

Anti-money laundering and counter-terrorism financing—customer identification and verification

Australia's anti-money laundering and counter-terrorism financing (AML/CTF) legislative framework consists of—

- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), and
- *Anti-Money Laundering and Counter-Terrorism Financing Rules* (AML/CTF Rules).

The primary objective of the AML/CTF Act is to address the risk of money laundering in Australia and the threat to national security caused by the financing of terrorism.

This fact sheet is designed to provide a brief outline of the AML/CTF obligations of fund managers and the options they have to comply with those obligations.

Who is regulated?

The AML/CTF Act regulates “reporting entities”, being any person or body corporate who carries on the business of providing a “designated service”. Designated services include (amongst other things) opening an account, accepting money on deposit and issuing a security (which includes interests in managed investment schemes).

Accordingly, the AML/CTF Act will apply to—

- financial institutions, such as banks and foreign currency traders
- responsible entities of registered funds

- trustees or managers of unregistered funds
- custodians holding assets of registered and unregistered funds, and
- entity's who arrange for customers to receive a designated service (such as a licensed intermediary or outsourced dealer).

When do the requirements commence?

The obligation to comply with the AML/CTF Act requires the reporting entity to have first provided a “designated service”. For most fund managers this will be when a security (such as an interest in a fund) is issued to a customer.

What are the implications?

The AML/CTF Act places various compliance obligations on reporting entities with respect to their dealings with “customers” and their involvement in particular transactions.

The key obligations include the following:

- **AML/CTF compliance program**—the reporting entity must determine its risk exposure to money laundering and terrorism financing. This requires the reporting entity to develop a risk framework to assess these risks across its business. The program must include a risk-based customer identification program and an ongoing customer due diligence program to ensure the reporting entity knows who it is doing business with and to be able to identify any unusual or suspicious behaviour.

- **AUSTRAC reporting**—the AML/CTF Act requires reporting entities to report a range of matters to AUSTRAC, including the following:
 - (a) Where the reporting entity suspects, on reasonable grounds, that information concerning the provision or possible provision of a designated service may be “relevant to the investigation or prosecution” of a person for tax evasion, a criminal offence, money laundering or financing terrorism.
 - (b) Cash transactions or transfers of \$10,000 or more.
 - (c) Compliance with the AML/CTF Act.
- **Training**—the reporting entity must establish a training and awareness program for staff to educate them in the AML/CTF requirements and make them aware of what may constitute suspicious activity.
- **Employee screening**—an employee due diligence program to screen staff members who may be in a position to assist in money laundering or terrorism financing.
- **AML/CTF compliance officer**—the reporting entity must appoint an AML/CTF compliance officer to take responsibility for AML/CTF compliance.
- **Record keeping**—the AML/CTF Act places further obligations on reporting entities to keep thorough records of information in connection with the above obligations for a period of seven years.

Customer identification and verification

A reporting entity can fulfil its customer identification and verification obligations through a number of methods, as follows:

- Perform the customer identification and verification itself.

- Appoint an agent to carry out the initial customer identification and verification on its behalf.
- Rely on the customer identification and verification that has been carried out by another entity.

Where a reporting entity intends to rely on the customer identification and verification performed by another entity, then it must be “reasonably satisfied” the entity has carried out the identification in accordance with the AML/CTF Rules.

This requires an agreement to be in place between the parties. Under the terms of the agreement, the entity performing the customer identification and verification must agree to retain documents used in the verification process and allow the reporting entity to inspect such documents.

Am I required to perform the customer identification and verification on all customers?

Customer identification and verification is only required to be performed on new customers.

Existing customers (i.e., those customers who have previously invested in a security or scheme operated by the reporting entity) are not required to be identified and verified. However, if a long period has elapsed since the previous investment, then the reporting entity may choose to perform the customer identification and verification.

Importantly, for a reporting entity to rely on the “existing customer” exemption, the customer must be the same entity, i.e., it cannot be a new entity, such as a new company, trust or self managed superannuation fund.

What are the implications for disclosure documents?

Fund managers have a number of alternatives available to them to include information in disclosure documents about AML/CTF, as follows:

- General disclosure

It is common practise to include at least a brief description of the AML/CTF obligations and the requirement on fund managers to collect information from prospective customers.

- Application form

- (a) List of identification and verification documents

The customer identification and verification requirements can be included in the application form.

Application forms prepared in this way outline the identification documents to be provided based on type of customer e.g., individual, company, trust etc.

- (b) Checkboxes

Application forms can also be prepared to include a number of AML/CTF checkboxes, including the following:

- (i) Confirmation another entity has performed the customer identification and verification.
 - (ii) Confirmation a customer has invested previously in a security or scheme operated by the reporting entity.

- (iii) Confirmation a customer is an unregistered scheme with wholesale clients only.

- AML/CTF booklet

As an alternative to including customer identification and verification information in the application form, a separate AML/CTF booklet can be used to accompany the disclosure document. This booklet provides details of all the identification and verification documents required to be provided by the customer.

Compliance committee members and compliance plans

It is prudent to include AML/CTF obligations in compliance plans based on the requirements under the *Corporations Act 2001*. Where such obligations are included, the compliance committee is required to monitor the reporting entity's compliance with the AML/CTF requirements.

However, just like other procedures in a compliance plan, this does not require the compliance committee to have direct involvement in performing or overseeing the identification or verification of customers; or reporting suspicious matters to AUSTRAC.

How McMahon Clarke Legal can help

McMahon Clarke Legal is experienced in assisting clients establish AML/CTF compliance and training programs, liaising with AUSTRAC and preparing agreements with third parties to undertake customer identification and verification.

For more information, contact—

David MacLeod | Partner | D: +61 7 3239 2906 | E: david.macleod@mcmahonclarke.com

This fact sheet is produced as general information in summary for clients and should not be relied upon as a substitute for detailed legal advice or as a basis for formulating business or other decisions. McMahon Clarke Legal asserts copyright over the contents of this document.