

25<sup>th</sup> September 2008

## **Anti-Money Laundering and Counter-Terrorism Financing Act (2006): AUSTRAC Audit**

SSAMM Management Consulting (SSAMM) supports many clients to meet their compliance obligations, such as compliance with the AML/CTF Act.

This outline is in response to requests from various financial services' clients facing forthcoming AUSTRAC audits. Note AUSTRAC may conduct a combination of desk reviews of information collected via the lodgement of compliance reports or requests for information made by them. AUSTRAC also conduct on-site audits at the offices of reporting entities.

### **Risk Based Approach to Compliance reporting**

As you may know the AML/CTF Act takes a risk based approach to compliance. Those steps include but are not limited to the following:

#### **1. Preparations**

A reporting entity must ensure that a risk assessment has been undertaken and fully documented. This needs to be done for each reporting entity within a designated business group. Risks that should be assessed include: governance risks, operational risk, IT and systems risk, outsourcing risk, agency risk, regulatory compliance risk, business planning risk, customer type risk, product risk, channels of distribution risk, jurisdictional risk and reputational risk even though it is only the ML/TF risk that AUSTRAC are interested in identifying, mitigating and managing.

AUSTRAC expects to see risk ratings, controls and control-effectiveness ratings together with details of clear risk owners and reporting lines. AUSTRAC regards the risk assessment as pivotal. Informed by its risk assessment, a reporting entity can then proceed to develop a relevant AML program and supporting policies, procedures and compliance plan.

AUSTRAC requires an AML program to not only mirror the provisions of the Act and Rules, but to be informed by Australian Standard AS 3806-2006 Compliance Programs, and ensure that the program suitable for the individual business. Equally, it expects any risk assessment to be informed by AS/NZS 4360:2004 Risk Management.

AUSTRAC will be particularly interested to review how a reporting entity addresses customer risk, product risk (i.e. how might people use the particular product to launder money?), channels and distribution risk, and jurisdictional risk — that is, increasing "know your client" (KYC) verification for customers from other jurisdictions, and reassessing risk when an Australian resident moved out of Australia into a foreign jurisdiction.

#### **2. Reassessment**

Once a risk assessment has been undertaken, it is necessary to monitor and review it and from time to time to reassess the AML/CTF program (and suitability of the program), the speed of its implementation and any supporting compliance plan developed to assist with this process. AUSTRAC officers have indicated that in the early stages of implementation it would expect to see a risk assessment, AML program and adjunct compliance plan reviewed at least six-monthly.

### **3. Compliance plan**

A compliance plan supporting the operation of the AML Program is a must from AUSTRAC's perspective. While strictly speaking not a legislative requirement, AUSTRAC Guidance Note, Risk Management and AML/CTF Programs makes it clear that good compliance includes the implementation of a robust compliance plan that encompasses relevant obligations and defines the control and review mechanisms needed to ensure compliance.

### **4. Board meeting agenda item**

AML/CTF issues/compliance should be a standing agenda item for each board meeting of each reporting entity/entities within the designated business group.

### **5. Incident register**

As is the case in other regulatory environments, reporting entities should have an incident register so that all systemic or significant breaches relating to a company's agreed compliance measures, controls, procedures and policies are reported back to the board.

### **6. Training calendar**

A training calendar is an imperative — and if not done so already, reporting entities should be rolling out AML training programs for all affected staff now at board level and below.

Know your client. KYC — identification and verification for post-commencement customers — systems should be in place as at 12 December 2007 and getting ready for a 12 December 2008 implementation of the ongoing due diligence and suspicious transactions reporting regime (see appendix A)

### **7. Disciplinary policy**

It is necessary to have an employee disciplinary policy (Rules stated as an employee due diligence program, in the Rules) that it is referenced in the AML/CTF program. This policy should be made available to all staff, AUSTRAC also recommends that particular attention should be paid to the monitoring of ongoing discipline issues with the development of a process to allow senior management to identify systemic problems particularly with staff in high risk money laundering/terrorism financing areas.

### **8. Tips for managing an AUSTRAC audit**

Develop AUSTRAC visit policy and procedures. Policy and procedures should set out how a reporting entity should respond to either: entry to premises by authorised AUSTRAC officers with the occupier's consent, or entry to premises by authorised AUSTRAC officers under a monitoring warrant issued by a magistrate.

AUSTRAC creates a regulatory profile for each reporting entity and takes the view that if an entity cannot ensure compliance to simple things, the entity will not be able to ensure more sign.

## Conclusion

In summary, carefully revisit obligations in Chapter 9 of the AML Rules (assuming YOU have a Joint AML/CTF Program). Additional items to revisit are as follows:

### 1. Risk Management

- How did you link your risk assessments to Part A? How do YOU link your risk assessments to KYC?
- Can YOU demonstrate your Risk assessment methodology? (NB - all your risks should not be low. If so are you may need to justify. What risk factors were used?
- What are your risk based systems and controls that identify, manage & mitigate.
- How do YOU check for PEPs?

2, Training: How did YOU segment, roles and provide specific training for those roles from the Board to frontline staff?

YOU needs to demonstrate a range of TMFL activity outlined above which would suffice as adequate and reasonable steps under the AML/CTF Act to comply with the Act's risk based approach to compliance.

## Statement of Responsibilities and Scope of Our Advice

We take responsibility for this letter, which is prepared on the basis of the limitations set out as follows:

Yours sincerely,



Ulysses Chioatto, LLB, MBA, MLLR  
Director  
**SSAMM Management Consulting**

Our comments are based solely on our reading of the AML/CTF Act 2006 and our experience of regulatory expectations gained from assisting other organisations with their AML/CTF compliance implementations and of 'better practice' compliance within the industry.

Our comments do not purport to address all issues regarding compliance with the AML/CTF Act 2006. They are intended only as a guide and not a warranty or guarantee that you are compliant with all components of the said legislation.

The matters raised in this letter are only those, which came to our attention during the course of our engagement and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. You should assess recommendations for improvements for their full commercial impact before they are implemented.

This letter has been prepared solely for your use and should not be quoted in whole or in part without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose.

## Appendix A: The Know Your Customer (KYC) requirements

AUSTRAC position on KYC non-compliance of Part 2, Divisions 2, 3, 4 and 5 of the AML/CTF Act came into effect on 12 December 2007.

In recognition that many reporting entities were not going to be in a position to fully comply with these requirements by this date, the Policy (Civil Penalty Orders) Principles 2006 (the "Principles") provide a 15 month period during which the AUSTRAC CEO may only apply for a civil penalty order against a reporting entity in circumstances where the reporting entity has failed to **take reasonable steps** to comply with the provisions of the Act. AUSTRAC has also issued a Guidance Note on the application of the Principles (the "Guidance Note").

AUSTRAC has received a range of questions from reporting entities on whether the Principles remove their obligation to collect KYC for customers captured by Part 2, after 12 December 2007 ( in particularly Division 4) and before an entity's full compliance.

AUSTRAC's view on this matter is that:

1. The Principles and Guidance Note do not alter the commencement date of Part 2 of the AML/CTF Act.
2. It is still a requirement of the AML/CTF Act to comply with Part 2 irrespective of whether the Principles are in place or not to avoid the possibility of enforcement action – including civil penalty orders - in respect of Divisions 2, 3, 4 and 5 of Part 2 of the AML/CTF Act, a reporting entity must, by 12 March 2009, at the very latest,
  - be compliant with Divisions 2, 3, 4 and 5 of Part 2
  - Have undertaken KYC procedures on all customers for which this was a legal requirement from 12 December 2007.

This applies regardless of the date during the 15 month period at which the reporting entity reached full compliance with these requirements.

Notwithstanding the application of the Principles and the Guidance Note, AUSTRAC has a number of regulatory powers available to it beyond the application of civil penalty orders. These powers may be applied irrespective of whether or not an entity is complying with the Principles and following the terms of the Guidance Note and within the relevant 15 month period.

A Reporting Entity is required to continue to maintain compliance with Part 2, Divisions 2, 3, 4 and 5 of the AML/CTF Act 2006 after 12 March 2009. Failure to do so will risk enforcement action by AUSTRAC including Civil Penalty Orders.

The view set out above is based on AUSTRAC's role in promoting compliance with the AML/CTF Act and to ensure competitive neutrality between reporting entities. In particular, it is important that AUSTRAC does not provide a competitive disadvantage to those entities which reach full compliance at an earlier date and provide an incentive to delay implementation of systems and commencement of KYC requirements.

Where a reporting entity believes that it has a particular set of circumstances that mean it will be unable to comply with provisions of the AML/CTF Act, it should approach AUSTRAC with a specific proposal for consideration of these matters. This proposal would need to address a range of issues including:

- The nature of the relevant service or product,
- Detail of what aspects of KYC information will not be captured or the process that will not be completed,
- An estimate of the likely number of customers affected and their profile,
- An estimate of the cost in complying with the KYC requirements, and
- A proposal from the entity for managing the risks (in terms of the AML/CTF Act) associated with non compliance.