

Financial Services Alert

June 2007

Anti-Money Laundering & Counter Terrorism Financing Explained.....

“ This wave of legislation brings with it a whole suite of changes in the way your business will interact with your customers in the provision of your designated services. It is imperative that you now review your list of designated services carefully and assess whether these changes affect you. ”

Background

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (“AML/CTF Act”) became law on 12 December 2006. Its introduction is aimed at matching international best practice standards on anti-money laundering and counter-terrorism by the international body, the Financial Action Task Force (“FATF”) so as to enable Australia’s financial sector to maintain its international business relationships and preserve its financial market reputation.

Australia is a founding member of FATF and has committed to a process of periodic peer assessment by other members. It was among the first group of countries to be evaluated against these standards. Its peer report which was released in October 2005 found, as one of its key findings, that the then current legislative framework in Australia was inadequate in the area of customer due diligence.

The Explanatory Memorandum to the AML/CTF Act states that this legislation seeks to address

this inadequacy. It also states that the legislation seeks to implement a fair and balanced framework in order to ensure that money laundering and terrorist financing risks in Australia are adequately identified, managed and mitigated in a dynamic market characterised by electronic commerce and non-face to face transactions.

Apart from the security risks inherent in not having such a framework, there is also an economic cost. The International Monetary Fund in 1996 estimated that the aggregate size of money laundering in the world would be somewhere between 2% and 5% of the world’s GDP. For the Australian economy this is estimated to be about \$11.5 billion per year.

The Framework

The legislative framework consists of the AML/CTF Act, Regulations, AML/CTF Rules and Guidance Notes. The AML/CTF Act contains the general principles and high level obligations. Regulations will be made under the Act which will deal with some technical



issues. AML/CTF Rules issued under the AML/CTF Act (and so legally binding) will flesh out the detail of the required obligations and will be prepared following previous consultation between the government body responsible for the administration of the AML/CTF Act, (The Australian Transaction Reports and Analysis Centre also known as AUSTRAC), industry and others and then formally registered. Finally, AUSTRAC will issue non-binding Guidance Notes.

The new legislation has a wider application than the existing financial transaction reporting legislation, the Financial Transactions Reports Act 1988 ("FTR Act"), as it applies to "reporting entities", being individuals and businesses who provide "designated services", and not just to cash dealers and ADIs. It will also impose a wider range of obligations than the FTR Act. This legislation is being introduced in parts and will gradually phase out the requirements of the FTR Act over a period of two years.

What are designated services?

Examples of designated services include:

- > opening an account with a bank, building society, credit union or cash management trust;

- > effecting a transaction in relation to such an account;
- > making a loan in the course of carrying on of a loans business;
- > supplying goods by way of a lease under a finance lease or hire purchase agreement (where the goods are not acquired by a consumer and where the supply is in the course of carrying on a finance leasing business);
- > issuing or selling a security (which includes shares, debentures and interests in managed investment schemes) or derivative;
- > sending and receiving electronic funds transfer instructions;
- > issuing a promissory note or letter of credit;
- > issuing a debit or stored value card; and
- > accepting a contribution or rollover in respect of a member of a superannuation fund.

This is not an exhaustive list. There are other designated services relating to specifically the gambling industry and bullion dealers which are captured by the AML/CTF Act.

In general, designated services are limited to those services which are carried on in the course of providing core activities of a business.



Who will be affected?

Individuals and businesses who will be affected because of the core services they provide include:

- > ADIs;
- > banks;
- > building societies;
- > credit unions;
- > non-bank lenders;
- > issuers of travellers cheques and currency exchange businesses;
- > issuers of stored value cards;
- > money remitters;
- > finance companies;
- > factoring businesses;



- > commercial leasing businesses;
- > fund managers (who offer debit arrangements);
- > securities and derivatives/brokering intermediaries;
- > issuers of securities and derivatives (other than where the issuer is a company, in respect of shares and options in that company);
- > life insurers;
- > providers of pensions and annuities;
- > trustees of superannuation funds (other than self-managed funds);
- > finance and mortgage brokers;
- > providers of custodial or depository services;
- > dealers in physical currency; and
- > holders of an Australian Financial Services Licence ("AFSL") which make arrangements for a person to receive designated services (eg financial planners including investment advisers).

Due to the distributional role that financial planners play in the finance sector they will be

subject to customer identification obligations under the legislation when they make arrangements for a person to receive a designated service. However, their obligations will, in general, be limited to customer identification, record keeping and suspicious matter reporting.

Geographical link

The AML/CTF Act will apply to providers of designated services at or through a permanent establishment in Australia. Certain provisions of the AML/CTF Act will also apply to Australian residents (and if they are a company, their subsidiaries) who provide designated services at, or through, a permanent establishment in a foreign country.



Action required by you

If you operate in any of the core businesses described above, and you have not already done so, it is imperative that you now review the list of designated

services carefully and assess whether you are a reporting entity. This is because if you are a reporting entity, the AML/CTF Act will introduce (as from 12 December this year) either new, or fundamental changes to your compliance and reporting obligations with AUSTRAC, as well as impose new identification and verification procedural requirements which will impact on the way you interact with your customers.

You will also need to take immediate steps to have your AML/CTF Program established in time for 12 December this year.

The AML/CTF Act imposes serious civil penalties (fines up to \$11 million in the case of body corporates and \$2.2 million for all other persons) and in some cases, criminal penalties. The Government has indicated that it will not prosecute for a period of 15 months after the introduction of each stage of the AML/CTF Act, however, this amnesty will only be afforded to you if you have made a genuine attempt to comply with the legislation during this period.

Key requirements

Set out below is a summary of the key requirements of these new or changed compliance and reporting obligations together with an overview of the customer identification and verification procedures which will apply to reporting entities.



Establishment of AML/CTF programs - commencing on 12 December 2007

If you are a reporting entity you must establish an AML/CTF Program in relation to the provision of your designated services. The AML/CTF Rules registered on 13 April 2007 ("Rules") set out the requirements with which the Program must comply.

A "standard " AML/CTF Program must have two parts.

- > **Part A** must be designed to identify, mitigate and manage ML/TF risk. This is defined in the Rules as the risk that a reporting entity may reasonably face that the provision of its designated services might (whether inadvertently or otherwise) involve or facilitate money laundering or the financing of terrorism.

Essentially this part must include appropriate risk-based systems and controls ("Systems") to assess ML/TF risk associated with the provision of your products and services. What these Systems should entail, depends on the nature, size and complexity of your business and the type of ML/TF risk that you might reasonably face. The Rules state that in identifying this risk you must consider your customer types, the type of designated services you provide, the methods by which you deliver these services and the foreign jurisdictions with which you deal. Following identification of the risk, you must analyse the risk to determine the likelihood of the risk occurring, then determine and put in place any necessary controls to manage the risk and finally put in place procedures to monitor residual risk and to report risk.

Part A must include an employee risk awareness training program. In addition, this part of the Program must contain an employee due diligence program to determine whether, and in what manner, you should screen prospective employees who may be in a position to

facilitate the commission of money laundering or financing of terrorism offences in connection with your designated services. If you outsource the provision of your designated services, this part should also contain a program for the training and monitoring of any third party agents.

In respect of Programs for permanent establishments in foreign countries, there are some exceptions from this Part including in relation to employee training and employee due diligence.

- > **Part B** of the Program must set out Systems to enable you to be reasonably satisfied that your customer or their agent is who they claim to be or, in the case of a customer who is not an individual, that the entity exists and that you have been provided with certain prescribed information about beneficial ownership of that entity. These Systems must include procedures to collect, as a minimum, the prescribed know your customer information ("KYC information") and also include measures to determine whether in addition to this minimum information, additional KYC information should



be collected. The Rules contain a definition of KYC information which is not intended to be exhaustive. The KYC information differs according to whether the customer is an individual, a company, a trust, a partnership, association, government body or registered co-operative (see below for examples in the case of an individual and company).

Part B of the program must also include verification procedures based on reliable and independent documentation or electronic data or a combination of both, and Systems to respond to any discrepancy that arises in the course of you verifying customer information.

It should be noted that when you collect any customer information or deal with any employee information the requirements of applicable Privacy Act legislation must still be complied with.

New rules for collection and verification of KYC information commencing 12 December 2007

Reporting entities will be required to collect KYC information and verify a customer's identity before providing the customer with the designated service.

Existing customers (that is persons who become your customers before 12 December 2007), will be exempt from the identification requirement of the AML/CTF Act although they will be subject to on-going customer due diligence rules (see below). All new customers will be required to verify their identity. For new customers of banks and some financial institutions this will impose similar requirements as currently imposed under the FTR Act. Customer identification and verification obligations will be new for new customers in other sectors.

The AML/CTF Act may in the future specify low risk services for which a customer will not need to be initially identified. At present none have been specified.

The appropriate identification and verification procedures will depend upon the level of ML/TF risk (low, medium or high) that the new customer poses as identified by the reporting entity under Part B of its Program as explained above.



Safe harbour procedure for individuals

If a customer is identified by the reporting entity as a medium to lower ML/TF risk and is an individual, the reporting entity may adopt the document or electronic based safe-harbour procedure prescribed under the Rules.

This involves :

- > collecting the minimum prescribed KYC information from a customer – being the individual's full name, date of birth, residential address and in the case of individual who is a sole trader, the full business name of business, its principal place of business and any ABN issued to the customer;
- > verifying the information from an original or certified copy of a primary photographic identification document or both an original or certified copy of a primary non-photographic identification document and a secondary identification document; and
- > verifying that the documentation has not expired.

In the case of electronic data the KYC information is to be verified using reliable and independent



electronic data from at least 2 separate data sources and either obtaining the customer's date of birth using reliable and independent electronic data from at least one data source or verifying that the customer has a transaction history for at least the past 3 years.

Where a customer is a domestic company, the minimum prescribed KYC information which must be collected is the name of the company as registered by ASIC, its registered office, principal place of business, ACN, whether it is a public or pty ltd company and, in the case of a pty ltd company, the name of each director and its beneficial owners (being any individual who owns through one or more shareholdings more than 25% of the issued share capital).

Compliance reporting - commencing 12 June 2007 for the period ended December 2008

If you are a reporting entity, you must at the end of the reporting period specified by the AML/CTF Rules, provide the AUSTRAC CEO with a prescribed report relating to your compliance with the AML/CTF Act, the AML/CTF Rules and the regulations. The AML/CTF Rules relating to these compliance reports have yet to be made, however the reporting period is expected to end on December 2008.

Reporting entities which are banks must also keep records about the due diligence assessments of correspondent banking relationships from 12 June 2007.



Transaction reporting obligations - commencing on 12 December 2008

As a reporting entity, you will be required to report the transactions below to AUSTRAC in respect of your designated services within specified time frames if the applicable circumstances arise:

> **Transactions over the threshold amount:** If you provide a designated service to a customer that involves a threshold transaction (being a transfer of not less than \$10,000 of physical currency or e-currency or an amount of money or property of a value specified in the regulations) you must report this transaction to the AUSTRAC CEO within 10 business days after the transaction takes place.

> **Suspicious matters such as financing of terrorism:** If you suspect, based on reasonable grounds that:

- your customer or your customer's agent is not the person that they claim to be; or
- that information you hold concerning the provision or prospective provision of your designated service may be relevant to

(a) the investigation or prosecution of the evasion of taxation laws or the commission of a crime or offence under Australian laws including financing of terrorism offences or money laundering offences; or

(b) of assistance in the enforcement of Proceeds of Crime laws; or

(c) that the provision or prospective of the service is preparatory to the commission of financing of terrorism offences or money laundering offences,

you must give the AUSTRAC CEO a report about the matter in the



prescribed form within 3 business days of forming the relevant suspicion or within 24 hours if the matter relates to the financing of terrorism offences.

Tipping off offences will apply and you must not disclose to your customer or their agent that you have formed an applicable suspicion or reported information to AUSTRAC.

- > **International funds transfer instructions:** If you are an institution which sends or receives international funds transfer instructions (these include designated remittance arrangements) into or out of Australia, you must report these instructions to AUSTRAC from 12 December 2008. The regulations may specify a threshold reporting amount.

Ongoing customer due diligence - commencing 12 December 2008

As a reporting entity you must continue to monitor your customers from 12 December 2008 with a view to identifying, mitigating and managing ML/TF risk in accordance with the AML/CTF Rules. The rules on ongoing due diligence are yet to be made.

Current operative provisions

Movements of bearer instruments/currency, electronic funds transfer information and registration of providers of designated remittance services.

Provisions of the AML/CTF Act, which have been operative since December 2006, relate to individuals having to report the movements of bearer negotiable instruments and \$10,000 currency into or out of Australia, the requirement that all institutions which send and receive electronic fund transfer instructions must now include complete payor information (and provide this information to the AUSTRAC CEO on request), and compulsory registration of the providers of designated remittance services with AUSTRAC.

With respect to this registration requirement, a person (other than an ADI, bank, building society, or credit union) will need to be registered if they accept money or property from one party to transfer to another party (not being an ADI, bank, building society or credit union). Examples of designated remittance arrangements given in the Explanatory Memorandum to the AML/CTF Act include hawala, hundi, fei-chien and the black market peso exchange.

However, this definition is very wide and would, on a literal interpretation, capture all remittance type arrangements other than those specifically excluded. AUSTRAC has stated that it will release guidelines soon which will hopefully clarify this requirement. They also encourage making application to them for a determination if registration is required where there is any doubt.



AUSTRAC

AUSTRAC has an enhanced regulatory role under this legislation and is required to advise and assist reporting entities with their obligations under the AML/CTF Act. It has announced that it will implement several education initiatives including an expanded advisory visit program, workplan and seminars as from April 2007, as well as web based learning products progressively from September 2007.

The AUSTRAC CEO is charged with monitoring compliance by reporting entities with their obligations with the AML/CTF



Act, regulations and AML/CTF Rules. He or she may give a remedial direction and may accept enforceable undertakings or require the reporting entities to carry out an external audit or assessment. AUSTRAC has stated that it will adopt a co-operative approach before formal intervention but does plan to conduct surveillance including on-site inspections, desk audits, annual consultations as well as liaison with other Regulators including ASIC and APRA.

Certain designated government agencies will be able to access information held by AUSTRAC for relevant law enforcement and security functions relating to money laundering and terrorist

financing. Except as permitted by the AML/CTF Act, no officer may disclose information or documentation obtained under the AML/CTF Act.

In summary - what this means to you

This wave of legislation brings with it a whole suite of changes in the way your business will interact with your customers in the provision of your designated services. The Government has determined that you, as a reporting entity, are at the frontline and must take steps to ensure that you do not facilitate money laundering or terrorism financing.

Future changes

A second tranche of legislation (draft to be released in 2008) will seek to cover real estate agents, jewellers and, in relation to a range of non-financial services, lawyers and accountants.

There is a planned review of the legislation in 7 years time just after the planned second FATF peer review of Australia in 6 years time.

Jill Milburn - Partner

+61 2 8248 3416

jmilburn@thomsonplayford.com.au

Jade Ng - Lawyer

+61 2 8248 3423

jng@thomsonplayford.com.au

Contact Details

For further information in relation to this subject please contact:

Adelaide

Stephen Lyons - Partner

T: +61 8 8236 1336

E: slyons@thomsonplayford.com.au

Sydney

Jill Milburn - Partner

T: +61 2 8248 3416

E: jmilburn@thomsonplayford.com.au



Adelaide

101 Pirie Street . Adelaide . SA 5000

T: +61 8 8236 1300 . F: +61 8 8232 1961

Melbourne

Level 40 . 140 William Street

Melbourne . VIC 3000

T: +61 3 8608 7000 . F: +61 3 8608 7199

Sydney

Australia Square Tower

264 George Street . Sydney . NSW 2000

T: +61 2 8248 5800 . F: +61 2 8248 5899

info@thomsonplayford.com.au

www.thomsonplayford.com.au



This Alert is produced by Thomson Playford. It is intended to provide general information in summary form on legal topics, current at the time of publication. The contents do not constitute legal advice and should not be relied upon as such. Formal legal advice should be sought in particular matters.

Liability limited by a scheme approved under Professional Standards Legislation.