



Australian Government
Attorney-General's Department

Criminal Justice Division

PRIVACY IMPACT STATEMENT

Anti-Money Laundering and Counter-Terrorism Financing Bill & Rules

**The Australian Government response to the Privacy Impact Assessment on the
Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules.**

BACKGROUND

As recommended by the Senate Legal and Constitutional Legislative Committee, the Minister for Justice and Customs, Senator the Hon Chris Ellison asked for an independent Privacy Impact Assessment (PIA) to be conducted to identify and address issues in the *Anti-Money-Laundering and Counter-Terrorism Financing Bill 2006* (the Bill) and Rules that may affect the personal privacy of Australians. The report would inform this Privacy Impact Statement in the Government's consideration of the proposed Anti-Money-Laundering and Counter-Terrorism Financing (AML/CTF) legislative package.

The report was conducted by Salinger & Co and was completed on 15 September 2006. The methodology for the PIA included an examination of the most recent exposure draft of the Bill and Rules, submissions made during the public consultation process and the Senate Report as well as interviews with officers from the Attorney General's Department (AGD), the Australian Transaction Reports and Analysis Centre (AUSTRAC), a sample of businesses which will be reporting entities under the Bill and representatives from community groups. The findings and recommendations of the PIA are included in this Privacy Impact Statement.

KEY FINDINGS

There were 96 recommendations in the report which centred on the following key issues:

- **Privacy Control Environment** – It was suggested that the privacy controls at several points in the proposed AML/CTF legislative package are inadequate and that strengthening the privacy control environment to cover all stages of the information 'data flows' could minimise the risk of privacy breaches.
- **Transparency** – It was suggested that because exemptions and some key definitions (eg designated services, threshold values, risk, what is considered 'suspicious' and requires reporting, the number and type of recipient agencies and types of collections by reporting entities) are located in the Rules rather than in the Bill the clarity of obligations might diminish and the likelihood that privacy impacts will be altered over time without Parliamentary debate might be increased.
- **Proportionality of the response to the risk** – It was suggested that some aspects of the proposal are overly intrusive into people's personal affairs compared with the current risks posed by money laundering and terrorism financing. While acknowledging the risk based regulatory framework of the legislation it was suggested that obligations should also be commensurate to a monetary threshold.
- **Use of personal information for the stated objectives** – There were significant concerns about the collection, use, and disclosure of personal information for purposes which were deemed to be unrelated to the objectives of tackling money laundering and terrorism financing (eg use by government agencies such as Australian Securities and Investment Commission, Centrelink and the Australian Competition and Consumer Commission). It was suggested that access to personal information should be limited to those agencies that exercise the

functions of investigating money laundering, terrorism financing, tax evasion and serious crime.

- **Extending the National Privacy Principles (NPPs) to all reporting entities** – Many reporting entities and government agencies will not be subject to privacy obligations in the collection and use of personal information by virtue of Constitutional and legislative limitations. It was suggested that reporting entities under the Bill could be subject to the NPPs by amending the *Privacy Act 1988* for the purposes of AML/CTF compliance. Where no or limited privacy obligations exist for government agencies, the Bill could also be amended to ensure that these agencies are subject to Commonwealth jurisdiction (ie Information Privacy Principles and the jurisdiction of the Australian Privacy Commissioner) as a condition of receiving AUSTRAC information.

COMMENT

The Australian Government has considered the report's findings and recommendations. A detailed response to the 96 recommendations is attached (*Attachment A*) and the Government's comments are summarised as follows:

Privacy Control Environment

The privacy control environment will be strengthened by the extension of the Privacy Act to include all reporting entities (including small business, which are currently exempt) providing designated services under the AML/CTF legislative package.

Transparency

The fundamental principles of the AML/CTF legislative package are clearly set out in the Bill. Operational detail has been placed in the Rules for maximum flexibility. This will allow AUSTRAC to tailor obligations to meet the needs of different sectors, and respond to any changes in the AML/CTF environment by adjusting the Rules accordingly. The Rules will also be legislative instruments and as disallowable instruments will be subject Parliamentary scrutiny. In performing its functions under the Bill, including its function to make the Rules, AUSTRAC is required to consult with the Office of the Federal Privacy Commissioner.

Proportionality of the response to the risk

The question of whether the privacy impacts of the AML/CTF legislative package can be justified as a proportional response to the problems caused by money laundering and terrorist financing in the current climate of heightened organised criminal and terrorist activity is a decision for the Australian Government.

The risk based approach proposed under the AML/CTF legislative package is flexible and recognises that business is best placed to understand and mitigate money laundering and terrorism financing risks. The risk based approach gives business discretion to determine the amount and type of personal information required to fulfil their obligations under the AML/CTF legislative package. Privacy advocates prefer a more prescriptive approach to ensure there is maximum protection for the collection and use of personal information.

While the impact on privacy should be minimised, the current global environment necessitates the need for a comprehensive and robust AML/CTF regime. The Financial Action Task Force's (FATF) revised Forty + Nine Recommendations

represent the international response to this environment. Regulatory regimes similar to that proposed in this legislative package, (including a risk based regulatory approach) have either been or are being adopted by FATF members (including the United States, United Kingdom and countries in the European Union) which represent a large proportion of the international business community. Apart from enhancing Australia's systems to detect and deter money laundering and terrorist financing, adopting the proposed AML/CTF regime will enable Australian business to compete internationally in foreign jurisdictions which demand the implementation of tougher AML/CTF measures.

Use of personal information for the stated objectives

The objectives of the AML/CTF legislative package are to combat money laundering terrorism financing and serious crime. Designated government agencies under the proposed legislative package have a role to play in this process 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 object of the Bill is to create a financial environment in Australia that is hostile to money laundering and terrorist financing. The Australian Securities and Investment Commission, Australian Prudential Regulation Authority and Australian Competition and Consumer Commission have been included on the basis of their roles as financial market and prudential regulators to avoid unnecessary duplication in obligations and investigations. The addition of Commonwealth and State and Territory anti-corruption agencies is also important to detect corruption.

Extending the NPPs to all reporting entities

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 their compliance with the AML/CTF regime.

Commonwealth agencies are subject to Information Privacy Principles (IPPs) set out in the Privacy Act. There are jurisdictional limitations to extending privacy obligations to other non-Commonwealth agencies and foreign entities. The PIA has recommended that the State and Territory agencies should submit to the jurisdiction of the Australian Privacy Commissioner in the context of providing a complaints mechanism. While such a mechanism is desirable, it is unlikely that all relevant agencies from each State and Territory would consent to the jurisdiction of the Australian Privacy Commissioner (a Commonwealth agency).

This action could result in the exclusion of such agencies from information sharing under the Bill, potentially undermining the objectives of the legislation and Australia's international obligation under FATF (Recommendation 40 requires spontaneity in exchange of information between jurisdictions). Additionally the issue of uniformity of privacy protection across Australian jurisdictions is a broader issue and should be appropriately addressed in that context.

The Government's response to the Privacy Impact Assessment's recommendations

	Bill (96 recommendations)	Response	Reason
1	That the draft Rules be reviewed to ensure there is consistent language and clear definitions of terms such as 'name' and 'full name', 'address', 'residential address' and 'business address'.	Accepted	
2	That Australian Transaction Reports and Analysis Centre (AUSTRAC), industry representatives and public interest representatives consider whether the collection of government-issued identifiers (such as driver's licence or passport numbers) is intended to be collected as part of customer verification.	Not Accepted	Record making rules to be made under cl 112 of the Bill will make it clear that the collection of government identifiers are required.
3	That, if they are intended to be collected as part of customer verification, the Bill be amended to authorise the collection of government-issued identifiers (such as driver's licence or passport numbers).	Accepted	Record making rules to be made under cl 112 of the Bill will make it clear that the collection of government identifiers are required. Including the authorisation in the Rules will be sufficient for the purposes of National Privacy Principle (NPP) 1.1.
4	That if the documents supplied by customers for face-to-face verification are intended to be copied as part of customer verification (see Recommendation 2 above), this copying be specifically authorised (or required) in the Bill, by amending sub-cl 86A(2) to state that copying, rather than transcribing, is authorised (or required) for the purposes of 'mak(ing) a record of information obtained'. [Note sub-cl 86A(2) as referred to above is equivalent to sub-cl 112(2) of the final Bill]	Accepted	Sub-clause 112(2) will clarify that a record can include copying or transcribing an identifier or a record containing information as prescribed in the Rules.
5	That the reference to Medicare card numbers should be deleted from the list of requirements for suspicious matters reports in Rule 9.2.2(f), because Medicare cards do not constitute 'reliable and independent documentation' under Rule 1.3.1.	Not Accepted	It is necessary to retain the reference to Medicare cards in paragraph 9.2.2(f) of the draft Rules for those reporting entities that choose to rely on Medicare cards as part of their applicable customer identification procedures.
6	That the definition of 'money-laundering and terrorism financing (ML/TF) risk' in the Rule 1.3.1 be amended to clarify that for the purposes of setting know your customer (KYC) rules, the risk assessment is to be conducted with reference to the product or service being offered and the environment in which it is offered, not with reference to each customer.	Not Accepted	The key factors that will be required to be examined in any ML/TF risk assessment are customer, product, channel distribution and jurisdiction. It would be inappropriate to delete references to customer risk from the relevant AML/CTF Rules. A reporting entity will not necessarily need to examine the risks posed by individual customers although it would be possible to do so if thought necessary by the reporting entity.
7	That Rules 2.2.12 and 2.2.14 be amended so that the application of the 'safe harbour' scheme is where the reporting entity has determined that 'the product or service being offered is of medium or lower ML/TF risk'. (That is, replace 'the relationship with the customer' with 'the product or service being offered'.)	Not Accepted	Unnecessary.

	Bill (96 recommendations)	Response	Reason
8	That any requirement for on-going customer due diligence (CDD) should be specifically defined, authorised and required in the Bill rather than the Rules.	Not Accepted	Clause 36 of the Bill defines ongoing CDD. A requirement of this is to act in accordance with the Rules. The details are set out in the Rules to allow for greater flexibility and adaptability.
9	That any requirement for employee screening should be specifically defined, authorised and required in the Bill rather than the Rules.	Not Accepted	Employee screening will be part of the operational detail of an AML/CTF Program. This detail is not appropriate for the Bill.
10	That the Government consider amending the Rules to limit the KYC information to be collected as part of identification and verification procedures, to only include information relevant to identity management (uniquely identifying a person), not information about their financial affairs.	Not Accepted	A customer's 'financial position' will be part of the KYC information menu in respect of an individual. Whether or not the collection of such information is warranted will depend on ML/TF risk.
11	That the Government consider amending the Rules, so that the requirement to collect information about a customer's financial affairs only applies if enhanced CDD has first been triggered under Rule 6.4.2, and only then in relation to clarifying the nature of the customer's business with the reporting entity.	Not Accepted	A customer's 'financial position' will be part of the KYC information menu in respect of an individual. Whether or not the collection of such information is warranted will depend on ML/TF risk.
12	That AUSTRAC and industry consider prohibiting reporting entities from copying documents supplied by customers for face-to-face verification, but instead allow just those details which relate to 'KYC information' to be transcribed, by amending sub-cl 86A(2) to state that only transcribing of KYC information, not copying, is authorised for the purposes of 'mak(ing) a record of information obtained'. (See also Recommendation 4 above.) [Note sub-cl 86A(2) as referred to above is equivalent to sub-cl 112(2) of the final Bill]	Not Accepted	Reporting entities should be allowed to make copies as an alternative to transcribing all of the information required to be recorded. It would be too burdensome to transcribe details in order to keep a record of the identification documents that were relied on for verification purposes.
13	That Rule 2.2.14 be amended to delete the requirement to check a person's credit bureau history for the purposes of customer verification when using e-verification.	Not Accepted	The purpose of the Rule is to check the fact that there is a credit history, rather than what is in the credit history.
14	That if and when the Document Verification Service is developed and made available as an online service to reporting entities, AUSTRAC and industry should consider amending the 'safe harbour' customer verification rules to allow reliance on that service.	Accepted	After a Government decision has been made on whether to give the private sector access, AUSTRAC would consider this.
15	That the definition of 'designated services' in the Bill be amended to exclude all services which involve a one-off transaction under a threshold of \$1,000.	Not Accepted	While it is likely that there will be exemptions for these type of services, that decision will be made by AUSTRAC on a case by case basis.
16	That the Bill specify that customer identification and verification is only required: <ul style="list-style-type: none"> • for 'low risk' services which involve, or could facilitate, a transaction over \$16,000, • for 'medium risk' services which involve, or could facilitate, a transaction over \$5,000, or • for 'high risk' services of any value. 	Not Accepted	This prescriptive approach goes against the principle of a risk based regime. Further, it would be administratively difficult and costly to have different thresholds. This recommendation is inconsistent with some the views expressed by industry representatives.
17	That the Bill or Rules specify that in the context of gambling, the relevant 'transaction' relates not to the	Accepted	This recommendation will likely be achieved through the Rules. In part, these matters

	Bill (96 recommendations)	Response	Reason
	placing of a bet, but to the payment of any winnings, or the exchange of tokens or chips for money.		have been addressed in the Chapter 11 rules which limit the circumstances in which identification is to be carried out.
18	That all threshold values in the Bill and Rules be re-set by Regulation every five years, in accordance with Consumer Price Index (CPI) changes, rounded to the nearest \$1,000. That all threshold values in the Bill and Rules be re-set by Regulation every five years, in accordance with CPI changes, rounded to the nearest \$1,000.	Not Accepted	Threshold values cannot be subject to a formula based on CPI as there are other factors that contribute to the setting of values including risk of ML/TF.
19	That the customer identification / verification Rules specify that: <ul style="list-style-type: none"> • a post office box, home address or work address can constitute 'KYC information' for low or medium risk services, and • only a street home address can constitute 'KYC information' for 'high risk' services. 	Not Accepted	'Post office box' details are of little or no intelligence value. A customer's residential address forms part of the minimum KYC information that must be collected.
20	That the Bill provide a mechanism by which customers can request a reporting entity to suppress their home address from view of, or use by, staff except as required for reporting to AUSTRAC or for other disclosures required under law.	Accepted	Accept to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
21	That any requirement for employee screening be specifically defined, authorised and required in the Bill, rather than the Rules. The definition should specifically exclude psychological / personality tests, lie detector tests, drug and alcohol tests as not relevant to determining ML/TF risk.	Not Accepted	Employee screening will be part of the operational details appropriate for the Rules. AUSTRAC can consider this when the Rules are reviewed
22	That any requirement for on-going employee due diligence be specifically defined, authorised and required in the Bill, rather than the Rules.	Not Accepted	Employee due diligence is an operational issue and as such will be more appropriately dealt with in the Rules rather than under the Bill. This will allow for the necessary flexibility and adaptability of the process.
23	That Rule 1.3.1 expressly prohibit 'sensitive personal information' (as defined in the Privacy Act) from being collected as KYC information.	Not Accepted	'Sensitive information' is defined in the Privacy Act to mean information about, for example, a person's racial or ethnic origin where warranted by particular circumstances. Information of this kind could be picked up by the definition of 'KYC information' as part of the assessment of ML/TF.
24	That AUSTRAC, industry and public interest representatives review Rule 1.3.1 to consider the necessity and utility of 'place of birth', 'country of residence' and 'country of citizenship' as KYC information.	Not Accepted	Information of this kind could be picked up by the definition of 'KYC information' as part of the assessment of ML/TF where warranted in particular circumstances.
25	That the Bill expressly prohibit reporting entities from adopting, using, or disclosing any government issued personal identifiers, collected for the purposes of KYC requirements, except as required to report to AUSTRAC. (As per the Privacy Act, Australian Business Numbers do not constitute personal identifiers.)	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
26	That the Rules require reporting entities to seek	Not	Industry may consider this to be

	Bill (96 recommendations)	Response	Reason
	written confirmation from the individual seeking a service on behalf of a corporate entity that they have the appropriate authority from, or permission of, the other individuals involved, to provide their personal information to the reporting entity, in particular where a home address is being requested.	Accepted	impracticable and unreasonable particularly in the context of corporate customers. Other regimes (eg licensing regime) that require the collection and disclosure of individual's personal details (eg directors' personal details) do require an individuals' authorisation.
27	That the Rules require reporting entities using e-verification to seek authorisation from the customer for the reporting entity to collect information about them from other data sources.	Not Accepted	Prescription is unnecessary
28	That the Rules require reporting entities using e-verification to notify customers which other data sources it will use to verify their identity.	Not Accepted	Prescription is unnecessary
29	That the Bill require reporting entities to give their customers a 'privacy notice' in relation to the customer identification and verification process. The notice must include the detail listed in NPP 1.3. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Accepted	Accept to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
30	That AUSTRAC work with industry and public interest representatives to devise model, layered privacy notices for reporting entities to use. The model notices must include alternatives depending on whether the service requested is considered low, medium or high ML/TF risk, and include alternatives for use with children, people of non-English speaking background, and people with decision-making disabilities.	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
31	That the Bill require reporting entities to take reasonable steps to protect the KYC and CDD information it holds from misuse and loss, and from unauthorised access, modification or disclosure. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
32	That the Bill require reporting entities to allow customers to access and correct their KYC and CDD information as if they were bound by NPP 6. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
33	That the Bill be amended to require reporting entities to take reasonable steps to confirm the accuracy of KYC and CDD information before they collect, use or disclose it. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
34	That the Bill be amended to create an offence of lodging a suspicious matters report, knowing it to be inaccurate or misleading.	Accepted	Clause 136 of the Bill includes the offence of providing information that is known to be false or misleading.

	Bill (96 recommendations)	Response	Reason
35	That the Bill prohibit any use of personal information collected under the KYC requirements for marketing purposes, except on an 'opt in' basis.	Not Accepted	Reporting entities will be subject to the Privacy Act when they provide services under the Bill. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
36	That the Bill prohibit delegates or agents of reporting entities from using personal information collected under the KYC requirements for any purpose beyond reporting back to the commissioning reporting entity.	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
37	That the Bill prohibit reporting entities from disclosing customer information collected under the KYC requirements, except as required by this or another statute or court order, where necessary to prevent or lessen and serious and imminent threat to any person, where reasonably necessary for law enforcement purposes, where necessary for the performance of a contract between the person and the reporting entity, or with the person's consent. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
38	That the Bill also allow disclosures to a contracted service provider, if the contract is for a directly related purpose (other than marketing) within the reasonable expectations of the customer, so long as the reporting entity reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the NPPs. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
39	That the Bill prohibit any disclosure of personal information collected under the KYC requirements for marketing purposes, except on an 'opt in' basis.	Not Accepted	Reporting entities will be subject to the Privacy Act when they provide services under the Bill. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
40	That the Bill prohibit any disclosure of personal information collected under the employee due diligence requirements, except as required by this or another statute or court order, where necessary to prevent or lessen and serious and imminent threat to any person, where necessary for law enforcement purposes, or with the person's consent.	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
41	That the Bill set a minimum data retention period of seven years for reporting entities in relation to reports lodged with AUSTRAC.	Not Accepted	There is no obligation for reporting entities to retain reports lodged with AUSTRAC.
42	That the Bill require reporting entities to dispose of their KYC and CDD records as soon as possible after the minimum data retention period has expired, or the relationship with the customer has ceased,	Accepted	Accept this recommendation to the extent that reporting entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not

	Bill (96 recommendations)	Response	Reason
	whichever comes later; and to dispose of their AUSTRAC report records as soon as possible after the minimum data retention period has expired. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)		seek to go beyond, the privacy regime under the Privacy Act.
43	That the Bill require reporting entities to use secure means of data disposal. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Accepted	Accept this recommendation to the extent that Reporting Entities will be subject to Privacy Act. The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
44	That the Rules require reporting entities to publish, and keep up-to-date, a plain language privacy policy setting out what sort of personal information it holds under the AML/CTF scheme, for what purposes, and how it collects, holds, uses and discloses that information. (However note that if Recommendation 49 is adopted, this Recommendation is not required.)	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
45	That Rule 8.1.2 (AML/CTF program) be amended to add '(d) ensure compliance with privacy responsibilities'.	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
46	That Rule 8.2 (AML/CTF risk awareness training program) be amended to include privacy responsibilities and risks.	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
47	That Rule 8.6 (AML/CTF compliance officer) be amended to also require the designated of a person as 'Privacy Officer'.	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
48	That Rule 8.7 (independent review) be amended to also require '(e) assess whether the reporting entity has complied with its privacy responsibilities'.	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
49	That a regulation be made by the Attorney General under s 6E of the Privacy Act, to the effect that all reporting entities under the AML/CTF Bill are to be treated as an 'organisation' for the purposes of the Privacy Act, in relation to those activities done in compliance or purported compliance with the AML/CTF Bill and Rules, even if they would otherwise be exempt from the Privacy Act by virtue of the 'small business' exemption.	Accepted	The <i>Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006</i> will make reporting entities subject to the Privacy Act as a requirement of compliance with the AML/CTF Bill.
50	That cl 103 of the Bill be amended to provide for the power of AUSTRAC to collect personal information from foreign countries in the same terms as it may disclose personal information to foreign countries. [Note cl 103 as referred to above is equivalent to cl 132 of the final Bill]	Not Accepted	These matters are sufficiently covered in Memoranda of Understanding (MOUs) with foreign jurisdictions.

	Bill (96 recommendations)	Response	Reason
51	That the threshold for significant cash transaction reports be increased to \$16,000, by amending the definition of 'threshold transaction' in cl 5 of the Bill. (See also Recommendation 18 in relation to also indexing values every five years.)	Not Accepted	According to law enforcement agencies' advice to Government, \$10,000 is a significant amount of cash to be handled in any one transaction, particularly since electronic alternatives to cash are more advanced now than was the case in 1988. The Bill contains a mechanism to vary the threshold figure if this is considered appropriate in the future.
52	That the reporting of 'threshold transactions' remain limited to cash and e-currency, not property transfers, by deleting sub-cl (d) in the definition of 'threshold transaction' in cl 5 of the Bill.	Not Accepted	Property transfers will only be subject to the Bill if the Regulations allow (currently they are not—this to allow an immediate response if this becomes a future problem area).
53	That the threshold for international currency transfer reports be increased to \$16,000, by amending cl 49 of the Bill. (See also Recommendation 18 in relation to also indexing values every five years.) [Note cl 49 as referred to above is equivalent to cl 53 of the final Bill]	Not Accepted	According to law enforcement agencies' advice to Government, \$10,000 is a significant amount of cash to be handled in any one transaction, particularly since electronic alternatives to cash are more advanced now than was the case in 1988. The Bill contains a mechanism to vary the threshold figure if this is considered appropriate in the future.
54	That cl 55 of the Bill be amended to provide that bearer negotiable instrument reports can only be made if a Customs or Police officer forms a reasonable suspicion that the carriage of the bearer negotiable instrument/s may be connected with money laundering, terrorism financing, tax evasion or serious crime. [Note cl 55 as referred to above is equivalent to cl 59 of the final Bill]	Not Accepted	These requirements will be the same as threshold transaction report requirements.
55	That paragraph 39(1)(f)(v) of the Bill be amended to require some element of 'serious crime' in the scope of offences against Commonwealth, State or Territory law, in relation to which a suspicion may be formed. 'Serious crime' should be defined in the Bill. [Note paragraph 39(1)(f)(v) as referred to above is equivalent to paragraph 41(f)(v) of the final Bill]	Not Accepted	Unnecessary as requirements that must relate to 'investigation and prosecution' eliminates matters that are not serious. This is an adaptation of existing provisions within the <i>Financial Transactions Reports Act 1988</i> (FTRA).
56	That the Bill be amended to require guidelines be in place before cl 39 is effective. [Note cl 39 as referred to above is equivalent to cl 41 of the final Bill]	Not Accepted	Unnecessary as AUSTRAC will continue the practice of working with industry including developing guidelines to assist them since the FTRA was implemented in 1988.

	Bill (96 recommendations)	Response	Reason
57	That a note be introduced to cl 39 in the Bill, to clarify that cl 39 does not authorise conduct that would otherwise breach the <i>Racial Discrimination Act 1975</i> , or any other Act. [Note cl 39 as referred to above is equivalent to cl 41 of the final Bill]	Not Accepted	However, the Explanatory Memorandum will clarify.
58	That a note be introduced to cl 195A (the immunity provision) in the Bill, to clarify that nothing in the Bill or Rules authorise conduct that would otherwise be considered unlawful discrimination. [Note cl 195A as referred to above is equivalent to cl 235 of the final Bill]	Not Accepted	However, the Explanatory Memorandum will clarify.
59	That the Government consider altering the language in cl 39 of the Bill (and throughout the legislative package), to replace 'matters' with 'transactions', 'services' or 'activities', or another suitable phrase more focussed on the provision of the designated service in question. [Note cl 39 as referred to above is equivalent to cl 41 of the final Bill]	Not Accepted	Suspicious matter reports need to be broadly defined because it is not only transactions that can raise a suspicion. This will be important for the reporting entities of the second tranche.
60	That AUSTRAC review procedures and ensure that AUSTRAC, Customs and Police are giving travellers a 'privacy notice' in relation to international currency transfer reports. The notice must include the detail listed in Information Privacy principle (IPP) 2.	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
61	That the Government consider a model for mediated access to reports more than seven years old, in which an independent body such as the Privacy Commissioner could review data held about a person by AUSTRAC, and determine whether or not access can be provided without comprising law enforcement operations or investigations, national security or the safety of the informant.	Not accept	Suspicious Matter Reports need to remain confidential for the purpose of law enforcement investigations and protection of the entity that made the report.
62	That AUSTRAC limit online access to its databases to the following agencies: Customs, Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and State and Territory police forces, the Australian Crime Commission (ACC) and State and Territory crime commissions, the Australian Taxation Office (ATO), and State and Territory revenue agencies. Therefore no online access should be allowed to: Australian Commission for Law Enforcement Integrity (ACLEI) and its State equivalents, Australian Competition and Consumer Commission (ACCC), Australian Prudential Regulation Authority (APRA), Australian Securities and Investment Commission (ASIC), Centrelink, the Child Support Agency, ad-hoc royal commissions, or any other	Not Accepted	The fight against ML/TF and major crime in Australia and beyond Australia's border relies on a collaborative effort between government agencies. Each agency mentioned has a mandate to investigate and enforce Commonwealth, State or Territory laws and each has provided a business case as to why they require access to AUSTRAC's information and has been (or will be) provided access as a result of this business case. Agencies such as Centrelink and ASIC work side by side with law enforcement agencies to fight crime such as identity fraud, etc. It is also vital that AUSTRAC be able to share information with other Australian regulators.

	Bill (96 recommendations)	Response	Reason
	recipient agencies added by regulation.		There are already measures in place to limit access to AUSTRAC data bases including security clearances, random checks of access patterns etc. Consideration is being given to tightening the access regime by inserting clauses into AUSTRAC's MOUs requiring partner agencies to inform of breaches by their staff of security procedures relating to AUSTRAC data. Measures along these lines are a more effective means of addressing potential security breaches, rather than further limiting online access to the data base. There could also be resource and disclosure issues. Agencies will be disclosing their interest to AUSTRAC when requesting information.
63	<p>That the definition of 'designated agencies' in the Bill be amended to include only the following agencies: Customs, ASIO, the AFP and State and Territory police forces, the ACC and State and Territory crime commissions, the ATO, and State and Territory revenue agencies.</p> <p>Therefore the following should be deleted: ACLEI and its State equivalents, ACCC, APRA, ASIC, Centrelink, the Child Support Agency, and ad-hoc royal commissions.</p>	Not Accepted	<p>The fight against money laundering, terrorism financing and major crime in Australia and beyond Australia's border relies on a collaborative effort between government agencies. Each agency mentioned has a mandate to investigate and enforce Commonwealth, State or Territory laws and each has provided a business case as to why they require access to AUSTRAC's information and has been (or will be) provided access as a result of this business case. Agencies such as Centrelink and ASIC work side by side with law enforcement agencies to fight crime such as identity fraud, etc. It is also vital that AUSTRAC be able to share information with other Australian regulators.</p> <p>The definition within the Bill is an adaptation of existing provisions within the current FTRA. The inclusion of additional agencies is an appropriate expansion of the term to include other relevant agencies that perform law enforcement functions.</p>
64	That the definition of 'designated agencies' be amended to exclude the addition of further agencies by regulation.	Not Accepted	This would make the process of amending the list inflexible should a need arise that requires an urgent response.

	Bill (96 recommendations)	Response	Reason
65	<p>That the Bill be amended to provide that in relation to disclosures to ACLEI and its State equivalents, ACCC, APRA, ASIC, Centrelink, the Child Support Agency and ad-hoc royal commissions, AUSTRAC must limit its disclosure of information to only being in response to a written 'notice to produce' from the agency, which names the individuals about whom data is sought, and only where AUSTRAC is satisfied that the disclosure is reasonably necessary for the purpose of that agency investigating or prosecuting serious crime, including significant amounts of tax evasion or benefit fraud. (Note if Recommendation 63 is accepted, this recommendation is not required.)</p>	Not Accepted	<p>This is not a workable solution. AUSTRAC does not have the resources to cover every single request from these agencies nor would AUSTRAC be able to make an informed decision regarding the purpose of the request. AUSTRAC information is used as an intelligence source; agencies utilise AUSTRAC information in the early stages of an investigation to build a case and therefore the agency may not be able to provide a reasonable argument to AUSTRAC in these early stages.</p> <p>AUSTRAC would also need to consider 'need to know'. AUSTRAC would prefer that an agency does not have to give them specific detail regarding a case prior to authorising access. Long term, the information will not be used by those agencies who should be able to access it as is the purpose of collecting, analysing and disseminating the information.</p> <p>AUSTRAC's partner agencies also work together on various matters and need to be able to share information with their counterparts. Such a recommendation restricts the work of all law enforcement, tax and national security.</p>
66	<p>That paragraph 103(1)(a) of the Bill be amended to require that before undertakings are accepted from a foreign country, the CEO of AUSTRAC must seek the written advice of the Australian Privacy Commissioner as to the adequacy of the privacy protection likely to be afforded the information once it reaches the foreign country. In providing its advice the Australian Privacy Commissioner should have regard to whether the financial intelligence unit (FIU) counterpart is regulated by a privacy law equivalent to the IPPs or NPPs, and/or is subject to the oversight of an independent Privacy Commissioner or equivalent, accredited by the International Privacy Commissioners' Conference.</p> <p>[Note paragraph 130(1)(a) as referred to above is equivalent to paragraph 132(1)(a) of the final Bill]</p>	Not Accepted	<p>FATF (Recommendation 40) requires spontaneity in exchange of information between jurisdictions. Jurisdictional limitations may mean this is impractical for other jurisdictions and so should not be prescribed in the legislation.</p> <p>AUSTRAC has clear guidelines in terms of the due diligence process prior to entering into an MOU with another jurisdiction. This includes an assessment of the privacy and information security capacity of the FIU. Our process could be enhanced to cover more detailed privacy issues. However, it would not be realistic to expect other jurisdictions to have privacy laws equivalent to Australia. Adoption of this recommendation could seriously undermine AUSTRAC's ability to enter into MOUs with other jurisdictions to exchange financial intelligence.</p>

	Bill (96 recommendations)	Response	Reason
67	<p>That paragraph 103(1)(a) of the Bill be amended to require that MOUs (undertakings from foreign countries) must be reviewed every five years, with fresh advice sought from the Australian Privacy Commissioner as to the adequacy of the privacy protection likely to be afforded the information once it reaches the foreign country.</p> <p>[Note paragraph 130(1)(a) as referred to above is equivalent to paragraph 132(1)(a) of the final Bill]</p>	Not Accepted	<p>Review dates of MOUs are an operational measure and cannot be considered based solely on chronological considerations. There are safeguard clauses in AUSTRAC MOUs to ensure AUSTRAC will not release information if it is not satisfied with any aspect of a request from a foreign jurisdiction including security and confidentiality of information.</p>
68	<p>That paragraph 103(1)(b) of the Bill be amended to require the CEO of AUSTRAC to also be satisfied that the request from a foreign country related to one or more named people or entities, and that there was a reasonable suspicion that the subject person is or was involved in money laundering, terrorism financing, or a crime of a type recognised as a ‘serious crime’ under Australian law, including significant tax evasion or benefit fraud.</p> <p>[Note paragraph 130(1)(b) as referred to above is equivalent to paragraph 132(1)(b) of the final Bill]</p>	Not Accepted	<p>FATF (Recommendation 40) requires spontaneity in exchange of information between jurisdictions.</p> <p>AUSTRAC MOUs require another jurisdiction to name the legal entity or entities concerned and state the reasons for the request (ie money laundering, terrorist financing etc). It also requires a brief statement of the underlying facts.</p>
69	<p>That sub-cl 103(3) and cl 104 of the Bill be amended to require the AFP and ASIO respectively to consult with the CEO of AUSTRAC if the recipient is not from one of the countries with whom AUSTRAC has a current MOU.</p> <p>[Note sub-cl 130(3) as referred to above is equivalent to sub-cl 132(3) of the final Bill, and cl 104 as referred to above is the equivalent of cl 133 of the final Bill]</p>	Not Accepted	<p>This already happens. Within each MOU there is a requirement to consult with AUSTRAC on these matters. Both agencies have specific guidelines in place. FATF (Recommendation 40) also requires spontaneity in exchange of information between jurisdictions.</p>
70	<p>That paragraph 103(3)(b) and cl 104(1)(b) of the Bill be amended to require the AFP and ASIO to be satisfied that there is a reasonable suspicion that the subject person is or was involved in money laundering, terrorism financing, or a crime of a type recognised as a ‘serious crime’ under Australian law, including significant tax evasion or benefit fraud.</p> <p>[Note paragraph 130(3)(b) as referred to above is equivalent to paragraph 132(3)(b) of the final Bill, and paragraph 104(1)(b) as referred to above is the equivalent of paragraph 133(1)(b) of the final Bill]</p>	Not Accepted	<p>The AFP and ASIO have guidelines in place outlining these requirements as directed by the MOU between our agencies. FATF (Recommendation 40) requires spontaneity in exchange of information between jurisdictions.</p>
71	<p>That AUSTRAC evaluate the continued utility of suspicious transaction reports lodged more than 15 years ago.</p>	Accepted	<p>AUSTRAC would be prepared to re-evaluate.</p>
72	<p>That AUSTRAC consider suspending suspicious transaction reports from online access after a period of seven years since the report was last utilised.</p>	Accepted	<p>AUSTRAC agrees to this in consultation with partner agencies.</p>

	Bill (96 recommendations)	Response	Reason
73	That AUSTRAC determine an appropriate retention period for suspicious transaction / matter reports, with reference to similar intelligence data and in consultation with National Archives and the Office of the Privacy Commissioner.	Accepted	AUSTRAC would be prepared to re-evaluate.
74	That AUSTRAC develop and publish, and keep up-to-date, a plain language privacy policy setting out what sort of personal information it will hold under the AML/CTF scheme, for what purposes, and how it collects, holds, uses and discloses that information.	Accepted	AUSTRAC already has met this recommendation.
75	That AUSTRAC conduct regular privacy audits of its operations, to ensure its compliance with the IPPs.	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.
76	That cl 129 of the Bill be deleted, and rights of appeal against a warrant be included in the Bill. [Note cl 129 as referred to above is equivalent to cl 160 of the final Bill]	Not Accepted	Constitutional implications only allow a magistrate acting in a personal capacity to exercise a warrant. They must act within the law.
77	That sub-cl 99(3) be amended so that each State or Territory Government partner agency must either: <ul style="list-style-type: none"> demonstrate to AUSTRAC that all their activities are subject to a statutory scheme which sets out privacy principles, includes independent oversight by a Privacy Commissioner (or equivalent), and enables a complainant to obtain an enforceable remedy from an independent body for any harm suffered as a result of breaching one or more of the privacy principles, or undertake to comply with the IPPs in the Privacy Act, and submit to the jurisdiction of the Australian Privacy Commissioner. [Note sub-cl 99(3) as referred to above is equivalent to sub-cl 126(3) of the final Bill]	Not Accepted	While it is clearly desirable to have a complaints mechanism, this must be balanced against the objectives of the Bill and Australia's international obligation under FATF which requires spontaneity in exchange of information between jurisdictions (FATF Recommendation 40). In reality it is unlikely that all relevant agencies from all jurisdictions will submit to the jurisdiction of the Australian Privacy Commissioner in this context. Such an outcome would have an adverse impact on the free flow of information and would diminish the effectiveness of the Bill. The recommendation raises issues of the non-uniformity of privacy protection in Australia at a broader level, and should be appropriately addressed in that context.
78	That sub-cl 99(3) be amended, to provide that a breach of the IPPs by a State or Territory government partner agency constitutes an 'interference with the privacy of an individual' for the purposes of s 13 of the Privacy Act, such that an individual may make a complaint to the Australian Privacy Commissioner under s 36 of that Act. [Note sub-cl 99(3) as referred to above is equivalent to sub-cl 126(3) of the final Bill]	Not Accepted	While it is clearly desirable to have a complaints mechanism, such as to the Australian Privacy Commissioner, this must be balanced against the objectives of the Bill and Australia's international obligation under FATF which requires spontaneity in exchange of information between jurisdictions (FATF Recommendation 40). In reality it is unlikely that all relevant agencies from all jurisdictions will submit to the jurisdiction of the Australian Privacy Commissioner in this context. Such an outcome would have an adverse impact on

	Bill (96 recommendations)	Response	Reason
			the free flow of information and would diminish the effectiveness of the Bill. The recommendation raises issues of the non-uniformity of privacy protection in Australia at a broader level, and should be appropriately addressed in that context.
79	That the Bill require recipient agencies to take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure. (However note that if Recommendation 77 is adopted, this Recommendation is not required.)	Not Accepted	In reality it is unlikely that all relevant agencies from all jurisdictions will submit to the jurisdiction of federal legislation in this context. Such an outcome would have an adverse impact on the free flow of information and would diminish the effectiveness of the Bill. Therefore, setting out these matters in MOU and Guidelines is a more practical and enforceable option.
80	That the Bill require recipient agencies to take reasonable steps to confirm the accuracy of personal information before they collect, use or disclose it. (However note that if Recommendation 77 is adopted, this Recommendation is not required.)	Not Accepted	Jurisdiction limitations may mean this is impractical and so should not be prescribed in the legislation. MOUs set out these matters.
81	That paragraph 100(2)(b) be amended to incorporate 'misuse' or 'disclosure' as alternative components of the offence. [Note paragraph 100(2)(b) as referred to above is equivalent to paragraph 127(2)(b) of the final Bill]	Not Accepted	Clause 127 is sufficient to cover this recommendation. Agencies are subject to the IPPs.
82	That the Bill require recipient agencies to destroy or de-identify personal information they collect from AUSTRAC once it is no longer needed for its intended purpose. (However note that if Recommendation 77 is adopted, this Recommendation is not required.)	Not Accepted	Commonwealth agencies are subject to privacy obligations. Jurisdiction limitations may mean this is impractical for other jurisdictions and so should not be prescribed in the legislation.
83	That cls 162 and 163 be amended to only allow powers to stop, question, search, seize or arrest a person in relation to their carriage, or suspected carriage, of bearer negotiable instruments where the officer first forms a reasonable suspicion that the carriage of the bearer negotiable instrument/s may be connected with money laundering, terrorism financing, tax evasion or serious crime. [Note cl 162 as referred to above is equivalent to cl 200 of the final Bill, and cl 163 as referred to above is equivalent to cl 201 of the final Bill]	Not Accepted	These requirements should not be any difference to threshold transaction report requirements.
84	That AUSTRAC work with industry and public interest representatives to devise appropriate guidelines for reporting entities on: <ul style="list-style-type: none"> • how they should maintain appropriate data security • how they should check the accuracy of information before use—with particular attention paid to confirming the accuracy of information before a suspicious matters 	Not Accepted	The privacy protection under the Bill should be consistent with, and not seek to go beyond, the privacy regime under the Privacy Act.

	Bill (96 recommendations)	Response	Reason
	<p>report is made to AUSTRAC</p> <ul style="list-style-type: none"> • how they should ensure the provision of access and correction rights, including reasonable costs and expected timeframes, and • how they should ensure the secure disposal of KYC, CDD and reporting records 		
85	That AUSTRAC, industry representatives and public interest representatives develop industry relevant guidelines on what may or may not constitute a 'suspicious matter'. The guidelines should be made subject to the approval of the Privacy Commissioner and the Human Rights and Equal Opportunity Commission (HREOC).	Accepted	It is AUSTRAC's practice to consult with the Privacy Consultative Committee on draft guidelines.
86	That additional funding be provided to the Australian Privacy Commissioner to develop training and educational materials for reporting entities new to the NPPs.	Accepted	
87	That this Report be provided to the Australian Privacy Commissioner and AUSTRAC	Accepted	
88	That this Report be published on the Attorney General's Department website prior to the Bill being tabled in Parliament.	Consider	
89	That the name and objects of the Bill be amended to reflect the additional uses of AUSTRAC information by recipient agencies, beyond AML/CTF.	Not Accepted	<p>The Bill's name reflects FATF international standards.</p> <p>It is noted that privacy is included as a consideration to AUSTRAC's operations under sub-cl 212(3) of the Bill.</p>
90	That adequate time be allowed reporting entities to be educated about, and prepare for, the commencement of the Bill.	Accepted	
91	That sub-cl 173(2) of the Bill be amended so that AUSTRAC must consult not only with reporting entities and recipient agencies, but also with public interest representatives, including but not limited to the Office of the Australian Privacy Commissioner.	Accepted	AGD to consider including the Australian Privacy Commissioner in the consultation process as a representative of the privacy interests of Australians. AUSTRAC already consults with such groups on a regular basis via the Privacy Consultative Committee.
	[Note sub-cl 173(2) as referred to above is equivalent to sub-cl 212(2) of the final Bill]		
92	That, before the Bill commences, AUSTRAC collect baseline data about exactly what AUSTRAC information is being used, by which recipient agencies, for what purposes, and whether not the information was critical to that purpose.	Accepted	This may delay the legislative process. It is a requirement under each MOU for partner agencies to provide AUSTRAC with feedback regarding the use of financial transaction report (FTR) information. This information is provided to AUSTRAC on a quarterly basis. All partner agencies regard FTR information (all report types and the information collected within) as a valuable source of intelligence. Partner agencies have also provided case study material in support of AML/CTF legislative reform over a number of years.

	Bill (96 recommendations)	Response	Reason
93	<p>That, after two years of operation, and before proceeding with the tranche 2 reforms, the Government commission an independent evaluation of the effectiveness of the tranche 1 reforms, in terms of the impact on ML/TF activities in Australia, arising from:</p> <ul style="list-style-type: none"> • the extension of the definition and scope of ‘reporting entities’ beyond ‘cash dealers’ • the implementation of the KYC requirements • the threshold transactions reporting obligations • the IFTI reporting obligations, and • the suspicious matters reporting obligations 	Not Accepted	<p>A review of the AML/CTF legislative regime will be conducted within 7 years of operation. In addition, a review of the current tranche including privacy impacts will be completed as part of providing the second tranche AML/CTF reforms to Government for its consideration.</p> <p>The Government has decided 7 years is an appropriate review period as designated under cl 251 of the Bill. The recommended 2 year review period is too soon as industry's full obligations will only just have occurred.</p>
94	<p>That, after two years of operation, AUSTRAC, industry and consumer representatives evaluate the necessity and effectiveness of each data item listed as ‘KYC information’, with a view to eliminating all but necessary and practical information from the list.</p>	Not Accepted	<p>A review of the AML/CTF legislative regime will be conducted within 7 years of operation. In addition, a review of the current tranche including privacy impacts will be completed as part of providing the second tranche AML/CTF reforms to Government for its consideration.</p> <p>The Government has decided 7 years is an appropriate review period as designated under cl 251 of the Bill. The recommended 2 year review period is too soon as industry's full obligations will only just have occurred.</p>
95	<p>That the definition of ‘designated services’ in the Bill be amended to delete the ability to add further industries or sectors by regulation.</p>	Not Accepted	<p>This recommendation would not enable the Government to respond quickly to services identified as vulnerable to money laundering and terrorism financing.</p>
96	<p>That a privacy impact assessment be commissioned on the tranche 2 proposals, for publication as part of widespread public consultation on those proposals.</p>	Accepted	