



**Credit Union**  
Industry Association

3 April 2006

Senator Marise Payne  
Chair  
Senate Legal and Constitutional Legislation Committee  
Parliament House  
CANBERRA ACT 2600

By email: [senator.payne@aph.gov.au](mailto:senator.payne@aph.gov.au)

Dear Senator Payne

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

I hope the Committee is able to consider these additional comments by CUIA on the Exposure Draft AML/CTF Bill, as flagged in our 8 March 2006 submission. I appreciate that your reporting date is very close.

We seek the committee's assistance in clarifying the boundaries of the policy trade-off where the proposed AML/CTF regime conflicts with existing policy objectives, such as reducing the regulatory cost burden on business and the right to privacy.

In particular, we see a need for non-prescriptive official guidance to ensure that regulatory compliance is proportionate to a reporting entity's reasonable assessment of its risks. There is also a need to resolve policy conflicts around the key obligation to verify identity and the capacity to do so.

**Privacy & KYC**

As mentioned in our earlier submission to the Committee and during the 14 March 2006 public hearing, the proposed AML/CTF regime has significant implications for the privacy of all Australians.

CUIA agrees with the view that people today are likely to be more tolerant of intrusions into their privacy due to concerns about terrorism. However, the proposed AML/CTF regime will authorise the collection and retention by private businesses of vast new amounts of personal information. (Many of these regulated entities have not been subject to the *Financial Transactions Reports Act 1988* and may not be subject to the *Privacy Act 1988*.)

So called "additional know your customer (KYC) information" set out in draft rules, currently includes:

- The customer's place of birth;
- The customer's occupation, business activities or functions;
- The nature of the customer's business with the reporting entity – including where appropriate:

- The purpose of specific transactions; or
- The expected nature and level of transaction behaviour.
- The income or assets available to the customer;
- The customer's source of funds, including where appropriate, origin of funds;
- The customer's financial position;
- Details in respect of the ownership and control structure of the customer;
- The beneficial ownership of the funds used by the customer with respect to designated services;
- The beneficiaries of the transactions being facilitated by the reporting entity on behalf of the customer, including where appropriate, destination of funds; and
- In the case of non-natural customers – the identity of any relevant party that may be related to the customer, such as a subsidiary company or an officer of the company.

Whether any or all of this additional KYC information must be collected is a matter for the reporting entity's AML/CTF Program and the risk classification assigned to the customer.

A reporting entity's decision to pursue information about a customer's "financial position" or "income and assets" will be entirely subjective and highly variable across the financial services sector.

CUA accepts that a degree of subjectivity and variability in outcomes for customers is a unavoidably a function of the risk-based, rather than prescriptive, approach. However, it is our strong view that the risk-based approach will only work effectively if there is sufficient official information and non-prescriptive guidance available to enable regulated entities to confidently and proportionately tailor their responses to the risks they face.

In the absence of such information and guidance, privacy and compliance costs will be too high for regulated entities that over-estimate their risks and too low for regulated entities who under-estimate their risks. (By risks I include the likelihood of regulatory action for inadequate compliance as well as money laundering and terrorism financing.)

Ultimately, customers will bear the burden of high regulatory and privacy costs without necessarily any proportionate impact on money laundering or terrorism financing.

Take the example of collecting "place of birth" as additional KYC. This could be collecting information about race or ethnic origin. Such information is "sensitive information" under the Privacy Act and its collection and retention has cost implications. According to the Office of the Privacy Commissioner, the sensitivity of personal information being stored is an important factor and higher levels of security could be expected for sensitive information.<sup>1</sup>

Another potential cost is responding to customers seeking to be advised about their ML/TF "risk classification" – particularly if they object to the classification.

Consumer-focused ADIs competing in the domestic deposit-taking, lending and payments product markets are likely to face a broadly similar range of risks that are of a different order of magnitude than the ML and TF risks faced by global banks. CUA urges the committee to support the provision of information and non-prescriptive guidance by the regulator to the small ADI sector about ML and TF risks and proportionate responses. Some consistency in the application of scarce resources to risks is surely the desired outcome. For example, it is impossible to estimate the cost to credit unions of the

---

<sup>1</sup> *Information Sheet 6 – 2001 Security and Personal Information* Office of the Privacy Commissioner, Dec 2001.

proposed mandatory requirement to carry out transaction monitoring without some indication of the regulator's expectations about the intensity of such monitoring.

Regulated entities should not be left in an information vacuum trying to guess the regulator's expectations.

At this stage we have no indication about AUSTRAC's likely approach. Draft guidelines released so far do not add significantly to the Rules in terms of information and guidance to regulated entities. I refer the committee to paragraphs 75 to 79 of the Draft Guidelines on AML/CTF Programs as an illustration of this paucity of information, particularly in regard to terrorism financing.

### **Verifying identity**

One of the core obligations of regulated entities is verifying that a customer is the person that he or she claims to be.

CUIA seeks the committee's support in urging Government to adopt a consistent approach to the primacy of this obligation by:

- giving the private sector the capacity to verify the authenticity of government-issued documents; and
- allowing the use of a wider range of databases, such as credit files, to be used for identity verification.

Identification documents issued by government are the key means for verifying identity. However, such documents can be faked and industry is unable to obtain a simple 'yes' or 'no' answer from the issuer about a document's authenticity.

Refusing this capacity to the financial sector makes little sense when compared to the wholesale enlistment of the sector in the AML/CTF battle proposed in the Draft Bill.

I note that Government agencies are already using an online, real-time system that verifies proof of identity documents.<sup>2</sup>

Improving industry's capacity to verify identity will not only reduce money-laundering and fraud but will be good for consumers because it will promote competition and choice. Smaller institutions, such as credit unions, do not have national branch networks to facilitate face-to-face identity verification and alternative verification methods will help them compete with big banks.

Please don't hesitate to contact me on 02 6232 6666 to discuss any aspect of this submission.

Yours sincerely,



**LUKE LAWLER**  
**Senior Adviser, Policy and Public Affairs**

---

<sup>2</sup> *Document Verification Prototype Central to Identity Protection* Media Release by Attorney General, 7 Feb 2006.