, a global defence for reasonable steps and due diligence should be included.[47]

3.53 Insurance Australia Group (IAG) emphasised that a risk-based approach should start from the assumption that most customers are not money launderers, and that businesses should be able to identify where financial crime risks lie in their own business:

> This approach allows firms to focus their efforts where they are most needed and where they will have the most impact. Factors to be considered can include issues such as jurisdiction, customer type, class of business and

---

44 *Submission 28*, p. 2.

45 *Submission 24*, p. 3.

46 *Committee Hansard*, 14 March 2006, p. 2.

47 *Committee Hansard*, 14 March 2006, p. 2.

> distribution channel. Taking a proportionate, risk based approach to anti-money laundering can have significant benefits to businesses, being cost effective (identifying where limited resources need to be deployed) enabling firms to identify and focus on high risk areas.[48]

3.54 Mr Luke Lawler from the Credit Union Industry Association (CUIA) also stressed the need for any AML/CTF measures to be reasonable and proportionate, particularly in the context of community expectations and community understanding:

> … everyone opposes money laundering and everyone opposes terrorism financing. There is no argument there. It is a question of what is realistic and proportionate and what are reasonable expectations in the community about information—what is suspicious; what is unusual; and what people consider to be a reasonable approach to tackling these money-laundering problems and terrorism financing problems. The point I am making is: potentially, it could be quite a monster. It depends on everyone taking a reasonable approach and, to some extent, the very first audit that AUSTRAC does of an institution will determine the shape of the regime.[49]

3.55 In their joint submission, CPA Australia and The Institute of Chartered of Accountants in Australia argued that the proposed regime 'is not adequately factoring in commercial realities and the practicalities of undertaking business in Australia' since, in their view, it will 'deliver complex, over-burdensome regulation'.[50] Further:

> It is a concern that despite the government's stated commitment to improving the regulatory process, there is an ongoing failure of agencies to reconcile their regulatory objectives with the commercial environment. A more focused risk based approach will result in a more robust partnership between industry and government to better monitor money-laundering and terrorism financing.[51]

3.56 The FPA again drew comparisons with the FSR regime which, while also purporting to be principles-based, has in its view been too prescriptive in nature. In relation to the AML/CTF regime, the FPA submitted that in order for it to be truly principles-based, 'it should explicitly recognise the role of risk in determining the extent of obligations'.[52] Further:

> Due to the shortcomings of the Exposure Draft in recognising the role of risk, it is only natural that industry has sought to see the whole of the draft regime – the Exposure Draft and subsidiary draft rules and guidelines –

48 *Submission 11A*, p. 7.

49 *Committee Hansard*, 14 March 2006, p. 9.

50 *Submission 7*, p. 1.

51 *Submission 7*, p. 2.

52 *Submission 24*, p. 3.

> before committing themselves to definitive comments on the proposed legislative package.[53]

3.57 Mr Mark Mullington from ING Direct emphasised the need for the regime to focus on *outcomes*, as opposed to compliance:

> We believe that, with legislation that is too prescriptive and coupled with relatively severe civil and criminal penalties or sanctions, we run the risk of the whole emphasis of the industry being on compliance. In other words, it will become a tick-the-box exercise. That is a little bit similar to where we have ended up with FSRA. It is fundamentally about compliance; it is fundamentally about ticking the boxes.
>
> The alternative is a risk based approach which really pushes institutions down the track of outcomes, in that an institution needs to build an anti-money laundering and CTF program to achieve certain outcomes. The regulator has the ability to review those programs and opine on whether they are adequate to achieve those outcomes or not, but it does not push the organisation down the track of compliance. We believe that the way the rules—the three that we have got—have developed to date are quite explicit, quite prescriptive and not risk based.

3.58 The Treasury also expressed its support for a risk-based approach:

> The financial sector comprises a broad range of institutions and service providers offering a diverse suite of products with varying features and risk profiles. The application of the AML/CTF obligations should take that diversity into account and ensure that the intensity of obligations is commensurate with the risks posed by particular products, the profile of the customer and the delivery method of the financial service.[54]

Comparable overseas legislation

3.59 The committee received some evidence pointing to the AML/CTF experiences in the United Kingdom (UK) and the United States (US), and the lessons that Australia might learn from those experiences.

3.60 For example, the ABA submitted that:

> The United Kingdom (UK) and the United States of America (USA) have had considerable experience with the implementation of AML/CTF regimes and have led international efforts in this area. Both countries have sought to implement regimes that are risk-based, consistent with international requirements, best practice and their domestic legal environment. Further, both countries have had significant enforcement experience.[55]

---

53 *Submission 24*, p. 3.

54 *Submission 29*, p. 3.

55 *Submission 18*, p. 7.

3.61 However, Mr Tony Burke from the ABA informed the committee that the UK experience was not without its problems as the UK 'initially went down a much more strongly prescriptive path than is currently the case and found enormous difficulty in doing so'.[56] In particular, Mr Burke noted that:

> There is head legislation; then the body of the detail was in guidance notes produced by … the Joint Money Laundering Steering Group. There were significant obligations, for example, in the verification of existing customers, not risk based. They found great difficulty implementing those obligations and significant customer push-back, and they have withdrawn from that approach to a more risk based approach. The UK is probably the model which we point to. There was a bad experience in doing it that way but now the new approach seems to be working far more effectively.[57]

3.62 IFSA also highlighted the UK experience as one which Australia could learn from, noting that it 'would be a costly and wasteful exercise that neither the industry nor the Regulator…would want to go through'[58] if Australia were to get its regime wrong in the first place.

3.63 Mr Brett Knight from American Express emphasised the importance of Australia utilising the experiences of other jurisdictions:

> There is a lot of international experience. The US implemented this type of legislation four or five years ago, and so has the UK. In my opinion and from what I have seen, the regulators have not really taken a lot of this global experience and applied it. In the AML-CTF advisory group meetings last week, there was a whole discussion on creating risk matrixes, which have been compiled very comprehensively in other jurisdictions for years. So I think they have not used the opportunity to look at other global jurisdictions that have this type of legislation to get best practices effectively.[59]

3.64 SunCorp Metway suggested that 'the final version of the Exposure Draft be rigorously compared' by the Department and/or AUSTRAC 'to assess parity with existing UK and US AML legislative models' to ensure that Australian requirements do not exceed those in other similar jurisdictions.[60]

Department response

3.65 In response to industry concerns with respect to the overly prescriptive approach taken in the Exposure Bill, a representative from the Department maintained that the Exposure Bill is principles-based with a risk base beneath it. The

---

56 *Committee Hansard*, 14 March 2006, p. 10.

57 *Committee Hansard*, 14 March 2006, p. 10.

58 *Submission 2*, p. 4.

59 *Committee Hansard*, 14 March 2006, p. 51.

60 *Submission 14*, p. 4.

representative stated that there is no explicit definition of 'risk-based' but that 'the concept is clear'. That is:

> The principles are in the legislation and then there is flexibility for the industry to determine, using a risk based assessment, what their regime shall be. Then that will be embodied in an AML-CTF program, which will be subject to audit.[61]

3.66 The representative also pointed out that the concerns of industry in relation to this issue have 'been taken on board' and that 'the documents that finally emerge from this process – the vital rules that need to be drafted – will reflect that discussion'.[62]

3.67 A representative from AUSTRAC confirmed that, specifically in relation to the AML/CTF Program Rules, 'we are feeling fairly comfortable that we have achieved a risk based approach – a set of rules that set out a framework in which entities can judge their own risk and deal with that in an appropriate way'.[63] She also noted that the Customer Identification Rules would be progressing on a similar basis.[64]

3.68 With respect to reference by some submissions and witnesses to the situation in the UK, a representative from the Department told the committee that 'some of the suggestions about learning from the UK experience might in fact be extrapolating from that, as opposed to considering whether [for example] the detail in their identification requirements is actually less or more than our suggestion'.[65]

3.69 Another departmental representative explained that it should be recognised that there are differences between the UK and US experiences on the one hand, and the Australian situation on the other:

> Yes, we have heard it said that we should be learning from the overseas experience. We accept that entirely and we have looked at the overseas experience, especially the UK and the US. But there are differences with the Australian system. I do not think we can pick up and apply overseas provisions slavishly. We have to modify them for the Australian environment. I make the point that although we can look at the UK experience there are limits to how far we can take that.[66]

---

61 *Committee Hansard*, 14 March 2006, p. 67.

62 *Committee Hansard*, 14 March 2006, p. 68.

63 *Committee Hansard*, 14 March 2006, p. 68.

64 *Committee Hansard*, 14 March 2006, p. 68.

65 *Committee Hansard*, 14 March 2006, p. 63.

66 *Committee Hansard*, 14 March 2006, p. 63.

Practical impact of the proposed regime

3.70 The committee received evidence from a variety of financial services industry sectors indicating that there are a number of common residual concerns regarding the practical impact of specific aspects of the proposed AML/CTF regime. The major concerns raised with the committee will be considered below.

Scope and coverage of the Exposure Bill – 'designated services'

3.71 Some submissions and witnesses commented on the wide scope of the Exposure Bill. For example, CPA Australia and The Institute of Chartered Accountants in Australia argued that, despite the Federal Government's claim that the first tranche of reforms will only impact on the financial services sector and businesses in competition with that sector, 'the definitions of designated services are so broad that they currently cover all businesses which provide trade credit' so that:

> … all consumer credit transactions will … be caught, so individuals buying a new television or fridge on credit will now be subject to full Customer identification procedures and will have to produce a birth certificate and/or other primary and secondary documents.[67]

3.72 In this respect, '(t)he descriptions of certain designated services in clause 6 of the Bill go far beyond the FATF Recommendations'.[68]

3.73 IAG agreed that the Exposure Bill's definition of 'business' is unqualified and, therefore, inconsistent with the FATF Recommendations. In IAG's view, the FATF Recommendations are:

> … expressed to impose obligations on 'financial institutions' (and in certain circumstances on 'non-financial businesses and professions'). 'Financial institution' under the FATF recommendations is defined as 'any person or entity who conducts as a business one or more' of the prescribed activities. The Draft Exposure Bill ignores this important qualification.[69]

3.74 IAG also made the point that the definition of 'business' in the Exposure Bill, by extending to one-off and occasional activity, goes beyond the FATF Recommendations. It argued that 'there is some scope for the ambit of the definition of "business" to be reduced without making it inconsistent with the FATF Recommendations'.[70]

3.75 The ABA noted that the list of designated services does not draw any distinctions on the basis of monetary limits (except a $1000 limit for stored value cards); nor does it take into account whether activity is carried out on an occasional or

---

67 *Submission 7*, p. 2.

68 *Submission 7*, p. 2.

69 *Submission 11A*, p. 6.

70 *Submission 11A*, p. 6.

a regular basis; nor does it recognise to whom the service is provided (for example, a related company).[71]

3.76 In relation to the threshold issue, Ms Michelle Mancy from American Express argued that to support a risk-based approach, 'meaningful thresholds should be set' since 'there is no appreciable risk of money laundering below certain minimal levels of transactional activity' and '(t)he absence of thresholds means it is simply overburdensome to require this kind of identification'.[72]

3.77 Ms Mancy elaborated:

> There are no thresholds for any designated service except stored value cards and we would like to see a threshold for consumer credit arrangements. American Express card members spend more than customers of other institutions. Even so, the average spend on the American Express card in Australia is not more than $10,000 each year.
>
> The reporting threshold should be increased as the current $10,000 figure dates back to the early days of the FTRA over 10 years ago and is no longer reasonable. It should be adjusted to account for inflation. The current $10,000 figure is also set substantially below the FATF recommendations. Lowering the threshold leads to significant increased compliance costs and there is no evidence that Australia presents higher risks than other countries with similar income levels.[73]

3.78 Others agreed that the threshold should be increased. The Deputy Privacy Commissioner told the committee that:

> Our view is that the Financial Transaction Reports Act has been in place for quite some years now, and the original threshold was set back in the early nineties. It may be useful to have that reviewed to see whether it is still an appropriate amount, so the basis of our comment there is generally on the length of time for which that amount has been set.[74]

3.79 Ms Johnston from the APF submitted that a threshold of approximately $US15,000 might be more appropriate:

> We believe there should be a threshold for all three categories: international transactions, domestic transactions and suspicious transactions—if you keep the third category. As Mr Pilgrim has mentioned, we believe the $10,000 threshold that was set some time ago is now too low, through the effects of inflation. If you want to pull a figure out of a hat, I would say

71 *Submission 18*, p. 9.

72 *Committee Hansard*, 14 March 2006, p. 48.

73 *Committee Hansard*, 14 March 2006, p. 48.

74 *Committee Hansard*, 14 March 2006, p. 33.

> something like $US15,000—so whatever that is in Australian dollars; it might be $A18,000 or $A20,000—might be more appropriate.[75]

Department response

3.80 In response to suggestions that the transaction threshold of $10,000 should be reviewed, a representative from AUSTRAC informed the committee that there are currently no plans to do so:

> Certainly we do not believe that there is any reason to review that level at the moment. Reporting at that level is of use to AUSTRAC and its partner agencies in their work. People from the privacy groups in particular have raised this in AUSTRAC's privacy consultative committee. While we are always open to reviewing that if necessary, at this stage we believe that the $10,000 threshold is still a reasonable threshold to have.[76]

3.81 In an answer to a question on notice, AUSTRAC expressed its view that $10,000 remains the appropriate level for the threshold:

> While the number of transactions at this level has increased, this amount remains significant. The Bill does provide for the threshold to be raised, as well as lowered, by regulation, not by AUSTRAC. The amount will be kept under continuing review and if it appears that it should be raised, recommendations will be made to the Minister for Justice and Customs about the need for regulations.[77]

Identification procedures (Part 2)

3.82 Most of the detail in relation to customer identification requirements will be contained in (as yet unreleased) Rules. This has created uncertainty for a number of groups who participated in the committee's inquiry.

Not risk-based and overly complicated

3.83 Some submissions and evidence argued that the customer identification requirements in Part 2 of the Exposure Bill are not risk-based. For example, Mr Tony Burke from the ABA told the committee that:

> … there is a failure to distinguish between high- and low-risk products through the definitions, which results in obligations that are not proportionate to risk. Rules relating to 'know your customer' are too complex and excessive for low-risk services. Key aspects of the operation of this part are contained in the rules. Without knowing the content of the rules, it is not possible to determine whether the scope of the obligation is

75 *Committee Hansard*, 14 March 2006, p. 33.

76 *Committee Hansard*, 14 March 2006, p. 69.

77 *Submission 33*, p. 3.

> sufficiently clear and whether regulated institutions will be capable of complying.[78]

3.84 CPA Australia and The Institute of Chartered Accountants in Australia agreed, particularly in relation to the customer due diligence requirements in Part 2:

> The requirements to perform Customer Due Diligence set out in Part 2 of the Bill are not risk based. They only provide for the exemption of certain services which must be specified in the AML/CTF Rules. The requirements of Part 2 and the AML/CTF Rules on Applicable Customer Identification Procedures apply to all other designated services, regardless of the level of risk posed by the customer, type of service or method of delivery or the jurisdictions in question (eg where the customer resides or where the product or service is to be delivered). This is an unnecessarily inflexible framework for the identification of customers.[79]

3.85 CPA Australia and The Institute of Chartered Accountants in Australia argued further that, despite proposed section 35 allowing for the exemption of designated services which are considered to be low risk:

> There is no consideration to be given to the risks associated with the customer or any other aspect of the transaction. In general terms, the designated service of processing transactions through an accountant's trust account may have some potential for risk and may not generally meet the AUSTRAC criteria as a low risk service for exemption. However, the customer, source and destination of the trust account transaction may all be of a low risk in relation to money laundering and/or terrorist financing. Despite this, they are unlikely to be services excluded from the application of Part 2 of the Bill or to which a lower level of Customer Due Diligence is applicable.[80]

3.86 Platinum Asset Management (Platinum), an Australia domiciled investment manager specialising in international equities, queried the burdensome nature of the obligations in Part 2:

> Given that all investment money comes to Platinum via the Australian banking system (which is subject to rigorous regulation) what benefit will be gained from requiring us to further scrutinise the identity of our clients?[81]

3.87 The ABA argued that the requirements in the draft Rules relating to 'Know Your Customer' and customer due diligence are too complicated:

> Industry proposed, in November 2005, that customer due diligence and enhanced customer due diligence be simplified into a unified approach but

---

78 *Committee Hansard*, 14 March 2006, p. 3.

79 *Submission 7*, p. 5.

80 *Submission 7*, p. 5.

81 *Submission 21*, p. 3.

> this has not appeared in the E[xposure] D[raft Bill]. The lack of further release of the suite of identification rules is making it almost impossible for industry to assess the scope of these due diligence requirements and their impact on businesses (and their customers).[82]

3.88 The ABA also highlighted the intrusiveness of the identification requirements for clients and customers:

> The proposed Customer Due Diligence will require customers to spend longer conducting transactions and a significant proportion may feel the information required under the proposed regime is invasive, particularly in relation to provision of information on country of birth, residence and citizenship. International experience indicates that this information is of little value in AML/CTF control and there is concern that an obligation to ask for a place of birth may raise complaints of 'racial profiling' from many customers.[83]

Electronic verification

3.89 A number of submissions and witnesses raised concerns that, while the Exposure Bill and the Rules are technologically neutral, electronic verification (EV) processes with respect to customer identification have not been expressly provided for. These groups argued that express recognition of EV should be set out in the Rules and should encompass current EV methods used by industry.[84] The committee understands that many businesses currently use EV to check customer information by carrying out (or engaging third party commercial service providers to carry out) searches of electronic databases that store information about people.

3.90 IFSA noted that this issue is critical to the financial services sector because it predominantly interacts with existing customers and potential customers on a non face-to-face basis.[85] By way of example of the significance of the EV process, Ms Lisa Claes from ING Direct informed the committee that eighty per cent of that company's new customers are verified using EV. American Express argued that EV 'is equally if not more robust than human inspection of documents … which may be forged or manipulated' and is, in fact, 'a powerful tool to thwart illicit activity'.[86]

3.91 American Express asserted that it is imperative that the proposed regime 'does not prescribe a narrow, traditional identification process based on physical or face-to-

---

82 *Submission 18*, p. 14.

83 *Submission 18*, p. 14.

84 For example, American Express Australia Limited, *Submission 15*, pp 2-3; GE Capital Finance Australasia Pty Ltd, *Submission 22*, p. 1; PayPal Australia Pty Ltd, *Submission 16*, pp 1-2; Securities & Derivatives Industry Association, *Submission 31*, p. 3; Ms Lisa Claes, ING Direct, *Committee Hansard*, 14 March 2006, p. 50.

85 *Submission 2*, p. 6.

86 *Submission 15A*, pp 2 & 3.

face presentation or inspection of identity documents, especially as more efficient alternatives are available'.[87] In this context, the concept of competitive neutrality is particularly relevant, since businesses such as American Express do not have physical branch networks through which to conduct face-to-face inquiries with clients:

> If the law does not allow ample flexibility and adaptability for financial institutions to adopt customer identification methodologies that are feasible within their business models, the legislation may have extremely negative impacts on competitiveness, business growth and expansion, without assisting the task of identifying and preventing unlawful activity. This will create unnecessary burden on financial institutions and businesses that operate in a non face-to-face environment and will curb business growth and expansion into non traditional channels – such as internet banking, global payments solutions and many other products & services that are provided in a non face-to-face environment.[88]

3.92 The ABA noted that the Department recently made it clear at a recent working group meeting that 'the intention (not reflected in the drafting) was to permit reporting entities to decide whether to adopt the face-to-face procedures or the non-face-to-face procedures, based on which is best suited to their business processes'.[89]

3.93 At the committee's hearing a representative from the Department explained that EV has not been expressly included in the Rules for the following reasons:

> It will not necessarily be expressly provided for because, under a risk based system, you do not have to express things because that would become prescriptive but certainly the intention is there. This is the problem that you run into. People want risk based flexibility. At the same time they want clear guidance on what they are required to do. I think that is fair enough, because different industry sectors want different things and we have to have a process which allows each of them to be given what they need.[90]

3.94 The representative continued:

> The message has been heard loud and clear. The minister in roundtable conferences has basically said that there has to be an electronic verification system ... The idea of this is not to stop legitimate industry which is operating in a certain way from operating in that way, unless the risks of money laundering are so high that they should not be operating in that way. You cannot take an industry which operates entirely in an electronic environment and say, 'Next week you have to have branches because of these provisions.' That has been the challenge: to come up with electronic

87 *Submission 15*, p. 3.

88 *Submission 15A*, p. 1.

89 *Submission 18*, p. 15.

90 *Committee Hansard*, 14 March 2006, p. 73.

> verification procedures which are as robust as paper—leaving aside, for the moment, how robust paper identification and verification are.[91]

3.95 Further:

> The risk based approach will say that you as an entity have to have robust verification procedures and if you are satisfied that electronic verification is sufficiently robust and is appropriate then an entity can develop that. That is a risk based approach. Then, the onus will move on to our good friends at AUSTRAC with their audit function. We think that the Attorney-General's Department is likely to be involved in further debate and discussion about what the electronic verification involves. I do not think that issue is going to go to bed for quite some time but we are talking about an implementation period for this legislation; we are not talking about everything being in place on day one.[92]

Third party verification

3.96 Some argued that the procedures relating to third party verification of customer identification may not be practicable.

3.97 For example, Mr Mark Mullington from ING Direct noted that ING Direct is one of the largest providers of home loans through the mortgage broker channel. He acknowledged that the proposed regime contemplates third parties such as mortgage brokers undertaking the identification process on behalf of lending institutions, however he pointed out that 'the exact mechanism for this at this stage is unclear'.[93] Further:

> … the way the draft bill operates, it will create complexity and bureaucratic burden for the mortgage broker channel. It also creates serious concerns regarding our reliance on mortgage brokers undertaking that identification. We believe the legislation needs to contemplate an accreditation and registration process—that is, individuals and organisations become accredited to undertake the customer identification and verification process and, subject to certain controls, financial institutions be permitted to rely in good faith on that identification. At this stage, we are continuing to work with AUSTRAC on developing a viable solution.[94]

3.98 CPA and The Institute of Chartered Accountants in Australia argued that the third party verification requirements are not workable in relation to the services provided by accountants and would lead to unnecessary duplication of resources of both accountants and customers:

---

91 *Committee Hansard*, 14 March 2006, p. 73.

92 *Committee Hansard*, 14 March 2006, p. 73.

93 *Committee Hansard*, 14 March 2006, p. 49.

94 *Committee Hansard*, 14 March 2006, pp 49-50.

> Clause 34 of the Bill allows a reporting entity to authorize another person in writing to conduct the applicable customer identification procedures required in Part 2. This presumes that the services are being provided concurrently. However, an accountant who is a reporting entity will be providing services to a client who is likely to have previously had services provided by another reporting entity which has already conducted customer identification procedures. The Bill does not allow the accountant to rely on that previously conducted customer identification. Coming at the end of the 'chain' of reporting entities the accountant cannot provide written authorization for another reporting entity to carry out the applicable customer identification procedures.[95]

3.99 Mr John Anning from the FPA also raised third party identification as a issue for financial planners:

> Third party identification is a key issue, because often financial planners are seen as the first link in a chain of financial services transactions. So it is vital for us to understand how financial planners will be impacted by the regime, and to do that we need the draft rules and guidelines for third party identification. It raises practical issues. A financial planner may be undertaking identification on behalf of a number of financial institutions, and if they each have their individual risk assessment processes they may rate products and customers at different risk levels—therefore requiring identification to be done at various levels. So this has the outcome that the financial planner conducts an initial identification of the client, covering the maximum information required, just to cover all possibilities.[96]

3.100 The Securities & Derivatives Industry Association (SDIA) argued that certain arrangements involving third parties should be exempt from the due diligence requirements:

> Where an AFSL licence holder is a reporting entity and proposes an arrangement with another AFS licensee such an arrangement should be exempt from the due diligence requirements. These entities have already been through an in depth screening process in their licence applications and, if there is no adverse finding against them by the Australian Securities & Investments Commission (ASIC) after the receipt of the licence, the reporting entity must be able to do business with them in the normal course. The expectation should be that they also comply with AML/CTF legislation and that they have completed the customer identification process for their clients. Both licensees should not be required to obtain customer identification – only the primary contact. Similarly, it should not be a requirement that reliance on another licensee requires that a stockbroker review and approve the process for customer identification employed by that other licensee. Examples of these types of arrangements are

95 *Submission 7*, p. 5.

96 *Committee Hansard*, 14 March 2006, p. 17.

> stockbrokers having arrangements with financial planners and other intermediaries, margin lenders and managed fund providers.[97]

3.101 Allens Arthur Robinson (Allens) pointed out that, while proposed section 34 authorises third parties to carry out customer identification procedures, proposed section 12 prohibits them from providing information obtained by that procedure to anyone other than the reporting entity. Allens argued that:

> In order to facilitate the sharing of information between related entities in a group structure (and thereby reducing costs) … external agents should be able to provide customer identification information to related entities of the reporting entity if so authorised by the reporting entity.[98]

Technical issues

3.102 Allens also drew the committee's attention to the interaction between the customer identification procedures required by the Exposure Bill and the 'Know Your Customer' and risk classification requirements of the AML/CTF Program Rules. Mr Peter Jones from Allens summarised the crux of the issue as follows:

> … the exposure draft appears not to require reporting entities to take any action in relation to what we would call dormant customers—people who, at the time of commencement of the act, as it would be then, would not be having designated services provided to them. But when we look to the rules that have been released, the one that deals with AML compliance programs, for example, seems to suggest that all customers need to be risk classified and that reporting entities need to consider whether they need to get further K[now] Y[our] C[ustomer] information in relation to all customers and whether they need to update the KYC information they do hold in respect of all customers. To us, that gives rise to the question of whether that is the intention and, if it is, whether AUSTRAC does actually have the power to make rules which do not appear to have any legislative basis.[99]

3.103 Allens' submission noted that this is relevant for two reasons:

> In the first instance the extension of the AML/CTF program rules to customers who may no longer have an ongoing relationship with the reporting entity and no KYC obligations under the Act has practical and resource implications.
>
> More importantly if the Rules can regulate beyond the Act it is imperative that AUSTRAC's Rule making power is subject to, (at the least) industry consultation and some form of parliamentary scrutiny. At present it is not.[100]

---

97 *Submission 31*, pp 3-4.

98 *Submission 27*, p. 4.

99 *Committee Hansard*, 14 March 2006, p. 56.

100 *Submission 27*, p. 3.

3.104 In evidence, Mr Jones submitted that the proposed regime's inclusion of both past and present customer identification, poses the following questions:

> … how far back do you go? Where do you draw the line? That is the practical issue. Who is a dormant customer? Who is beyond the reach of needing to be risk classified? If they have not done anything with you for five years and then walk in the door tomorrow, are they a new or an existing customer? Part of this will be dealt with when we get the rules about continuity of relationships and what disqualifies a relationship from being a continuous one. I do not want to jump the gun on that score, but I do think you need to address the practical issue about dormancy.[101]

3.105 In response to a question on notice from the committee in relation to some of the technical issues raised by Allens, the Department advised that:

> The Attorney-General's Department is currently considering a range of issues raised in submissions to the Senate Legal and Constitutional Committee's Inquiry. The submission from Allens Arthur Robinson raises seven sets of issues, all of which will be addressed as part of the Department's consideration of suggested amendments to the exposure draft AML/CTF Bill.[102]

3.106 With specific reference to concerns about AUSTRAC's rule-making power, a representative from the Department indicated that consultation by AUSTRAC with industry and law enforcement groups when making the Rules might also be properly supplemented by consultation with privacy groups.[103]

Reporting obligations (Part 3)

3.107 Some submissions and witnesses commented on the reporting of suspicious matters requirements in Part 3 of the Exposure Bill.

3.108 For example, Mr Tony Burke from the ABA told the committee that:

> The industry has concerns that the suspicious matter reporting rules may be too prescriptive, as it appears that as many as 24 matters—many of which are difficult to assess—must be taken into account in determining whether there are reasonable grounds for forming a suspicion that would require a suspicious matter report, and as many as 19 details must be included in such a report.[104]

3.109 Mr Peter Jones of Allens pointed out that there is an apparent inconsistency between the scope of the obligation contained in proposed subsection 39(1) of the Exposure Bill and the reporting obligation in proposed subsection 39(2):

---

101 *Committee Hansard*, 14 March 2006, p. 58.

102 *Submission 32*, p. 1.

103 *Committee Hansard*, 14 March 2006, p. 74.

104 *Committee Hansard*, 14 March 2006, p. 3.

> That is an issue that we see in the FTRA as well but, given the detailed process—the exhaustive process—we are going through now and the extension of the suspicious reporting regime beyond financial institutions or cash dealers to a much wider audience, we thought it was worth raising this particular point. That point is the apparent mismatch between an objective test as to when one has reasonable grounds to have a suspicion, which might give rise, you would think, to an obligation to report, and the actual obligation to report, which only arises once a suspicion has arisen. It is a technical drafting issue but it is one that we thought was important, given that context.[105]

3.110 Liberty Victoria argued that proposed section 39 goes well beyond the requirements of the FATF Recommendations and also represents a significant extension of the current suspicious reporting regime under section 16 of the FTR Act:

> To portray cl 39 as an implementation of the FATF 40 Recommendations is nonsense. To portray it as a modification of the existing regime to conform with the FATF 40 Recommendations is equally untrue. It is, in truth, a wholesale revision of the suspicious reporting regime, which bears little or no resemblance to the FATF 40 Recommendations and extends the regime well beyond the current law. The Government should be asked to explain why this is necessary.[106]

3.111 Similarly, Allens asserted that elements of proposed section 40 are unworkable in practice and extend beyond the requirements of relevant FATF Recommendations.[107] Both Allens and Liberty Victoria pointed out that proposed section 40's extension of the suspicious reporting obligation to cases where it is suspected that there has been a breach of foreign law is onerous and unrealistic.[108]

3.112 Platinum again emphasised the overly burdensome obligations in the Exposure Bill, the costs of which would ultimately be borne by its small client base:

> Given that all monetary transactions with our clients are executed through an Australian bank, building society or credit union, what benefit will be gained from requiring us (a non-cash intermediary) to replicate the reporting of threshold transactions and international funds transfer instructions that will be carried out (and also reported) by the bank, building society or credit union concerned?[109]

---

105 *Committee Hansard*, 14 March 2006, p. 56.

106 *Submission 26*, pp 9-10.

107 *Submission 27*, pp 5-6; Mr Peter Jones, Allens Arthur Robinson, *Committee Hansard*, 14 March 2006, pp 57-58.

108 *Submission 26*, p. 11; *Submission* 27, pp 5-6; Mr Peter Jones, Allens Arthur Robinson, *Committee Hansard*, 14 March 2006, pp 57-58.

109 *Submission 21*, p. 4.

Department response

3.113 In response to some of the issues raised in relation to reporting of suspicious matters, including concerns that reporting entities would be required to consider and have knowledge of offences in foreign jurisdictions, a representative of the committee informed the committee that:

> The intention of those provisions of the legislation is not to require people to become experts in foreign law, Australian law or anything else. What they are intended to do is to ensure that, if people have suspicions about the source of the money or the activities that people are engaged in when they present to them, they then put in a report. I would submit it is a fairly simple concept: if you do not have a suspicion because there is no basis for you having grounds for suspicion then there is no suspicion and there is no report.[110]

3.114 However, despite this contention, the representative expressly acknowledged the comments made by submissions and witnesses to the committee's inquiry in relation to suspicious matters reporting, and indicated that this is an area of the Exposure Bill that would be revisited by the Department.[111]

AML/CTF Programs (Part 7)

3.115 Some specific issues relating to AML/CTF Programs under Part 7 of the Exposure Bill arose in the course of the committee's inquiry, namely:

- the costs involved in implementation of an AML/CTF Program;
- the merging of the separate activities of AML and CTF in AML/CTF Programs; and
- the possible legal implications of a reporting entity rejecting a potential customer on the basis of its AML/CTF Program.

3.116 For example, Mr Luke Lawler from the Credit Union Industry Association highlighted the costs of setting up the AML/CTF Programs:

> There will be a significant cost in setting up the AML CTF program, which is kind of the core of the compliance obligation in this proposed legislation. In the lead-up to the passage of legislation and in the transition period, we will get a better understanding of what the regulators' expectations are about the risks and the response to the risks but it is potentially quite incredibly invasive and intrusive of people's privacy …[112]

3.117 Some argued that money laundering and counter-terrorist financing issues are inappropriately conflated in the Exposure Bill, including the AML/CTF Programs,

---

110 *Committee Hansard*, 14 March 2006, p. 62.

111 *Committee Hansard*, 14 March 2006, p. 62.

112 *Committee Hansard*, 14 March 2006, p. 8.

when they are quite distinct activities. As the ABA submitted, '(t)here must be separate and different obligations applying to each threat, with which it is possible in practice to comply'.[113]

3.118 The Australian Friendly Societies Association noted concerns in relation to the possible legal implications of rejecting potential customers on the basis of a reporting entity's AML/CTF Program:

> Concerns have been raised about the legal implications of an organisation rejecting a potential customer on the basis of their AML/CTF program and customer due diligence, particularly where there could be allegations of discrimination on the grounds of race, given the collection of information about country of birth and citizenship. We would query whether consideration has been given to what protections there might be for financial institutions that reject a potential customer and are later subject to legal suit?[114]

3.119 This is particularly significant given that a reporting entity would be unable to reveal to the customer the reasons for rejection (under the 'tipping off' offence in proposed section 95 of the Exposure Bill).[115]

Obligation to 'materially mitigate' risk

3.120 Several witnesses and submissions raised as problematic proposed section 74's requirement that an AML/CTF Program 'materially mitigate' the risk of money laundering and terrorist financing. For instance, Mr Tony Burke from the ABA told the committee that:

> While we have spent quite a deal of time discussing 'materially mitigate' with the department and AUSTRAC, we have not yet come to an agreed position on that. Our concern is that it is too prescriptive. Our concern also is that it will not do the job. An organisation could be said to have materially mitigated risk in that no money laundering had been discovered, so the outcome was positive but the processes were very shoddy indeed. The converse may apply—an organisation may have fantastic processes but, unfortunately, has been the victim of money laundering and hence could be said not to have materially mitigated risk.[116]

3.121 The ABA's submission drew comparisons with the UK and US AML/CTF regimes in relation to this issue:

> Neither of these two countries imposes an obligation to materially mitigate AML/CTF risk as part of the obligation to implement AML/CTF programs.

---

113 *Submission 18*, p. 14.

114 *Submission 17*, p. 3.

115 'Tipping off' is discussed more fully later in this report in relation to privacy issues.

116 *Committee Hansard*, 14 March 2006, pp 6-7.

> For example, in the UK, under the Money Laundering Regulations 2003 (ML Regulations), relevant businesses are required to establish internal control and communication procedures which are 'appropriate for forestalling and preventing' money laundering. A defence to prosecution is provided where an entity 'took reasonable steps and exercised all due diligence' to implement such a program. In deciding whether an offence has been committed a court must take into account whether the person followed relevant industry guidance.[117]

3.122 The ABA's submission continued:

> The AUSTRAC response to industry's concerns about "materially mitigate" is that the UK obligation to 'prevent' is a higher standard than mitigation. This response ignores the legislative elements that make the UK approach fundamentally different from the proposed regime. It ignores the qualifier 'appropriate' and critically, ignores the overall defences. The US obligation contains no reference to 'materially mitigate' or to any particular outcome. It requires the establishment of programs (defined solely in accordance with FATF minimum recommendations) with the objective of guarding against money laundering.[118]

3.123 American Express argued that the 'materially mitigate' risk requirement is 'unrealistic and unattainable' since 'it is not possible to quantify levels of money laundering and terrorist activity with any level of precision, nor to predict future directions and developments of such activity'. It suggested that:

> The requirement should be changed to require providers to implement programs which 'effectively mitigate such risks as are reasonably apparent' of the provider's products and services being misused.[119]

3.124 SDIA also argued that clearer guidance is needed on the meaning of 'materially mitigates'.[120]

Secrecy and access (Part 11)

3.125 Some submissions and witnesses raised concerns in relation to Part 11 of the Exposure Bill. Under proposed section 95, reporting entities must not disclose that they have formed an applicable suspicion or have reported information to AUSTRAC under the suspicious matter reporting requirements, or that they have given further information to a law enforcement agency in response to a request.

---

117 *Submission 18*, p. 7.

118 *Submission 18*, p. 7.

119 *Submission 15*, p. 4.

120 *Submission 31*, p. 6.

Corporate groups

3.126 Such concerns related primarily to the Exposure Bill's failure to recognise the existence of corporate groups, where customers have multiple products and services, and where the group potentially needs to monitor multiple activities of that class of customers to satisfy the AML/CTF requirements. Conglomerate operations raise a number of complex issues, including the issue of information-sharing between group entities.[121]

3.127 Similarly to the point raised in paragraph 3.101, Allens made the following suggestion in relation to this issue:

> Where the reporting entity is part of a corporate group we suggest that the reporting entity should be able to make the same disclosure to another member of the group, so long as that disclosure is not likely to prejudice an investigation which might be conducted following the report [of a suspicious matter].
>
> As a matter of sound business practice and risk management, if one member of a corporate group has information relevant to an offence or attempted offence it should be able to advise other members of the group of that suspicion, for example, to minimise the likelihood of offences being perpetrated across the group or another member of the group unwittingly facilitating a money laundering or terrorist financing offence.[122]

3.128 American Express also argued that the Exposure Bill should be amended to take reasonable account of corporate group structures and to allow them to share information.[123]

3.129 The SDIA went further, suggesting that:

> … it is important for its members to be able to share information (under notice to AUSTRAC for AML/CTF purposes) regarding certain activities of certain people. This would help prohibit more than one of our members becoming involved with an individual or entity, if the member who first suspected an instance where money laundering or terrorist financing was the reason behind a transaction, could inform other members. To be successful there must be immunity from prosecution for sharing such information. We recognise that tipping off could be a problem arising from such sharing of information as it would be difficult to identify the source however not sharing the information could have a significant impact on the industry.[124]

---

121 For example, IFSA, *Submission 2*, p. 7; Suncorp-Metway Limited, *Submission 14*, p. 3; American Express Australia Limited, *Submission 15*, p. 4.

122 *Submission27*, p. 7.

123 *Submission 15*, p. 4.

124 *Submission 31*, p. 8.

Lack of available defences

3.130 The committee also received evidence expressing concern about the lack of defences in the Exposure Bill in relation to the secrecy provisions. Many groups were fearful that legitimate actions by their employees pursuant to obligations under the regime may result in inadvertent breach of proposed section 95.

3.131 Mr Chris Downy of the Australian Casino Association, explained how employees of reporting entities may be caught by the tipping off provisions:

> The concern our members have is this whole question of alerting a high-risk customer to the fact that they are under suspicion. Asking them to provide identification basically alerts them to the fact that they may be under investigation.[125]

3.132 Some suggestions with respect to the tipping off provision included:

- a defence for employees of reporting entities who act in compliance with the Rules and Guidelines;[126] and
- a 'safe haven' provision, where employees of a reporting entity could make a disclosure to a customer as long as that disclosure does not prejudice an investigation.[127]

3.133 A representative of the Department assured the committee that defences to the tipping off offence in the Exposure Bill are available in the Criminal Code:

> We have had this discussion and it has been raised at the outset with industry. There is nothing in here for the moment. What they want is to see a provision in here saying, 'Whatever happens, if you have taken reasonable steps and exercised due diligence, you have a defence against criminal prosecution.' The reason we have not put it in there is because it is odd in these days of having the Criminal Code to have a provision like that in specific legislation. We think it is covered by the Criminal Code.[128]

AUSTRAC resources

3.134 The committee received evidence suggesting that, at the present time, AUSTRAC is not adequately resourced to produce draft Rules in the required timeframe;[129] nor is it resourced to effectively undertake its other obligations under the proposed regime. For example, IFSA suggested that the Federal Government

---

125 *Committee Hansard*, 14 March 2006, p. 25.

126 See, for example, Financial Planning Association of Australia, *Committee Hansard*, 14 March 2006, p. 20.

127 See, for example, Mr Peter Jones, Allens Arthur Robinson, *Committee Hansard*, 14 March 2006, p. 57.

128 *Committee Hansard*, 14 March 2006, p. 71.

129 See, for example, IFSA, *Submission 2*, p. 4; ING Direct, *Submission 13*, p. 3.

'consider whether AUSTRAC is adequately resourced to effectively carry out its obligations in relation to its Rule making function'.[130]

3.135 In response to questioning by the committee, a representative from AUSTRAC stated that, in her view, the slow release of the Rules is not a resource issue:

> One of the issues around resources is that having more people will not get the rules out any faster. The rules are so interrelated that the people working on them need to be across all the issues. So we have a group of three particular people who are directly involved in drafting the rules together and who have that across-the-board knowledge to be able to put them together.[131]

3.136 Nevertheless, the committee considers it essential that AUSTRAC be given adequate resources to effectively carry out its obligations under the regime, including its Rule-making function. Such resources should include provision of adequate numbers of staff with appropriate expertise and experience, as well as implementation of strategic planning capabilities within the organisation.

Interaction between the Exposure Bill and other legislative regimes

3.137 Some submissions and witnesses pointed out that the interaction between the Exposure Bill and other legislation must be taken into account when considering the impact of the new regime. Any inconsistencies or overlap must be addressed in order to create certainty for business. For example, Ms Michelle Mancy of American Express argued that:

> The government needs to prioritise laws relating to money-laundering prevention, privacy and discrimination, thereby ensuring that compliance with one will not affect a breach of another, rather than leaving it to business to tip-toe through a minefield of compliance regimes that seem to be at odds with each other.[132]

3.138 The ABA also highlighted the potential inconsistency between the Exposure Bill and other legislation with which financial service providers must comply. It argued that the interrelationship between the Exposure Bill and other laws, including privacy, discrimination, proceeds of crime, corporations and electronic transactions legislation, needs consideration.[133]

---

130 *Submission 2*, p. 4.

131 *Committee Hansard*, 14 March 2006, p. 76.

132 *Committee Hansard*, 14 March 2006, p. 49.

133 *Submission 18*, p. 25.

Specific issues arising for particular industry sectors

3.139 The committee also received evidence indicating the existence of specific concerns relating to the following industry sectors:

- superannuation;
- casinos/clubs;
- financial planning; and
- insurance.

3.140 Some of these concerns are discussed below.

Superannuation

3.141 Superannuation fund trustees will be considered reporting entities for the purposes of AML/CTF obligations because they provide a designated service. Evidence provided to the committee highlighted that superannuation raises a number of unique issues. Further, the risk profiles for AML/CTF will differ significantly between the various types of superannuation funds.

Regulated superannuation funds

3.142 Some submissions argued that the particular characteristics of regulated superannuation funds mean that they should be considered differently to many other services for the purposes of the AML/CTF regime; that is, they should not be subject to the same stringent requirements as those services that are considered to be high-risk.

3.143 Insurance Australia Group (IAG) suggested that:

> Given [superannuation contributions] are statutory contributions that cannot be withdrawn prior to retirement there is an extremely low risk of money laundering.[134]

3.144 IFSA supported the position that superannuation should be considered low-risk. It argued that:

> These products contain a number of important features that ensure they are neither suitable nor likely to be used by individuals seeking to launder money or finance terrorism.[135]

3.145 ISFA also noted that '[s]uperannuation is specifically mentioned in paragraph 12 of the Interpretive Notes to FATF Recommendation 5 as an example of a low risk

134 *Submission 11A*, p. 5.

135 *Submission 2*, p. 5.

product for which simplified or reduced customer due diligence measures may be appropriate.'[136]

3.146 In addition, The Association of Superannuation Funds of Australia (ASFA) argued that:

> It is when the benefit is actually paid out of the superannuation system or when the member asserts control over their interest, rather than when contributions are received by the fund, that particulate risks arise and customer identification is required.[137]

Self-managed superannuation funds (SMSFs)

3.147 A self-managed superannuation fund has less than five members and the trustee and members are generally the same people. Self-managed super funds are regulated by the ATO rather than the Australian Prudential Regulation Authority (APRA), which are responsible for regulated superannuation funds.

3.148 Advice to the committee was that self-managed super funds present a higher risk profile in terms of AML/CTF than other regulated superannuation funds. Nevertheless, the application of the proposed regime to SMSFs would not be without its challenges.

3.149 IFSA stated that:

> Given the greater control and flexibility allowed to members of SMSFs, these schemes lack a number of the features which make regulated superannuation products low risk.[138]

3.150 The submission provided by CPA Australia and The Institute of Chartered Accountants in Australia highlighted the practical issues created by the Exposure Bill for self-managed super funds. They submitted that:

> In practical terms the Bill would require a trustee to perform Customer Due Diligence on themselves, implement an AML/CTF Program and possibly report on suspicious matters arising out of their own actions.[139]

3.151 AFSA also pointed out that:

> The large number of difficult-to-supervise entities and the potential for collusion between the trustee and member (who are usually the same person) may represent a risk for money laundering and terrorist financing, but, if that is the case, the provision in the Bill requiring customer information and AML/CTF Programs do not work for this group. Although

136 *Submission 2A*, p. 4.

137 *Submission 28*, p. 4.

138 *Submission 2*, p. 6.

139 *Submission 7*, p. 3.

> self-managed funds represent a particular challenge to any AML/CTF system, in the interest of competitive neutrality they should not be exempted from the AML/CTF regime.[140]

Threshold transaction reporting

3.152 ASFA argued that the threshold transaction reporting requirement would significantly impact on superannuation funds. It argued that the proposed reporting threshold could require superannuation administrators to report every transfer, rollover or benefit payment over $10,000 and this 'would be inappropriate for superannuation funds'.[141]

3.153 ASFA noted that:

> The tax-free threshold (which represents a modest benefit) for superannuation is $129,751. $10,000 is a very low amount for superannuation benefits – which are often taken as a lump sum.[142]

3.154 ASFA went on to suggest that:

> The proposed $10,000 threshold for reporting a transaction is too low for superannuation contributions, rollovers, transfers and benefit payments, if all such payments are captured. It may also be too low for reporting of contributions in some funds and in some situations. The need to report a transaction could be risk-based and ways that funds might put this into operations should be explored.[143]

AML/CTF Programs

3.155 ASFA advised that '[b]y 1 July 2006, all superannuation fund trustees other than self-managed superannuation funds (SMSFs) will be licensed under new APRA licensing requirements'.[144] Therefore:

> [I]n this context, AML/CTF Program requirement appear too prescriptive and fail to recognise how APRA-regulated superannuation fund trustees already manage risk.[145]

3.156 ASFA suggested that regulated superannuation funds should be able to integrate the AML/CTF Program requirements into the existing regulatory requirements.

---

140 *Submission 28*, p. 8.

141 *Submission 28*, p. 5.

142 *Submission 28*, p. 5.

143 *Submission 28*, p. 5.

144 *Submission 28*, p. 6.

145 *Submission 28*, p. 6.

Casinos/clubs

3.157 The Exposure Bill lists the provision of 'a gambling service, where the service is provided in the course of carrying on a business'[146] as a designated service. Therefore, AML/CTF obligations are imposed on businesses operating in the gaming industry.

3.158 The committee heard that there are key differences between the gaming industry and the financial services industry. As a consequence, some of the AML/CTF obligations may not necessary and, if imposed, may negatively impact on the effective procedures that are currently in place or result in higher operational costs.

3.159 The committee received evidence from Clubs Australia, representing registered and licensed clubs, and the Australian Casino Association (ACA) which represents the casino operators of Australia.

Casinos – customer due diligence

3.160 Mr Chris Downy from the ACA argued that '[f]rom both a consumer's perspective and a business perspective, gambling is fundamentally different from the services provided by financial institutions'.[147] The ACA highlighted the proposed customer due diligence regime as an area where there is substantial difference between the two industries.

3.161 Mr Downy argued further that:

> The vast majority of casino customers are small recreational gamblers, typically occasional customers, who are no different from customers of restaurants or other entertainment services. To attempt to identify their transactions, record them, data match them or otherwise track them makes no sense because it is almost inconceivable that they are associated with money laundering or terrorism financing.[148]

3.162 Mr Anthony Seyfort, also for the ACA, continued:

> … at the moment we simply do not know the vast majority of people who come in once in a blue moon and spend a tiny amount of money, and there are thousands and thousands of those people … [W]e have a problem with the whole part 2 of the bill – simply this concept in the bill at the moment that you have to know every customer, full stop, whether they are suspicious, large or whatever.[149]

---

146 Proposed table 2, section 6.

147 *Committee Hansard*, 14 March 2006, p. 23.

148 *Committee Hansard*, 14 March 2006, pp 23-24.

149 *Committee Hansard*, 14 March 2006, pp 25-26.

3.163 Mr Downy raised an additional issue with respect to the obligation in the Exposure Bill that casinos must obtain detailed information about high-risk customers. Current legislation already requires that casinos report the activities of high-risk customers to AUSTRAC. Casinos may also be required to provide ongoing assistance to any review of these activities.[150]

3.164 The ACA suggested to the committee that the system that is currently in place works well and should be incorporated into the Exposure Bill.

Casinos – safe harbours

3.165 Mr Downy also advised the committee that members of the ACA fear the consequences, under statute and civil law, if despite their best efforts, they fail to comply with 'a complex and unwieldy set of requirements'.[151] He also submitted that:

> It is also very unclear how a broadly cast program required by a federal law would reconcile with the obligations of the specific state statutes such as the Casino Control Act if there were some inconsistency.[152]

3.166 Mr Downy suggested that 'the draft exposure bill could be amended to ensure that nothing casinos do in lawful compliance with their respective state based obligations would constitute non-compliance with the draft exposure bill'.[153]

Registered/licensed clubs

3.167 The Exposure Bill acknowledges that not all industries will pose the same level of risk in terms of money laundering or terrorism financing. Proposed section 28 provides identification procedures for certain low-risk services.

3.168 Clubs Australia argued that clubs already have player verification procedures in place and that the highly regulated gambling environment means that 'the imposition of any additional identification requirements to address risk cannot, in our view, be justified'.[154]

3.169 Clubs Australia also highlighted that electronic gaming machines are required to be connected to a centralised monitoring system. The submission went on:

> State Governments already have full access to EGM performance data which in our view is capable of identifying suspicious EGM activity if appropriate data analysis techniques are applied. Clubs Australia again notes that the cost of collecting this data is already borne by the clubs and

150 *Committee Hansard*, 14 March 2006, p. 24.

151 *Committee Hansard*, 14 March 2006, p. 24.

152 *Committee Hansard*, 14 March 2006, p. 24.

153 *Committee Hansard*, 14 March 2006, p. 24.

154 *Submission* 6, p. 2.

> the imposition of additional costs as a result of the proposed legislation is not in our view warranted.[155]

3.170 In conclusion, Clubs Australia argued that:

> It is our view that the gambling environment in clubs already poses a very low risk in the context of money laundering and terrorist financing and that … clubs should be excluded from the AML/CTF legislation.[156]

Financial planners

3.171 Currently, proposed section 6 lists personal advice given by a licensed financial planner in relation to securities and derivatives, life policy or sinking fund policy, superannuation funds or retirement savings accounts as a designated service.

3.172 The issue of whether the provision of financial advice should be listed as a designated service for the purpose of the AML/CTF regime was raised with the committee.

3.173 The FPA argued that:

> There does not seem to be any convincing reasons why the provision of financial advice in itself should trigger the AML/CTF obligations. The obligation for financial planners should instead rest on actions taken to implement their client's strategy.[157]

3.174 The FPA highlighted that the practical affect of the regime would result in customers having to identify themselves each time they consult with a financial planner. This may not sit comfortably with general advice from authorities such as ASIC that consumers consult with a number of planners before finalising their decision.[158]

3.175 Mr John Anning of the FPA acknowledged that:

> It may be the practices of financial planners would be better served if they did the identification up-front, at the initial contact with the client. But we believe that is a flexible point, and that they should be able to decide for themselves.[159]

3.176 The FPA suggested that 'it is highly unlikely that identification at the advice stage would result in greater benefits in terms of AML/CTF intelligence than

---

155 *Submission 6*, p. 3.

156 *Submission 6*, p. 4.

157 *Submission 24*, p. 5.

158 *Submission 24*, p. 5.

159 *Committee Hansard*, 14 March 2006, p. 17.

identification at the implementation stage'[160] and, as such, favoured the position that the provision of financial advice should not be a designated service.

Sole practitioners

3.177 The APF highlighted that:

> There are many thousands of financial advisers and planners, as well as solicitors and accountants acting in a financial advisory capacity. These advisers – often sole practitioners – will acquire obligations under the law with customer identification, reporting and monitoring requirements which will be extremely onerous both for the service provider and for the customer or client.[161]

3.178 The APF went on to argue the likelihood that:

> The burden and inevitable cost of compliance by small financial advisers and planners [would] have significant implications for the availability and affordability of financial advice at a time when governments are expecting individuals to take increasing responsibility for their financial security. [162]

3.179 The FPA supported this view:

> … it would be clearly impractical for financial planners to bear all of these obligations individually. FPA considers that effective fulfilment of the AML/CTF obligations will require recognition in the legislation of the pivotal role played by the A[ustralian] F[inancial] S[ervices] Licensee in the provision of financial services.[163]

Department response

3.180 In relation to some of the issues raised in relation to financial planning (and accountants), a representative from the Department told the committee that:

> The financial planners are picked up in table 1 if they provide specific product advice, but they are not if they provide general advice. The concept was that they are gatekeepers, so let us bring in the regulations and the rest of it at an early point. They have raised the question of whether, one, it is appropriate and whether, two, it is feasible, and the problems that it poses to their members to suddenly take off one hat and put on another and then require a person to provide identification material. Again, we have heard that. The accountants for the most part will be caught up in the second tranche of this legislation, because that is where we will have to grapple with how we regulate a lot of industry sectors that have not formerly been

160 *Submission 24*, p. 5.

161 *Submission 4*, p. 5.

162 *Submission 4*, p. 6.

163 *Submission 24*, p. 5.

> regulated. One of the issues that will be looked at in the wash-out after the consultation period is whether those provisions remain in table 1.[164]

Insurance

3.181 General insurance is not listed in the Exposure Bill as a designated service. Many organisations supported the exemption of general insurance from the AML/CTF regime.

3.182 The Insurance Council of Australia (ICA) stated that:

> ICA supports the exclusion of general insurance from the proposed legislation … [I]t is our recommendation that the proposed exemption of general insurance is maintained.[165]

3.183 Insurance Australia Group (IAG) expressed a similar view:

> IAG agrees with the assessment of the Australian Attorney General's Department that general insurance should not be a designated service, due to its extremely low risk nature, an assessment that is consistent with the FATF recommendations.[166]

3.184 However, IAG noted an unintended consequence of the Exposure Bill with respect to insurance:

> As an A[ustralian] F[inancial] S[ervices License] holder, a general insurer could be authorised to provide financial product advice in relation to life products, limited life risk insurance products and any products issued by a registered life insurance company relating to C[onsumer] C[redit] I[nsurance] products. Based on the AFSL authorisations, the general insurer would be deemed to be providing a designated service if it provides personal financial product advice. IAG submits that this is an unintended consequence of the Draft Exposure Bill.[167]

Life Products

3.185 Life products can be divided into two broad categories:

- life risk products; and
- investment life products.

---

164 *Committee Hansard*, 14 March 2006, p. 75.

165 *Submission 30*, p. 2.

166 *Submission 11A*, p. 3.

167 *Submission 11A*, p. 5.

3.186 Commonly both products are referred to as life insurance but 'the two classes of product must be carefully distinguished as they can present very different AML/CTF profiles'.[168]

3.187 IFSA highlighted that life risk insurance products share most of the characteristics of general insurance and therefore suggested that 'most life risk insurance products present a minimal to low money laundering risk'.[169]

3.188 In contrast, investment life products are or can be used for investment purposes. IFSA stated that:

> Such products have a surrender value, are transferable, can be used as collateral of a loan and can have high, lump sum premiums and payouts. As a result, and subject to some exceptions … these products can be considered to be medium risk and require a greater level of due diligence than life risk products.[170]

3.189 IFSA submitted that life risk insurance; life products acquired by superannuation funds; and life products having an annual premium of no more than A$1,500 or a single premium of no more than A$4,000 generally present a low to minimal risk of money laundering and should be classified by the Rules as low risk designated services for the purposes of proposed section 28 of the Bill.[171]

3.190 IFSA also suggested that a similar level of customer due diligence as applies to other investment products may be appropriate for investment life products not identified as low risk.[172]

Committee view

3.191 The committee applauds the extent and nature of the ongoing consultations between the Minister, the Department and AUSTRAC, and business and industry groups in relation to the proposed AML/CTF regime. However, the committee shares concerns that, without the full package of draft legislative instruments, affected industry bodies are unable to analyse sufficiently the full impact of the regime on their business operations. Since much of the detail of the regime is contained in the Rules, **the committee believes it is imperative that the complete set of Rules be released for comment prior to the final version of the bill being introduced into Parliament**.

168 IFSA, *Submission 2A*, p. 6.

169 *Submission 2A*, p. 7.

170 *Submission 2A*, p. 8.

171 *Submission 2A*, p. 9.

172 *Submission 2A*, p. 11.

3.192 In stating this, the committee is aware that development of the Exposure Bill and its associated documentation is an evolving process, and that the bill to be introduced into Parliament can be expected to differ from the publicly-released version which has been the subject of this inquiry. The committee is encouraged by assurances from the Department that it will continue to work closely with stakeholders to ensure that outstanding contentious issues and concerns will be resolved prior to the bill's introduction into Parliament.

3.193 Accordingly, and cognisant of the fluid nature of the process, the committee has used its inquiry as a vehicle for concerns to be aired and debated. The committee does not consider it appropriate, and is not inclined, to make recommendations in relation to technical aspects of the Exposure Bill as it currently stands. Rather, **the committee strongly encourages the Minister, the Department and AUSTRAC to utilise the expertise and knowledge of industry bodies to ensure the measures in the final AML/CTF package are truly risk-based, in order to reflect and promote business efficacy.** This is particularly important given that there appears to be a significant divergence between the Department and AUSTRAC, on the one hand, and industry, on the other, about what the term 'risk-based' actually means and whether the Exposure Bill encompasses a risk-based approach. The committee encourages the Department and AUSTRAC to work more closely with industry in order to achieve greater consensus in relation to the meaning and application of a risk-based approach.

3.194 **The committee also encourages the adoption of a realistic and workable timeframe for implementation of the new regime to allow business to undertake appropriate system changes**. The committee acknowledges the concerns expressed by many submissions and witnesses with respect to timing issues, particularly given the staggered and late release of the Rules. Accordingly, **the committee also encourages an extension of the consultation period to accommodate those concerns and to ensure effective consultation on any residual matters**. The committee notes that, at the time of writing (11 April 2006), the outstanding Rules are yet to be released publicly. This is of particular concern given that a period of at least five or six weeks from the date of delivery of the Rules was nominated by many groups as a minimum timeframe for analysis and completion of detailed submissions to the Department's consultation process.

CHAPTER 4

PRIVACY CONCERNS

4.1 The Office of the Privacy Commissioner (OPC), the Australian Privacy Foundation (APF), the Office of the NSW Privacy Commissioner (NSWPC), the NSW Council for Civil Liberties (NSWCCL) and Liberty Victoria provided the committee with a non-industry perspective on the possible impact of the proposed AML/CTF regime on the privacy and civil liberties rights of individuals.[1]

4.2 In particular, the concerns raised by these organisations related to:

- the lack of consultation on privacy issues prior to the release of the Exposure Bill;
- the need for a privacy impact assessment for the Exposure Bill;
- the wide range of entities collecting information under the regime;
- the type and extent of information to be collected under the regime;
- use of information collected pursuant to the regime; and
- the application of the *Privacy Act 1988* (Privacy Act).

Consultation on privacy issues

4.3 As noted in Chapter 3, the proposed AML/CTF regime has been developed since January 2004 in consultation between government and industry groups. NSWCCL and the APF both raised concerns that, despite this lengthy consultation period, privacy and civil liberties groups and consumer representatives were not given the opportunity to be involved in the drafting of the legislation until after the release of the Exposure Bill.[2] Ms Anna Johnson of the APF also stated that there was a lack of transparency to the process, citing the Department's reluctance to make available submissions received during public consultations in 2004.[3]

4.4 In evidence to the committee, the Department stated that while consumer advocate and privacy groups are not involved in the ministerial advisory group, parallel discussions are occurring with these organisations. It is proposed that these consultations will take the form of an ongoing body which will meet quarterly; and it is anticipated that the Minister would attend one or two of those meetings.[4]

---

1 See Australian Privacy Foundation, *Submission 4*; Office of the NSW Privacy Commissioner, *Submission 5*; NSW Council for Civil Liberties, *Submission 10*; Office of the Privacy Commissioner, *Submission 23*.

2 *Submission 4*, p. 2; *Submission 10*, p. 3.

3 *Committee Hansard*, 14 March 2006, p. 31.

4 *Committee Hansard*, 14 March 2006, p. 64.

4.5 AUSTRAC also confirmed that the Department and AUSTRAC have been involved in discussions with privacy, civil liberties and consumer groups, and that issues about coverage of the Privacy Act are being dealt with between the OPC and the Department. Further:

> All matters raised during the consultation period, including in submissions to this Committee, will be taken into account in reviewing the drafting of the Bill and the Rules. AUSTRAC is consulting with the Privacy Commissioner's office on the draft Rules and on guidance which will underlie the Rules, both directly and through its Privacy Consultative Committee, which also includes privacy, civil liberties and consumer groups.[5]

Privacy impact assessment

4.6 The committee's attention was directed to the issue of whether the potentially invasive measures in the Exposure Bill are necessary and proportionate to the risks they are meant to address; namely, money laundering and financing terrorism. [6]

4.7 To address this concern, the OPC suggested that a Privacy Impact Assessment (PIA) be performed for the legislation. The OPC described a PIA as:

> … an assessment tool that describes, in detail, the personal information flows in a project, and analyses the possible privacy impacts of the project. A PIA may assist in identifying and evaluating the impact of such matters as the Exposure Bill's coverage and issues around uses and disclosures of personal data.[7]

4.8 The OPC indicated that it had previously recommended to the Department that a PIA be conducted on the legislation:

> The Office provided comments to the Criminal Justice Division (CJD) of the Attorney-General's Department on a draft of the *Anti-Money Laundering Bill* 2004 on 14 January 2005. In these comments the Office suggested that at the end of the second round of consultations, it would be useful for the CJD to conduct a Privacy Impact Assessment (PIA) regarding the next version of the Bill.
>
> The Office believes that PIAs are a good practice approach to assessing the privacy risks associated with projects that have complex information flows.
>
> … Accordingly, I anticipate that the Office will again recommend to the Attorney-General's Department as part of our response to their request for comments on the Exposure Draft that they should consider undertaking a PIA.[8]

---

5 *Submission 33*, p. 3.

6 See, for example, *Submission 4*, p. 3; *Submission 23*, p. 7.

7 *Submission 23*, pp 7-8.

8 *Submission 23A*, p. 1.

4.9 In evidence to the committee, Mr David Vaile of the APF also indicated its support for a PIA.[9] Mr Stephen Blanks of the CCL supported both a PIA and a human rights impact assessment for the Exposure Bill.[10]

4.10 The Department indicated to the committee that, at this stage, the Minister has not agreed to a PIA being conducted for the Exposure Bill.[11]

4.11 In view of the far-ranging nature of the provisions contained in the Exposure Bill, the committee is of the view that a PIA would be beneficial.

Range of entities collecting information

4.12 The APF pointed out that there has been no attempt to quantify the number of entities expected to be captured by the various types of services listed in section 6 of the Exposure Bill.[12] This makes it difficult to ascertain the extent to which some reporting entities will be covered by the National Privacy Principles (NPPs) in the Privacy Act. However, what is known, is that:

> … [i]f enacted in its current form and with both tranches implemented, the Exposure Bill will impose personal information collection and disclosure obligations on far more entities than is currently the case under the FTR Act.[13]

4.13 A number of submissions also raised concerns about the use of reporting entities for performing security surveillance. Mr Luke Lawler from the Credit Union Industry Association (CUIA) described the situation as follows:

> There is a kind of deputisation of the entire financial sector to gather information on people and report information on people to a vast number of federal agencies.

4.14 NSWCCL described the regime as 'drastically reducing' the extent to which government and government agencies will be accountable for Australia's national security and intelligence regime.[14]

Type and extent of information to be collected under the regime

4.15 Submissions and witnesses raised concerns with respect to the wide range of information to be collected by reporting entities under the regime.

---

9 *Committee Hansard*, 14 March 2006, p. 34.

10 *Committee Hansard*, 14 March 2006, p. 37.

11 *Committee Hansard*, 14 March 2006, p. 69.

12 *Submission 4*, p. 5.

13 OPC, *Submission 23*, p. 3.

14 *Submission 10*, p. 8.

Customer identification information

4.16 The APF considered that the customer identification procedures in Part 2 of the Exposure Bill are contrary to the principle of anonymity provided for in NPP 8; that is, wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.[15] The APF was particularly concerned at the effect on individuals' ability to search for an acceptable financial advisor without identifying themselves.[16]

4.17 Mr Raj Venga of the Australian Association of Permanent Building Societies also argued against aspects of the identification process, anticipating that they would be regarded by customers as overly intrusive:

> We do not believe that the government and its agencies have properly considered how intrusive the customer identification and monitoring requirements of the bill and rules actually are. We see such intrusion as a bad thing. The fact of the matter is that the overwhelming majority of our members—almost all of them—are neither money launderers nor terrorists. Customers will not welcome the prospect of providing ID information—although they do it now on a limited basis—or responding to queries in relation to the source of funds, income and financial assets or their financial situation. These are personal and confidential matters that customers would understandably not wish to share, unless absolutely necessary in relation to the designated service—for example, applying for a loan. If a customer chooses not to cooperate, do we terminate our business relationship with the customer? And are we required to lodge a suspect matter report on the basis that the customer has not been forthcoming in providing this information?[17]

4.18 American Express considered that the scope of the minimum customer information required under the Rules is unnecessarily wide:

> For the purpose of issuing a relatively low risk product such as a credit card, it is of no business value to record: place of birth, nationality or country of residence. Verifying these particulars would be disproportionately costly and labour intensive and would yield no information of regulatory value for AML/CTF purposes. In addition, such information of necessity becomes a surrogate for identifying ethnicity, which in turn may lead to inappropriate assumptions being used as a basis for decision-making. The legitimate objectives of privacy and anti-discrimination laws may thus be undermined.[18]

4.19 In response to this comment, the Department and AUSTRAC pointed out that American Express' concerns appeared to be directed to a draft version of the customer

---

15 See, for example, *Submission 5*, pp 2-3; *Submission 23*, p. 6.

16 *Submission 4*, p. 5.

17 *Committee Hansard*, 14 March 2006, p. 4.

18 *Submission 15*, p. 4.

identification Rules, which had included a list of specific prescribed requirements. The Department indicated that these Rules would be redrafted to reflect a more risk-based approach. [19]

4.20 In an answer to a question on notice, AUSTRAC confirmed that the policy in relation to customer identification has changed since the committee's hearing:

> The Bill will be redrafted to provide for customer identification programs, to be developed by reporting entities, which take into account the level of risk in determining what identification process is to be applied to particular customers. Draft Rules have been prepared reflecting this change. Those Rules are currently with industry working groups but will be made more widely available after industry's views have been received. This will include discussions with the Privacy Commissioner's office.[20]

AML/CTF Programs

4.21 The AML/CTF Program requirements also triggered concerns from a privacy perspective; namely, the volume and type of information being provided to reporting entities under the customer due diligence requirements in the AML/CTF Program Rules.

4.22 The APF stated that reducing the risk of money-laundering and counter terrorism should not require monitoring of all customers and all transactions. The APF submitted that the 'floor' for the minimum 'Know Your Customer' information is set too low and the additional 'Know Your Customer' information and enhanced due diligence requirements are likely to apply to too many customers.[21]

4.23 The APF acknowledged that there was provision for full or partial exemption from identification procedures for some low-risk services. However, in its view, the drafting of such exemptions should not be 'left to the discretion and judgement of AUSTRAC to make in Rules'.[22]

4.24 Further, privacy implications are likely to arise from the requirement that reporting entities assign customers a risk classification.[23] The APF and the NSWPC noted that an assessment that a customer is 'higher risk' will potentially have an adverse affect on the customer, and the Exposure Bill lacks a review mechanism for a customer to challenge the risk assessment.[24]

---

19 *Committee Hansard*, 14 March 2006, p. 70.

20 *Submission 33*, p. 3.

21 *Submission 4*, p. 8.

22 *Submission 4*, p. 6.

23 *Submission 5*, p. 2

24 *Submission 4*, p. 8.

Impact of extensive 'suspicious matters' reporting obligations

4.25 Part 3 of the Exposure Bill provides that reporting entities must report certain 'suspicious matters' and transactions to AUSTRAC. 'Suspicious matters' is not defined in the Exposure Bill. The matters to be taken into account in determining whether there are reasonable grounds to report a suspicious matter will be set out in the Rules. Proposed subsection 39(4) makes it an offence if reporting entities fail to notify AUSTRAC of suspicious matters.

4.26 Five issues were raised in submissions and in evidence to the committee, regarding the obligation on reporting entities to report suspicious matters:

- the lack of precision in the definition of suspicious matters, particularly that the matters are not necessarily restricted to reports regarding money-laundering or terrorist financing;
- the probability of over-reporting of suspicious matters by reporting entities to avoid prosecution;
- the potentially discriminatory impacts of the reporting obligation;
- the lack of notice and openness in relation to the reporting regime, given that there is no requirement that reporting entities inform their clients that a suspicious matter report has been made to AUSTRAC; and
- the potentially conflicting obligations of employees of reporting entities to make suspicious matter reports, but not to tip off customers.[25]

4.27 The APF argued that the whole concept of reporting 'suspicions' by employees of reporting entities who are not qualified and trained investigators is inherently flawed:

> The criteria suggested in AUSTRAC guidance on suspect transaction reporting have always been highly subjective. The draft AML/CTF Rules and Guidelines for suspicious matter reporting which accompany the draft Bill are no better. They include appearance and behavioural factors as well as supposedly factual matters which there is no reason for employees of reporting entities to know.[26]

4.28 The APF argued further that the result of such broad and subjective guidance, and of the penalties for failure to report, would be either:

> • Even greater intrusion into customers' personal affairs, often based on 'guesswork', and/or,

25 See *Submission 4*, pp 6-7; *Submission 10*, pp 6-8; *Submission 23*, p. 4; *Submission 26*, pp 8-11; *Committee Hansard*, 14 March 2006, pp 20, 24-25, and 57.

26 *Submission 4*, pp 6-7.

> • Over-reporting because of an absence of information – 'to be on the safe side'.[27]

4.29 NSWCCL highlighted the potential impact of the obligation to report suspicious matters with other elements of the Exposure Bill:

> Part 9 (Countermeasures) of the proposed legislation allow the government to prohibit financial transaction to and from residents of particular countries. The combined effect of these provisions could be to encourage unwarranted 'suspicion' against persons of particular ethnic backgrounds or appearances. If so, this may create discrimination against individuals from non English-speaking backgrounds, because their behaviour, language, and lack of familiarity with Australian institutions and laws could lead to false 'suspicions [matter]' reports against them.[28]

4.30 In response to arguments suggesting 'racial profiling' may be a consequence of the suspicious matters reporting requirements, the Department had the following comments:

> If a person's appearance and behaviour give rise to suspicion on the part of the bank then there would be an obligation to report. I do not see how we can write into the legislation 'as long as you don't form that suspicion on a racist basis'. I think there are limits to what the legislation can do. If we decide that we want suspicions reported then some suspicions will be reported, if people do it properly. Some of those suspicions will be groundless and some will be based on things they should not base suspicions on.[29]

4.31 When asked about the training of staff to report suspicious matters and transactions, the Department said:

> I suggest that in relation to the question on how you are going to train staff to recognise risks and so on, there is at least an attempt in this bill to ensure that the programs require that sort of training for staff, whereas if you look at the existing FTR Act there is just the broad obligation. We recognise that experience will build over time and that at least there is an attempt to build a platform.[30]

4.32 The OPC noted that the reporting obligation in proposed section 39 goes beyond the reporting of information in relation to money-laundering and terrorism offences themselves.[31] Liberty Victoria highlighted that the obligation extends even

---

27 *Submission 4*, pp 6-7.

28 *Submission 10*, p. 8.

29 *Committee Hansard*, 14 March 2006, p. 70.

30 *Committee Hansard*, 14 March 2006, p. 63.

31 *Submission 23*, p. 4.

beyond information which might be relevant to serious offences, to encompass *any* offence – state or federal, and offences against foreign laws.[32]

4.33 Mr Luke Lawler of the CUIA told the committee of the experience in the US when similar legislation was introduced:

> One of the lessons from the experience of the United States is on the sheer number of reports being filed. There was an incredible increase in the number of suspicious activity reports that were being filed, so the financial intelligence unit over there was flooded with these reports with personal information about individuals, to the point where they were trying to advise industry to ease off a bit and be a bit more selective about the kinds of reports they were lodging. But industry was concerned because there were some high profile cases where some regulated entities were hit with very big fines for having inadequate anti-money laundering regimes. So in order to avoid any prospect of being prosecuted, they were pumping out these suspicious activity reports.[33]

4.34 Similarly, Ms Rhonda Luo of the NSWCCL told the committee that there was no utility in a system which generates over-reporting:

> Over-reporting is also very likely to result in misinformation being collected against individuals. If the object of the legislation is to identify and prevent international financial crimes, there is simply no use in having a large volume of possibly useless and wrong information against our citizens. It is possible that many innocent people will be caught up in these measures. More experienced, if I may say that, money launderers and financiers will be more likely to escape the simple pitfalls in the legislation.[34]

4.35 To rectify some of these problems, NSWCCL suggested that there be provision in the Exposure Bill for:

- notification to be given to customers at the beginning of a business relationship that business and service providers are required to report their financial activities that are regarded as 'suspicious';
- ex post facto notice to be given to individuals that a suspicious matter report has been made; and
- mechanisms by which individuals may be warned against financial products or transactions that are likely to generate a suspicious matter report.[35]

4.36 The Department justified the suspicious matters reporting requirements on several grounds. In its view, the legislation builds on what is already in the FTR Act,

---

32 *Submission 26*, p. 10.

33 *Committee Hansard*, 14 March 2006, p. 11.

34 *Committee Hansard*, 14 March 2006, p. 39.

35 *Submission 10*, pp 6-7.

since the key parts of the reporting requirement provisions are taken word for word from the existing Act:

> Those provisions have been there since 1988 and the number of suspicious transaction reports has gradually risen during that period from a fairly low level to the level that it is now at. They have never produced the sorts of problems which people are now saying that these provisions will produce.[36]

4.37 Further:

> In relation to the privacy issues, I hear what they say… But I do not know that there is a solution to some of the issues that they have raised. But what we then expect of the entity is that essentially they forget that they have put in a suspect transaction report, because it becomes the responsibility of AUSTRAC and the law enforcement agencies to decide whether to take action. We do not want reporting entities to be keeping records and blacklists of people who have put in suspicious transaction reports. [37]

Secrecy and access

4.38 The privacy implications of the wide collection requirements outlined above are compounded by the secrecy provisions in Part 11 of the Exposure Bill and, in particular, their application to suspicious matters reporting.

4.39 Ms Anna Johnson of the APF made the following comment on the provisions:

> We reserve our strongest criticism for the notion of secret reporting of suspicious matters. In our view, the concept of secret files compiled on the basis of amateur assessments and wholly subjective criteria is inconsistent with a free society.[38]

4.40 Having noted that the information in suspicious matter reports could be of 'dubious quality', because the reports are based on the subjective judgement of the employees of reporting entities, NSWCCL went on to say:

> … [t]he proposed regime also offends against individuals' access and correction rights under privacy laws, as the privacy-exempt suspicious transactions list thus created will be exempt from [Freedom of Information] law. It is uncertain how AUSTRAC will deal with information that appears to be unreliable, but it is submitted that the object of the legislation – prevention of terrorist financing – cannot be met if government or international investigations proceed on unreliable information. CCL notes that these secrecy provisions go beyond any existing regime in Australia, and even beyond the controversial wire-tapping laws in the United States.[39]

---

36 *Committee Hansard*, 14 March 2006, p. 62.

37 *Committee Hansard*, 14 March 2006, pp 62-63.

38 *Committee Hansard*, 14 March 2006, p. 30.

39 *Submission 10*, p. 6.

4.41 NSWCCL also suggested that there should be a notification given to customers at the beginning of a business relationship that business and service providers are required to monitor their financial activities.[40]

4.42 Representatives from the Department and AUSTRAC responded to the concerns with respect to secrecy as follows:

> The only tipping-off provisions in here are if you have put in a suspicious transaction report, you are not allowed to tell people that you have put in the report.
>
> … [T]here will be nothing at law stopping them from saying, if they wanted to, 'We consider you to be a high risk.' All they are not allowed to disclose is if in fact something has triggered an actual suspicion rather than a view that the customer is high risk. Somebody can be a high risk customer and never raise a suspicion, because even though they are high risk, their business is completely legitimate. It is only about putting in the suspicious matter report that the tipping off provision applies. If a customer comes to bank or a casino under privacy laws and asks whether they have been classified as high risk, I do not see that there is any way they can refuse to tell them.[41]

Need for public education campaign

4.43 The committee heard that there is a need for a public education campaign about the implications of the new regime. For example, Mr Luke Lawler of the CUIA told the committee that he anticipated that credit union customers would not react positively to a number of elements of the regime:

> Credit unions and other regulated entities will be required to collect baseline information on all customers. They will have to give all customers a risk classification, they will have to identify customers and services that pose a high risk, and they will have to collect quite detailed information on some customers and carry out transaction monitoring. Regulated entities will be obliged to report suspicious matters, even in cases where there is no actual transaction. Because of the impact on customers of these proposals, we have said from the outset that a significant public education campaign will be needed to explain why your financial institution will be asking you for more information about your personal affairs. We think this will come as a shock and a surprise to a lot of customers.[42]

4.44 Mr Lawler emphasised that such a public awareness campaign should inform customers that the actions taken by reporting entities are due to legislative requirements and are not being taken merely of their own volition:

---

40 *Submission 10*, p. 7.

41 *Committee Hansard*, 14 March 2006, p. 71.

42 *Committee Hansard*, 14 March 2006, p. 5.

> We would anticipate that, depending on the extent to which one has to gather this sort of additional information on customers beyond what is gathered in the ordinary course of business now, many of our members would be quite affronted and quite surprised at being asked to provide this sort of information. Even some of the baseline information that is proposed to be provided includes, for example, place of birth. If you provide a birth certificate as ID, that is all taken care of but if you provide, for example, a drivers licence as ID, you are not necessarily disclosing your place of birth. Nevertheless, the regulated entity will have to ask you for your place of birth. Some people might find that unnecessary and a little creepy…
>
> [W]e will be quite keen to explain that if we have to collect this sort of information—and in cases where someone fits a profile of possibly a high risk or a high-risk product, we will have to go and get some more information on them—we will want them to be aware that this is a legislative requirement and that we are not doing this simply to intrude in their personal affairs.[43]

4.45 The Department noted that it had considered the need for an awareness campaign to inform the public that these obligations stemmed from government and not from industry. The Department has given a commitment that such a campaign will take place, although the appropriate time for such a campaign remains to be determined.[44]

Use of information

4.46 Not only does the Exposure Bill provide for the collection of a great deal of additional material, it would also permit the use of that information for a wide range of purposes that arguably go beyond the objectives of the legislation. This has obvious privacy implications.

4.47 This issue has two elements: the first is the uses permitted by reporting entities of information collected from their customers; the second is the extent of AUSTRAC's authority to disseminate information contained in its system to other agencies.

Use of information for secondary purposes

4.48 Some submissions and evidence drew to the committee's attention the issue of use by reporting entities of information collected under the regime for secondary purposes. This matter is particularly relevant to those reporting entities not bound by the NPPs (discussed below).

4.49 As an example of the potential misuse of this information, Ms Anna Johnson of the APF drew the committee's attention to a recent article in the Law Society

---

43 *Committee Hansard*, 14 March 2006, pp 8-9.

44 *Committee Hansard*, 14 March 2006, p. 73.

Journal that promoted the benefits of the Exposure Bill as a way of generating further business because reporting entities will be required to know more about their customers' finances.[45] The article pointed out that the Exposure Bill would allow lawyers to have 'at their fingertips' information that would effectively allow them to sell a raft of additional services to their customers.[46]

4.50 This article raised the concern that reporting entities could use the proposed legislative requirements to compulsorily collect a wide range of personal customer information and use it for the general purposes of marketing and profiling.

Access to AUSTRAC-held data

4.51 Division 4 of Part 11 of the Exposure Bill provides for government agencies to access information held by AUSTRAC. In particular, proposed section 99 provides for AUSTRAC to grant access to 'designated agencies' 'for the purposes of performing the agency's functions and exercising the agency's powers';[47] that is, for purposes that may be completely unrelated to AML or CTF. Designated agencies are defined in proposed section 5, and include not only law enforcement agencies such as the Australian Federal Police, but also a wider group of agencies including the Child Support Agency and Centrelink. Further provision is also made to disseminate information to 'an authority of agency of a State or Territory, where the authority or agency is specified in the regulations'.[48]

4.52 The scope of the information dissemination by AUSTRAC pursuant to this provision raised some concerns. The OPC understood that the intention is that agencies with current access to AUSTRAC data under the FTR Act would retain that access, and it will be up to AUSTRAC to decide if other agencies are able to access information collected under the Exposure Bill.[49] The OPC's view on such an arrangement was that:

> … the replacement of the FTR Act with new legislation with its greater scope and impact does not, of itself, necessarily justify the continuance of the present data-sharing arrangements so as to permit access to the welfare and assistance agencies. In the event that the welfare and assistance agencies are to be given access to AUSTRAC data, then a statement of the legislative objects of the Exposure Bill should reflect an intention to allow such agencies to scrutinise the AUSTRAC data for their purposes.

45 *Committee Hansard*, 14 March 2006, p. 30.

46 See further, Professor John Broome, as quoted in J. Lewis, 'Cleaning up: Anti-money laundering laws need not spell disaster', *Law Society Journal*, March 2006, p. 22.

47 See, for example, *Submission 4*, p. 10; *Submission 10*, p. 5; *Submission 23*, pp 9-11.

48 Proposed section 5.

49 *Submission 23*, pp 9-10.

> Accordingly, community consultation should be conducted expressly on this policy setting.[50]

4.53 The OPC suggested that proposed section 99 be amended 'to a more privacy sensitive form' in which access to AUSTRAC-held data is restricted to purposes consistent with and relevant to the underlying purpose of the AML/CTF scheme.[51]

4.54 A representative of AUSTRAC clarified the scope of the information-sharing provisions of the Exposure Bill:

> … section 99(1) of the bill allows AUSTRAC to authorise specified officials of specified designated agencies. It does not allow us to decide which agencies may have access. The designated agencies are those agencies listed in section 5 under the definition. That provision is about what we do now, which is not specifically set out in our Act. In our MOUs with our partner agencies, we actually specify a limited number of officers who have access to our information. This is a provision that legislatively for the future will require us to specify them. So it is not like AUSTRAC can say, 'These are more agencies, other than are on the face of the bill, that can have access to our information.'

4.55 On the issue of the purposes for which designated agencies could access AUSTRAC-held data, representatives of AUSTRAC and the Department said:

> Some of this comes back to the questions about the definition of money laundering and the fact that the predicate offences for money laundering are extremely broad … [S]ome of those issues are matters of government policy about who should have access to our information and for what purposes.

4.56 In an answer to a question on notice, AUSTRAC noted that FTR information currently available to designated agencies is used to combat money laundering:

> The FTR information available to the designated agencies assists them to stop illegal conduct which would otherwise result in the laundering of money. If the agencies were not able to use the information to identify and prosecute offenders for predicate offences, where money laundering has not occurred because of the timing of the identification and investigation of the predicate offence, then the success of Australia's very effective anti-money laundering program would be severely diminished.[52]

4.57 The Department also noted specifically in relation to tax that the close relationship between tax, tax evasion and money laundering, and the fact that the taxation power underpins the FTR Act, makes it appropriate for the ATO to have

---

50 *Submission 23*, pp 9-10.

51 *Submission 23*, p. 10.

52 *Submission 33*, p. 3.

access. The Department undertook to consider the other comments in relation to which matters should be made explicit in the objects clause.[53]

Application of the Privacy Act

4.58 An important consideration in assessing the privacy implications of the Exposure Bill is the extent to which protections afforded by the Privacy Act apply to both AUSTRAC and government agencies, and the various service providers that would become reporting entities under the Exposure Bill.

AUSTRAC

4.59 A number of submissions noted that the Exposure Bill does make provision for AUSTRAC to obtain assurances from state, territory and foreign agencies about compliance with the Information Privacy Principles (IPPs) in the Privacy Act. However, the submissions questioned the enforceability of such assurances and what remedies individuals may have in the event that their privacy is interfered with.[54]

4.60 In response, AUSTRAC indicated to the committee that:

> … the memoranda of understanding that we currently have with our state and territory partner agencies actually state that they undertake to comply with the information privacy principles.[55]

Application of the National Privacy Principles to reporting entities

4.61 The NPPs in the Privacy Act regulate the collection, use and disclosure and handling of personal information by private sector 'organisations'. Reporting entities that are 'organisations' for the purposes of the Privacy Act will be required to comply with the NPPs.

4.62 The OPC outlined its concern that many of the privacy protections offered in the NPPs, such as the obligations in relation to data quality, notice and openness, will only apply to reporting entities to the extent that they are 'organisations' – as defined in the Privacy Act.[56]

4.63 Of particular concern is the fact that 'small businesses' – that is, businesses with an annual turnover of $3 million or less – are generally exempt from the NPPs.[57] NSWPC had the following comment in this regard:

---

53 *Committee Hansard*, 14 March 2006, p. 81.

54 See, for example, *Submission 4*, p. 10; *Submission 23*, p. 8.

55 *Committee Hansard*, 14 March 2006, p. 81.

56 *Submission 23*, pp 5-6.

57 See section 6D of the *Privacy Act 1988*; *Submission 23*, p. 5.

> It is out experience that many small businesses are either not very familiar with best privacy practice or choose not to follow it for a variety of reasons, predominantly because they do not have an obligation under the law to protect personal information of individuals. We receive a steady stream of complaints from members of the public alleging privacy breaches by medium and small businesses of the like that are likely to become reporting entities under the Bill. Unfortunately, under the current legislative regime neither state nor federal privacy agencies have effective powers to deal with such complaints.[58]

4.64 Witnesses before the committee demonstrate the mixed extent to which the NPPs might apply to reporting entities:

- All members of the Credit Union Industry Association are subject to the NPPs, because even those members to whom the NPPs did not apply had opted into the regime.[59] This is probably also the case for members of the Australian Association of Permanent Building Societies.[60]
- Some members of the Institute of Chartered Accountants in Australia are subject to the NPPs but not all.[61]
- Most members of the Financial Planning Association of Australia are subject to the NPPs, either because they are required to under the Privacy Act, or they had opted into the regime.[62]

4.65 The OPC, the NSWPC, and the APF all recommended that, given the personal and sensitive nature of the information being handled, all reporting entities should have privacy obligations imposed on them that are at least equal to the requirements of the NPPs.[63] The APF went further in suggesting that the Exposure Bill should be amended to specifically remove from reporting entities any exemption they may enjoy under the Privacy Act.[64]

4.66 The OPC also stated that the Exposure Bill should include additional privacy provisions which are consistent with the Privacy Act for all reporting entities, regardless of size or type.[65] The OPC made the following suggestions as to how this could be achieved:

---

58 *Submission 5*, p. 1.

59 *Committee Hansard*, 14 March 2006, p. 9

60 *Committee Hansard*, 14 March 2006, p. 9.

61 *Committee Hansard*, 14 March 2006, p. 46.

62 *Committee Hansard*, 14 March 2006, p. 21.

63 *Submission 23*, p. 5; *Submission 5*, p. 1; *Submission 4*, p. 13.

64 *Submission 4*, p. 13.

65 *Submission 23*, p. 8.

- Through privacy protections set out in a Schedule to the Exposure Bill, with an enforcement provision to the effect that a breach of the protection measures constitutes interference with the privacy of an individual for the purposes of section 13 of the Privacy Act.
- Amending the Privacy Act to specifically incorporate privacy with respect to AML/CTF.
- Including privacy provisions by way of an enforceable rule under section 191 of the Exposure Bill.
- Regulations under section 6E of the Privacy Act to include small businesses as 'organisations' for the purposes of the AML/CTF legislation.[66]

4.67 In the course of the public hearing, the Department acknowledged that the issue of the small business exemption to the NPPs was an issue that the Federal Government would have to, and will, address.[67]

Retention of information

4.68 An associated issue is the rules regulating the retention of information gathered by reporting agencies pursuant to the proposed regime. Part 10 of the Exposure Bill sets out the record-keeping requirements for reporting entities, and public comment has been invited on the duration of retention periods for records and documents.

4.69 The OPC considered that, while any period may be arbitrary, some guidance could be taken from the NPPs, which provides for the destruction of that personal information once it is no longer needed for any purpose for which the information may be used or disclosed. In the OPC's view such an approach highlights that there must be a 'specific and clearly justified' purpose for the retention of personal information.[68]

4.70 The APF also referred to the NPPs, and stated that the retention period should be for the shortest period possible to fulfil the objectives of the legislation. The APF noted that while there may be a temptation to set long or indefinite retention periods on the basis of a hypothetical utility, this should be resisted, particularly for suspicious matter reports which are 'hidden' from the subject.[69]

4.71 In considering the period for retention, Liberty Victoria suggested a period of five years, stating that anything outside of that time frame is:

---

66 *Submission 23*, pp 8-9.

67 *Committee Hansard*, 14 March 2006, p. 82.

68 *Submission 23*, p. 9, referring specifically to NPP 4.2.

69 *Submission 4*, p. 9.

> … likely to be of limited value in money laundering or terrorism offences which are far more likely to occur contemporaneously with the transaction.[70]

Committee view

4.72 Despite expressing optimism in the previous chapter that the majority of outstanding issues will be resolved before finalisation of the regime, the committee does remain concerned about the apparent lack of formal consultation with privacy, civil rights and consumer representative groups in the development of the regime to this point. The committee is of the view that this may have resulted in some fundamental privacy, consumer and civil rights issues being overlooked. Nevertheless, the committee is also hopeful that these issues will be addressed through the parallel discussion groups established by the Department.

4.73 The committee notes the OPC's suggestion that an independent PIA would be useful in relation to the Exposure Bill. **The committee agrees with this view and believes that a PIA would be beneficial in achieving a more balanced approach to the AML/CTF regime**. This is particularly important given the complexity of the Exposure Bill, the vast number of reporting entities and transactions covered by the Exposure Bill's operation, the amount and type of information to be collected, and the ability of various agencies to access that information. **The committee therefore strongly suggests that such an assessment be conducted**.

4.74 The committee also notes that the Federal Government intends to address the issue of the small business exemption to the NPPs in relation to reporting entities. However, the committee believes that the concerns raised in submissions and evidence highlight a larger problem in relation to the privacy obligations of reporting entities. The committee's view is that any PIA should include a review as to whether the privacy protections set out in the NPPs are sufficient for the purposes of the information being collected and handled by reporting entities.

4.75 If it is found that the privacy protections in the NPPs are not sufficient for the purposes of reporting entities, then adequate privacy protections could usefully be included in the AML/CTF legislative package. If the privacy protections in the NPPs are considered adequate for the purposes of reporting entities, then the Federal Government should ensure that all reporting entities are made subject to privacy obligations equivalent to those contained in the NPPs.

4.76 In line with a further suggestion by the OPC, **the committee also considers that the Exposure Bill should contain a clear objective statement that is reflective of the intention to allow federal, state and territory agencies, including welfare and support agencies, to access and utilise AUSTRAC data for their own purposes – purposes which may not be related in any way to AML or CTF**.

---

70 *Submission 26*, p. 14.

4.77 The committee considers that such a statement should be included in the final version of the bill to make it clear at the outset that this may occur.

Senator Marise Payne
Committee Chair

ADDITIONAL COMMENTS AND POINTS OF DISSENT BY THE AUSTRALIAN DEMOCRATS

1.1 The Democrats agree substantially with the evidence presented in the Chair's report in relation to recommendations for processes to be implemented prior to introduction of the Bill. We share the concerns raised and endorse the recommendations contained therein, subject to the following points.

1.2 The Democrats understand the need for ensuring protection of financial regulatory systems and procedures from the threat of money laundering and terrorist financing. However, we consider that this Exposure Draft Bill as a work in progress demands substantial improvement before it should be introduced.

1.3 As it is currently drafted, this Exposure Draft represents another disproportionate response to security issues facing Australia and will have severe implications for the rights of Australians. The threat of terrorism is not an adequate argument for the introduction of such invasive legislative changes.

1.4 The Democrats note the evidence provided by the Australian Privacy Foundation on this point:

> If the proposals represented in this exposure bill can be described in one word it is 'disproportionate'. In so many ways, these proposals are a heavy-handed approach and may be even a ham-fisted approach to managing the risks of money laundering and terrorist financing. Instead of taking a balanced and risk assessment based approach to monitoring financial transactions, an attempt has been made to sweep all manner of perfectly innocent transactions and innocent people into a vast net of surveillance.[1]

1.5 The Australian Privacy Foundation also expressed concern about the cumulative effect of this bill when considered with other proposals that already do or will potentially invade the privacy of Australians.[2]

1.6 The Democrats are deeply concerned about the veritable landslide of privacy incursions made possible by the recent changes in the name of combating terrorism. The absence of assessments as to the impact of these changes and any legislative framework to provide adequate protection for civil liberties compounds our concern.

---

[1] *Committee Hansard*, 14 March 2006, p. 30.

[2] *Committee Hansard*, 14 March 2006, p. 31.

Object of the Exposure Bill

1.7 The Democrats note the Committee's suggestion relating to the inclusion of a clear objective statement that reflects the true intention of the ways in which information collected in accordance with the Bill can be used.

1.8 The Democrats also note the evidence provided by the New South Wales Council for Civil Liberties on this issue:

> The true extent of the regime is obscured by the objects clause and title of the bill, which are highly misleading. The reference to anti money laundering and counter terrorism belies the fact that the data currently collected by AUSTRAC will be routinely accessible to a range of government agencies that have little or nothing to so with combating serious crime.[3]

1.9 The Democrats strongly believe that the Bill should be strictly limited to the collection of information for the anti-money laundering and counter-terrorism purposes stated in the objects of the Bill.

1.10 In the event that the Bill is not limited in this way, the Democrats strongly support the Chair's suggestion that the objects of the Bill be amended to clarify its true purpose.

Privacy

1.11 The Democrats reiterate the concerns of the Committee that fundamental privacy, consumer and civil rights issues have been overlooked.

1.12 We strongly support the Committee's recommendation that an independent Privacy Impact Assessment be undertaken in relation to this Bill. The Democrats strongly support the use of independent Privacy Impact Assessments to analyse all legislative changes that may infringe the privacy rights of Australians.

Human Rights Impact Statement

1.13 The Democrats support the suggestion by the New South Wales Council for Civil Liberties that, further to a Privacy Impact Statement, a Human Rights Impact Statement should be conducted.

1.14 The Democrats note and concur with evidence provided to the Committee that:

> … best parliamentary practice would be to have a human rights impact statement prepared before proceeding with this bill.[4]

---

[3] *Committee Hansard*, 14 March 2006, p. 37.

[4] *Committee Hansard*, 14 March 2006, p. 37.

1.15 The Democrats consider that similar to the heightened significance of a Privacy Impact Assessment in the context of totally inadequate privacy laws, the absence of a Bill of Rights against which to frame potential abuses and seek recourse demonstrates a heightened need for assessment of any potential infringements.

Senator Natasha Stott Despoja
Australian Democrats

APPENDIX 1

SUBMISSIONS RECEIVED

1	Real Estate Institute of Australia
2	Investment & Financial Services Association
2A	Investment & Financial Services Association
3	KPMG
4	Australian Privacy Foundation
5	Office of the NSW Privacy Commissioner
6	Clubs Australia
7	CPA Australia and The Institute of Chartered Accountants in Australia
8	Australian Association of Permanent Building Societies
9	Commonwealth Director of Public Prosecutions
10	NSW Council for Civil Liberties
11	Insurance Australia Group
11A	Insurance Australia Group
12	Australian Federal Police
13	ING Direct
14	Suncorp-Metway Limited
15	American Express Australia Limited
15A	American Express Australia Limited
16	PayPal Australia Pty Ltd
17	Australian Friendly Societies Association
18	Australian Bankers' Association
19	Credit Union Industry Association

20	Australian Securities and Investments Commission
21	Platinum Asset Management Limited
22	GE Capital Finance Australasia Pty Ltd
23	Office of the Privacy Commissioner
23A	Office of the Privacy Commissioner
24	Financial Planning Association of Australia
25	Australian Securities Intelligence Organisation
26	Liberty Victoria
27	Allens Arthur Robinson
28	The Association of Superannuation Funds of Australia
29	The Treasury
30	Insurance Council of Australia
31	Securities & Derivatives Industry Association
32	Attorney-General's Department
33	AUSTRAC

TABLED DOCUMENTS

Documents tabled at the public hearing on 14 March 2006

Australian Privacy Foundation

- J. Lewis, 'Cleaning up: Anti-money laundering laws need not spell disaster', *Law Society Journal*, March 2006

Investment & Financial Services Association

- JMLSG, Information on the Joint Money Laundering Steering Group
- JMLSG, 'JMLSG welcomes HM Treasury approval of new industry guidance', Media Release, 13 February 2006

- JMLSG, *Prevention of money laundering/combating the financing of terrorism* Guidance for the UK Financial Sector, Part I, January 2006

- JMLSG, *Prevention of money laundering/combating the financing of terrorism* Guidance for the UK Financial Sector, Part II: Sectorial Guidance, January 2006

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Sydney, 14 March 2006

Australian Bankers' Association

Mr Tony Burke, Director

Australian Association of Permanent Building Societies

Mr Raj Venga, Executive Director

Credit Union Industry Association

Mr Luke Lawler, Senior Advisor, Policy and Public Affairs

Investment and Financial Services Association

Mr Richard Gilbert, Chief Executive Officer

Ms Jenifer Wells, AML Working Group

Mr Michael Callow, AML Working Group

Financial Planning Association of Australia

Mr John Anning, Manager, Policy and Government Relations

Mr Tim Roberts, Member, AML/CTF Taskforce

Australian Casino Association

Mr Chris Downy, Executive Director

Mr Anthony Seyfort, Partner, Lander & Rogers, Lawyers for the Australian Casino Association

Office of the Privacy Commissioner

Mr Timothy Pilgrim, Deputy Privacy Commissioner

Mr Andrew Solomon, Director, Policy

Australian Privacy Foundation

Ms Anna Johnston, Chair

Mr David Vaile, Vice Chair

NSW Council for Civil Liberties

Mr Stephen Blanks, Secretary

Mr Anish Bhasin, Committee Member

Ms Rhonda Luo, Member

CPA Australia

Ms Judy Hartcher, Business Policy Advisor

The Institute of Chartered Accountants

Mr Bill Palmer, General Manager, Standards and Public Affairs

Ms Catherine Kennedy, Professional Standards Consultant

American Express

Mr Brett Knight, Head of Compliance

Ms Michelle Mancy, Manager, Legal Affairs

ING Direct

Mr Mark Mullington, Executive Director, Risk Management

Ms Lisa Claes, Executive Director, Sales and Operations

Allens Arthur Robinson

Mr Peter Jones, Partner, Banking and Finance

Attorney-General's Department

Mr Geoff Gray, Assistant Director, Criminal Law Branch, Criminal Justice Division

Mr Bruce Bannerman, Principal Legal Officer, Funding and Assets of Crime, Criminal Law Branch, Criminal Justice Division

AUSTRAC

Ms Liz Atkins, Acting Director, AML Reform

Ms Louise Link, AML Reform Team Leader

Mr Paul Ryan, Acting Deputy Director, Regulatory and Corporate

Ms Sonja Marsic, Senior Executive Lawyer, Australian Government Solicitor (Acting for AUSTRAC)

Australian Federal Police

Federal Agent Peter Drennan, National Manager, Economic and Special Operations

Mr Peter Whowell, Manager, Legislation Program