**User Warning**

This advance guidance document has been prepared in anticipation of anti-money laundering reforms being made applicable to the legal profession in Queensland.

While these reforms are expected, the QLS is not aware of their final form and has accordingly prepared this document as an indicative guide only.

This guide was produced by the Legal & Policy department at QLS.

Enquiries/comments to:

**Giles Watson**  
QLS Legal Practice Consultant  
Tel: 07 3842 5853  
Email: g.watson@qls.com.au

**Matt Dunn**  
QLS Principal Policy Lawyer  
Tel: 07 3842 5889  
Email: m.dunn@qls.com.au
1.1 Introduction

1.2 Existing Legal Framework
   (a) Tranche 1 Reforms
   (b) Implications for Solicitors

1.3 Current developments
   (a) Status of Tranche 2 Reforms

1.4 Likely elements in and impact of Tranche 2 legislation

1.5 Offences, Sanctions & other risks

1.7 Implementing AML Compliance arrangements
   (a) A risk based approach to AML
   (b) Initial client identification and ongoing client due diligence
   (c) Record keeping
   (d) Auditing
   (e) Employee training programs
   (f) The nomination of AML compliance officer (AMLCO)
   (g) Suspicious transaction reporting

1.8 Client Confidentiality & Legal Professional Privilege

1.9 Regulation

Further Reading
1.1 Introduction

“It is estimated that up to $4.5 billion is involved in money laundering in Australia every year.”

This particularly concerning statement starts the Federal Attorney-General’s Department’s Factsheet on why anti-money laundering and counter-terrorism financing reforms are required in Australia and regardless of whether the figures quoted are accurate or not, a new anti-money laundering / counter terrorism financing system is being systematically rolled out in this country.

The Government rationale for the new regulation is succinctly stated on the Federal Attorney-General’s Department’s AML Customer website:

Why has new legislation been introduced?

The new laws were introduced to:

- bring Australia’s AML/CTF system into line with international standards
- reduce the risk of Australian businesses being misused for the purposes of money laundering or terrorism financing, and
- meet the needs of law enforcement agencies for targeted information about possible criminal activity and terrorism.

1.2 Existing Legal Framework

(a) Tranche 1 Reforms

In Australia the original system implemented to monitor the flows of money in business and consumer transactions was the Financial Transaction Reports Act 1988. It relied on the reporting of transactions over threshold amounts and came at a time when banking and financial transactions were significantly different to those of today’s interconnected global financial system.

To address concerns about money laundering in 1989 several nations formed the Financial Action Task Force (FATF), now comprising 33 nations, who agreed Forty Recommendations on Anti-Money Laundering and Nine Special Recommendations on Counter-Terrorist Financing. In 2003 lawyers were included within FATF’s designation of Non Financial Business & Professions which is the focus of recommendations relating to:

- Customer due diligence and record-keeping; and
- Reporting of suspicious transactions and compliance.

A 2005 review by FATF of Australia’s implementation of these recommendations found that the Australian systems were well behind best practice.

The response of the Australian Government was the release of the Anti-Money Laundering and Counter-Terrorism Financing Bill in December 2005 for consultation which became an Act (the AML/CTF Act) on 12 December 2006.

The reforms implemented were designed to be rolled out in various tranches with the first directed toward the financial sector, gambling sector, bullion dealers and businesses that provide particular ‘designated services’. The Commonwealth Agency Austrac, which had responsibility for administering the Financial Transaction Reports Act 1988, was to be the regulator for the new obligations under the AML/CTF Act.
The implementation of these first tranche obligations were to be staged:

- record-keeping obligations started in various stages 6 months and 12 months after Royal Assent of the AML/CTF Act;
- customer identification and verification of identity obligations started 12 months after Royal Assent;
- establishing and maintaining an AML/CTF program obligations commenced 12 months after Royal Assent; and
- ongoing customer due diligence and reporting (suspicious matters, threshold transactions and international funds transfer instructions) started 24 months after Royal Assent.

(b) Implications for Solicitors

The scope of those enterprises subject to the first tranche obligations has been somewhat unclear.

Austrac has published guidance notes which would indicate that lawyers generally were not intended to be subject to these first cut of obligations but where practices hold an Australian Financial Services License or deal with financial securities as an agent of person such obligations may arise. Practitioners would be well advised to review the existing legislation to ensure their activities do not give rise to these reporting requirements.

Due to an anomaly in the AML / CTF Act there has also been some concern that practitioners were required to submit compliance reports to AUSTRAC because some legal services inadvertently fall within the ambit of:

- items 31 and 32 (receiving or making property available under a designated remittance arrangement)
- items 46 and 47 (providing a custodial or depository service).

In order to clarify the position AUSTRAC introduced Chapter 23 of the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1), which relevantly included:-

23.2 For subparagraphs 10(1)(a)(v) and 10(1)(b)(v) of the AML/CTF Act1, the following persons are specified:

(1) a person who in the course of carrying on a law practice, accepts money or property from a transferor entity to be transferred under a designated remittance arrangement and/or makes money or property available to an ultimate transferee entity as a result of a transfer under a designated remittance arrangement; and

23.3 In this Chapter:

(2) 'law practice' means a business carried out by either of the following:

(a) a legal practitioner (however described) that supplies professional legal services; or
(b) a partnership or company that uses legal practitioners (however described) to supply professional legal services.

This rule is understood to give effect to the intention of AUSTRAC that persons simply operating a legal practice are not expected to report transactions.

1.3 Current developments

(a) Status of Tranche 2 Reforms

With the first tranche of the legislation passed and commencing implementation Government attention turned to the second tranche of obligations which were to be focused on certain professions, including legal practitioners. The Attorney-General’s Department announced in July 2007 that the following sectors would be affected by the second tranche of the legislation:

- lawyers, notaries, other independent legal professionals and accountants when preparing for or carrying out certain transactions;
- real estate agents in relation to buying and selling of real estate;
- dealers in precious metals and stones engaged in transactions above a designated threshold; and
- trust and company service providers when they prepare for or carry out for a client the certain transactions

Government consultation commenced on the composition of the second tranche in the latter half of 2007 with various bodies on some very preliminary draft amendments. The Law Council of Australia made a detailed submission on the initial proposals which is informative and available at:


However, the processes of consultation were delayed by the Federal Election and with a change of Government Neil Jensen, chief executive of Austrac was quoted in The Age on 12 December 2007 saying that the process had stopped until the new Government decides what its policy is as regards the second tranche.

During March and April this year, officers from the Attorney-General’s Department and AUSTRAC met with industry stakeholders, including the Law Council to commence discussions on what AML/CTF obligations will apply. On 20 May 2008, the Minister for Home Affairs chaired a meeting of the AML/CTF Council (which included representatives of the Law Council of Australia) to resume ministerial level consultation and to engage again with industry.

It is anticipated that the tranche 2 reforms will be implemented with a staggered implementation period of at least two years, but without a “non prosecution period”. 

1 When an arrangement is not a designated remittance arrangement for the purposes of the AML / CTF Act
1.4 Likely elements in and impact of Tranche 2 legislation

Tranche 2 legislation will be likely to implement the FATF recommendations, or at least a substantial part of them, as they relate to Non Financial Business & Professions.

Recommendations 12 and 16 apply record keeping, customer due diligence obligations and suspicious transaction reporting requirements to Non Financial Business & Professions and in particular to lawyers when they prepare for or carry out transactions for their clients concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

However according to Recommendation 16 lawyers are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. Note this is a different threshold than merely being information confidential to the client.

It is anticipated that the second tranche legislation will facilitate some or all of the following FATF recommendations:

Recommendation 5 – Customer Due Diligence

A legal practice should not keep anonymous accounts or accounts in obviously fictitious names.

A legal practice should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions:
  - (i) above an applicable designated threshold; or
  - (ii) that are special wire transfers;
- there is a suspicion of money laundering or terrorist financing; or
- the legal practice has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

(a) Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the legal practice is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include the legal practice taking reasonable measures to understand the ownership and control structure of the customer.

(c) Obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

A legal practice should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, a legal practice should perform enhanced due diligence.

A legal practice should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. A legal practice may be permitted to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the legal practice is unable to comply with paragraphs (a) to (c) above, it should not act for the client and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though a legal practice should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

Recommendation 6 – Politically Exposed Persons

A legal practice should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.

b) Obtain senior management approval for establishing business relationships with such customers.
c) Take reasonable measures to establish the source of wealth and source of funds.

d) Conduct enhanced ongoing monitoring of the business relationship.

Recommendation 8 – Distant Clients

A legal practice should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, a legal practice should have policies and procedures in place to address any specific risks associated with non-face-to-face clients.

Recommendation 9 – Third Party Customer Due Diligence Providers

Countries may permit a legal practice to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the legal practice relying on the third party.

The criteria that should be met are as follows:

(a) legal practice relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. A legal practice should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(b) The legal practice should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

Recommendation 10 – Record Keeping

A legal practice should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

A legal practice should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

Recommendation 11 – Recording Suspicious Transactions

A legal practice should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

Recommendation 13 – Suspicious Transaction Reporting

If a legal practice suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

Recommendation 14 – Secrecy of Reporting

A legal practice, their directors, officers and employees should be:

(a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

(b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

Recommendation 15 – AML / CTF Programmes

A legal practice should develop programmes against money laundering and terrorist financing. These programmes should include:

(a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

(b) An ongoing employee training programme.

(c) An audit function to test the system.
Recommendation 21 – Special Treatment of Certain Countries

A legal practice should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

1.5 Offences, Sanctions & other risks

There are two major sources of offences and sanctions relating to money laundering and similar activity. The AML / CTF Act contains many offences and sanctions associated with compliance and enforcement with the report regime and other act requirements. The Commonwealth Criminal Code contains offences relating to the actual conduct of money laundering.

Division 400 of the Commonwealth Criminal Code relates to money laundering offences and provides numerous offences for dealing with money or property that is or is likely to become proceeds or an instrument of crime. For example in section 400.3 for money or property with a value of $1,000,000:

- Knowingly dealing with the proceeds of crime has a maximum imprisonment of 25 years or a fine of 1500 penalty units, or both;
- Recklessly dealing with the proceeds of crime has a maximum imprisonment of 12 years or a fine of 720 penalty units, or both; and
- Negligently dealing with the proceeds of crime has a maximum imprisonment of 5 years or a fine of 300 penalty units, or both.

While there are stepped offences for dealing with the proceeds of crime relating to the value of property the AML / CTF Act provides for a maximum imprisonment of 12 months for negligently dealing with $1,000 which is the proceeds of crime [section 400.7(3)].

For the purposes of the Criminal Code dealing with money or other property is defined as:-

- receiving, possessing, concealing or disposing of money or other property; or
- importing money or other property into, or exporting money or other property from, Australia; and
- the money or other property is proceeds of crime, or could become an instrument of crime, in relation to an indictable offence.

While presently legal practitioners have not been the subject of conviction under these laws in Australia, in the United Kingdom there are examples of solicitors receiving custodial sentences for failing to disclose to the authorities:

R v Mc Cartan [2004] NICA 43 solicitor Gavin David McCartan convicted of failing to disclose information, contrary to article 44 of the Proceeds of Crime (Northern Ireland) Order 1996 and using a false instrument, contrary to section 3 of the Forgery and Counterfeiting Act 1981 and was sentenced to two concurrent terms of imprisonment of six months and two months.

R v Duff [2002] EWCA Crim 2117 solicitor Jonathan Michael DUFF convicted of failing to disclose knowledge or suspicion of money laundering contrary to section 52(1) of the Drug Trafficking Act 1994 and sentenced to six months imprisonment.

R v Griffiths [2006] EWCA Crim 2155 solicitor Philip John Griffith was convicted of failing to disclose to the authorities that he knew or suspected that a money laundering offence was taking place and was convicted to 15 months imprisonment which was reduced to 6 months on appeal.

The AML / CTF Act itself contains offences and sanctions relating to compliance with the obligations it imposes upon businesses and individuals performing ‘designated services’. The Act takes two approaches to sanctions including both offences and civil penalty provisions.

Offences are included in Part 12 and include up to ten years imprisonment² for:

- producing false or misleading information;
- producing a false or misleading document;
- making or possessing a false document; and
- making or possessing a equipment for making false documents.

Five year imprisonment offences³ exist for:-

- Conducting transactions so as to avoid reporting requirements relating to threshold transactions; and
- Conducting transfers so as to avoid reporting requirements relating to cross-border movements of physical currency.

---

² AML / CTF Act sections 136 - 138
³ AML / CTF Act sections 142 & 143
Two year imprisonment offences exist for providing or receiving a designated service using false customer names or ensuring customer anonymity.

Civil penalty provisions exist throughout the AML / CTF Act with respect to detailed compliance issues relating to issues, including:

- Carrying out the applicable customer identification procedures before the commencement of the provision of a designated service;
- Conducting ongoing customer due diligence;
- Reporting entity must have an anti-money laundering and counter-terrorism financing program;
- Retaining transaction records;
- Retention of records of identification procedures;
- Retention of records about electronic funds transfer instructions; and
- Conducting money laundering and terrorism financing risk assessments.

Tipping Off

Another serious risk for practitioners is ‘tipping off’ – a criminal offence with a potential penalty of 2 years imprisonment. Practitioners must not disclose to a client that a suspicious matter report has been made to AUSTRAC, that a suspicion has been formed, or disclose any information that may assist a practitioner to infer that a suspicion has been formed.

These requirements pose a particular challenge for practitioners because it will often be necessary to ask legitimate questions or seek additional information from clients to check the risk profile of a matter before a suspicion is formed. This should be clearly distinguished, however, from disclosing any information, or asking additional questions that may lead a client to infer that a suspicion has been formed.

Lawyers and staff need to be trained on this issue, and arrangements implemented as required. A common approach is to consistently attempt to gain as much relevant information as possible from the client at the start of the matter - ‘as standard’. This addresses risk management issues, limits the need or temptation for additional questions when suspicions have been formed, and also offers reassurance to the client that all questions are standard, and are not led by any suspicions. Another common arrangement is to restrict any knowledge of a suspicion or a suspicious transaction report to only those who ‘need to know’. Best practice may be to remove, or keep separate from client files, report investigations or other documentation concerning suspicions.

1.6 Money Laundering Warning Signs

The second tranche of AML legislation will require solicitors to conduct ongoing monitoring of business relationships and to take steps to ensure that they identify and as necessary report clients or transactions that carry a greater risk of money-laundering or counter-terrorist financing.

---

4 AML / CTF Act sections 139 - 141
Although different practices will face different risks, below are some key factors which may heighten a client’s risk profile or raise suspicions:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
<th>Suggested Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large quantities of cash</td>
<td>Large quantities of cash are one of the most obvious signs of potential money laundering.</td>
<td><strong>Suggested Risk Management:</strong> develop policies on handling cash: place a $ limit on how much cash can be accepted.</td>
</tr>
<tr>
<td>Secretive clients</td>
<td>Although high levels of client contact or in-depth understanding of their business activities is not always necessary, unusually secretive or obstructive clients might give cause for concern.</td>
<td><strong>RM:</strong> If a client appears unusually or unnecessarily secretive, consider whether you are comfortable continuing to act for them.</td>
</tr>
<tr>
<td>Unusual or unexpected sources of funding or settlement requests</td>
<td>Related transactions will often be funded and settled in similar ways – home purchases for instance might commonly be financed by a mix of mortgage, deposit and proceeds from the sale of a current property. Transactions that are funded through an unusual source or unusual mix of sources might be considered suspicious. Particular attention should be given to private funding, funds from an unrelated 3rd party, and direct payments between buyers &amp; sellers.</td>
<td><strong>RM:</strong> Implement processes to check the source of funds. Do they come from the client? Similarly with settlements: where is the money going and why?</td>
</tr>
<tr>
<td>Unusual or unnecessarily complicated business structures or transaction paths</td>
<td>Any business structures or transaction paths which seem unnecessarily complicated, or that the client fails to adequately explain, should be treated as suspicious: what is the client trying to hide?</td>
<td><strong>RM:</strong> Discuss all arrangements with the clients. Ask them to justify or explain arrangements</td>
</tr>
<tr>
<td>Loss-making or mis-valued transactions</td>
<td>An unusual transaction value can be an indication of money laundering. Any transactions where the ultimate value is either significantly more or significantly less than what you might expect should be treated as suspicious.</td>
<td><strong>RM:</strong> Ask how the client has valued the assets being traded. Is there a logical explanation for the discrepancy between the market and actual value of the transaction.</td>
</tr>
<tr>
<td>Litigation matters that are settled too easily</td>
<td>As with transactions, litigation matters that are settled for a value either significantly above or below what you might normally expect should be treated as suspicious.</td>
<td><strong>RM:</strong> Ask your client to justify their approach to the settlement.</td>
</tr>
<tr>
<td>Suspect territories</td>
<td>Transactions involving some territories or jurisdictions may heighten the risk profile of those transactions</td>
<td><strong>RM:</strong> The International Bar Association provides a summary of money laundering legislation around the world at <a href="http://www.anti-moneylaundering.org">www.anti-moneylaundering.org</a> This will help you assess the money-laundering risks associated with different territories.</td>
</tr>
<tr>
<td>Unexplained changes in instructions or business entities</td>
<td>Any changes that have no logical explanation, or that the client fails to explain sufficiently should be treated as suspicious.</td>
<td><strong>RM:</strong> Ask the client to explain or justify the recent changes</td>
</tr>
<tr>
<td>Instructions outside your normal geographic area, area of expertise, or client market</td>
<td>Often clients will choose a law practice specifically because they do not have any knowledge of the client or entities involved, or because they will not ask too many tricky questions.</td>
<td><strong>RM:</strong> Don’t dabble: stick to what you know. Distribute lists of work the practice will and will not undertake. Ask yourself: why is this client instructing me?</td>
</tr>
<tr>
<td>Clients wanting to take ‘short-cuts’ or forego standard processes or activities</td>
<td>Clients that request or apply pressure on solicitors to miss out key stages of a transaction, such as due diligence, may be attempting to hide or disguise evidence of criminal activity, and such transactions therefore might be considered suspicious.</td>
<td><strong>RM:</strong> Ask the client to explain their approach and consider if you are happy accepting such instructions.</td>
</tr>
</tbody>
</table>
1.7 Implementing AML Compliance arrangements

Although the legislation is not yet released, it is likely that the compliance requirements for solicitors in Australia will be similar to the requirements under tranche 1, reflecting the FATF Forty recommendations and comparable to compliance regimes in other jurisdictions.

- A risk based approach to AML
- Initial client identification and ongoing client due diligence
- Record keeping
- Auditing
- Employee training programs
- The nomination of an anti-money laundering compliance officer (AMLCO); and
- Suspicious matter reporting.

(a) A risk based approach to AML

The regulations are likely to require practices to take steps to be aware of transactions with heightened money laundering or terrorist financing risks. While guidance will highlight common risks, practices will need to identify the risks specific to their practice areas and client groupings, and then to manage and mitigate and risks arising.

As with other risk management, a risk based approach to AML involves four stages:

| Identification | Identifying the potential ML/TF risks specific to the practice – focussing both on client-related and matter-related risks. |
| Analysis       | Understanding the risks. High risk or low risk? |
| Management     | Designing and implementing arrangements (policies, processes, procedures) that limit the impact or likelihood of risks materialising. |
| Review         | Are the arrangements we have implemented effective? Could they be improved? Is everyone following the agreed procedures? Are we addressing all the risks? |

This process should result in the implementation of a number of effective risk management arrangements, which in addition to the formal requirements might or might not include:

- Policies on the handling of cash e.g. $ limits
- Opening and closing risk assessments in relation to money laundering
- Internal reporting or referral arrangements re AML suspicions
- Checks on funding sources and settlement destinations
- Transaction value thresholds
- Restricted access to account details to prevent unsanctioned deposits

For other practices, however, compliance will be a significant task, requiring significant attention and necessitating a cultural change that can later be built on with other beneficial risk management or practice management arrangements. Research from the UK has found that compliance has been a particular burden for sole practitioners and smaller practices, but that the implementation of AML arrangements has led to a greater focus on general client engagement arrangements which has itself led to fewer negligence claims.

(b) Initial client identification and ongoing client due diligence

Practices will have to develop appropriate processes for checking the identity of clients and for the recording of relevant customer information. Arrangements will vary between individuals, charities, government and different corporate entities, between new or repeat clients, and there might need to be additional checks on, for example, overseas clients. Internal guidelines should be developed on what forms of identity are acceptable in what circumstances, and initial arrangements implemented to ensure these arrangements are consistently observed.
The introduction of client due diligence requirements is likely to contribute significantly to the general risk management strategies of law practices. Data from legal insurers shows that high percentages of claims and complaints could have been avoided if practices had more robust client selection and acceptance policies. In addition to conflicts of interest considerations, a number of claims arise out of failing to adequately define the identify of the client, and from filing to identify the risks associated with specific clients and transactions.

(c) Record keeping
Practices will be required to maintain records of identity, transaction details and any AML suspicions of reports for a number of years. This might require changes to a practice’s file management and archiving arrangements, but for many practices will only reinforce the importance of existing requirements and practices.

The Act specifies that records must be kept for 7 years, which mirrors current requirements in most States. It is important to note, however, that the 7 years requirement applies for the life of the customer relationship plus an additional seven years. In many instances, therefore, files and records, and specifically client identification records, will need to be kept for significantly longer than 7 years.

(d) Auditing
Practice AML arrangements should be reviewed and audited on a regular basis, and any new arrangements implemented as required. It might be appropriate to develop new processes, new forms, new policies etc. on issues such as identification requirements, tipping off risks, the acceptance of cash, transaction value thresholds etc. Audits can be conducted by either internal or external auditors.

As with a number of the AML compliance requirements, many practices will already have implemented auditing requirements as part of the risk management strategies. Specifically, practices that undertake regular file audits will be able to check files for AML compliance in relation to, for instance:

- Initial AML risk assessment
- Client identification records
- Any noted suspicions
- Any necessary checks on funding sources or settlements
- Closing matter AML risk assessment.

Practices should aim to produce an annual documented AML audit report based on either ongoing audit activities throughout the year and/or a single comprehensive audit of all arrangements and the practices compliance with both the requirements of the legislation and their own stated arrangements.

(e) Employee training programs
Compliance will be an issue for all staff, who should be trained on the issues, risks, internal procedures and consequences of non-compliance. All staff applies to support staff as well as fee-earning staff because it is not uncommon for criminals or launderers to circumvent practitioners by dealing directly with accounts or other support staff.

To be effective, AML training should be included as a part of all induction programs, and should be repeated on a regular basis, with supporting guidance or reference materials provided as required.

(f) The nomination of AML compliance officer (AMLCO)
Practices will need to identify one person with specific responsibility for ensuring that satisfactory internal AML procedures are maintained, ensuring that internal suspicions are raised, and ensuring that notifications are made or appropriate action taken.

This is a key position for any practice, and practices should aim to nominate a senior person who knows and understands the AML risk profile of the practice, and who has the authority to take the appropriate action – whether making suspicious transaction reports or declining instructions – as required.

(g) Suspicious transaction reporting
Practices will be required to report any reasonable money laundering suspicions to AUSTRAC. Practices should therefore ensure that appropriate arrangements are in place to define reasonable suspicions, define how suspicions are raised and handled internally, and how any suspicions are reported.

Suspicious transaction reporting obligations arise when a reporting entity (the legal practice) provides, offers to provide, or is requested to provide, a designated service. If the practice has reasonable grounds for suspicion, it must formally contact AUSTRAC within 24 hours for terrorist financing matters and 3 days for all other matters.

What must be reported includes:

- A person who is not who they claim to be;
- Having information likely to be of relevance to an investigation or prosecution of a person for an evasion, or an attempted evasion of Commonwealth, State or territory taxation law;
- Having information likely to be of relevance to an investigation or prosecution of a person for an offence against a Commonwealth, State or Territory law; and
- Information that may be of assistance in the enforcement of the Proceeds of Crime Act 2002; or a State or Territory equivalent.
1.8 Client Confidentiality & Legal Professional Privilege

One of the key issues to be resolved with the introduction of tranche 2 of anti-money laundering legislation is how the requirement for suspicious transaction reporting will affect laws and rules relating to client confidentiality and legal professional privilege.

Section 242 of the current legislation states that the Act does not affect the law relating to legal professional privilege, suggesting that a legal practice may not be compelled to make reports that are based on information subject to legal professional privilege.

That, however, might not be the end of the matter. Legal professional privilege has a narrower application than client confidentiality, and the experience of the UK was that the application of privilege was not as wide as many solicitors thought. If the information came to a practitioner in privileged circumstances, it might not be necessary to report a suspicious transaction, but it is rarely a simple matter to decide if information was provided in privileged circumstances.

Practitioners should seek guidance from their respective professional bodies on the application of privilege in different circumstances. As with the UK and other jurisdictions, the application of privilege in relation to AML legislation might be an issue which is only given greater clarity by subsequent court cases following the release of any legislation.

The different State professional bodies have based their rules on confidentiality, in their respective Conduct Rules, on the Law Council of Australia's 'Model Rules of Professional Conduct and Practice'.

Rule 3 states that:

3.1 A practitioner must never disclose to any person, who is not a partner, director or employee of the practitioner’s firm any information, which is confidential to a client and acquired by the practitioner or by the practitioner’s firm during the client engagement, unless:

3.1.2 the practitioner is permitted or compelled by law to disclose;

The rules on client confidentiality do not, therefore, exempt practitioners from AML reporting obligations. Whilst legal professional privilege may exempt practitioners from reporting obligations, practitioners will need to develop a good understanding of when information was provided in privileged circumstances, and when legal professional privilege applies.

1.9 Regulation

The principal AML/CTF regulator under the existing legislation will be AUSTRAC – the Australian Transaction Reports and Analysis Centre. In addition to receiving suspicious transaction reports, AUSTRAC will also be able to:

- Appoint external auditors to assess reporting entities’ risk management and compliance;
- Require annual compliance reports;
- Issue remedial directions to reporting entities; and
- Enter into enforceable undertakings with reporting entities.

It is currently uncertain the extent to which AUSTRAC will seek to use their powers in relation to audits and requiring annual compliance reports.

There has been discussion as to whether AUSTRAC will be the most effective regulator of the profession, and what the role of State professional bodies (the State Law Societies) should be. Although the State Law Societies currently have oversight of trust account regulations, and there is an argument that such expertise should be used, there are also concerns about both the funding of regulatory resources and the potential conflict between adopting AML regulatory roles whilst also pursuing an advocacy role and lobbying for change in the legislation.

The State Law Societies are currently neither pursuing nor expecting any active AML regulatory role, and there are no plans for State Law Societies to take an intermediary role in suspicious transaction reporting. Instead the State Law Societies will focus on providing education, guidance and support to practitioners in relation to anti-money laundering. The second tranche of AML legislation is, however, likely to impact on existing trust account regulation, and in future, the State Law Society’s might also consider amending their Conduct Rules to address AML/CTF compliance.

Other potential regulators are the different State Legal Services Commissioners or Boards, who might or might not seek some formal regulatory role in relation to AML. They could potentially seek an intermediary role in relation to suspicious transaction reporting, or could seek other regulatory powers. The Legal Services Commissions and Boards currently audit the management systems of incorporated legal practices, and may in future take the same responsibility for all practices. It would be a simple step for the Legal Services Commissions and Boards to add a requirement for AML management systems to the existing ‘ten commandments’ and thus to audit AML compliance, initially of incorporated legal practices but potentially of all legal practices.
Further Reading
Practitioners may find the following resources of interest to read further on this topic:

QLS AML / CTF Information Page (Members Only)
https://www.qls.com.au/content/lwp/wcm/myconnect/QLS/For+the+Profession/Resources+for+Practitioners/Anti-Money+Laundering

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Draft Table of Second Tranche Designated Services

LCA Brief on AML / CTF Laws, October 2007

Law Society of England & Wales’ Anti-Money Laundering Practice note
http://www.lawsociety.org.uk/productsandservices/practicenotes/aml.page

Commonwealth Attorney-General’s AML Page

AUSTRAC’s AML Page

Financial Action Task Force (FATF)
http://www.fatf-gafi.org/

The Asia/Pacific Group on Money Laundering
http://www.apgml.org/

International Money Laundering Information Network
http://www.imolin.org/imolin/index.html

Consultation on New Zealand AML Reforms

NZ Law Society Article on NZ AML Reforms

Canadian Model Rule on Client Identification and Verification Requirements

Upper Canada Law Society News Article on Canadian AML Reforms