Banking and Financial Services Law Association Conference
10 August 2007

Some Practical Implications of Australia's new Anti-Money Laundering and Counter-Terrorism Financing regime

Mark Sneddon, Partner, and Peter Harman, Solicitor, Clayton Utz[1]

msneddon@claytonutz.com pharman@clayotnutz.com

1. Introduction

The Anti Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (**"AML/CTF"**) Act represents Australia's adoption of a risk-based approach to Money Laundering (**"ML"**) and Terrorism Financing (**"TF"**) Risk in response to the Financial Action Task Forces ("FATF") 40 Recommendations.

The AML/CTF regime is principles-based legislation and subordinate Regulations and Rules, the first of two tranches. The first tranche covers the financial and gambling sectors and bullion dealers. The second tranche will cover real estate agents, jewellers, and some transactions provided by accountants and lawyers. The Government has indicated that the second tranche will also be developed in consultation with industry.

Additional funding of $139 million over four years has been provided to the Australian Transaction Reports Analysis Centre (**"AUSTRAC"**), which has a range of new regulatory functions under the AML/CTF Act. In addition to its enhanced role as a financial intelligence unit, AUSTRAC now has a significantly expanded role as the national AML/CTF regulator with supervisory, monitoring and enforcement functions over a diverse range of industry sectors (for example, including gambling, bullion services and a potentially broad range of providers of designated remittance services).

This paper is intended to discuss some key practical implications of the AML/CTF Act for reporting entities, including the AML/CTF Compliance Program, the risk-based approach and Designated Business Groups. The paper concludes by examining two interpretations problems which have become apparent – the scope of designated remittance services and the application of the AML/CTF regime offshore including in New Zealand.

2. The development and content of the AML/CTF package

The history of the Anti-Money Laundering and Counter-Terrorism Financing Act (**"AML/CTF Act"**) dates back to Australia's 2003 commitment to implement the Financial Action Task Force on Money Laundering's 40 Recommendations (**"FATF Recommendations"**). The Recommendations were initially developed in 1990, and have subsequently been revised twice to take account of changes in money laundering trends. The most recent full-scale review took place in 2003. The AML/CTF Act builds significantly on the Anti-Money Laundering (**"AML"**) provisions in the *Financial Transaction Reports Act 1988* (Cth) (**"FTRA"**) which continues to apply to cash dealers who are not covered by the AML/CTF Act.

---

[1] The assistance of Gabe Hau, Solicitor, Clayton Utz in preparing this paper is gratefully acknowledged.

2.1 Passage of the AML/CTF Act

On 16 December 2005, the Federal Attorney-General's Department released the first exposure draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill (**"AML/CTF Bill"**), with a suite of explanatory material, for public comment.

Over the course of the year that followed, the AML/CTF Bill was refined in consultation with industry, an AML Advisory Group representing affected stakeholders and the Senate Legal and Constitutional Legislation Committee. A second iteration of the AML/CTF Bill was released on 13 July 2006 for public comment. Approximately 200 submissions were received over the three weeks that followed, with submissions closing on 4 August 2006.

The Minister for Justice and Customs introduced a further revised AML/CTF Bill, accompanied by a Transitional Provisions and Consequential Amendments Bill and relevant Explanatory Memorandum into parliament on 1 November 2006. At the time, the Minister stated that the release of the package represented:

> *"... an agreed and innovative risk-based approach to regulation in line with Government commitments to reduce regulatory burdens on business. Implicit in this approach is the recognition that industry has the most experience and best knowledge of how to implement measures appropriate to the money laundering and terrorism financing risks encountered by their business."*[2]

The Bill was passed and received Royal Assent on 12 December 2006, and its provisions, a number of which have already come into operation, are to be implemented in stages over the course of the coming two years. The Anti-Money Laundering and Counter-Terrorism Financing Act (**"AML/CTF Act"**) was amended by the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act (**"Amendment Act"**), which received Royal Assent on 12 April 2007. The Amendment Act was passed in order to address several technical issues raised by two Senate Inquiries into the AML/CTF Act.[3]

2.2 Obligations on Reporting Entities

The AML/CTF Act is principles-based legislation that sets out the framework for Australia's response to the FATF recommendations in relation to global AML/CTF standards. It specifies in tables in section 6 the **"designated services"** which are the subject of regulation. **"Reporting entities"** who provide those designated services to customers are required to comply with the legislation. The specific obligations of those reporting entities include the following:

(a) Establish, maintain, update, comply with and report on an AML/CTF Compliance Program which includes initial and ongoing customer due diligence (this is the most significant obligation and is described further below);

(b) monitor those customers and their transaction activities to manage the ML/TF risk they present;

---

[2] See the Minister's media release at http://www.ag.gov.au/agd/www/Justiceministerhome.nsf/Page/Media_Releases_2006_4th_Quarter_27_October_2006_-_Anti-Money_Laundering_and_Counter-Terrorism_Financing_Reforms.

[3] For example, the amendments included, amongst other things, exempting transactions conducted via merchant terminals from the requirement to obtain complete payer information where only one institution is involved in a funds transfer, and establishing the function of Evidentiary Certificates in relation to proceedings for breach of the requirement to be registered as a designated remittance service provider.

(c) make reports to AUSTRAC in relation to Threshold Transactions (transfers of physical currency or e-currency of $10,000 or more), International Funds Transfer Instructions, Electronic Funds Transfer Instructions, cross-border movements of physical currency and bearer negotiable instruments, and suspicious matters;

(d) register if a provider of designated remittance services;

(e) maintain records;

(f) conduct regular due diligence of relations with correspondent banks and avoid relationships with shell banks; and

(g) comply with any countermeasures regulations.

There are related obligations under the Proceeds of Crimes Act 2002, the Criminal Code money – laundering offences and the suppression of financing of terrorism provisions in the Charter of the United Nations Act.

2.3 Implementation and Enforcement Policy

The implementation schedule for the AML/CTF Act provides some relief to reporting entities faced with the challenge of achieving compliance with the Act's requirements. Implementation is staggered over the course of approximately two years (from December 2006 to December 2008), and the *Policy (Civil Penalty Orders) Principles 2006* (**"Policy Principles"**) provide for an "enforcement light" period (not an enforcement free period) of fifteen months following the commencement of civil penalty provisions of the Act.

The Policy Principles provide that, during the "enforcement light" period, the AUSTRAC CEO may only make application for a civil penalty order against a reporting entity for contravention where the reporting entity to which the application relates has failed to take reasonable steps to comply with the provision. The AUSTRAC CEO must consider "all relevant matters" in determining whether a reporting entity has failed to take reasonable steps to comply with a civil penalty provision, including:

- Whether the entity has previously failed to take such steps;
- Any steps that the entity has taken to comply with its obligations under the Act;
- Whether the entity complied with any applicable obligations under the FTRA;
- Any discussions and agreements that the reporting entity has had with AUSTRAC staff; and
- Any explanation given by the reporting entity to AUSTRAC.

It should be noted that the Policy Principles do not provide for a "prosecution light" period in respect of criminal offences under the AML/CTF Act. It may be hoped that criminal prosecutional discretion would be exercised consistently with the "enforcement light" principles regarding court penalties but there is no legal requirement for this.

AUSTRAC's Enforcement Policy relevantly states:

> *"The policy principles dictate that each case will be assessed on its merits. However, AUSTRAC emphasises that this policy principle will not limit its resolve to pursue criminal penalties where the circumstances warrant it, nor civil penalties, where there has been a history of blatant disregard for the law under either the FTR Act or during the implementation period for the AML/CTF Act.*

AUSTRAC's preference is to promote an environment of continuous voluntary compliance with the letter and spirit of the FTR and AML/CTF Acts, and related Regulations and Rules. It is anticipated that most regulated entities will seek to comply with their responsibilities. Where AUSTRAC finds evidence of significant non-compliance or detects material systems weaknesses in a regulated entity's ML/TF risk management, the regulator will seek in the first instance to resolve those issues in a cooperative manner through negotiation and guidance."

2.4 AML/CTF Rules

Anti-Money Laundering and Counter-Terrorism Financing Rules (**"AML/CTF Rules"**) have been registered by AUSTRAC in several tranches, summarised below:

Subject Matter	Rules
• Movements of Bearer Negotiable Instruments; • Movements of Physical Currency into or out of Australia; • Receipts of Physical Currency from outside Australia; and • Register of Providers of Designated Remittance Services.	Anti-Money Laundering and Counter-Terrorism Financing Rules registered on 20 December 2006
• Designated Business Groups; • Correspondent Banking; • Customer Identification; • AML/CTF Programs; and • Gambling Services.	Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) registered on 13 April 2007.
• Paragraph (5) of the definition of "correspondent banking relationship" in section 5 of the AML/CTF Act	Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 2) registered on 13 April 2007.
• AML/CTF Compliance Reports	Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2007 (No. 1) Registered on 28 June 2007.

Draft Rules have been released in relation to "approved third-party bill payment systems" for the purposes of section 70(a)(i), ongoing customer due diligence and threshold amounts in respect of items 17 (issuing bills of exchange, promissory notes, letters of credit), 25 (issuing traveller's cheques), 26 (as issuer of a traveller's cheque, cashing or redeeming a traveller's cheque) and 50 (currency exchange).

Further draft Rules are anticipated.

2.5 AUSTRAC Policies and Guidance Notes

AUSTRAC has released a Supervisory Framework as well as a suite of Policies in relation to Education, Monitoring, Enforcement, and Exemptions and Modifications under the AML/CTF Act. Each of these is available on the AUSTRAC website.

Consultation was undertaken in late 2006 / early 2007 in relation to AUSTRAC's Draft Guidance Notes on Correspondent Banking, Designated Business Groups, the Register of Providers of Designated Remittance Services and Exemptions and Modifications under the AML/CTF Act. Final versions of those Guidance Notes were published in July 2007 will be published shortly.

Draft Guidance Notes in relation to Opening Accounts and Risk Management and AML/CTF Programs were released for consultation in May 2007.

3. Practical implications – the AML/CTF Compliance Program

The potential impacts of the AML/CTF Act are far-reaching for reporting entities that provide designated services. In a number of instances, the AML/CTF Act may apply to the business activities of entities that do not appear to fall within the scope of the Act at first, or may not have contemplated that it may apply to them. In addition, under the AML/CTF Rules, many of the obligations of reporting entities extend not only to all parts of the entity's business, but to third party service providers and to offshore permanent establishments and, potentially, to offshore subsidiaries.

Perhaps the most significant and expensive requirement is in section 81 of the AML/CTF Act, which states that a reporting entity must not commence to provide a designated service to a customer unless it has adopted and maintains an AML/CTF Program. The program must comprise of two parts:

Program Part	Requirements
Part A	General compliance practices and procedures designed to identify, mitigate and manage the risk of money laundering and terrorism financing that the entity may reasonably face (in relation to all designated services provided by the entity), including: • Identify the ML/TF risk that the reporting entity might reasonably face considering: 1. its customer types, including any politically exposed persons; 2. the types of designated services it provides; 3. the methods by which it delivers designated services; and 4. the foreign jurisdictions with which it deals. • Put in place appropriate risk-based systems and controls to manage the identified ML/TF risks (this will include some type of transaction monitoring system for reporting entities like banks which process a high volume of transactions); • Development and rollout of AML/CTF training for staff; • Development and rollout of an employee due diligence program • Oversight of the AML/CTF Program by boards and senior management; • Appointment of an AML/CTF Compliance Officer; • A process for independent review; • Procedures to enable the reporting entity to have regard to any AUSTRAC feedback

Part B	Practices and procedures for customer identification. The practices and procedures must: • Ensure that, as a general rule, customers are identified prior to a designated service being provided to them; • Apply to customers of all types (including individuals, sole traders, Australian and foreign companies, (including beneficial owners of companies), trusts (including trustees and beneficiaries of trusts), partnerships and associations) as well as agents of those customers; • Provide for the verification of customer identity (including by using simplified procedures or safe-harbours where appropriate); • Set out processes to be followed where discrepancies arise between identity information provided by customers and information obtained by way of verification; and • Set out the basis upon which sources of verification data will be assessed for reliability (including documentary and electronic safe harbours).

The cost and effort involved in developing and implementing a compliance program should not be underestimated. KPMG's recently published Global AML Survey 2007 found that AML compliance costs had grown well beyond the expectations of the banks that participated in its global Survey:

> *"Average AML costs were reported by the participants in our survey to have increased by 58% over the last three years. This was more than banks expected when we carried out our 2004 survey – at that time, banks predicted costs would only rise by 43% over the following three years. Despite the unexpectedly high increase in AML costs, respondents anticipate that growth will slow, with banks predicting an average increase of 34% on AML costs over the next three years."*[4]

Of note, AUSTRAC's Supervisory Framework recognises that "while principles-based legislation has numerous advantages, it does entail considerable work on the part of the regulator and reporting entities in order to understand and implement practical solutions which will achieve legislative objectives."[5]

4. Practical Implications - The risk-based approach

A risk-based approach requires regulated entities to establish, within the broad confines of the AML/CTF legislation, their own protocols to assess and manage ML/TF risk they face according to customer type, product type, delivery channel type and the expected and actual patterns of transactions and product use of their customers.

Industry sought and obtained risk-based obligations in preference to being subjected to detailed prescriptive and rigid obligations. However, the successful escape from a prison of prescription to the freedom of flexibility has left industry (and perhaps the regulator) with the unease of uncertainty. Uncertainty as to what the regulator will think is a reasonable approach to managing ML/TF risk in particular situations. And uncertainty as to how competitors will

[4] KPMG Global Anti-Money Laundering Survey 2007, page 11. A copy of the survey can be requested from KPMG's internet site at: http://www.kpmg.com.au/Default.aspx?TabID=1410.

[5] AUSTRAC Supervisory Framework, page 2. Available at: www.austrac.gov.au.

manage that risk and whether different risk management approaches (for example to customer due diligence and identity verification and transaction monitoring) will give or take away a competitive edge in attracting and keeping customers.

The risk-based approach is evident in a number of key parts of the legislation, such as those parts which require reporting entities to assess the level of ML/TF risk associated with customer types, types of services provided to customers, service delivery channels and foreign jurisdictions in which designated services are provided.

By way of example, AML/CTF Rule 4.2.3 requires Part B of a reporting entity's AML/CTF Program to incorporate a procedure for the reporting entity to collect the full name, date of birth and residential address of a customer who is an individual. The reporting entity must then verify the customer's full name and either of the customer's date of birth or residential address based on reliable and independent documentation, reliable and independent electronic data, or a combination of the two.

However, under Rule 4.2.5, Part B must also include appropriate risk-based systems and controls for the reporting entity to determine whether, and if so what, additional information in relation to the customer will be collected and should be verified (presumably when the information already obtained about the customer, or the nature of the designated services provided or the channel or the country of the customer or the transactions or some combination of these suggests an inconsistency or a heightened risk).

Not only must the reporting entity make an assessment in order to determine what additional information should be collected about a particular individual or class of individuals, it must also determine to what extent that information should be verified, and what it considers to be reliable and independent documentation and electronic data for the purposes of verifying that information. Clearly there are choices presented which will involve greater or lesser compliance cost, greater or lesser customer inconvenience and greater or lesser risk mitigation.

There is a safe harbour which deems the obtaining of minimum identification information about a customer to be sufficient if the ML risk is assessed as medium or lower. The minimum identification information for an individual is their name, date of birth and residential address[6]. It is worth noting that the minimum information is unlikely to reveal anything about the inherent risk associated with the provision of designated services to that individual (unless they are on a DFAT or other government's prohibited list). So unless other risk factors arise for example from the product being provided or the location of the customer or the pattern of transactions, most individual customers will likely be assigned a default category of lower risk.

5. Risk Profile of reporting entity: setting acceptable risk levels

In the context of risk-based AML/CTF legislation, a fundamental aspect involves establishing a reporting entity's risk position or risk appetite in terms of ML/TF risk. A reporting entity must take into account a range of factors in order to determine the level of ML/TF risk it is prepared to tolerate as a consequence of doing business.

The consequences of setting an appropriate risk level should not be underestimated. For example, if a particular reporting entity puts in place a customer identification process requiring six forms of identification to be produced by intending customers, while a competitor puts in place a process requiring three forms of identification, potential customers may be inclined to take their business to the competitor because of the perceived ease with which an account can be established or a designated service provided.

---

[6] Two of these, including the full name of the individual, must be verified.

Equally, if a reporting entity collects only the minimum KYC information from an individual customer (eg. full name, date of birth and residential address), what will this tell the reporting entity about the ML/TF risk associated with the customer?

The need to take a pragmatic approach to setting acceptable risk levels at the high policy level is reflected in AS3806 Principle 2, which is predicated on the fact that an organisation's compliance policy should be aligned to the organisation's strategy and business objectives, and endorsed by the governing body of the organisation.

AS3806 recommends that an organisation's compliance policy should articulate:

- the organisation's commitment to compliance;
- the scope of the compliance program;
- the application and context of the program in relation to the size, nature and complexity of the organisation and its operating environment;
- responsibility for managing and reporting compliance; and
- required standards of conduct, accountability and consequences of non-compliance.

Each of the elements listed above also has a bearing on the level of risk that an organisation is willing to treat as acceptable.

It should be kept in mind that the occurrence of specific events, such as the commission of a widely publicised ML/TF offence, the damaged reputation of a competitor, new product, service or channel offerings or a regulatory breach identified during the course of compliance testing may alter a reporting entity's inherent risk profile, and ultimately lead that reporting entity to revisit its risk appetite. That is to say, a reporting entity should not consider its risk profile to be set in stone from the outset.

FATF Guidance on Risk-based approach

The FATF June 2007 publication entitled "Guidance on the risk-based approach to combating money laundering and terrorist financing – high level principles and procedures" (**"FATF Guidance"**) provides some helpful assistance to reporting entities undertaking the process of establishing risk profile and setting levels of acceptable risk.

The FATF Guidance provides that:

> *"Implementing a risk based approach requires that financial institutions have a good understanding of the risks and are able to exercise sound judgement. This requires the building of expertise within financial institutions, including for example, through training, recruitment, taking professional advice and 'learning by doing'...*
>
> *Financial institutions may find that some staff members are uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. This may also be true at various levels of management. However, in situations where management fails to recognise or underestimates the risks, a culture may develop within the financial institution that allows for inadequate resources to be devoted to compliance leading to potentially significant compliance failures...*

In implementing the risk-based approach financial institutions should be given the opportunity to make reasonable judgements. This will mean that no two financial institutions are likely to adopt the exact same detailed practices."

6. Designated Business Groups

Where a group of related entities is comprised of more than one reporting entity as defined by the AML/CTF Act, establishing a designated business group (**"DBG"**) may serve to reduce the regulatory burden of complying with the Act.

Under Rule 2 of the AML/CTF Rules, two or more reporting entities may establish a DBG in circumstances where those reporting entities:

- Make an election in writing (using the approved form set out in the Rules) to join the DBG;
- Nominate a particular person to AUSTRAC as the DBG's Nominated Contact Officer (**"NCO"**); and
- Are related to each other within the meaning of section 50 of the *Corporations Act 2001* (Cth).

A DBG is established by the NCO providing notification to the AUSTRAC CEO using the approved form. Once the DBG has been established, the NCO must inform AUSTRAC of any changes to the membership of the DBG or it termination, within 14 days of the change taking effect (see AML/CTF Rule 2.1).

Benefits of establishing or joining a DBG

The main benefit of related reporting entities establishing a DBG is that most compliance activities of each group member may be discharged by any other member of the DBG, including:

1. **Customer Due Diligence** – This is only required to be performed by one member of the DBG, once. Any other member which subsequently provides services to that customer does not need to perform another customer due diligence for the same customer (section 36) .
2. **Compliance Reporting** – Compliance Reports can be prepared by any member of the DBG and can be compiled into one document (section 47).
3. **Joint Anti-Money Laundering and Counter-Terrorism Financing Program** – This is a program that applies to each entity in the DBG, making it more efficient to comply with the Act when a large number of reporting entities are members of the DBG (section 85).
4. **Records and designated services** – Each reporting entity is required to keep a record of the information relating to any provision of designated services to a customer for 7 years. This record may be kept by any member of the DBG (sections 106 and 107).
5. **Customer Identification Procedures** – The Act also requires reporting entities to make records relating to the customer identification procedure and the information obtained in the course of carrying out the procedure relating to the provision of designated services for 7 years, and may be kept by any member of the DBG (sections 112 – 114)
6. **Records of Joint Anti-Money Laundering and Counter-Terrorism Financing Program** – The Act requires that a record of the adoption of a Joint Anti-Money Laundering and Counter-Terrorism Financing Program and a copy of the program itself be

kept whilst it is in force and for 7 years after it ceases to be in force. This may be kept by any member of the DBG (section 116).

These benefits mean that compliance with the Act can be maintained at group level, reducing duplicated efforts and increasing compliance efficiency. However, there are some traps a DBG should be aware of:

1. **Tipping Off** – Generally, the Act prohibits a person providing information relating to a suspicious matter or relating to whether information has been provided to AUSTRAC except where the person provides the information to the AUSTRAC CEO or a member of the staff of AUSTRAC (see sub-sections 123(1) and (2)). The Act, however, permits entities within a DBG to provide information (which could reasonably be expected to infer that a suspicion has been formed in relation to a customer) to another member of the DBG relating to the affairs of a customer of the entity for the purpose of informing that other member of the DBG about the risks involved in dealing with the customer when it has formed a suspicion about a suspicious matter in relation to the customer (see sub-sections 123(2) and (7)).

   It should be noted that, if information relating to a suspicious matter was reported to AUSTRAC by a member of the DBG, it must not inform another member of the DBG that the information has been communicated to AUSTRAC (sub-section 123(1)). In short, one member of a DBG can inform another member of the DBG about its customer's affairs about a suspicious matter but it cannot inform another member of the DBG that the information has been provided to AUSTRAC. It is unclear why one member of a DBG cannot inform another member of a DBG that a matter has been reported to AUSTRAC. Perhaps it is intended that each entity forms its own opinion on the level of suspicion it places on a customer's affairs. In practice, the AML/CTF Compliance Officer is likely to be the same person for the entities within the DBG and therefore any reporting to AUSTRAC is likely to be within the scope of that person's role.

2. **External Audits** – Where the Act requires the appointment of an external auditor, an officer, employee or agent of one member of the DBG cannot act as an external auditor of another member of the DBG (section 108).

3. **Disclosing existence or nature of a notice** – If a notice is issued to a member of a DBG under section 202 of the Act and it specifies that the notice must not be disclosed, a member can disclose information relating to the notice to another member of the DBG (see sub-sections 202(2) and 207(3)).

Although the DBG regime will reduce compliance costs of corporate groups, it has not satisfied everyone. Some financial institutions have argued that a DBG should not be restricted to companies that are 'related to each other' and should include "franchise, agency and alliance relationships".[7] In a financial market where franchises brokers, agents and financial advisers form an integral part of marketing and distribution channels, a definition of a group under section 50 of the Corporations Act may be seen as somewhat restrictive. On the other hand, DBGs involving non-related corporations may involve shared risk without the prospect of real control and monitoring by group members of each other and, from the regulator's point of view, may leave too much scope for buck-passing.

---

[7] Bank of Queensland, *Submission on the revised exposure draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill*, 4 August 2006, p 2.

7. Putting a Compliance Program in place: undertaking a Gap Analysis & developing an implementation schedule

Gap Analysis

The key to determining where compliance efforts should be focussed involves, first, identifying where deficiencies and gaps exist. Thereafter, a compliance plan can be developed to address the identified (and documented) deficiencies and achieve compliance with the requirements of the AML/CTF Act. The role and importance of ongoing compliance management and monitoring can then be considered in context, including the preparation of a testing regime to ensure compliance obligations are met.

For reporting entities that have been through the process of implementing new or revised regulatory regimes such as Privacy, Code of Banking Practice or Financial Services Reform, much can be gained from considering material produced during the course of a post implementation review. Key questions to ask about prior implementation projects include:

- Who were the compliance champions in respect of prior implementation programs? Are those particular persons/roles on board with the AML/CTF Compliance Program development and implementation process?
- Which parts of the business demonstrated the greatest levels of non-compliance in the past? Which encountered the most difficulty in implementing the new requirements?
- Was the project completed on time, and within the allocated budget? If not, which areas of the business experienced cost blowouts or lagged behind the others in achieving compliance?
- What recommendations, if any, were made in relation to the conduct of future projects to implement new regulatory requirements when the implementation project reached completion?
- How has the structure or risk profile of the organisation changed since the last regulatory implementation project was completed?

In undertaking a gap analysis, reporting entities will find useful guidance in Australian Standards 4360:2004 Risk Management and 3806:2006 Compliance Programs. In particular, the compliance principles set out in AS3806 under the broad categories of Commitment, Implementation, Monitoring and Measuring and Continual Improvement provide useful guidance for reporting entities faced with the challenge of undertaking a gap analysis and developing an implementation schedule.

Support from the top down is integral to the success of a regulatory implementation project. Not only is senior management commitment an essential element of any good compliance program (see AS3806 Principle 1), it is requirement under AML/CTF Rule 8.4.1 (Standard AML/CTF Programs) and its equivalent, Rule 9.4.1 (Joint AML/CTF Programs) that a reporting entity's AML/CTF Program be approved by the Board.

Key steps to undertake at the initial gap analysis stage are:

- Securing adequate funding to develop and implement an AML/CTF Program;
- Ensuring support from the top down;

- Determining which provisions of the AML/CTF Act apply to your business activities (for example, which designated services does, or may, your organisation provide?). The Self Assessment Questionnaire available on the AUSTRAC website will be of assistance to reporting entities undertaking this analysis;

- Creating a general level of awareness about the potential impact of the AML/CTF Act on the business (based on the above). This is consistent with the "no surprises" risk management strategy;

- Assessing customer types, product types and access channels for inherent risk (for example, will the program be based on the assumption that a customer who is identified remotely is more or less likely to be the person they purport to be?). Can the outcome of these assessments be used to set boundaries in terms of acceptable risk;

- Assessing the demonstrated level of compliance with the core requirements of the AML/CTF Act as things currently stand (for example, are all customers identified in accordance with a particular existing standard, what policies are in place in relation to transaction or customer monitoring?). This will likely be different for different parts of the business;

- Reviewing contracts and other arrangements with service providers, and considering whether they adequately address the ML/TF risk that the relationship may entail and how the service providers can assist the reporting entity in managing the ML/TF risk entailed.

Once the answers to the questions above have been determined, a comprehensive gap analysis should be undertaken by listing applicable obligations set out in the AML/CTF Act and Rules, specifying how, in the opinion of the reporting entity, compliance with those requirements can be demonstrated, and documenting the work required in order to achieve the desired outcome. This will then feed into the development of an implementation schedule to achieve compliance.

Documenting the process of AML/CTF Program development not only enables a reporting entity to map its course to achieving compliance, it also provides a record of the analysis undertaken and steps identified should there be cause to provide that information to AUSTRAC, or an independent auditor.

Design of an effective and achievable implementation schedule

Clearly, the implementation schedule for a reporting entity's Compliance Program will be subject to the constraints of the legislation. In the case of the AML/CTF Act, the staggered implementation of legislative requirements provides some guidance as to the implementation timeframes that are both achievable and practical.

Informed by the staggered implementation of the AML/CTF Act, the documentation generated during the course of the gap analysis should form the basis of a reporting entity's schedule for the development and rollout of its compliance program. Efforts will necessarily be focused on those aspects with which low levels of compliance can be demonstrated based on existing policies, processes and procedures.

It is suggested that reporting entities take a pragmatic approach to implementation timelines. Being overzealous in anticipating the effort required to achieve compliance can lead to unmet deadlines, and cost overruns. Perhaps more importantly, such an approach can lead to legislative requirements being overlooked or misinterpreted. While an implementation

timeline will of its nature be ambitious, it should also represent a carefully determined estimate of work required to achieve compliance, and allow for some slippage in terms of due dates.

We turn now to two specific interpretation issues which have been raised in implementation experience so far – designated remittance arrangements and application to services provided at or through permanent establishments in foreign countries.

8. The overbroad scope of designated remittance arrangements

A "designated service" includes a service where:

money or property is accepted from a transferor entity transferred under a designated remittance arrangement;[8] or

(a) money or property is made available to an ultimate transferee entity as a result of a transfer under a designated remittance arrangement[9].

"Designated remittance arrangement" is defined as any remittance arrangement where:

(a) a person, not being an ADI, bank, building society or credit union, accepts money or property from a transferor entity under a remittance arrangement; and

(b) a person, not being an ADI, bank, building society or credit union, makes money or property available to an ultimate transferee entity as a result of a transfer under a remittance arrangement.[10]

Although the Act allows the AML/CTF Rules to specify other persons to whom this definition does not apply, there are no such specified persons in the Rules at present.[11] The scope of this definition can be narrowed by the Rule imposing other specified conditions but there are currently neither specified conditions nor has any specified conditions been proposed.[12]

A "remittance arrangement" is broadly defined as an arrangement that is for the transfer of money or property, and includes any arrangements taken to be a remittance arrangement by the Rules.[13] The definition of "transfer" in the Act is similarly wide and includes any act or thing, or any series or combination of acts or things, that may reasonably be regarded as the economic equivalent of a transfer.[14] This wide definition means that, for example, an arrangement to debit an amount from one person's account and to credit an equivalent amount to another person's account is a "remittance arrangement" within the meaning of the Act.[15] "Property" has also been given a broad definition in the Act, to include any legal and equitable estate or interest in real or personal property, including a contingent or prospective one.[16]

---

[8] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 6, item 31

[9] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 6, item 32

[10] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 10(1).

[11] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) ss 10(1)(a)(v) and 10(1)(b)(v) and *Anti-Money Laundering and Counter Terrorism Finance Rules 2006*, made under s 229 of the Act.

[12] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 10(1)(c).

[13] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 10(2).

[14] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 5.

[15] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 5.

[16] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 5.

Examples of *designated remittance arrangements* include hawala, hundi, fei-chien, the black market peso exchange and other forms of money laundering.[17]

The Act's broad definition of designated remittance arrangements is likely to create a number of problems for organisations which are not ADIs, banks, building, societies or credit unions.

First, for many such businesses, it is not intuitively obvious that the Act is intended to apply to them. Such a business may never even consider whether any AML/CTF compliance requirement is applicable to it.

For example, a company which is not an ADI receives money from a person in Australia which the person owes to a related company overseas. Related companies overseas receive money from persons in those jurisdictions which are owed to the Australian company. Instead of sending the money to each other by international funds transfer through the banking system, those companies maintain accounts for each other and, by account entry, set off their mutual obligations. This is an arrangement for the transfer of money or property and without more is a designated remittance arrangement. But it may be an entirely innocent and convenient way of facilitating customer payments through one group member to the account of another without incurring funds transfer fees.

Second, certain types of non-financial businesses which transfer or deliver physical property are potentially providing designated remittance services under the Act. For example, a company providing shipping services which is not an ADI may need to comply with the Act as their services may include effecting a transfer of property at the direction of consignor or consignee. A goods or commodities warehousing company which is a contractual bailee and delivers as directed by the bailor could also be a reporting entity under the Act. These are examples of businesses to which the broad drafting of the Act appears to apply but their ordinary commercial activities do not present a ML/TF risk – rather a potentially vast category of services for AUSTRAC to supervise for no policy benefit.

The broad definition of a designated remittance arrangement means any person or entity which potentially may be caught by it needs to consider registering as a provider of designated remittance services.[18] A designated remittance service is a designated remittance arrangement that is provided by a person at or through a permanent establishment of the person in Australia and is not of a type excluded in the Rules.[19] Strict liability applies to the requirement (which became effective on 13 December 2006) not to engage in conduct which involves providing a designated remittance service if a person is not registered. A breach of this requirement attracts a penalty of 2 years imprisonment or $55,000 or both.[20] Repeat offenders attract a maximum penalty of 7 years imprisonment or $220,000 or both.[21]

AUSTRAC has been made aware of this issue. In July 2007, AUSTRAC issued a Guidance Note on Register of Providers of Designated Remittance Services (**"DRA Guidance Note"**). The Guidance Note states that the types of designated remittance service providers required to register include those commonly known as remittance dealers, money remitters, money transmitters, alternative remitters, providers of money transfers and various services usually

---

[17] *Anti-Money Laundering and Counter Terrorism Financing Bill 2006 Replacement Explanatory Memorandum*, p 67.

[18] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) ss 73 to 79A.

[19] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) s 5.

[20] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) ss 74(2) and (3).

[21] *Anti-Money Laundering and Counter Terrorism Finance Act 2006* (Cth) ss 74(6), (7), (8) and (9).

provided within community groups (such as hawala).[22] It also states (clause 3.4) that AUSTRAC will develop AML/CTF Rules to treat certain remittance arrangements so that they do not constitute designated remittance arrangements under the AML/CTF. We understand from AUSTRAC that these draft Rules are expected in September and that it is a difficult task to distinguish legitimate from potentially criminal remittance arrangements.

Given that there are no registration fees or charges, registration can be completed online with an estimated completion time of 20 minutes and the significant penalty for providing a service without registration, it might be tempting to register if there is the slightest possibility that an entity might be caught as a provider of designated remittance services. However, registration involves an implicit concession that the entity is a reporting entity which requires the development of an AML/CTF compliance program, customer due diligence and reporting obligations which are onerous compliance obligations if no other part of the entity's business involves providing a designated service. Waiting for the draft Rules may be more attractive.

9. Considering the application of the AML/CTF law to offshore operations of Australian persons and subsidiaries of Australian persons, notably in New Zealand

As a general principle of international comity and because of the practical difficulties of enforcement, nation states usually do not legislate in relation to the conduct of persons occurring within other nation states. Some exceptions are more likely to be tolerated, for example, legislation concerning certain conduct of the legislating nation state's residents (natural or legal persons) in the other jurisdiction, or conduct of persons outside the legislating nation which has a clear detrimental effect on persons or circumstances within the legislating nation.

Difficult conflicts can arise where the legislating nation seeks to control the conduct of its residents in other jurisdictions, where the other jurisdiction has quite different laws or regulation in place with regard to the same conduct. Even more difficult is the case where the legislating nation goes one step further and seeks to control the conduct of legal persons resident in the other jurisdiction who are not resident in the legislating jurisdiction but are related to a legal person resident in the legislating jurisdiction (for example, a subsidiary or an agent or a subsidiary of a subsidiary of a resident of the legislating jurisdiction). It would normally be expected that a legal person resident and carrying on business only in one jurisdiction would be primarily subject to the laws of that jurisdiction and not those of another jurisdiction in which a related entity was resident.

The USA has not been the country most averse to legislating for persons or conduct in other jurisdictions. Hence some of the USA PATRIOT Act provisions extend to conduct of permanent establishments or subsidiaries of US persons in other countries.

The UK and Australia historically have been more reluctant to test the reach of their legislative arms to regulate conduct of persons in other jurisdictions.

The revised UK Money Laundering Regulations 2007[23] apply to described categories of persons acting in the course of business carried on by them in the UK. There is some long-arm extension of this in regulation 15 to offshore branches and subsidiaries of UK credit or financial institutions which at least recognises the problem of potentially conflicting laws:

---

[22] AUSTRAC, *Guidance Note on Register of Providers of Designated Remittance Services*, July 2007, cl 3.1 and 3.2.

[23] SI 2157 of 2007, made 24 July 2007 to come into force on 15 December 2007 – Regulation 3.

"**15**(1) A credit or financial institution must require its branches and subsidiary undertakings which are located in a non-EEA state to apply, to the extent permitted by the law of that state, measures at least equivalent to those set out in these Regulations with regard to customer due diligence measures, ongoing monitoring and record-keeping.

(2) Where the law of a non-EEA state does not permit the application of such equivalent measures by the branch or subsidiary undertaking located in that state, the credit or financial institution must -

(a) inform its supervisory authority accordingly; and

(b) take additional measures to handle effectively the risk of money laundering and terrorist financing.

The Australian AML/CTF Act has a curious and somewhat convoluted regime for extra-territorial application in sections 26 and 6(6):

"26 **Extra-territorial application**

(1) Unless the contrary intention appears, this Act extends to acts, omissions, matters and things outside Australia."

Section 6(6) of the Act provides for the geographical link of the services described in the designated services tables in section 6 to Australia as follows:

"**Geographical link**

(6) An item of a table in this section does not apply to the provision by a person of a service to a customer unless:

(a) the service is provided at or through a permanent establishment of the person in Australia; or

(b) both of the following subparagraphs apply:

(i) the person is a resident of Australia;

(ii) the service is provided at or through a permanent establishment of the person in a foreign country; or

(c) both of the following subparagraphs apply:

(i) the person is a subsidiary of a company that is a resident of Australia;

(ii) the service is provided at or through a permanent establishment of the person in a foreign country."

Paragraph (b) covers the provision of a service by an Australian resident company at or through a permanent establishment of the company in a foreign country (such as an offshore branch on representative office of an Australian bank). This is similar to the UK approach.

Paragraph (c) covers the provision of a service by a subsidiary of a company that a resident of Australia and the service is provided at or through a permanent establishment of the subsidiary in a foreign country. We understand that AUSTRAC takes the view that paragraph (c) means that a subsidiary of a company resident in Australia (and this includes a subsidiary of a

subsidiary and so on) is regulated as a reporting entity when that subsidiary provides a service through a permanent establishment of the subsidiary in a foreign country.

The upshot of AUSTRAC's current interpretation is that if a third level subsidiary (incorporated in a foreign country) of any Australian incorporated company (the Australian parent need not be a reporting entity unlike the UK regulation) provides a service in a section 6 table through a permanent establishment in a foreign country, then the subsidiary is a reporting entity for the purposes of the AML/CTF Act.

Thus a New Zealand bank which is a subsidiary of an Australian bank and any subsidiary of the New Zealand bank which provides a section 6 table service in Auckland, Fiji, Vanuatu or the UK is a reporting entity under the Australian AML/CTF Act on this interpretation. We do not know if the New Zealand Treasury and Reserve Bank are aware of this interpretation. The interpretation appears to us to be open to some doubt.

The AML/CTF Rules and the Act do provide substantial (but not wholesale) relief in respect of compliance obligations for the activities of reporting entities through permanent establishments in foreign countries, for example in relation to Part A of an AML/CTF Program[24] and customer identification procedures.[25]

In addition, for those aspects of Part A of an AML/CTF Program which remain applicable to foreign permanent establishments, more relief is given if that foreign permanent establishment is regulated by anti-money laundering and counter-terrorism financing laws comparable to Australia.

No guidance has been provided on what laws may be "comparable" to Australia's AML/CTF regime. For example, New Zealand currently has a regime like the one Australia has just replaced – centred on the *Financial Transaction Reporting Act 1996 (NZ)*. A new FATF compliant regime is not expected to be operational in New Zealand until late 2008 or 2009. In the meantime is New Zealand law "comparable" to Australia's law or must New Zealand banks (and their subsidiaries) which are subsidiaries of Australian banks comply with those aspects of the Australian AML/CTF Act and Rules for which relief is not afforded?

The question may have a practical answer which is to roll all of the New Zealand subsidiaries into a Designated Business Group with central AML/CTF risk management from the Australian parent's head office but whether that is in all respects palatable to the New Zealand authorities remains to be seen.

For further information contact:

Mark Sneddon
Partner,
Clayton Utz
18/333 Collins Street
Melbourne VIC 3000
P: 03 9286 6353
F: 03 9629 8488
msneddon@claytonutz.com

---

[24] Eg AML/CTF Rules 8.8.4 and 9.8.4

[25] Section 39(5).