

Anti Money–Laundering & Counter Terrorism Financing Act

Omega Performance Corporation is a global consulting and training firm that increases the profitability of financial services institutions by improving the performance of their people.

Omega helps financial institutions reach new levels of performance by integrating intensive skill development, comprehensive learning systems, and a motivational learning environment to create a positive, lasting behavioural change.

Since 1976, more than two million financial service professionals from over 2,500 global financial institutions have completed Omega programmes in credit and risk management, and service, sales and sales management.

Omega's clients include financial service organisations of all sizes in Africa, Australia, Canada, China, New Zealand, Singapore, United Kingdom and United States.

N O T I C E

This publication is protected by copyright and is licensed to be used by a single individual only.

It is illegal to reproduce this training system or any part of it in any way, to share these materials, or to lend or rent them to anyone else.

Copyright © 1989–2008 by Omega Performance Corporation. All rights reserved.



Omega Performance Corporation, Asia Pacific

Australia & New Zealand
Level 12
45 Clarence Street
Sydney NSW 2000
Australia

+ 61 2 9236 8400

111 Somerset Road
#10-06 Singapore
Power Building
Singapore 238164

+ 65 6505 2060

Unit 13A
13B2 East Ocean Centre II
No. 618 YanAn Road East
Shanghai China, 200001

+ 86 21 6289 1977

www.omega-performance.com

Table of Contents

Overview & Objectives	1
Purpose of the Act	2
The Risk Based Approach	4
What is Anti-Moneylaundering	4-9
– Placement	
– Layering	
– Integration	
Reporting Obligations	10
New Customer Identification	11
Job Aid: New Customer Identification	15-17
– Individual	
– Partnership	
– Australian Company	
– Trust	
– Association	
Practice Exercise	19

Anti-Money Laundering and Counter-Terrorism Financing Act

Overview

This unit will introduce you to the requirements imposed under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act). Our goal is not to make you AML/CTF experts, but to highlight the requirements with which you should be familiar.

Among other things, the AML/CTF Act outlines requirements which deal with the identification process when funding a new loan or opening a new account.

This unit explains in detail the requirements and prohibitions of the act.

Objectives

When you complete this unit, you will be able to:

- State the purpose of the AML/CTF Act
- Elicit the information required by your organisation to identify new clients
- Give examples of situations in which you must comply with the Act and its interpretation
- Identify situations that violate the Act and correct them

Purpose of the Act

The purpose of the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act) is the regulation of financial transactions in a way that will help detect and prevent money laundering and terrorism financing.

The Act will replace the *Financial Transactions Reports Act*

The AML/CTF Act covers industry sectors with obligations under existing legislation, including:

- the financial sector (banks; building societies; credit unions; lending, leasing and hire purchase companies; issuers of travellers' cheques; foreign exchange dealers; asset management companies; remittance dealers; financial planners who arrange for the issue of products; life insurers; superannuation fund managers; custodial service companies; cash couriers, and securities dealers)
- the gambling sector (casinos, internet and electronic gaming service providers, bookmakers)
- bullion dealers, and
- other persons or businesses, such as lawyers and accountants, which provide designated services.

The Act covers 71 separate activities referred to as designated services that are generally provided by businesses (*Reporting Entities* (REs) within those industry sectors.

The legislative framework comprises:

- The AML/CTF Act which is high-level, principles based;
- Rules that are developed and administered by the *Australian Transaction Reports and Analysis Centre* (AUSTRAC). The Rules provide the operational detail and have legislative force; and
- Guidance Notes which provide non-binding interpretation of the Act and the Rules

The Act implements a risk-based approach to regulation. Reporting entities will determine the way in which they meet their obligations based on their assessment of the risk of whether providing a designated service to a customer may facilitate Money Laundering or Terrorist Financing (ML/TF).

Reporting entities must develop a program to ensure compliance with the Act. The program must be subject to the continuing oversight of the organisation's board and senior management. The following are some of the requirements to be included in an RE's program:

- Determine and put in place appropriate risk-based systems and controls having regard to the following factors:
 - (1) the nature, size and complexity of business; and
 - (2) the type of ML/TF risk that might be reasonably faced.
- A risk awareness training program must be designed to give employees appropriate training at appropriate intervals, having regard to ML/TF risk the RE may reasonably face
- An employee due diligence program must put in place appropriate -systems and controls to determine whether to, and in what manner to, screen any prospective employee who may be in a position to facilitate the commission of a money laundering or financing of terrorism offence

The AML/CTF Act will be implemented in stages with the most complex and costly obligations to be implemented 24 months after Royal Assent which was given on 12 December 2006. This will allow each business time to develop necessary systems in the most cost efficient way. Some of the implementation steps include:

12 June 2007

- Reporting obligations (to AUSTRAC)

12 December 2007

- Identification procedures for existing customers
- Identification procedures for certain low risk customers
- REs' programs for managing obligations under the Act

12 December 2008

- Ongoing customer due diligence
- Reporting obligations for suspect matters
- Reporting obligations for International Funds Transfer instructions

The Risk-Based Approach

When determining and putting in place appropriate risk-based systems or controls, the reporting entity must have regard to the nature, size and complexity of its business and the type of ML/TF risk that it might reasonably face.

In identifying the risk a reporting entity must consider the risk posed by the following factors:

- (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.

The reporting entity must be able to identify and act upon significant changes in ML/TF risk. Additionally a reporting entity must be able to assess the ML/TF risk posed by:

- (a) all new designated services and methods of delivery prior to introducing them to the market;
- (b) all new or developing technologies used to provide designated services prior to adopting them.

What is Money Laundering?

‘Money laundering’ describes the way some criminals use the legitimate financial system to try to hide or disguise the proceeds of crimes. Anti-money laundering laws are designed to prevent this behaviour by establishing an ‘audit trail’, or transaction history, which provides evidence linking criminal acts and their organisers.

The source of the illegal funds may include:

- tax avoidance
- theft
- dealing in illicit drugs
- illegal arms trading
- terrorism

In distancing the cash from its illegal origins to give the appearance of legitimate funds, three stages are frequently, but not always, used.

Placement

In this initial stage, the illegal funds are placed into the financial system.

Mode of Placement	Technique
Multiple placement	The funds are broken into amounts usually less than \$10,000 and placed in separate bank accounts, usually in false names. The bank accounts may be in Australia or in offshore havens such as the Cayman Islands, Panama or Switzerland
Alternative remittances	Funds are transferred to accomplices in off-shore locations through underground remittance agents. Cash is lodged with the remittance agent and cash is paid out at the destination with little or no documentation to trace it. These remittance agents are active in Central and South America and in Asia. This method is less effective in Australia as a result of existing reporting requirements.
Electronic transfer	Transfer of funds off-shore through legitimate non-bank remittance agents. This method is similar to <i>alternative remittances</i> , in that it does not rely on the banking system. The advancement of electronic technology enhances the effectiveness of this system as funds that may come under notice are moved on through multiple transfers before they can be investigated.
Asset conversion	The illegal cash is used to purchase high value items that are easy to transport and on-sell, e.g. jewellery, gold bullion, exotic motor vehicles, etc.
Bulk movement	Currency or other assets are smuggled across international borders. U.S. currency is often preferred because of its global acceptance. In Europe the Euro is often used as it is the official currency of several European nations.

Mode of Placement	Technique
Gambling	Gambling chips are purchased at casinos and at the end of a “pleasant evening”, the chips are cashed back to currency, under the guise of “winnings”.
Life Insurance	The criminal pays cash for an up-front single premium purchase of a life insurance policy that has a redemption value. At a later date the policy is redeemed with the request that the proceeds be paid to a nominated bank account, thus giving the appearance of legitimacy. The initial purchase is usually made through an agent or broker who may be acting in collusion with the criminal.

Alternative remittances, electronic transfers and bulk transfers are the first stage of “placement” as the funds still need to be placed into the legitimate financial system. Havens with strict secrecy rules such as Cayman Islands, Panama and Switzerland are frequently used to receive the funds.

Many placement techniques rely on assistance from friends and associates, professionals such as solicitors and accountants, and brokering firms.

Layering

Layering refers to the breaking down of the large amounts and moving the funds through the financial system to create a complicated trail that is difficult to trace back.

Mode of Layering	Technique
Electronic Funds Transfer (EFT)	Funds are transferred frequently using EFT> With over 700,000 transaction world-wide annually the movement of illegal funds is difficult to detect because of the vast volume of transactions
Off-shore banks	Funds are transferred to off-shore financial institutions that protect the privacy and identity of the account holders. Banks in the Cayman Islands, Panama and Switzerland are predominant in this activity.
Shell companies	Criminals frequently register "shell" companies that do not actually conduct any business activity. The companies' bank accounts receive deposits and effect payments (in cash, by cheque or by electronic transfer), but no actual trading takes place. Thus, the payments made by the companies to other companies and persons have the appearance of being legitimate payments.
Trusts	Trusts are created using corporate trustee companies as the trustee, naming a shell company as the beneficiary. Money is then moved through the trustee's bank account, with distributions being made to the beneficiary shell company. This method is not frequently used due to the complication involved.
Walking account	"Clearing" accounts are set up with several different banks and associates make deposits to the accounts which are then cleared daily to a central bank account. The money appears to "walk" away.

Mode of Layering	Technique
Intermediaries	Non-financial professionals such as solicitors and accountants, acting on behalf of their criminal clients who remain anonymous to the observer, transfer money deposited in their trust accounts to shell company bank accounts creating the impression of legitimacy.

In Australia, layering frequently involves the movement of amounts of money. Employees of financial institutions should be alert to frequent movements of amounts slightly less than \$10,000 in cash or by electronic transfer.

Integration

In this final stage of the money laundering process, the money is integrated into the financial system without any of the appearances of being illegally sourced funds.

Mode of Integration	Technique
Credit and debit cards	With the money being held in bank accounts the account holders sign up for credit or debit cards which are used for asset purchases or cash transfers.
Consultants	The shell company that holds illegally sourced money hires a “consultant” to perform services (that frequently do not exist). Payments made to the consultant are often excessive, but the appearance of legitimacy exists.

Mode of Integration	Technique
Corporate financing	<p>The criminals may operate legitimate business enterprises. Financing for the enterprise comes from an (on-shore or off-shore) shell company through loans or equity injection. The interest payments on loans or share dividend payment may be excessive in relation to the amount of principal loaned/invested.</p> <p><i>Note:</i> the interest payment may be tax deductible, so the Australian Taxation Office unwittingly becomes a party to assisting the funding of criminal elements.</p>
Asset purchases and sales	<p>The funds are used to purchase large assets (e.g. real estate) or make investments. If the assets are purchased from associates highly inflated prices may be paid.</p>
Business recycling	<p>Money is “recycled” through legitimate business, with “phantom” sales being made and excessive expenses being “incurred”. The legitimate business has the appearance of successful trading well above the true level of activity. There is often a loss of relativity between the financial turn-over of the business and its actual size.</p>
Import/Export	<p>The legitimate “front” company imports (or exports) goods at highly inflated values, thereby enabling the international movement of money that has the appearance of being legitimate.</p>

The three stages of money laundering might not be present in every laundering activity. For example, layering might be omitted and the placement and integration of the funds might be intermingled.

Some Unusual Behaviour

- A request to open an account and then refusal to proceed when the requirements for identification are explained.
- Keeping a large number of accounts out of proportion to the needs of the business.
- Significant cash transactions undertaken by someone who is not usually recognised as having access to large sums of money, e.g., a person who gives his or her occupation as social security recipient, a student, or domestic.

Reporting Obligations

Under the legislation business will be required to report to AUSTRAC suspicious matters. The reporting obligations commence in December 2008.

In the interim period, reporting entities will continue to report to AUSTRAC “suspicious transactions” and “significant cash transactions” and, in any case, cash transactions exceeding \$10,000 as provided for in the Cash Transactions Reports Act.

What does the AUSTRAC do with the Information?

The Australian Transaction Reports and Analysis Centre (AUSTRAC) has been established to collect and collate information which may be of use in the fight against criminal activity. It does not act on information it receives except to make it available to law enforcement authorities, e.g., state or federal police, taxation office, and other relevant bodies. It also analyses the information it receives with a view to drawing conclusions or inferences about the source or destination of the funds. It may, for example, be able to establish that payments being remitted from a certain account or certain locations in Sydney are going to a country which is recognised as a source of illicit drugs.

Procedures to be Followed



As the procedures to be adopted by each RE are risk-based, having regard to the customer profile and products being offered, the procedures adopted within each financial institution may vary. Therefore, it is imperative that each employee learns and adheres to the internal directions of the employer.

The identification procedures adopted by an RE must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a customer is an individual, that the customer is the individual that he or she claims to be.

New Customer Identification

The following provisions do not apply to pre-commencement customers.



The Rules issued by AUSTRAC specify the minimum requirements for identification of new customers who are seeking products or services. The information is referred to as *Know Your Customer (KYC)* information. If the customer is unable to provide the level of identification required by the reporting entity, the product or service may not be provided.

The Rules also stipulate minimum verification procedures.

The RE may collect and record additional information, or may go to a greater effort to verify information if the ML/TF risk is deemed to be greater because of the category of customer and/or the product or service being provided.

REs need to consider their obligations under other legislation, including the Privacy Act 1988, when deciding what information is required to be collected to fulfil their obligations under the Rules.



The Job Aids that appear at the end of this section and in the Reference Guide detail the minimum information required to identify the various categories of customers. Your organisation has a responsibility to satisfy itself that the appropriate amount of KYC information has been collected and verified relevant to the perceived risks of the product/service and/or the category of customer.



It is imperative that in addition to the minimum requirements specified within the Rules, you must be thoroughly familiar with the instructions of your own organisation. Your organisation's instructions may over-ride the information in the Job Aids.

The Job Aids contain details of the minimum KYC information required for the following categories of Customers:

- Individuals (including sole traders)
- Partners in Partnerships
- Companies
- Trusts
- Incorporated and Unincorporated Associations
- Registered Co-operatives
- Government Bodies and
- Agents

Note:

An **Agent** may be considered to be:

- A person who is authorised to act for or on behalf of an individual customer in relation to a designated service;
- A person who is authorised to act for or on behalf of a customer who is a non-natural person/entity.

In addition, the Job Aid *Acceptable Identification Documents* defines the photographic and non-photographic documents that are acceptable as customer identification.

Verification of the Identity of Pre-commencement Customers

A reporting entity is not required to re-verify the identity of existing customers unless individual cases warrant this.

Where the reporting entity suspects on reasonable grounds that a customer is not the person that he or she claims to be, the reporting entity must, within 14 days carry out the applicable customer identification procedure (unless it has previously been carried out by the same or comparable procedure).

It must collect KYC information in respect of the customer and verify the information in accordance with the Rules. The purpose of the action is to enable the reporting entity to be reasonably satisfied that the customer is the person that he or she claims to be.

Customer Due Diligence

From December 2008, reporting entities will have to carry out customer 'due diligence' which will require that reporting entities monitor customer transactions on an ongoing basis.

The Rules for Customer Due Diligence will be issued during 2008.

Employee Due Diligence Program

The Act requires reporting entities to put in place appropriate risk-based systems and controls to determine whether to, and in what manner to, screen any prospective employee who, if employed, may be in a position to facilitate the commission of a money laundering or financing of terrorism offence. The systems and controls must also provide for

The employee due diligence program must include appropriate risk-based systems and controls for the reporting entity to determine whether, and how, to re-screen an employee where the employee is transferred or promoted to a position where it may be possible to facilitate the commission of a money laundering or financing of terrorism offence.

The employee due diligence program must also establish and maintain a system for the reporting entity to manage any employee who fails, without reasonable excuse, to comply with any relevant AML/CTF system, control or procedure.

	Individual (inc. Sole Trader)	Partnership	Australian Company	Trust	Association
<p>Information to be collected</p>	<p>(1) the customer's full name; (2) the customer's date of birth (3) the customer's residential address or the full address of the customer's principal place of business (if any) (4) the full business name (if any) under which the customer carries on business; and (5) any ABN issued to the customer.</p>	<p>(1) the full name of the partnership; (2) the full business name (if any) of the partnership as registered under any State or Territory business names legislation; (3) the country in which the partnership was established; (4) in respect of one of the partners – the information required to be collected from an individual under the applicable customer identification procedure with respect to individuals; and (5) the full name and residential address of each partner in the partnership except where the regulated status of the partnership is confirmed through reference to the current membership directory of the relevant professional association.</p>	<p>(1) the full name of the company as registered by ASIC; (2) the full address of the company's registered office; (3) the full address of the company's principal place of business, if any; (4) the ACN issued to the company; (5) whether the company is registered by ASIC as a proprietary or public company; and (6) if the company is registered as a proprietary company, the name of each director of the company.</p>	<p>(1) the full name of the trust; (2) the full business name (if any) of the trustee in respect of the trust; (3) the type of the trust; (4) the country in which the trust was established; (5) if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual; (6) if any of the trustees is a company, then in respect of one of those companies – the information required to be collected from a company; and (7) if the trustees comprise individuals and companies, the information required to be collected from the individual or company (as the case may be).</p>	<p>Incorporated: (1) full name of the Association; (2) address of place of administration or registered office (if any) or the residential address of the public officer or (if there is no such person) the president, secretary or treasurer; (3) identifying number issued by the State, Territory or overseas body responsible for the incorporation of the association.</p> <p>Unincorporated: (1) full name of the Association; (2) address of the principal place of administration; (3) name of the chairman, secretary and treasurer; and (4) in respect of the member – the information required to be collected from an individual.</p>

	Individual (inc. Sole Trader)	Partnership	Australian Company	Trust	Association
Verify, at a minimum, the following KYC information	<p>(1) the customer's full name; and</p> <p>(2) either</p> <p>a) the customer's date of birth; or</p> <p>b) the customer's residential address.</p>	<p>(1) the full name of the partnership; and</p> <p>(2) information about one of the partners in accordance with the applicable customer identification procedure with respect to individuals</p>	<p>(1) the full name of the company as registered by ASIC;</p> <p>(2) whether the company is registered by ASIC as a proprietary or public company; and</p> <p>(3) the ACN issued to the company</p>	<p>(1) the full name of the trust; if any of the trustees is an individual, information about the individual in accordance with the applicable identification procedure;</p> <p>(3) if any of the trustees is a company, information about the company in accordance with the applicable identification procedure; and</p> <p>(4) if the trustees comprise individuals and companies, the information about the individual or company in accordance with the applicable procedures</p>	<p>Incorporated:</p> <p>(1) name of the Association;</p> <p>(2) identifying number.</p> <p>Unincorporated:</p> <p>(1) full name of the Association;</p> <p>(2) verify information about the member in accordance with the applicable procedure.</p>
Verification Code	<p>(1) an original or certified copy of a primary photographic identification document; or</p> <p>(2) both</p> <p>(a) an original or certified copy of a primary non-photographic identification document; and</p> <p>(b) an original or certified copy of a secondary identification document; and</p> <p>(3) verify that any document produced by the customer has not expired (other than a passport issued by the Commonwealth that expired within preceding 2 years)..</p>	<p>(1) the full name of the partnership; and</p> <p>(2) information about one of the partners in accordance with the applicable customer identification procedure with respect to individuals</p>	<p>(1) the full name of the company as registered by ASIC;</p> <p>(2) whether the company is registered by ASIC as a proprietary or public company; and</p> <p>(3) the ACN issued to the company</p>	<p>(1) the full name of the trust from a trust deed, certified copy or certified extract of the trust deed, reliable and independent documents relating to the trust or reliable and independent electronic data;</p> <p>(2) in respect of the trustee(s), information about the individual(s) or company(s) in accordance with the applicable identification procedure.</p>	<p>Incorporated:</p> <p>(1) from the State, Territory, or overseas body responsible for the incorporation of the association;</p> <p>(2) the rules or constitution of the association; or</p> <p>(3) reliable and independent documents relating to the association; or</p> <p>(4) reliable and independent electronic data.</p> <p>Unincorporated:</p> <p>(1) the rules or constitution of the association; or</p> <p>(2) reliable and independent documents relating to the association; or</p> <p>(3) reliable and independent electronic data.</p>

	Individual (inc. Sole Trader)	Partnership	Australian Company	Trust	Association
<p>Electronic Verification</p>	<p>(1) collect the KYC information described above from a customer;</p> <p>(2) verify:</p> <ul style="list-style-type: none"> (a) the customer's name and the customer's residential address using reliable and independent electronic data from at least two separate data sources; and either (b) the customer's date of birth using reliable and independent electronic data from at least one data source; or (c) the customer has a transaction history for at least the past 3 years. 				

Practice Exercise

1. What does AUSTRAC do with the information it receives?
2. What are the possible consequences of a financial institution's failure to properly identify a person who opens a new account?
3. A person makes an enquiry as to what she must do to open a new account with a Bank. Is that a suspicious transaction?
4. Give an example of a suspicious transaction.
5. Give three examples of primary photographic identification documents and three examples of primary non-photographic identification documents.

Answers

1. It makes it available to law enforcement authorities so that they might uncover and prevent criminal activities.
2. a) Funds cannot be withdrawn from the account.
b) The cash dealer may be liable to prosecution for a breach of the Act.
3. No. The making of a simple enquiry about the opening of an account is not in itself suspicious.
4. A person who regularly deposits three social security cheques, all in different names, into the same account without explanation.

5. **Photographic**

Driver's licence

Australian Passport

Foreign Passport (with a translation by an accredited translator attached if necessary)

Proof of age card

Foreign identity card (with a translation by an accredited translator attached if necessary)

Non-photographic

Birth Certificate or birth extract

Australian citizenship certificate

Foreign citizenship certificate (with a translation by an accredited translator attached if necessary)

Foreign birth certificate (with a translation by an accredited translator attached if necessary)

Pension card issued by Centrelink