The Senate

Standing Committee on Legal and Constitutional Affairs

Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions]

Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]

November 2006

ISBN 0 642 71734 6

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

MEMBERS OF THE COMMITTEE

Members

Senator Marise Payne, **Chair**, LP, NSW
Senator Patricia Crossin, **Deputy Chair**, ALP, NT
Senator Andrew Bartlett, AD, QLD
Senator George Brandis, LP, QLD
Senator Linda Kirk, ALP, SA
Senator Joseph Ludwig, ALP, QLD
Senator Nigel Scullion, CLP, NT
Senator Russell Trood, LP, QLD

Participating Members

Senator Andrew Murray, AD, WA
Senator Stephen Parry, LP, TAS

Secretariat

Ms Jackie Morris	A/g Secretary, Legal and Constitutional Affairs Committee
Ms Kerrie Martain	Principal Research Officer
Ms Monika Sheppard	Senior Research Officer
Ms Julie Connor	Executive Assistant

Suite S1.61 Telephone: (02) 6277 3560 Fax: (02) 6277 5794
Parliament House E-mail: legcon.sen@aph.gov.au

TABLE OF CONTENTS

ABBREVIATIONS

ABA	Australian Bankers' Association
Abacus	Abacus - Australian Mutuals
ACA	Australian Casino Association
ADI	authorised deposit taking institution
AFC	Australian Finance Conference
AFSL	Australian Financial Services Licence
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
Baycorp	Baycorp Advantage Limited
Bendigo Bank	Bendigo Bank Limited
CCIP	Consumer Credit Insurance products
CEO	Chief Executive Officer
Computershare	Computershare Limited
Cth	Commonwealth
CUIA	Credit Union Industry Association
Department	Attorney-General's Department
DBG	designated business group
DVS	document verification system

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*
FSU	Financial Sector Union
FTR Act	*Financial Transaction Reports Act 1988*
HREOC	Human Rights and Equal Opportunity Commission
IAG	Insurance Australia Group
ICA	Institute of Chartered Accountants
IFSA	Investment & Financial Services Association
ING	ING Bank
Law Council	Law Council of Australia
Mallesons	Mallesons Stephen Jaques
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*
Privacy Victoria	Office of the Victorian Privacy Commissioner

RDA	*Racial Discrimination Act 1975*
SDIA	Securities & Derivatives Industry Association
SMSFs	self-managed superannuation funds
Special Recommendations	FATF Nine Special Recommendations on CTF
Telstra	Telstra Corporation Limited
UK	United Kingdom
US	United States
Visa	Visa International
Westpac	Westpac Banking Corporation

RECOMMENDATIONS

Recommendation 1

5.21 The committee recommends that the Bill be amended to delay the first stage of implementation until three months after the date of Royal Assent.

Recommendation 2

5.22 The committee recommends that AUSTRAC when amending or making further Rules after commencement of the Act thoroughly consult with industry and other stakeholders.

Recommendation 3

5.23 The committee considers that the AML/CTF Rules which provide safe harbour provisions for customer identification should be re-examined during the review of the legislation required by clause 251.

Recommendation 4

5.24 The committee recommends that subclause 6(7) be deleted from the Bill.

Recommendation 5

5.25 The committee recommends that the Department consider whether Part 6 of the Bill should be amended to provide the AUSTRAC CEO with powers to refuse registration as a designated remittance services provider and to de-register providers; or to maintain a register of persons who are not permitted to provide remittance services.

Recommendation 6

5.26 The committee recommends that the penalties for the offences in subclauses 138(3) and (5) which relate to possessing false documents or possessing equipment for making false documents be reduced.

Recommendation 7

5.27 The committee recommends that the Department continue to work with industry groups and other stakeholders to resolve technical drafting issues including:

(a) the exclusion of services relating to stored value cards by the drafting of items 21-24 of table 1 in clause 6;

(b) the capture of fund managers selling securities on an exchange by item 35 of table 1 in clause 6; and

(c) the exclusion of some community bank branches from the definition of 'owner-managed branch' in clause 12.

Recommendation 8

5.28 The committee recommends that the Federal Government consider amending the Bill to include further threshold value limits, to exclude low risk, low value services (such as the provision of travellers cheques and foreign currency transactions) from the definition of 'designated services' and that consideration be given to indexing these thresholds every five years.

Recommendation 9

5.29 The committee recommends that the Office of the Privacy Commissioner conduct periodic audits of AUSTRAC's compliance with privacy obligations in its administration of the Bill.

Recommendation 10

5.30 The committee recommends that Division 4 of Part 11 of the Bill should be amended to restrict access to AUSTRAC held information to access for the purposes of responding to money laundering, terrorist financing or other serious crime.

Recommendation 11

5.31 The committee recommends that clause 235 be amended to provide that protection from liability does not extend to actions which breach federal, state or territory anti-discrimination laws.

Recommendation 12

5.32 The committee recommends that AUSTRAC work with stakeholders to develop an objective, non-discriminatory model for assessing the risk of money laundering and terrorism financing to assist reporting entities in performing their obligations.

Recommendation 13

5.33 The committee recommends that clause 251 be amended to provide for review of the legislation in four years and for that review to incorporate consultation with industry and other stakeholders.

Recommendation 14

5.34 Subject to the preceding recommendations, the committee recommends that the Bill be passed.

CHAPTER 1

INTRODUCTION

Background

1.1 On 8 November 2006, the provisions of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (the Bill) and the Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 (the Amending Bill) were referred to the Legal and Constitutional Affairs Committee for inquiry and report by 28 November 2006.

1.2 The Attorney-General explained in his Second Reading Speech that the purpose of the Bill is to combat money laundering and financing of terrorism by ensuring Australia has a financial sector which is hostile to criminal activity and terrorism. The Bill implements a first tranche of anti-money laundering (AML) and counter-terrorism financing (CTF) reforms which cover the financial sector, gambling sector and bullion dealers as well as lawyers and accountants (to the extent that they provide financial services).[1]

1.3 The Bill will impose obligations on businesses (referred to as 'reporting entities' under the legislation) including customer due diligence, reporting, record-keeping and developing and maintaining an AML/CTF program. The banking sector will also be obliged to conduct due diligence on its correspondent banking relationships and ensure appropriate identifying information is included in international electronic transfers of funds.[2]

1.4 The Legal and Constitutional Legislation Committee reported on 13 April 2006 on the exposure draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005 (the Exposure Bill).

1.5 As noted in that report, the Exposure Bill was not a static document.[3] The Attorney-General's Department (Department), in conjunction with the Australian Transaction Reports and Analysis Centre (AUSTRAC), was conducting simultaneous public consultations which resulted in over 120 submissions to the Department. After consideration of those submissions and the committee's report, the Minister for Justice and Customs released a revised exposure draft of the Bill and further consultation was undertaken by the Department and AUSTRAC.

---

1 The Hon. Philip Ruddock MP, Attorney-General, Second Reading Speech, *House of Representatives Hansard*, 1 November 2006, p.1.

2 Second Reading Speech, 1 November 2006, p.2.

3 Senate Legal and Constitutional Legislation Committee, *Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005*, April 2006, p.1.

1.6 For the purposes of this inquiry, the committee has focused upon how the Bill materially differs from the Exposure Bill. Where appropriate, reference will be made to the committee's earlier report. Chapter 2 sets out the main provisions of the Bill which have been revised since the Exposure Bill.

Conduct of the inquiry

1.7 The committee advertised the inquiry in *The Australian* newspaper on 13 and 22 November 2006, and invited submissions by 17 November 2006. Details of the inquiry, the Bill, and associated documents were placed on the committee's website. The committee also wrote to 86 organisations and individuals.

1.8 The committee received 42 submissions which are listed at Appendix 1. Submissions were placed on the committee's website for ease of access by the public.

1.9 The committee held public hearings in Melbourne on 14 November 2006 and in Sydney on 22 November 2006 and 23 November 2006. A list of witnesses who appeared at the hearings is at Appendix 2 and copies of the Hansard transcript are available through the Internet at http://aph.gov.au/hansard.

Acknowledgement

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

Note on references

1.11 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 Script.

CHAPTER 2

MAJOR CHANGES TO THE BILL

2.1 This chapter briefly outlines the main provisions of the Bill which have been revised following publication of the Exposure Bill on 16 December 2005.

Part 1 – Introduction

2.2 The Bill has introduced a phased implementation period in respect of various obligations (clause 2). There will be a 'prosecution free' period for the first 12 months of each implementation period and a formal review of the Bill will be required within seven years of commencement.

2.3 The term 'designated business group' has been inserted into the Definitions (clause 5). This will allow associated business entities to share customer identity information without committing a 'tipping off' offence and to subscribe to a joint anti-money laundering and counter-terrorism financing (AML/CTF) program.

2.4 The designated services identified in clause 6 have been split into four tables. Table 1 covers financial services, table 2 covers buying and selling bullion, table 3 covers gambling services and table 4 covers prescribed services provided in the regulations.

2.5 Table 1 now contains 54 designated services. Some items have been amended for clarity, whereas other items have been removed in their entirety.[1]

2.6 The new table 2 previously comprised items 62 and 63 in table 1 and deals with the buying and selling of bullion.

2.7 Table 3 was originally table 2 in the Exposure Bill and contained a single item: provision of a gambling service in the course of carrying on a business. The term 'gambling service' was defined in clause 5. 'Gambling service' is no longer defined in the Bill and has been replaced with the new table comprising 14 items. These items have been distinguished to facilitate the application of identification obligations at a time appropriate to the provision of the particular designated service.

Part 2 – Identification procedures

2.8 Existing customers are not subject to applicable customer identification procedures. In the Exposure Bill verification of an existing customer's identity was determined on the basis of materiality and risk. The Bill now establishes a trigger

---

1 For example, former items 38, 42-43, 48 and 52 which concern advice provided by licensed financial advisers. The obligations of designated non-financial businesses and professions, including licensed financial advisers will be addressed in the second tranche of the AML/CTF legislation.

(clause 29): if a reporting entity identifies circumstances which give rise to a suspicious matter reporting obligation, then the reporting entity must take the action specified in the AML/CTF Rules within the time allowed under the rules.

2.9 Similarly, the AML/CTF Rules can classify some designated services as low risk services. A low risk service customer is not subject to customer identification procedures except when a suspicious matter reporting obligation arises (clause 31). Again the AML/CTF rules will specify the action the reporting entity must take and the time allowed for taking that action.

2.10 The new Division 6 requires reporting entities to monitor their customers to identify, mitigate and manage the risk the responsible entity may reasonably face that the provision of a designated service might involve or facilitate money laundering or financing of terrorism (clause 36). The AML/CTF Rules establish the method by which a reporting entity will comply with this ongoing customer due diligence obligation.[2]

2.11 An agent may carry out applicable customer identification procedures on behalf of a reporting entity (clause 37). The common law principles of agency apply and the reporting entity will be responsible for the acts or omissions of its agent. There is no requirement to verify the identity of the agent.

2.12 Under certain conditions, a reporting entity may rely on an applicable customer identification procedure carried out by another reporting entity (clause 38).

2.13 There are particular designated services to which the customer identification procedures will not apply (clause 39). For example, a designated service that is of a kind specified in the AML/CTF Rules or provided in circumstances specified in the AML/CTF Rules.

Part 3 – Reporting obligations of reporting entities

2.14 The term 'suspicious matters', which was prevalent in the Exposure Bill, has largely been replaced by the term 'suspicious matter reporting obligation'. This latter term has been defined in the Bill (subclause 41(1)).

2.15 There are two elements in relation to a suspicious matter reporting obligation: circumstance and physical. The circumstance elements indicate when the obligation arises and the physical elements specify the kinds of suspicious matters which require the matter to be reported to the AUSTRAC CEO by the reporting entity.[3]

2.16 Three examples of the physical elements are that the reporting entity suspects on reasonable grounds that:

---

2 Australian Government, Australian Transaction Reports and Analysis Centre, *Draft Consolidated AML/CTF Rules for Discussion*, 4 July 2006, Chapter 6.

3 Proposed paragraphs (a)-(c), inclusive, and proposed paragraphs (d)-(j), inclusive, respectively.

- the customer is not the person they claim to be (paragraph (d));
- the provision of the service is preparatory to the commission of an offence covered by the definition of financing of terrorism (paragraph (g));
- the provision of the service is preparatory to the commission of an offence covered by the definition of money laundering (paragraph (i)).

2.17 A reporting entity must give the AUSTRAC CEO a report about the matter, within a specified timeframe: generally within 3 business days or, if the suspicion relates to financing of terrorism, within 24 hours. The AML/CTF Rules may specify the information to be included within that report.[4]

2.18 The AML/CTF Rules may exempt some designated services from the reporting obligations. The Rules may also provide for the lodgement of regular reports in which case a reporting entity must give the AUSTRAC CEO a report regarding the reporting entity's compliance with the legislation, regulations and the AML/CTF Rules.[5]

2.19 Competent authorities are now able to obtain information and documents for use in investigations of money laundering and underlying predicate offences.[6] If a reporting entity is obliged to report to the AUSTRAC CEO, including in respect of a threshold amount or electronic funds transfer, then authorities such as the AFP Commissioner, the Commissioner of Taxation and the CEO of the Australian Crime Commission may obtain further information or require the production of documents from the reporting entity (clause 49).

2.20 Where a request for information or documents relates to the identity of an account holder of a credit or debit card issued outside Australia, the AUSTRAC CEO or the Commissioner of Taxation may direct the reporting entity to obtain the necessary information from the card issuer (clause 50).

Part 6 – Register of providers of designated remittance services

2.21 The provisions of Part 6 have been substantially amended. In the Exposure Bill the primary obligation was for AUSTRAC to maintain a register of designated remittance service providers. Those providers were required to furnish AUSTRAC with all necessary details.

2.22 Persons are now expressly prohibited from providing a registrable designated remittance service unless their name and details are entered on a Register of Providers of Designated Remittance Services (subclause 74(1)).

---

4 Australian Government, Australian Transaction Reports and Analysis Centre, *Draft Consolidated AML/CTF Rules for Discussion*, 4 July 2006, Chapter 9.2.

5 Proposed clauses 42, 44-45 and 47.

6 Proposed clauses 49–50 and Explanatory Memorandum, p.91.

2.23 AUSTRAC continues to be responsible for the maintenance of an electronic register. A reporting entity may request advice from the AUSTRAC CEO as to whether a specified person is entered on the register however the register is not available to the public as it is not a legislative instrument.

Part 7 – Anti-money laundering and counter-terrorism financing programs

2.24 In the Exposure Bill a reporting entity was required to develop, maintain and comply with an AML/CTF program, which was defined in former clause 73.

2.25 In the Bill a reporting entity is expressly prohibited from commencing to provide a designated service to a customer unless the reporting entity has adopted, maintained and complied with an AML/CTF program (clauses 81-82).

2.26 An AML/CTF program is comprised of two parts: Part A (general) and Part B (customer identification). The purpose of Part A is to identify, mitigate and manage the money laundering or financing of terrorism risks a reporting entity may face. The purpose of Part B is to establish the customer identification procedures.

2.27 Reporting entities are now subject to three types of program:

(a) a standard program;

(b) a joint program which applies to each reporting entity that belongs to a designated business group; or

(c) a special program which applies where the only designated services provided by the reporting entity are covered by item 54 in table 1 of clause 6 (This item covers a holder of an Australian Financial Services Licence who arranges for a person to receive a designated service).

2.28 AML/CTF standard and joint programs must incorporate the prescriptive Parts A and B. A special AML/CTF program need only address Part B.

Part 8 – Correspondent banking

2.29 The provisions regarding correspondent banking relationships with shell banks have been re-drafted to reflect the fact that it can be difficult to identify shell banks. A 'shell bank' is defined in clause 15 and essentially means a bank incorporated in a foreign country which has no physical presence in that country.

2.30 A financial institution is prohibited from entering into a correspondent banking relationship with another person if the financial institution does so reckless as to whether that person is a shell bank or is a financial institution that has a correspondent banking relationship with a shell bank (clause 95).[7]

---

7 Note that clause 5 defines 'person' to include an individual, company, trust, partnership, corporation sole or body politic.

2.31 The Bill continues to require financial institutions to assess the risk that the correspondent banking relationship might involve or facilitate money laundering or financing of terrorism ('the preliminary risk assessment') (subclause 97(1)). This is a precondition to the formation of a correspondent banking relationship.

2.32 If warranted by the risk identified in the preliminary risk assessment, financial institutions must also carry out an assessment of the matters specified in the AML/CTF Rules (that is 'a due diligence assessment') (subclause 97(2)).

2.33 Financial institutions which have already entered into a correspondent banking relationship must also conduct regular preliminary risk and due diligence assessments. The assessments must be carried out in accordance with the AML/CTF Rules.

2.34 Financial institutions which are in correspondent banking relationships and which become aware that the other person is a shell bank, or a financial institution which has a correspondent banking relationship with a shell bank, have obligations to terminate the relationship under clause 96.

Part 10 – Record keeping requirements

2.35 This Part has been substantially expanded in the Bill. Clause 105 provides that this Part does not override the credit reporting provisions in Part IIIA of the *Privacy Act 1988*. Effectively this means that records retained by reporting entities in compliance with this Part for longer than the maximum period permitted under the Privacy Act should only be used for purposes associated with this legislation, its Regulations and the AML/CTF Rules, or in compliance with a warrant issued by law enforcement and national security agencies.[8]

2.36 The AML/CTF Rules may now require a reporting entity to make a record of information relating to the provision of a specified kind of designated service or the provision of a designated service in specific circumstances (clause 106). Under clause 108, any documents relating to a designated service which have been given to the reporting entity by or on behalf of the customer concerned are to be retained. The retention period for transaction records and customer provided transaction documents is seven years.

2.37 Clauses 109 and 110 require retained documents to be transferred between banks within 120 days after the transfer or closure of an active account. The transferring bank is then released from its document retention obligations, whereas the receiving bank is bound to observe a fresh seven year document retention period. The intention of these provisions is to avoid duplication and to ensure that a reporting entity can expeditiously comply with its obligations under the Bill.

8 Explanatory Memorandum, p.122.

2.38 A reporting entity must now document all 'applicable customer identification procedures' carried out by it. Each record is to include information obtained during the procedure and any other information required by the AML/CTF Rules (clause 112). The retention period for records of identification procedures is seven years.

2.39 Electronic funds transfer instructions are also captured by a seven year record keeping requirement (clause 115).

Part 11 – Secrecy and access

2.40 Under clause 123, a reporting entity is prohibited from disclosing to someone other than the AUSTRAC CEO or a staff member of AUSTRAC that a suspicious matter reporting obligation has arisen and been communicated to the AUSTRAC CEO. This tipping off prohibition has some exceptions.

2.41 In particular, the Bill now allows qualified accountants to disclose that information. The disclosure must relate to the affairs of a customer and be made for the purposes of dissuading the customer from engaging in unlawful activity (clause 123). This provision has been inserted into the Bill in recognition of the fact that qualified accountants often provide their customers with tax advice.

Part 13 – Audit

2.42 New Division 7 enables the AUSTRAC CEO to require a reporting entity to appoint an external auditor to audit of the reporting entity's capacity and endeavours to comply with its obligations under the legislation, its regulations and AML/CTF Rules. Clause 161 allows the AUSTRAC CEO to require the conduct of a risk management audit. While clause 162 gives the AUSTRAC CEO the power to require a compliance audit.

Part 15 – Enforcement

2.43 This Part establishes the various ways in which compliance with the obligations imposed by the Bill can be enforced by AUSTRAC. The Exposure Bill contained a number of enforcement options which allowed for application of the most appropriate enforcement mechanism. The Bill now contains two further enforcement options: remedial directions and enforceable undertakings.

2.44 The AUSTRAC CEO may direct a reporting entity to take specified action aimed at preventing the contravention of a civil penalty clause, or minimising the likelihood that such a contravention will occur (clause 191).

2.45 New Division 7 enables the AUSTRAC CEO to accept written undertakings from reporting entities and to seek an order from the Federal Court in the event that the undertaking is breached. An undertaking can be compliance based or remedial in nature. AUSTRAC may publish undertakings on its Internet site.

Part 18 – Miscellaneous

2.46 The Exposure Bill contained a number of protection from liability clauses.[9] These have been replaced with a single protection from liability clause (clause 235). A reporting entity and its employees or agents, are indemnified for acts and omissions done in good faith in relation to compliance or purported compliance with the legislation, its regulations or the AML/CTF Rules. The conduct of an applicable customer identification procedure and fulfilment, or purported fulfilment, of a requirement to discontinue or not provide a designated service are specifically covered by the indemnity.

2.47 There is now also a general defence to both criminal and civil proceedings (clause 236). A reporting entity can establish the defence if it proves that it took reasonable precautions, and exercised due diligence, to avoid the contravention in respect of which the proceedings were instituted.

9 *Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005*, Clauses 36, 46 and 64.

CHAPTER 3

KEY CONCERNS FOR INDUSTRY

3.1 Submissions and evidence presented for the purposes of this inquiry indicate that business and industry bodies are generally comfortable with the Bill however some general and several specific issues remain unresolved. These issues will be discussed in this chapter. Chapter 4 will discuss privacy and discrimination issues in relation to the Bill.

Consultations with stakeholders

3.2 The committee was particularly interested in the extent and nature of consultations undertaken by the Department and AUSTRAC since its inquiry into the Exposure Bill. Most submissions and evidence indicated that the consultations have been extremely productive. Smaller businesses and industry groups felt that they became involved late in the process however the criticisms of the consultation process were not confined to these groups.

3.3 The minor criticisms generally consisted of a slow response or non-incorporation of suggestions. In relation to the latter criticism, the stakeholders acknowledged that consultations were continuing and they expected to resolve outstanding matters directly with the Department and AUSTRAC. The committee notes that many such matters involve technical drafting issues rather than issues of content.

3.4 The major criticism of the consultation process was that the AML/CTF Rules which were released on 13 July 2006 comprise an incomplete draft document.[1] For example, the Insurance Australia Group (IAG) said:

> There should be an adequate period in which industry can consider all aspects of the legislative package i.e. including the Bill, Rules and Regulations. This would enable training, intra group relationships and compliance arrangements to be simultaneously assessed and gaps identified against the requirements of the package.[2]

Department response

3.5 The Department stated that the draft indicative set of Rules provides prospective reporting entities with an understanding of how to comply with AML/CTF obligations. The committee was also told that the Rules are being finalised in a staggered fashion to coincide with implementation dates, with some stages already substantially complete, and that all Rules will be finalised by late 2007.[3]

---

1 For example, *Submission 23*, p.2; *Submission 26*, p.1; *Submission 8*, p.2; *Submission 20*, p.1.

2 *Submission 3*, p.2.

3 *Submission 37*, p.1.

Evidence from the Department and AUSTRAC suggested that some of the concern in relation to the availability of Rules arose from a misconception that the government intended to issue rules in relation to all provisions of the Bill when there was no intention to do so:

> The inclusion in many of the provisions of the ability to designate further things by rules is a very deliberate insertion of an ability in the future to respond to…unintended consequences or deliberate structuring and creation by industry of products which technically fall outside the definitions of the legislation…All of our conversations to date on rules have focused on those rules which we all know need to be available either on commencement or with sufficient lead time for the commencement of the operative provisions.[4]

3.6 To address this confusion, AUSTRAC provided a table setting out provisions in the Bill which provide for the making of Rules, whether Rules are required or contemplated under each provision, and the status of draft rules.[5] AUSTRAC released further draft rules in relation to movements of physical currency into or out of Australia and movements of bearable negotiable instruments on 22 November 2006.

Implementation of obligations

3.7 Business and industry bodies have universally welcomed the 24 month implementation period, as well as the 12 month prosecution free period.[6] However, the staggered approach has caused concern.[7] The cause of the concern was essentially related to the status of the Rules and business and industry bodies' ability to implement their obligations on time.

3.8 ING Bank (ING) proposed:

> Commencement dates should begin from the date that Rules applicable to the relevant Part have been released and finalised. Alternatively, Royal Assent should not occur until the Rules have been finalised. This is because, whilst in theory, implementation can begin from the date of Royal Assent, the detailed obligations are contained within the Rules and implementation can not realistically commence until Reporting Entities are aware of the requirements outlined in the Rules.[8]

3.9 The Australian Bankers' Association Inc. (ABA) highlighted that:

---

4 *Committee Hansard*, 23 November 2006, p.34.

5 *Submission 37a.*

6 For example, *Submission 3*, p.2; *Submission 23*, p.2.

7 One submission even queried whether the staggered approach to implementation was either necessary or appropriate - see *Submission 5*, p.4.

8 *Submission 23*, p.2. Also, see *Submission 15*, p.2; *Submission 26*, p.3; *Submission 10*, p.2.

> The prosecution free period does not allow for Rules development. It is not workable for industry to implement a Rule after Royal Assent either concurrently with or shortly preceding the commencement date...Compliance, enforcement and prosecution activity should then not commence until 12 months after commencement of the Part, including publication and finalisation of all necessary Rules to give effect to the Part.[9]

3.10 The majority of submissions and evidence given to the committee by business and industry groups indicated that a substantial amount of lead time would be required to implement AML/CTF obligations. Smaller businesses, which are not currently regulated under the *Financial Transaction Reports Act 1988*, particularly felt disadvantaged in this regard.

3.11 The Australian Finance Conference (AFC) said:

> A number of our members are stand-alone finance businesses and do not benefit from the sharing of resources which may be available within large corporate groups. For smaller businesses, the cost of preparing for the new regime will be considerable in the context of their overall size.[10]

3.12 The Finance Sector Union of Australia (FSU) also told the committee:

> We believe the Government is effectively requiring finance sector staff to help with law enforcement activity but is not implementing mechanisms to ensure that these staff are given enough resources to carry out these activities…[our] main concern is ensuring that financial sector staff receive adequate training to comply with the new requirements and that finance sector staff are not unfairly burdened.[11]

3.13 Small and medium-sized enterprises have indicated that they will require some formal assistance for effective implementation of the AML/CTF regime.[12]

Department response

3.14 The Department informed the committee that the implementation timetable incorporated in the Bill provides time for reporting entities to implement AML/CTF obligations:

> We have a staged implementation timetable which has a 12-month period from royal assent to the commencement of the first substantive new

9 *Submission 16*, pp 1–2. Also, see *Submission 20*, p.2.

10 *Submission 15*, p.2. Also, see *Submission 2b*, p.2.

11 *Submission 33*, p.1.

12 For example, *Submission 2b*, p.2 where the CPA Australia and the Institute of Chartered Accountants suggested a national education program, ongoing technical support and advice, and development of profession wide compliance programs.

> obligations under this bill. At this stage, we have committed to those rules being available by 31 March.[13]

3.15 In relation to formal assistance, the Office of the Privacy Commissioner (OPC) will be providing guidance and assistance to small business operators to meet their obligations under the *Privacy Act 1988*. In addition, AUSTRAC will receive funding to conduct a public awareness campaign.[14]

Formation of the Rules

3.16 A second common concern in relation to consultation was that there is no agreed formal consultation process with respect to the Rules.

3.17 Allens Arthur Robinson (Allens) pointed out that:

> [Although the AUSTRAC CEO is required] to consult with reporting entities or their representatives in performing his functions (such as making Rules) section 212(5) provides that any failure to do so does not invalidate any action he might take in performing his function. In practice this means that the AUSTRAC CEO can issue Rules under section 212 without effective industry consultation.[15]

3.18 Liberty Victoria stated:

> Arguably, the central feature of the Bill is the wide power and discretion it confers upon the AUSTRAC CEO…most significantly, the AUSTRAC CEO will be responsible for making AML/CTF Rules...these rules are legislative instruments…this process of law-making is largely based on primary accountability to the responsible Minister and confines the consultation process principally to industry sectors...other persons and groups likely to be affected by the Bill…are not formally recognised in these procedures.[16]

3.19 Many submissions indicated a willingness to be involved in further consultations both generally and in relation to specific provisions of the Bill. [17]

Department response

3.20 AUSTRAC advised the committee that it intends to maintain consultation with stakeholders:

> [T]he consultation process will continue down to the level of the guidelines with industry. Consultation into the future, again, is something that we have

---

13 *Committee Hansard*, 23 November 2006, p.35.

14 *Submission 40*, p.3. This formal assistance will include materials and educational activities.

15 *Submission 38*, p.6. Also, see *Submission 14*, p.4.

16 *Submission 1*, pp 13–14.

17 For example, *Submission 14*, p.3; *Submission 26*, p.3; *Submission 35*, p.3;*Submission 3*, p.5.

> worked on quite extensively in the past 17 years that the organisation has been in operation and more extensively over the last couple of years, and that process will continue on into the future.[18]

3.21 Additionally, AUSTRAC will maintain and consult its Privacy Consultative Committee.[19]

Lack of parliamentary review

3.22 Several submissions argued that review of the Bill and its associated instruments was vital and should be timely and transparent, particularly in light of AUSTRAC's extensive Rule and Regulation making powers.

3.23 In response to concerns regarding subclause 6(7) which allows the broadening or narrowing of the definition of 'designated service', the Department provided the following response:

> It is reasonable to expect that while every attempt has been made in the AML/CTF Bill to cover all of the services which could be used for the purposes of money laundering or terrorism financing, those determined to avoid the operation of the provisions may find new and unforseen ways to structure activities so that they achieve the same outcomes as designated services but fall outside the definitions in clause 6. Sub-clause 6(7) will enable the Government to respond quickly to the emergence of such activities. Regulations will be disallowable instruments and subject to the normal procedures under the Legislative Instruments Act 2003.[20]

3.24 Minter Ellison, Lawyers (Minter Ellison) told the committee:

> [AUSTRAC] should be subject to the scrutiny of and accountable to a Parliamentary Committee. We also believe that it should be required to consult with other regulators of the financial services industry (such as ASIC and the Australian Prudential Regulation Authority), in addition to the industry itself, when making Rules or modifications to ensure that the impact of its proposals are fully considered and understood and to limit any regulatory overlap.[21]

3.25 More generally, Privacy Victoria stated:

> [G]reater transparency and public accountability should be guaranteed. The Bill should specify the matters that will be examined, establish an independent review committee, compel public consultation, and provide for timely tabling of the review report.[22]

---

18 *Committee Hansard*, 23 November 2006, pp 33–34.

19 *Submission 37*, p.2.

20 *Submission 30a,* p.6.

21 *Submission 5a,* p.6.

22 *Submission* 14, p.4.

Suspicious matter reporting obligation

3.26 The committee received several submissions raising concerns about the breadth of the suspicious matter reporting obligation. In addition to the privacy and discrimination implications, it was said that this reporting obligation would result in AUSTRAC being inundated with suspicious matter reports.[23]

3.27 CPA Australia (CPA) and the Institute of Chartered Accountants (ICA) commented that:

> This piece of legislation is aimed at money laundering and terrorism [financing] and there really does not seem to be any justification for including breaches or having to report anything that is relevant to the prosecution or investigation of an offence against the Commonwealth, state and territory law.[24]

3.28 A suspicion that provision of a service relates to 'financing of terrorism' is a ground giving rise to suspicion matter reporting obligations under paragraphs 41(1)(g) and (h). Liberty Victoria argued more specifically that the definition of 'financing of terrorism' is extremely broad and improperly captures funding organisations where there may be no intention or knowledge that the funds will be used to carry out terrorism.[25]

3.29 Privacy Victoria added:

> The proposed measures effectively require financial agencies and others to police their customers for possible breaches of the taxation and criminal laws of every Australian jurisdiction. The Bill also requires these agencies to recognise situations where reporting a matter may assist government in enforcing the complex provision of the various confiscations laws across Australia…this appears to be an impossible task for financial institutions and other reporting entities.[26]

3.30 The FSU as well as the CPA and ICA expressed similar concerns that small business customer relationships might be adversely affected by the reporting obligation.[27]

---

23 *Submission 2a*, p.4; *Submission 1a*, p.3; Submission *14*, p.2; *Submission 40*, p.6 and *Submission 7*, p.9 which suggested that reporting entities would be likely to err on the side of caution and over-report due to the enforcement provisions within the Bill. Also, see Chapter 2 of this Report.

24 *Committee Hansard*, 14 November 2006, p.3; Also, see *Submission 41*, p.1 and *Submission 38*, p.3 which noted an extension of the obligation to overseas law enforcement.

25 *Submission 1*, pp 1–4.

26 *Submission 14*, p.2.

27 *Submission 2*, p.1 and *Submission 33*, p.2.

Register of Providers of Designated Remittance Services

3.31 The committee examined Part 6 clauses 75 to 79 which relate to the requirement of the AUSTRAC CEO to maintain a *Register of Providers of Designated Remittance Services*. In particular the Department was questioned about whether these provisions should include the ability to refuse registration to or to de-register providers. The Department responded:

> This bill is not about the terms and conditions on which you can conduct the business; it merely says that, if you conduct the business, it must be done in accordance with these rules. Because there is no current system that even identifies remittance providers, we have taken the approach in this bill.[28]

Penalties and sanctions

3.32 The expansion of the civil penalties and criminal sanctions provisions drew a wide range of comments. For example the submission from the CPA and ICA stated:

> The majority of the breaches…would be breaches of process and not specific intent to commit a crime…in our view [the maximum penalties] are probably a bit disproportionate.[29]

3.33 IAG similarly submitted that:

> We consider that there needs to be further consultation and discussion around, or at least consideration given to, the standard of proof that is required in respect of the civil penalty provisions…the penalties are potentially so significant for a reporting entity that we consider that a higher standard of proof should apply and that consideration should be given to whether an element of fault should also apply.[30]

3.34 The submission from Minter Ellison went further, arguing that:

> Most if not all the obligations imposed on Reporting Entities should not directly give rise to civil penalties or criminal offences. We submit that they should be legal obligations which can be enforced by AUSTRAC directing the Reporting Entity to comply with the obligation. A Reporting Entity should only be liable to prosecution if it fails to comply with such a direction.[31]

3.35 Infosys Technologies Australia Pty Ltd (Infosys) argued that the 'tipping off' provisions should not encompass the suspicion that triggered the reporting obligation or the business records and source information on which the suspicion is based.

---

28 *Committee Hansard* , 23 November 2006, p.44.

29 *Committee Hansard,* 14 November 2006, p.5.

30 *Committee Hansard,* 14 November 2006, p.8.

31 *Submission 5a,* p.7.

Infosys submitted that by providing otherwise the Bill goes beyond FATF Recommendation 14, does not accord with comparable jurisdictions and has the practical effect of prejudicing the rights of innocent third parties.[32]

3.36 In relation to a specific form of banking entity, Bendigo Bank argued:

> If owner-managed branches are to be put on the same footing as other branches (thereby ensuring a level playing field), the exemption in section 123(8) should extend to sections 123(1), (2) and (3)…The sharing of information between banking groups (including between the bank branches) is critical to ensure that suspicious activity is properly tracked and dealt with throughout the group.[33]

Customer identification obligations

3.37 Some submissions raised concerns in relation to the customer identification obligation. Abacus Australian Mutuals (Abacus) was concerned that its members will no longer be able to rely on the Acceptable Referee identification method. This method will expire 12 months after the Bill receives royal assent. Abacus argued that smaller approved deposit taking institutions (ADIs) will then have to either engage an agent or a reciprocal reporting entity to verify and validate identification documentation. The latter option would 'in effect [involve] sending a potential customer, where there is no established relationship, to a competitor'.[34] It was argued that the identification obligation would pose a risk to competitive neutrality and choice in retail banking.

3.38 This argument was based on the lack of a viable alternative to the Acceptable Referee identification method. The alternative, electronic verification (e-verification) found universal support as a necessary component of modern banking.[35] However, business and industry groups debated whether electronic data is sufficiently available and reliable for use in e-verification.

3.39 Abacus told the committee:

> The capacity for [reporting entities] to verify the authenticity of core government-issued documents – such as Passports, Driver's Licences and Birth Certificates – is severely limited…unfortunately, the AML/CTF Bill does not expand access to available databases for identification purposes. The proposed Medicare and welfare services Access card will not be an identity panacea and access to the planned government document verification system (DVS) remains a distant possibility.[36]

---

32 *Submission 7*, pp 5–9.

33 *Submission 28*, p.4.

34 *Submission 17*, pp 1–2.

35 *Submission 22*, p.4. Baycorp identified remote customers and organisations with no branch networks as persons who particularly rely upon e-verification.

36 *Submission 17*, p.2.

3.40 ING submitted that:

> In order to facilitate the 'safe harbour' contained in the draft Rule, a provision must be inserted [into the Amending Bill] authorising Reporting Entities to have access to information held within credit reports for the limited purposes of verification of identity in accordance with the Reporting Entities' AML/CTF programs, and authorising credit reporting agencies to disclose such information to Reporting Entities.[37]

3.41 Baycorp Advantage Limited (Baycorp) argued that one hurdle to the establishment of effective electronic verification systems was that the provisions supporting electronic verification were included in the Rules and not the Bill itself:

> All references to electronic verification as a component of an appropriate customer identification procedure identification system are only within the Rules…[which] may be easily amended as AUSTRAC sees fit. It is unreasonable to expect an organisation such as Baycorp to invest in the significant development of its business infrastructure to cater for a method of customer identification that is so easily subject to change…[electronic verification] should be included in the body of the legislation…or the safe harbour provisions should be included in Regulations, as these are subject to direct ministerial oversight.[38]

3.42 Westpac Banking Corporation (Westpac) expressed concerns about whether the safe harbour provisions would maintain reliable customer verification. Westpac acknowledged that a suitable document verification system could facilitate e-verification, however, in the interim:

> The safe harbour provisions present a weaker form of identification compared to the current *Financial Transaction Reports Act* (FTRA) standards and are inadequate in establishing that the person is who they are purporting to be…this would represent a 'wind-back' of the FTRA, weakening the financial system and increasing rather than decreasing the risk of ML/TF as well as fraud and identity theft for Australia.[39]

3.43 With reference to securities issued by trusts, Computershare Limited (Computershare) argued in favour of an exemption from the identification obligation. Computershare told the committee that in practice an identification process will already have been undertaken by either or both the bank on which a cheque for the application money has been drawn or the CHESS participant, who processes the application.

---

37 *Submission 23*, p.3 and *Submission 15*, pp 2–3 which noted that the Amending Bill has the effect of narrowing access to information obtained under the *Commonwealth Electoral Act 1918*. This position was at odds with *Submission 22*, p.7 which advocated greater access for less limited purposes but *Submission 9*, p.8 which argued that any access by reporting agencies would be subject to commercial abuse.

38 *Submission 22*, pp 4–5.

39 *Submission 26*, p.2.

> To add in a requirement that the issuer of the security (in this case the issuer of the units in the trust) also to carry out an identification, is an unnecessary and costly duplication...It has the potential to require the establishment of two differing processing requirements…[and] where there is an issue of a stapled security that involves a share and a unit, a longer application period may need to be implemented to cater for the additional identification requirements.[40]

3.44 Superannuation funds are treated slightly differently in relation to the customer identification obligation. Superannuation funds are only required to identify their members when money is leaving the superannuation system. The Bill recognises that complying regulated superannuation funds present a low-risk of money laundering and financing of terrorism. However, the Association of Superannuation Funds of Australia Limited (ASFA) has drawn attention to the fact that:

> Cashing is not exempted from the up-front identification requirements…[but] there are cashing transactions that are prescribed by law and not initiated by the member…The regime should ensure such transactions [are] not captured by inappropriate customer identification requirements.[41]

Recognition of corporate groups

3.45 The broadening of the definition of 'designated business group' in clause 5 was generally welcomed.[42] There were two suggestions in relation to such groups. IAG submitted:

> There should be a general provision to the effect that any obligations of a reporting entity under the Bill can be discharged by another member of a designated business group.[43]

3.46 Telstra Corporation Limited (Telstra) added that:

> The Bill still provides no qualification or exception where a designated service is provided to another member of a designated business group.[44]

---

40 *Submission 27*, p.2.

41 *Submission 10*, p.3. For example, the payment of unclaimed monies to a state registrar of unclaimed funds. Also, see *Submission 5*, p.8 where Minter Ellison, Lawyers presented similar arguments in respect of transfers and roll-overs between reporting entities.

42 Although the Australian Privacy Foundation did not support these changes arguing that designated business groups could effectively 'blacklist' customers – see *Submission* 9, p.7.

43 *Submission 3*, p.4 and *Submission 38*, p.2.

44 *Submission 24*, p.2. For instance, intra-group loans and parent company guarantees. The Business Council of Australia made similar comments in relation to corporate treasuries adding that the lack of qualifications and/or exemptions would increase compliance costs for corporations operating internal treasuries – see *Submission 1*, p.2.

Limited use of agents

3.47 Some submissions raised concerns regarding the limited use of agents for applicable customer identification procedures. For example Baycorp was critical of the deemed agency provision in clause 38 which applies only when a 'reporting entity' has carried out the original applicable customer identity procedure.[45] Allens and IFSA expressed a broader concern that there is no provision for the general use of agents in the Bill.[46]

Overseas permanent establishments

3.48 The Bill requires reporting entities to implement AML/CTF Programs in respect of any overseas permanent establishments (OPEs) through which a reporting entity provides designated services to the extent it is reasonable and practicable to do so having regard to local laws and circumstances.

3.49 Westpac sought an exemption for OPEs in New Zealand noting that New Zealand is in the process of developing AML/CTF legislation:

> It is therefore possible, depending on the transition timeline, that many Australian reporting entities will have to 'roll-out' AML/CTF procedures twice in NZ as a result of Australia's regime having extra-territorial application. NZ has existing suspicious transaction reporting obligations, and this will operate to mitigate NZ being a target for money laundering in the interim.[47]

Department Response

3.50 The Department noted that reporting entities do not generally have to comply with AML/CTF obligations in relation to OPEs, except in relation to inclusion of these OPEs in their AML/CTF program. In addition, Part 7 which imposes these obligations does not commence for 12 months after Royal Assent.[48]

International electronic funds transfers

3.51 Under the Bill international electronic funds transfer instructions must include certain information about the origin of transferred money. Debit and credit card transactions are exempted from the operation of this Part except when the transaction involves a cash advance other than via an ATM.

---

45 *Submission 22*, pp 8–9.

46 *Submission 38*, pp 1–2 and *Submission 20*, pp 6–7.

47 *Submission 26*, p.4.

48 *Submission 30c*, p.9.

3.52 Visa International (Visa) told the inquiry that the protocols of providing the required customer information cannot be met in a debit or credit card transaction involving a cash advance and that:

> We are not aware of the rationale for the requirements for complete payer information for cash advances involving debit and credit cards at bank branch or merchant terminals, while ATM transactions are exempted …since the electronic routing and information exchanged in both types of transactions is identical, this is somewhat anomalous.[49]

3.53 In relation to electronic funds transfer reporting obligation, the Securities & Derivatives Industry Association (SDIA) noted that:

> There should be a carve out / exemption to comply with this obligation for those reporting entities who are not ADIs, Credit Unions or similar …every reporting entity is obliged to make the relevant reports and one would assume the relevant ADIs that these reporting entities use, will be required to make the same report. …this part of the legislation should be re-worded in such a way that reporting entities who are not ADIs or similar, can rely on their relevant ADI to do the reporting for them.[50]

Minimum value thresholds

Travellers' cheques and foreign currency transactions

3.54 The committee received several submissions regarding the absence of minimum value thresholds with respect to travellers' cheques and foreign currency transactions. Travelex Limited (Travelex) argued that in not applying minimum value thresholds to these services the Bill is at odds with internationally accepted recommendations, best practice and has additional impacts, including unnecessary collection of personal information.[51] Similarly American Express gave evidence that:

> [There is a] de minimis exception for certain stored value products, namely stored value cards, postal orders and money orders. These are only designated services…for transactions of $1,000 or more. For travellers' cheques, on the other hand—they are also stored value products with largely similar characteristics and risk profile to these other products—there is no $1,000 threshold. In our view, this anomaly unfairly discriminates against travellers' cheques, which, in our submission, should be similarly treated under the bill.[52]

3.55 The Australian Financial Markets Association (AFMA) added:

---

49 *Submission 29*, pp 1–2. The practical effect of this submission was that Visa's Australian members believe that they would be forced to deny cash advances at Merchants or bank branches to Australian Visa cardholders travelling overseas.

50 *Submission 13*, p.1.

51 *Submission 12*, pp 1–2 and *Submission 19*, pp 1–2 and Attachment pp 1–5.

52 *Committee Hansard*, 22 November 2006, p. 35.

> The Bill should apply a realistic and practical threshold to the requirement on currency exchange providers to check the identity of customers …in our view the threshold should not be specified in the AML/CTF Bill but set by regulation or by Rule that can be varied more easily from time to time to take into account changes in AML/CTF risk factors, customer usage and transaction values.[53]

Gift, store and phone cards

3.56 In addition, it was argued that while stored valued cards, such as phone cards or gift cards, are intended to be subject to minimum thresholds the current drafting of items 21 to 24 in table 1 of clause 6 actually excludes most stored value cards because the value is not stored on the card itself. Mallesons Stephen Jaques (Mallesons) argued that:

> Issuing SVCs is intended to be a designated service. The relevant designated services are drafted to exclude low risk, low value SVCs from regulation. Unfortunately, the definition used for "stored value card" (SVC) does not apply to [gift cards or many similar, low-risk products] for technical reasons.[54]

3.57 Mallesons argued that if gift cards fell outside the stored value card provisions in table 1 then they would risk being captured as debit cards under items 18 to 20 which are not subject to a minimum threshold amount.[55]

3.58 It was similarly argued that phone cards and pre-paid mobile phone credit were captured by the debit card provisions of the Bill. For example, the Australian Mobile Telecommunications Association (AMTA) gave evidence that:

> Perhaps we can help the committee by giving some examples…where we do not think the intention of the legislation is to capture these types of products but where we think we are caught—for example, where providers of mobile phones issue a debit card when they sell a prepaid mobile phone and calling card. Because that may be an article that allows the customer to debit their account for the cost of phone calls, is that caught as a debit card under the bill? We think in the current drafting it would be.[56]

Department response

3.59 The Department responded that if industry puts forward a case demonstrating, on the basis of risk of money laundering and terrorism financing, that thresholds are appropriate for walk-in customers in relation to services such as foreign currency

---

53 *Submission 19*, Attachment p.1. The most commonly suggested minimum value threshold was $1 000.

54 *Submission 11*, p.1.

55 *Submission 11*, pp 3–4.

56 *Committee Hansard*, 23 November 2006, p.3.

exchange and bank cheques, this will be considered. Furthermore, arguments for a threshold for travellers' cheques are currently under consideration.[57]

3.60 The Department also advised the committee that:

> A pre-paid phone card or a card which allows people to charge calls made on one phone to an account for another phone does not fall within the definition of a debit card.[58]

3.61 The Department's view is that if such cards are captured by the Bill they will be subject to the stored value card provisions in items 21 to 24 which are subject to minimum threshold amounts.[59]

3.62 In response to a question from the committee the Department also indicated that it is intended to establish thresholds of $10,000 in relation to customer identification obligations for some designated services provided by casinos.[60]

Reporting of Threshold Transactions

3.63 Some concerns were raised in relation to the requirements to report threshold transactions which apply to transactions over $10,000 (clauses 43 and 44). OPC pointed out that the $10,000 threshold has not been increased in the 18 years since the *Financial Transaction Reports Act 1988* was introduced:

> The Office notes that the number of significant cash transaction reports has increased approximately 200% since 1991. In 2005-06, the number of reported significant cash transactions was 2,416,427. The prescribed significant cash transaction threshold has remained constant at $10,000 since the scheme was introduced and, as a consequence of price inflation, the reporting scheme will increasingly capture personal information regarding transactions that may not have been anticipated when the legislation was first drafted.[61]

3.64 The submission from ASFA raised specific concerns about the impact of the provisions on superannuation funds:

> Uncertainty remains as to exactly which transactions are captured under the reporting requirement as the term *threshold transaction* is broadly defined and contains linked definitions…Without proper exemptions, the threshold transaction reporting requirement would significantly impact on superannuation funds. Funds would be required to report every transaction of $10 000 or more to the Regulator within 10 business days of performing

57 *Submission 30c*, p.8.

58 *Submission 30c*, p.3.

59 *Submission 30c*, p.3.

60 *Submission 30a*, p.2.

61 *Submission 40*, p. 6.

> the transaction. Contributions, rollovers and transfers should be exempted from threshold transaction reporting.[62]

Industry Specific Concerns

3.65 A number of submissions were received by the committee which concerned the application of the Bill to particular businesses or industry groups. Many of these submitters stated that they were working directly with the Department in order to resolve outstanding issues.[63]

Telecommunication industry

3.66 In addition to the concerns about phone cards and pre-paid mobile phone credit, it was argued that other telecommunications products and services such as post paid third party content and trade promotions were inadvertently captured by the Bill. These products were said to be 'in no way in competition with the financial sector' and to have a low or negligible risk of money laundering or terrorist financing activity.[64]

3.67 Telstra stated that:

> The Bill would impose onerous and impractical legislative obligations on the telecommunications sector without any clear anti-money laundering or counter-terrorism financing benefit. Such an outcome appears to be inconsistent with the Government's purported intention, and an unintended consequence of the first tranche of reforms.[65]

Department response

3.68 The Department's view is that the provision of post paid third party content by the telecommunications industry is not captured as a loan by item 6 of table 1 in clause 6 because the loan is not made 'in the course of carrying on a loans business'.[66]

3.69 The Department advised that it is reviewing the provisions in table 3 of clause 6 to ensure they do not capture as 'gambling services' competitions and promotions run by businesses, which include an element of skill, with low value prizes of goods or services.[67]

---

62 *Submission 10*, p. 4.

63 See for example *Submission 35*, pp 1–2.

64 *Submission 24*, p. 1 and *Submission 4a*, p. 1.

65 *Submission 24*, p.2. It was also pointed out that the telecommunications industry is regulated by the Australian Communications and Media Authority however it is noted that many other stakeholders are also regulated independently of AUSTRAC.

66 *Submission 30c*, p.3.

67 *Submission 30c*, p.3.

Legal profession

3.70 The Law Council of Australia (Law Council) acknowledged that the Bill has limited application to the legal profession but argued that the particular role of legal practitioners means that they ought to be dealt with separately to other businesses:

> The Law Council is fundamentally opposed to the imposition of reporting obligations on legal practitioners which undermine the independence of the profession and which are at odds with legal practitioners' well established duties to their clients, the court and the public...The Law Council believes that any AML/CTF reforms affecting the legal profession should be dealt with separately from the regulation of other business relationships. This is appropriate both because of the special nature of the lawyer-client relationship and because the Australian legal profession is already subject to extensive specialist regulation.[68]

Department response

3.71 The Department noted that clause 242 of the Bill ensures that the Bill does not affect the law relating to legal professional privilege. The Department stated that:

> Legal practitioners will be obliged by the Bill to lodge suspicious matter reports in relation to the provision of designated services under the Bill. As providers of designated services they are appropriately subject to the same reporting obligation as any other provider of designated services. The tipping off provision will not prevent a client of a legal practitioner making a claim for legal professional privilege in any legal proceedings. The question of what action a legal practitioner must take under their professional rules as a result of making a suspicious matter report is a matter for determination by the profession.[69]

Community banks

3.72 Bendigo Bank Limited (Bendigo Bank) expressed concern that the Bill does not properly classify its Community Bank and Tasmanian Banking Services branches as 'owner-managed branches'. In particular, Bendigo Bank considered that clause 12 which defines 'owner-managed branches' was too narrow to encompass the Community Bank and Tasmanian Banking Services branches because it requires the arrangements with the bank to be 'exclusive' and for services to be offered 'under a single brand, trademark or business name'.[70]

3.73 Accordingly Bendigo Bank argued, that these branches will be treated as reporting entities:

---

68 *Submission 25*, p.3. Also, see *Submission 38*.

69 *Submission 30d*, pp 2–3.

70 *Submission 28*, p.1.

> As reporting entities these branches will be under a range of obligations that an ordinary branch of a bank is not, including the requirement to have their own AML/CTF Program…in addition, there is no provision in section 123 which allows [Bendigo Bank] to disclose information regarding suspicious activity reporting except via the Designated Business Group exception.[71]

3.74 Bendigo Bank noted that it was working cooperatively with the Department to address this issue.[72]

General insurers

3.75 IAG argued that its Consumer Credit Insurance products (CCIP) have unintentionally been captured by the Bill on account of their life insurance component. IAG believes that CCIP are fundamentally low-risk and should be excluded from the operation of the Bill by consequential amendments.[73]

Financial planners

3.76 The AFSL holders' designated services provision (item 54 of table 1 in clause 6) was described in submissions as vague with the potential to capture almost any service provided by a reporting entity.[74]

3.77 The Financial Planning Association of Australia Limited (FPA) submitted that:

> The wide drafting of this item has led to a situation where, as license holder, a financial planner may potentially have greater responsibilities in providing designated services (other than those financial services covered by an AFS Licence) than an intermediary who provides similar services but is not licensed…this raises issues in terms of competitive neutrality and does not appear justified in terms of a policy outcome…Item 54 should explicitly state that it relates only to the financial services that the Licensee carries out under its licence.[75]

3.78 In addition the FPA told the committee that AFSL holders were concerned that the Bill does not afford them sufficient protection from prosecution in the event of their agents' disregard or wilful neglect of AML/CTF obligations.[76]

---

71 *Submission 28,* p.3. Note that only designated services are covered by the ambit of the designated business group exception.

72 *Submission 28,* p.1.

73 *Committee Hansard*, 14 November 2006, pp 11–12.

74 *Submission 13*, p. 2 and *Submission 39,* p. 1.

75 *Submission 39*, Attachment p.1. Also, see *Submission 3,* p.3 and *Submission 20,* p.5.

76 Also, see *Submission 20,* p.7.

> It remains unclear whether a well constructed and effectively implemented training and supervisory program would enable a Licensee to avail itself of s236.[77]

3.79 IFSA noted that item 54 arrangers are excluded from the requirement of having to provide a suspicious matter report and argued that this exclusion exposes the item 54 arranger to a number of adverse consequences.[78]

Department response

3.80 The Department has advised that:

> It is proposed that the Bill will be amended to delete subclause 42(6) so that AFSL holders will have suspicious matter reporting obligations for the period during which they provide designated services.[79]

77 *Submission 39,* Attachment p.1.

78 *Submission 20,* pp 4–5. For example, not being able to communicate the risk to the reporting entity providing the designated service on account of the tipping off provisions.

79 *Submission 30c,* p.2.

CHAPTER 4

PRIVACY AND DISCRIMINATION CONCERNS

Introduction

4.1 The committee suggested in its report on the Exposure Bill that a Privacy Impact Assessment of the proposed legislation should be conducted. The committee is pleased to note that the Department has obtained such an assessment. However, some issues relating to privacy and discrimination remain a concern for stakeholders. In particular, witnesses expressed concern that the Bill may lead to discrimination by financial institutions based on race, religion, nationality or ethnic origin.

4.2 The privacy and discrimination issues raised by witnesses related to provisions in the Bill regarding:

- customer identification;
- customer verification;
- customer due diligence;
- the collection and storage of personal and sensitive information;
- the sharing of AUSTRAC held information with various agencies;
- the reporting of suspicious matters; and
- the performance of money-laundering and terrorism financing risk-assessments.

Discrimination

Risk-based approach

4.3 Liberty Victoria considers that the existing risk-based approach to the regime will 'mean that reporting entities will have significant discretion in complying with their AML/CTF obligations. In particular, financial institutions have considerable discretion in constructing the risk profiles of their customers. This discretion carries a serious danger of discrimination based on race, religion and nationality'.[1]

4.4 Witnesses expressed concern regarding the ability of staff to appropriately perform risk assessments and in particular the level of training required to undertake intelligence assessments.

---

1 *Submission 1*, p.5. Also, see *Submission 32*, p.2.

> …under the *Financial Transactions Reports Act 1988* (Cth), one commentator has described the money-laundering related training provided by Australian financial institutions to their staff as 'lax'.[2]
>
> How can the Australian public be confident that the subjective nature of suspicious matter reports will not become even less reliable an indicator of wrong-doing once reporting obligations are extended to thousands of clerks and shop assistants who, despite the Bill's requirements and best intentions will never be able to be adequately trained for such a task?[3]

4.5 In relation to the issue of suspicious matter reporting, Liberty Victoria also drew attention to a Muslim religious obligation known as *zakat*, a type of charitable giving, and the process of non-bank remittance through the Islamic *hawala*.[4] The commercial model used to identify suspect funds classifies as 'suspect' an activity that makes little or no business sense. This creates a risk that religious activities may be characterised as a suspicious activity and result in a suspicious matter report.

Provision of immunity increases the risk of discrimination

4.6 Under clause 235 protection from liability is provided to a reporting entity, its officers, employees and agents from action or suit under any law 'in relation to anything done, or omitted to be done, in good faith' by a reporting entity 'in compliance, or in purported compliance' with provisions of the Act, regulations and AML/CTF rules. Liberty Victoria commented that conduct undertaken in 'good faith' may still breach anti-discrimination statutes and the provision of immunity increases the risk of discrimination and even sanctions discrimination.[5]

4.7 Liberty Victoria discussed the Explanatory Memorandum of the Bill which states that the provision of immunity under clause 235 is not intended to override the *Racial Discrimination Act 1975* (Cth) and stated 'if it is the intention of the government not to override the *Racial Discrimination Act 1975* then this should be expressly stated in the Bill'.[6]

4.8 The Department considered the concerns raised regarding clause 235 and responded:

> Clause 235…does not operate to displace the *Racial Discrimination Act 1975* (RDA). A person can only rely on the indemnity provided by clause 235…where they have acted in good faith. There is nothing in the AML/CTF Bill which permits or authorises compliance with the AML/CTF Bill to be met by actions which breach the RDA. The indemnity in clause

---

2 *Submission 1*, p.5.

3 *Submission 9*, p.6.

4 *Submission 1*, pp 6–7, p.15.

5 *Submission 1*, p.8. Also, see *Submission 32*, p.4.

6 *Submission 1*, p.8.

> 235 would not be available in circumstances where the reason for denial of service or disclosure was discriminatory or based on matters other than those properly encompassed by the object and operative provisions of the AML/CTF Bill.[7]

Secrecy undermines the rule of law

4.9 Another specific issue is that a concerned individual will not be fully aware of the collection, use and disclosure of personal information. The 'tipping off' provisions of the Bill ensure that a concerned individual will not normally be told that a suspicious matter report has been made to AUSTRAC, nor will that individual be told the reasons for the making of the report.

4.10 Liberty Victoria argued:

> It is the secrecy surrounding these flows of information that undermines the rule of law. Citizens subject to a Suspicious Matter report are not in a position to ensure that the 'reporting entity', AUSTRAC or other authorities in possession of his or her personal information are complying with the law. This is simply because s/he would not know such information has been communicated. The rule of law is put under even greater pressure when information flows onto foreign authorities where there are additional practical difficulties of monitoring the compliance of these foreign authorities with their undertakings.[8]

4.11 For this reason, Liberty Victoria supports a regular audit of the informational practices to ensure compliance with the law and suggests that the audit be conducted either by the Privacy Commissioner or the Human Rights and Equal Opportunities Commission (HREOC).

Privacy

Lack of consideration of privacy issues

4.12 The inquiry into the Exposure Bill revealed that privacy and civil liberty groups and consumer representatives had not been adequately consulted in relation to the Exposure Bill. The current inquiry has heard evidence in the same vein from stakeholder groups who believe that privacy issues are not being considered a priority.

4.13 The Australian Privacy Foundation (APF) commented on the failure of the Commonwealth Government to address privacy related issues and engage interested groups:

> During more than two years of consultation, the government has failed to significantly address the major privacy concerns drawn to its attention by

---

7 Attorney General's Department, answer to question on notice, 15 November 2006 (received 21 November 2006).

8 *Submission 1*, p.11.

> the APF, the Privacy Commissioner and other interested parties (and now it appears by the PIA).[9]

Type of and scope of information collected

Lack of customer anonymity

4.14 Clauses 139 and 140 of Part 12 (Offences) of the Bill concern the provision and receipt of a designated service using a false name or on the basis of customer anonymity. The APF comments that the provision of criminal offences in these circumstances 'hangs like a sword over anyone seeking to offer individuals simple advice, but also directly undermines the intent of National Privacy Principle 8 (anonymity)'.[10]

Information held on electoral rolls

4.15 Clause 13 of the Amending Bill makes consequential amendments to the *Electoral Act 1918* which allow bulk release of the joint Commonwealth and State electoral roll to reporting entities for the purposes of complying with their customer identification obligations.

4.16 The APF raised concerns on the ability to access information held on the electoral roll for identity verification and suggested that mechanisms be in place to ensure that this information is not used for secondary purposes (an entity's own business purpose). The APF commented:

> It is completely unrealistic, for example, to expect a bank which uses the electoral roll to establish that a customer has different name and/or address particulars not to also record that information in its customer database and use it for commercial purposes, including normal customer contact and marketing.[11]

4.17 Not all witnesses expressed concerns regarding the release of information held on electoral rolls. Some witnesses in their evidence requested an extension to the use of information held on electoral rolls. Baycorp suggested that access be extended to allow organisations, such as credit reporting agencies, which perform customer verification services to use this information to assist reporting entities in undertaking their customer due diligence obligations under the Bill.[12]

---

9 *Submission 9,* p.2.

10 *Submission 9,* p.3.

11 *Submission 9,* pp 8–9. Also, see *Submission 14,* p.4, *Submission 40a,* p.1.

12 *Committee Hansard*, 23 November 2006, pp 17–18. Also, see *Submission 15,* pp 2–3, *Submission 17,* p.2.

Population-wide surveillance of financial affairs

4.18 Privacy Victoria commented that the reporting obligations (including threshold amounts) in the Bill result in a significant risk of pervasive monitoring of the financial affairs of ordinary citizens. This monitoring would not necessarily be due to the suspect nature of transactions or the risk of money-laundering and terrorism financing. Ordinary citizens by virtue of engaging in everyday financial transaction such as wiring money overseas, purchasing a stored value card and taking a loan of $10,000 may be caught within these obligations.[13]

4.19 Privacy Victoria considered that addressing this potential of the reporting obligations to cover such a significant portion of the population should not occur by regulation. Privacy Victoria recommended that 'the scope of the measures should be set out in the legislation after due scrutiny and debate by Parliament, and be accompanied by safeguards that are proportionate to the measures that are to be enacted'.[14]

Requests to override Part IIIA of the Privacy Act

4.20 Many witnesses raised issues around the operation of the Bill and Part IIIA of the *Privacy Act 1988*. Witnesses expressed concerns that existing inconsistencies create uncertainty regarding the use of customer credit information for the purpose of the Bill, for example to assist in the customer verification process. Baycorp stated:

> An amendment to the current version of the Bill [is] required to make it expressly clear that credit information could be used for identity verification purposes. As the Act currently stands Part IIIA prohibits disclosure of credit information unless the information is contained in a credit report given to a credit provider who requested the report for the purposes of assessing an application for credit.[15]

4.21 The Office of the Privacy Commissioner (OPC) considered this matter and expressed caution that the AML/CTF Rules may allow for the disclosure of consumer credit reports in an expanded range of circumstances. OPC stated:

> The Office would be particularly concerned if this clause [Rules paragraph 2.2.14] intends to give reporting entities access to consumer credit reports where such access is currently prohibited by Part IIIA of the Privacy Act. Part IIIA restricts access to the consumer credit reporting system by providing prescriptive regulation and includes criminal sanctions for non-compliance, including fines of up to $150,000. The Office would caution against the Rules opening this system to reporting entities for purposes

13 *Submission 14,* pp 1–2. Also, see *Submission 40,* p.5.

14 *Submission 14,* p.2.

15 *Submission 22a,* p.4. Also, see *Submission 17,* p.2; *Submission 16a,* p.13.

> unrelated to consumer credit, unless such a measure is subject to careful consideration and clear justification.[16]

Access to AUSTRAC information

4.22 The Bill, under Division 4 (clauses 125 and 126), allows the Australian Taxation Office and approximately 30 different designated agencies to access information held by AUSTRAC. Under certain conditions, information can also be passed on to foreign authorities. The fact that such a broad range of agencies have access to AUSTRAC information concerned some stakeholders.[17]

4.23 Privacy Victoria raised the question of why it is necessary for agencies such as Centrelink and the Child Support Agency to have access to such sensitive information and why regulations are being used to authorise other State and Territory authorities and agencies to seek AUSTRAC data:

> Specifying the intended users and purposes for which the information is accessed would improve the transparency and enable Parliament to properly scrutinise and debate the appropriate scope and safeguards that should apply.[18]

Purpose of collection

4.24 Evidence received during the inquiry also expressed concern that AUSTRAC information, once accessed by designated agencies, may be used for secondary purposes which are unrelated to the initial purpose of collection, being the prevention of money-laundering and terrorism financing.[19]

4.25 The APF explained their concerns regarding designated agencies accessing AUSTRAC held information:

> There is no attempt to limit uses to AML-CTF investigations or even to investigation of other serious or organised crime. AUSTRAC information, misleadingly collected under the apparent justification of AML-CTF, becomes a general resource.[20]

4.26 Similarly, Liberty Victoria commented on the potential for reporting entities to make ancillary use of information they are required to collect:

> Some commentators have pointed to the commercial opportunities that this larger base of information provides with one calling it 'the greatest business lever' and another suggesting that 'financial institutions can turn their anti-

16 *Submission 40a,* pp 3–4.

17 *Submission 40,* p.4. Also, see *Submission 9*, pp 7–8.

18 *Submission 14,* p.3. Also, see *Submission 40,* p.4.

19 *Submission 9*, pp 7–8. Also, see, *Submission 40a,* p.2.

20 *Submission 9*, pp 7–8.

> money laundering compliance systems into robust surveillance and identification systems that deliver benefits well beyond the regulatory requirements'.[21]

Retention period for records

4.27 The APF expressed concerns on the requirement that records be retained for seven years.

> The Bill will require reporting entities to retain detailed records, including of customer identification, for seven years. This is a completely disproportionate requirement both in terms of the level of continuing intrusion and in terms of the compliance burden. It also creates a dangerous precedent for similar future requirements in other sectors and for other purposes. A proper application of privacy principles would see records kept for no longer than is necessary for the primary business purpose.[22]

Privacy Impact Assessment

4.28 A Privacy Impact Assessment (PIA) measures the privacy impacts posed by legislative, policy or technological initiatives. A PIA report should describe and de-mystify the initiative, identify and analyse the privacy implications, and make recommendations for minimising privacy intrusion, and maximising privacy protection – while ensuring that the initiative's objectives are met.[23]

4.29 The Department engaged the services of Salinger & Co to conduct a PIA on the Bill which concluded on 15 September 2006.

Key findings and recommendations

4.30 The key findings of the report included:

- widespread support for the objectives of tackling money-laundering and terrorism financing;
- concerns about whether the scheme will actually be effective in achieving those objectives;
- concerns that in some respects the proposal is disproportionate to the risks and overly intrusive into people's personal affairs;
- significant concerns about the collection, use and disclosure of personal information for purposes unrelated to the objectives of tackling money-laundering and terrorism financing; and

---

21 *Submission 1*, p.12.

22 *Submission 9*, p.6.

23 Salinger & Co, *Privacy impacts of the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules, 2006: A Privacy Impact Assessment for the Australian Government Attorney-General's Department* (2006), pp 5–6.

- an inadequate privacy control environment at several points in the scheme.[24]

4.31 The PIA report made 96 recommendations in total, of which some were identified as critical recommendations[25] and are briefly detailed below.

Scheme should be proportionate to risk

4.32 Industry, public interest representatives and people want and expect a system designed and targeted to find those committing money laundering or crimes at the 'serious end' of the scale, but not such that small or minor transactions (or even transgressions) are caught in the net as well.

Use of personal information should be limited to stated objectives

4.33 The PIA stated that disclosures to law enforcement authorities such as the AFP, ASIO, ATO and State and Territory police forces did not receive wide criticism from either industry or public interest representatives. Such disclosures are seen as being appropriate for the purpose of 'serious crime' such as money laundering, terrorism financing and tax evasion. However, the fact that AUSTRAC held data can be used by a range of agencies for varying purposes has raised a number of issues.

4.34 The PIA report made recommendations to limit the use of personal information collected under the scheme to purposes related to the investigation of money laundering, terrorism-financing, tax evasion or serious crime.

Extend the National Privacy Principles to all reporting entities

4.35 The PIA recommends the extension of the National Privacy Principles (NPP) to all reporting entities, but that where the NPPs are seen to be inadequate, more specific provisions should also be added to the Bill and Rules. Recommendations have also been made to ensure all recipient agencies are likewise covered by the Information Privacy Principles in the federal Privacy Act, if they are not already regulated by an equivalent scheme in their own jurisdiction.

Further work required

4.36 The PIA suggested that further work should be undertaken including:

- adequate time prior to commencement;
- the provision of guidance and education for reporting entities;
- an independent evaluation of operations to occur after two years; and
- the tranche 2 reforms not to proceed without considerable further thought, review and consultation.

---

24 Salinger & Co, p.99.

25 Salinger & Co, pp 100–104.

The Department's response to the Privacy Impact Assessment

4.37 The Department provided a formal response to the PIA and has adopted 30 recommendations with one recommendation still under consideration. The following responses[26] to the PIA were provided by the Department:

- While the impact on privacy should be minimised, the current global environment necessitates the need for a comprehensive and robust AML/CTF regime. The risk based approach is flexible and recognises the unique roll of business in preventing money laundering and terrorism financing. Risk based approaches have either been or are being adopted by FATF members.
- The Privacy Act will be amended to ensure that all reporting entities (including small businesses that are currently exempt) are subject to the NPPs in relation to their compliance with the AML/CTF regime.
- The Rules will be legislative instruments and as disallowable instruments will be subject to Parliamentary scrutiny. In addition, in performing its functions under the Bill, AUSTRAC is required to consult with the Office of the Federal Privacy Commissioner (subclause 212(2)).
- Designated government agencies under the proposed legislative package have a role to play in combating money laundering and terrorism financing and as such will have access to AUSTRAC information. Most of these agencies are already empowered for the same purposes under the *Financial Transaction Reports Act 1988* (FTRA). The addition of Commonwealth and State and Territory anti-corruption agencies is also important to detect corruption.
- There are jurisdictional limitations to extending privacy obligations to other non-Commonwealth agencies and foreign entities. While a complaint mechanism is desirable, it is unlikely that all relevant agencies from each State and Territory would consent to the jurisdiction of the Federal Privacy Commissioner.[27]

4.38 The Department specifically commented during the public hearing on the PIA recommendations relating to designated agencies having access to AUSTRAC held information and stated:

> Finally, 16 of the unaccepted recommendations related to the disclosure of personal information and protections against its misuse. We have some concern that these recommendations were based on a misconception of the purpose and use of AUSTRAC information, which in the end is of intelligence value only. That information does not of itself support a prosecution and can at best only lead to further investigation by authorised

26 Attorney-General's Department, Criminal Justice Division, *Privacy Impact Statement: Anti-Money Laundering and Counter-Terrorism Financing Bill & Rules* (2006) pp 3–4.

27 For further Department comment in response to the PIA, see *Committee Hansard*, 23 November 2006, p.33.

agencies in accordance with the rules which govern the conduct of those agencies.[28]

Criticism's of the Department's response to the PIA

4.39 Some witnesses expressed criticism that the PIA report was not made publicly available to stakeholders immediately upon completion, restricting the time available for consideration and comment by stakeholders.[29] The committee also heard from witnesses who were concerned that two-thirds of the PIA's recommendations were not accepted and who considered that the reasons provided by the Department for not adopting these recommendations were inadequate.[30]

28 *Committee Hansard*, 23 November 2006, p.33.

29 *Submission 1a*, p.3. Also, see, *Submission 9*, p.1.

30 *Submission 9*, p.1.

CHAPTER 5

COMMITTEE VIEW

Committee view

5.1 The committee acknowledges the efforts of the Department and AUSTRAC to consult extensively with stakeholders in relation to AML/CTF legislation. The majority of witnesses appearing before the committee indicated that they had been consulted in relation to the legislation and many considered that the Department and AUSTRAC had been receptive to addressing their concerns.

5.2 However, evidence received during this inquiry indicated that industry groups and stakeholders have continuing specific issues ranging from requests for technical re-drafting to issues regarding the intent and the scope of the Bill. In particular, stakeholders still have concerns in relation to the practical impact of some provisions as well as privacy and discrimination issues.

Key concerns for industry

5.3 Evidence received during this inquiry indicated that industry stakeholders were generally supportive of the Bill though some general, and several specific, issues remain unresolved.

5.4 Major criticism was expressed by stakeholders regarding the proposed timetable of the release of the AML/CTF Rules. Complaints concentrated on the lack of time available to adequately consider the Rules prior to the implementation of the Bill. Specific suggestions related to delaying the obligations immediately after Royal Assent and extending the transition periods to allow the development of necessary systems and support mechanisms.

5.5 The committee is concerned that reporting entities have adequate time to engage with AUSTRAC on the implications of the Rules and are able to analyse and process the content of the Rules to effectively carry out their obligations. Given that there has been some confusion in relation to the government's intentions with respect to the Rules which may have hampered the efforts of industry to prepare for compliance with the new regime, the committee recommends that the first stage of implementation should not commence until three months after the date of Royal Assent. In making this recommendation, the committee notes that the FATF recommendations are not a binding international agreement subject to a defined implementation timetable. The committee is also conscious of the importance of ensuring that the anti-money laundering and counter-terrorism financing regime functions effectively from the outset.

5.6 The committee also considers that it is imperative that the Department and AUSTRAC commence the proposed public education campaigns in relation to the new regime as soon as possible.

5.7 Another area of concern was the extent of power that AUSTRAC and the AUSTRAC CEO have under the Bill. The ability of AUSTRAC to make Rules prescribing matters and also exempt significant provisions of the Bill is an issue. The committee notes that AUSTRAC has in the past undertaken extensive consultation with stakeholders and intends to continue this approach in the future. In addition, the Bill imposes obligations of the CEO to consult with various persons in exercising the functions of CEO. The committee recommends that AUSTRAC when amending or making further Rules after commencement of the Act thoroughly consult with industry and other stakeholders.

5.8 Subclause 6(7) is a Henry VIII clause. A Henry VIII clause is defined as follows:

> An express provision which authorises the amendment of either the empowering legislation, or any other legislation, by means of delegated legislation is called a Henry VIII clause. The Macquarie Dictionary of Modern Law defines a Henry VIII clause as a clause in an enabling Act providing that the delegated legislation under it overrides earlier Acts or the enabling Act itself; so named because of its autocratic flavour.[1]

5.9 The Bill imposes extensive obligations on reporting entities in relation to the provision of designated services. Subclause 6(7) permits amendment of the definition of 'designated services' by regulation and thus undermines robust scrutiny of changes to the obligations of reporting entities by the Parliament. The committee considers that the definition of 'designated services' should not be amended by regulation and recommends that subclause 6(7) be deleted from the Bill.

5.10 The committee is concerned that the Department's intention to establish thresholds of $10,000 in relation to customer identification obligations for some designated services provided by casinos is not consistent with FATF recommendation 12 which requires a threshold of USD 3,000.

5.11 Some evidence to the committee raised concerns about whether the safe harbour provisions for customer identification which are set out in the draft Rules would maintain reliable customer identification. The committee considers that the safe harbour provisions ought to be re-examined during the review of the legislation required under clause 251.

5.12 The committee is concerned that Part 6 of the Bill which deals with the register of designated remittance services providers does not provide the AUSTRAC CEO with a power to refuse registration or de-register providers who are involved in money laundering or terrorism financing. The committee suggests that the Department should consider whether there should be a capacity to exclude such providers from the register. Alternatively, it may be appropriate to establish a register of persons who are not permitted to provide designated remittance services.

---

1 Senate Standing Committee for the Scrutiny of Bills, *The Work of the Committee during the 39th Parliament November 1998 -October 2001,* p.77.

5.13 The committee considers that in clause 138 the offences relating to manufacturing false documents or equipment for producing false documents should be regarded as more serious than those relating to possession of false documents or equipment for making false documents. Accordingly the penalties for the possession offences ought to be decreased.

5.14 Several industry groups indicated to the committee that they have concerns that are specific to the operation of their business. For example, there are concerns that relate to services being caught unintentionally or inappropriately by the definition of 'designated services' in clause 6 and in relation to the possible exclusion of some community bank branches from the definition of 'owner managed branch' in clause 12. The committee is pleased to note that many stakeholders are working directly with the Department and AUSTRAC in order to resolve outstanding issues. The committee suggests that the Department and AUSTRAC, in consultation with industry stakeholders, continue their endeavours to address these technical drafting issues.

Privacy and Discrimination

5.15 The committee welcomes the Privacy Impact Assessment undertaken by the Department. The committee notes that approximately two thirds of these recommendations were not accepted by the Department and that reasons for this were given in the Department's formal response as well as in evidence provided at the public hearing. Achieving an appropriate balance between a consumer's right to privacy with legislation intended to combat money laundering and prevent terrorism financing is inherently difficult.

5.16 Privacy concerns mainly centre on the gathering, reporting and retention of customer information which is of a personal, financial and sensitive nature. The committee acknowledges the concerns of stakeholders regarding the scope of financial services caught under the Bill. The committee believes that further consideration should be given to excluding low value transactions which represent a low risk in the context of money-laundering and terrorism financing from the definition of 'designated services'. It may also be appropriate to make provision for periodic indexing of the thresholds applied by the Bill.

5.17 The ability for AUSTRAC held data to be accessed by a wide range of designated agencies is also of concern to the committee. The committee considers that Division 4 of Part 11 of the Bill should be amended to restrict access to AUSTRAC held information to access for the purposes of responding to money laundering, terrorist financing or other serious crime. In addition, the committee recommends that the Office of the Privacy Commissioner should audit AUSTRAC's administration of the Bill with respect to compliance with privacy obligations, particularly as they relate to the distribution of AUSTRAC information to other agencies.

5.18 Concerns remain regarding the risk of discrimination from reporting entities performing customer risk-assessments and suspicious matter reports with a risk-based approach which results in high levels of discretion and potentially subjective criteria.

The committee considers that it should be placed beyond doubt that clause 235 does not exclude the operation of federal, state or territory anti-discrimination legislation. The committee also recommends that AUSTRAC work with stakeholders to ensure reporting entities and their staff are able to perform these obligations based on non-discriminatory, objective criteria.

5.19 Overall the committee is generally satisfied with the provisions of the Bill. Nevertheless, specific issues remain, of which some are significant, and these need to be addressed. The committee has made a number of recommendations to address these concerns and encourages the Department and AUSTRAC to continue to consult and engage with stakeholders.

5.20 Given the complexity and scale of the new regime, the committee considers that review of the legislation, as provided for in clause 251, should occur in four years rather than seven years. The review should include further consultation with industry and other stakeholders.

Recommendations

Recommendation 1

5.21 The committee recommends that the Bill be amended to delay the first stage of implementation until three months after the date of Royal Assent.

Recommendation 2

5.22 The committee recommends that AUSTRAC when amending or making further Rules after commencement of the Act thoroughly consult with industry and other stakeholders.

Recommendation 3

5.23 The committee considers that the AML/CTF Rules which provide safe harbour provisions for customer identification should be re-examined during the review of the legislation required by clause 251.

Recommendation 4

5.24 The committee recommends that subclause 6(7) be deleted from the Bill.

Recommendation 5

5.25 The committee recommends that the Department consider whether Part 6 of the Bill should be amended to provide the AUSTRAC CEO with powers to refuse registration as a designated remittance services provider and to de-register providers; or to maintain a register of persons who are not permitted to provide remittance services.

Recommendation 6

5.26 The committee recommends that the penalties for the offences in subclauses 138(3) and (5) which relate to possessing false documents or possessing equipment for making false documents be reduced.

Recommendation 7

5.27 The committee recommends that the Department continue to work with industry groups and other stakeholders to resolve technical drafting issues including:

(a) the exclusion of services relating to stored value cards by the drafting of items 21-24 of table 1 in clause 6;

(b) the capture of fund managers selling securities on an exchange by item 35 of table 1 in clause 6; and

(c) the exclusion of some community bank branches from the definition of 'owner-managed branch' in clause 12.

Recommendation 8

5.28 The committee recommends that the Federal Government consider amending the Bill to include further threshold value limits, to exclude low risk, low value services (such as the provision of travellers cheques and foreign currency transactions) from the definition of 'designated services' and that consideration be given to indexing these thresholds every five years.

Recommendation 9

5.29 The committee recommends that the Office of the Privacy Commissioner conduct periodic audits of AUSTRAC's compliance with privacy obligations in its administration of the Bill.

Recommendation 10

5.30 The committee recommends that Division 4 of Part 11 of the Bill should be amended to restrict access to AUSTRAC held information to access for the purposes of responding to money laundering, terrorist financing or other serious crime.

Recommendation 11

5.31 The committee recommends that clause 235 be amended to provide that protection from liability does not extend to actions which breach federal, state or territory anti-discrimination laws.

Recommendation 12

5.32 The committee recommends that AUSTRAC work with stakeholders to develop an objective, non-discriminatory model for assessing the risk of money laundering and terrorism financing to assist reporting entities in performing their obligations.

Recommendation 13

5.33 The committee recommends that clause 251 be amended to provide for review of the legislation in four years and for that review to incorporate consultation with industry and other stakeholders.

Recommendation 14

5.34 Subject to the preceding recommendations, the committee recommends that the Bill be passed.

Senator Marise Payne

Chair

ADDITIONAL COMMENTS BY THE AUSTRALIAN LABOR PARTY

1.1 Labor Senators support the majority report and endorse its recommendations. However Labor Senators wish to make additional comments in relation to the scrutiny of the operations of AUSTRAC.

1.2 The Bill establishes significant new powers for AUSTRAC and the AUSTRAC CEO. In particular, it gives AUSTRAC a new regulatory role in relation to reporting entities and the registration of designated remittance service providers.

1.3 Labor Senators consider that it is crucial that a body which exercises such extensive powers is subject to independent oversight. The need for independent scrutiny is made even more acute by the inherent potential for corruption where a body is tasked with combating money laundering.

1.4 The Australian Commission for Law Enforcement Integrity has been designed specifically to detect and investigate corruption within federal law enforcement agencies. Labor Senators consider that, once it is established, the Commission would be an appropriate body to perform this oversight role.

Additional Recommendation 1

1.5 Labor Senators recommend that AUSTRAC be subject to oversight by the Australian Commission for Law Enforcement Integrity upon its establishment.

Senator Patricia Crossin **Senator Linda Kirk**

Deputy Chair

Senator Joseph Ludwig

APPENDIX 1

SUBMISSIONS RECEIVED

1	Liberty Victoria
1A	Liberty Victoria
2	CPA Australia & The Institute of Chartered Accountants in Australia
2A	CPA Australia & The Institute of Chartered Accountants in Australia
3	Insurance Australia Group (IAG)
3A	Insurance Australia Group (IAG)
4	Australian Mobile Telecommunications Association (AMTA)
4A	Australian Mobile Telecommunications Association (AMTA)
4B	Australian Mobile Telecommunications Association (AMTA)
5	MinterEllison Lawyers
5A	MinterEllison Lawyers
6	Chartered Secretaries Australia Ltd
7	Infosys Technologies Australia Pty Ltd
8	Australian Friendly Societies Association (ASFA)
9	Australian Privacy Foundation (APF)
9A	Australian Privacy Foundation (APF)
9B	Australian Privacy Foundation (APF)
10	The Association of Superannuation Funds of Australia Limited (ASFA)
11	Mallesons Stephen Jaques on behalf of Westfield Gift Cards Pty Limited and the Westfield Limited Group
12	Travelex Australasia Group
13	Securities & Derivatives Industry Association (SDIA)
14	Office of the Victorian Privacy Commissioner

15	Australian Finance Conference (AFC)
16	Australian Bankers' Association Inc.
17	Abacus - Australian Mutuals
18	Business Council of Australia
19	Australian Financial Markets Association (AFMA)
20	Investment & Financial Services Association Ltd (IFSA)
21	Insurance Council of Australia
22	Baycorp Advantage Ltd
22A	Baycorp Advantage Ltd
22B	Confidential
23	ING Bank (Australia) Limited
24	Telstra
25	Law Council of Australia
26	Westpac Banking Corporation
27	Computershare Limited
28	Bendigo Bank Group
29	Visa International
30	Attorney-General's Department
30A	Attorney-General's Department
30B	Attorney-General's Department
30C	Attorney-General's Department
30D	Attorney-General's Department
30E	Attorney-General's Department
30F	Attorney-General's Department
30G	Attorney-General's Department

31	Privacy NSW
32	Human Rights and Equal Opportunity Commission (HREOC)
33	Finance Sector Union of Australia (FSUA)
34	NSW Cabinet Office
35	PayPal Australia Pty Ltd
36	Western Australia Police
37	AUSTRAC
37A	AUSTRAC
38	Allens Arthur Robinson (Allens)
39	Financial Planning Association of Australia Limited (FPA)
40	Office of the Privacy Commissioner (OPC)
40A	Office of the Privacy Commissioner (OPC)
41	Department of Police and Public Safety, Tasmania
42	Queensland Police Service

TABLED DOCUMENTS

Documents tabled at the public hearings.

Thursday 23 November 2006

Senator Joseph Ludwig

- HM Treasury, The Regulation of Money Service Business: A Consultation, September 2006

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Melbourne, Tuesday 14 November 2006

CPA Australia

Ms Judith Hartcher, Manager, Business Policy

Institute of Chartered Accountants in Australia

Ms Catherine Kennedy, Professional Standards Consultant

Insurance Australia Group

Ms Ann Stubbings, Australian General Counsel

Liberty Victoria

Dr Joo-Cheong Tham, Committee Member

Minter Ellison

Mr Richard Batten, Partner

Mr George Spiteri, Senior Lawyer

Sydney, Wednesday 22 November 2006

Financial Planning Association of Australia

Mr John Anning, Manager, Policy and Government Relations

Investment and Financial Services Association

Mr Martin Codina, Senior Policy Manager

Ms Nicola Martin, IFSA Representative, IFSA AML Working Group

Mrs Jennifer Pinson, Head of Compliance, Morgan Stanley

Securities and Derivatives Industry Association

Mrs Jill Thompson, Policy Executive

Australian Privacy Foundation

Mr David Vaile, Vice Chair

Mr Nigel Waters, Board Member and Policy Coordinator

Office of the Privacy Commissioner

Ms Karen Curtis, Privacy Commissioner

Mr Andrew Solomon, Director, Policy

Australian Bankers Association

Mr Anthony Burke, Director

Abacus – Australian Mutuals

Mr Joshua Moyes, Senior Adviser, Policy and Public Affairs

American Express Australia Ltd

Mr Brett Knight, Head of Compliance

Mr Colm Lorigan, General Counsel

Ms Luisa Megale, Head of Public Affairs

Sydney, Thursday 23 November 2006

Australian Mobile Telecommunications Association

Mr Christopher Althaus, Chief Executive

Mr George Dionisopoulos, Regulatory Manager, Security, AAPT

Ms Emma Mill, Legal Counsel, Telstra Corporation Ltd

Ms Carmel Mulhern, General Counsel, Telstra Corporation Ltd

Westpac Banking Corporation

Mr Andrew Carriline, General Manager, Risk and Enterprise Services

Mr Andrew Smith, Head of Portfolio and Strategic Risk

Baycorp Advantage

Ms Olga Ganopolsky, Legal Counsel

Mr Colin Shadbolt, Business Strategy and Partnerships Adviser

Mr Matthew Walker, Senior Adviser, External Relations and Compliance

Law Council of Australia

Mr Ross Ray QC, President Elect

Attorney-General's Department

Ms Joanne Blackburn, First Assistant Secretary

Mr Geoffrey Gray, Assistant Secretary

AUSTRAC

Mr Neil Jensen, Director

Ms Liz Atkins, General Manager, Regulatory Policy