



Australian Government

Australian Transaction Reports
and Analysis Centre

AUSTRAC e-learning 

Module 3

AML/CTF program: Part B (customer identification)

AML/CTF Programs



Australian Government

**Australian Transaction Reports
and Analysis Centre**

Module 3

AML/CTF program: Part B (customer identification)



Module 3

AML/CTF program: Part B (customer identification)

Module overview

In this unit we will examine the requirements for Part B of your AML/CTF program, and consider processes and practices to meet this obligation. Part B requires reporting entities to implement applicable customer identification procedures.

Customer identification procedures include:

- collection of documentation-based and electronic-based information from the customer
- verification, assuring the reliability and independence of the information
- authentication, determining whether and in what circumstances an entity will take steps to determine if information provided has been forged, tampered with, altered or stolen.

A legal requirement for customer identification procedures is that they should adequately identify the customer **before** a designated service is provided, or that the provision of the designated service can not be undertaken if the customer identification is unsatisfactory. As with other components of your AML/CTF program it is possible that your organisation already has a framework in place that may be able to be adapted or expanded to cover your 'know your customer' (KYC) obligations. This module is aimed at assisting your business to integrate AML/CTF customer identification and verification requirements into your normal business practices.

Core concepts

This module will address the following:

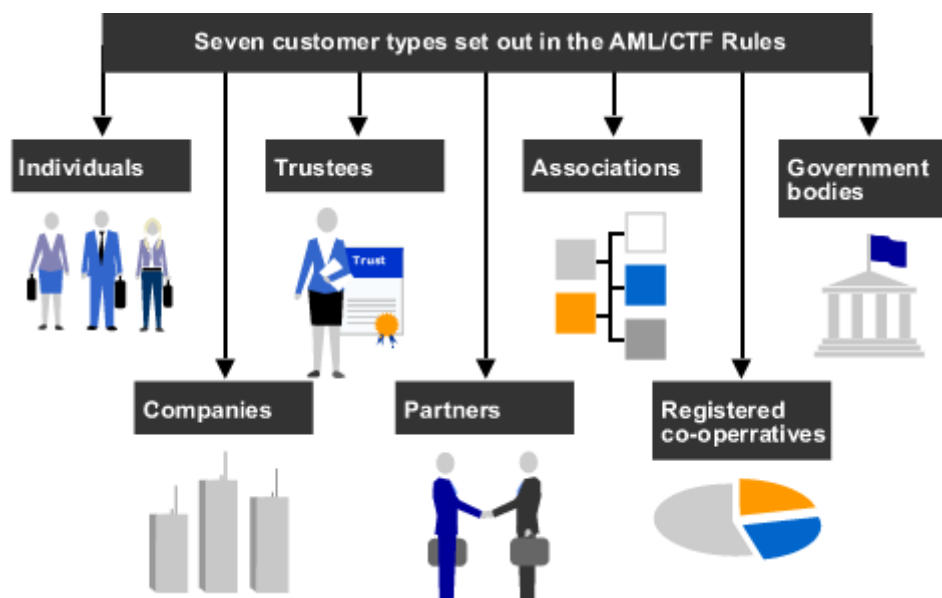
- Who are customers?
- Know your customer (KYC)
- Identifying customers who may pose higher ML/TF risks
- Identifying existing customers
- Customer identification
- Authentication
- Relying on others to identify your customers
- Customer identification record keeping
- Customers' obligations
- Ongoing customer due diligence (OCDD)

Who are customers?

Reporting entities may use a number of terms when referring to their customers. For example, businesses in the financial services sector may refer to clients rather than customers. Another example is the gambling sector; customers may be referred to as patrons, members or associates. Irrespective of the different terms that are used in different industries, the AML/CTF Act defines a customer (including a prospective customer) as the person to whom a designated service is provided. Whatever the terms used by an entity to describe a customer the obligations under the Act apply.

The AML/CTF Rules list seven customer types for which customer identification procedures will seek different types of information. The seven types are:

- individuals (including sole traders)
- companies, including
 - domestic companies
 - registered foreign companies
 - foreign companies not registered in Australia
- trustees
- partners
- associations (both incorporated and unincorporated)
- registered co-operatives
- government bodies.



For customers that are non-human legal entities, such as a company, the identification procedure may include both the legal entity and key individuals within the entity, or other individuals who may benefit from the workings of the entity.

| |
|---|
| AML/CTF Rules |
| The AML/CTF Rules in chapters 4, 6 and 7 detail the Part B requirements for standard and joint AML/CTF programs and chapter 5 covers provisions for special AML/CTF programs. |

Know your customer (KYC)

Knowledge about a customer is necessary to determine the money laundering and terrorism financing (ML/TF) risk that the organisation may face if providing a designated service to that customer. The requirement to establish and verify the identity of a customer before providing a designated service to that customer is a key obligation of the AML/CTF Act. Customer identification is also a core risk management process that characterises ML/TF risk management. Customer identification is given prominence as it forms the whole of Part B of the required AML/CTF program.

The process of a reporting entity learning about its customers is called know your customer (KYC). The two essential elements of KYC are:

- adequately verifying your customer's identity
- developing an understanding of who your customer is and their expected financial activities.

Appropriate KYC measures are determined through risk analysis of the customer relationship, covering:

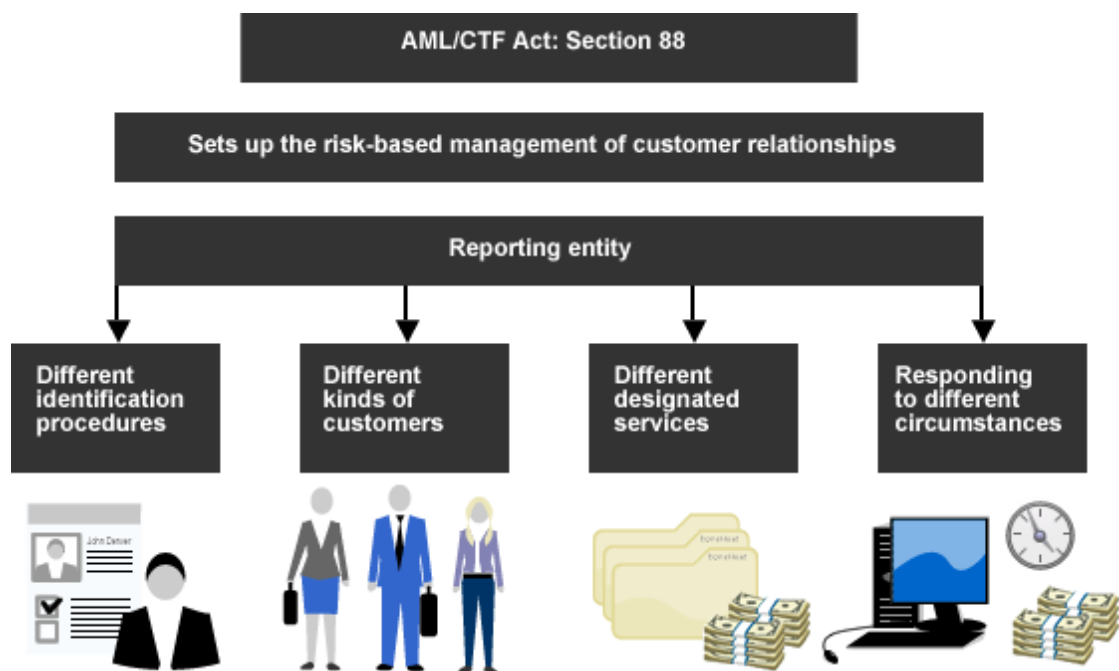
- the type of customer
- the methods used to deliver the designated services
- the types of products or services provided
- whether the customer operates in foreign jurisdictions that have less stringent AML/CTF legislation than Australia, or if the country is identified as being at high risk for ML/TF.

Once these risks have been assessed, businesses will need to consider the level of identification and verification procedure that will match the level of assessed risk. These practices will need to be in a documented or electronic format that can be shown to AUSTRAC if necessary.

Like other elements of your AML/CTF program, customer identification procedures may be able to be incorporated or adapted into existing business practices. An evaluation of existing practices can identify gaps in customer identification procedures that may expose your business to be an easy target for use by criminals to launder illegal funds and/or fund terrorism.

Identifying customers who may pose higher ML/TF risks

It is necessary to consider the different ML/TF risks that the full range of your customers pose to your business when you formulate your customer identification procedures. Most customers using the designated services you provide will be legitimate; however your systems and procedures need to be alert and responsive to instances where a customer's background places them into a category of a higher risk customer. For this reason it is a legal requirement to correctly identify a customer **before** providing the customer with a designated service, so that you can begin assessing the relevant risks the customer may present. The AML/CTF Rules will detail any special conditions where this requirement does not apply. Failure to correctly identify and verify the customer at the outset may prevent any effective ongoing customer due diligence activity.



Customer identification controls are only part of ensuring that the true identity of a customer is established. Criminals (including money launderers) are likely to have convincing documentation. The knowledge, experience and alertness of staff members provide the essential human intervention to ensure that systems and controls are routinely monitored and modified to identify abnormal behaviour.

Risk assessment must be realistic. Knowing who your customers are and having a good understanding of which, if any, of your designated services are vulnerable to

ML/TF risks, is the basis of developing an AML/CTF program suitable to your business needs. For example, the ML/TF risk for the same product may differ if the customer is a domestically-based individual, or an offshore trust. Customer identification procedures need to be developed relative to the nature, size, complexity and resource capacity of your business. For example, with internet access you may be able to determine the level of risk posed by persons from certain countries that may be exposed to levels of economic and political corruption.

Your risk assessment methodology and associated AML/CTF policies and procedures could specify the factors that your staff should spell out when a customer does fall into a higher risk category. In these situations, when your business has assessed a customer to be high risk, additional KYC information should be sought. The type of additional information you will request in each situation should be documented as part of the processes in your AML/CTF program and communicated to your staff.

The AML/CTF Act does not prescribe what additional documents you should request, however chapter 4 of the AML/CTF Rules does provide some suggestions for consideration.

Identifying existing customers

In most cases it will not be necessary to re-identify customers to whom you provided a designated service before 12 December 2007. These are referred to as 'pre-commencement customers'. An exception to this is where a customer's behaviour or transaction raises suspicion that would warrant your business lodging a suspicious matter report (SMR) to AUSTRAC. It is important to remember that it is unlawful to disclose to a customer that an SMR is being lodged. For more information about suspicious matter reporting, review the 'Reporting obligations' module of the AUSTRAC *Introduction to AML/CTF* e-learning course.

Requesting proof of identity from customers will be familiar to reporting entities who offered accounts and were required to verify customer information under the FTR Act by using the 100 point check or 'reference from an acceptable referee'. However, the AML/CTF Act broadens the range of services where customer identification is now required. Prior to 12 December 2007 your business may have provided certain services without the need to identify customers. Those customers who received a particular service before that time may not need to be identified now, however if they seek a designated service they were not previously using, then identification may be required.

Although existing customers will likely not be required to be identified, they will be subject to risk-based ongoing customer due diligence from 12 December 2008.

These obligations are contained in sections 28 and 29 of the AML/CTF Act and chapter 6 of the AML/CTF Rules.

Subsection 36(1) of the AML/CTF Act requires a reporting entity to monitor customers in relation to designated services provided. This does not apply to a reporting entity's permanent establishment(s) in foreign countries or designated services covered by item 54 of table 1 in section 6 of the AML/CTF Act. Chapter 15 of the AML/CTF Rules sets out the main components of ongoing customer due diligence.

If a suspicious matter reporting obligation (section 41 of the AML/CTF Act) arises in relation to a pre-commencement customer, under section 29 of the AML/CTF Act the identity of the customer will need to be verified.

Customer identification

Customer identification involves:

- the collection of KYC information from the customer that will allow you to identify that customer
- the verification of this information in documented or electronic form by reliable and independent means.

The minimum required information and the means of verification will depend upon the type of customer being identified.

Chapter 4 of the AML/CTF Rules specifies the collection of the minimum KYC information for each of the different types of customers and the means for verifying this information. In addition, it is the responsibility of the reporting entity to include in Part B of its AML/CTF program such controls that will allow it to realise when a discrepancy exists in the verification of information and to respond to the discrepancy; that is, be able to make a judgement that the customer exists and information about specific key individuals has been provided.

Authentication

On occasion, documents produced might not be genuine and may appear to be forged, tampered with, cancelled or stolen. In these instances examples of what your AML/CTF program might cover include any:

- procedures put in place to establish if the documents are genuine
- controls or testing you will include determining if documents are genuine
- risk-based procedures you have in place to use document authentication services
- procedures to determine whether and how to confirm the KYC information is correct, for example by independently contacting the customer to establish they are who they claim to be.

As with Part A of your AML/CTF program, the procedures your organisation puts in place should be appropriate to the nature, size and complexity of your business.

Relying on others to identify your customers

Under the AML/CTF Act, a reporting entity can contract out the task of carrying out the applicable customer identification procedure on its behalf to an agent. However, the ultimate responsibility of identification and verification of customers still remains with the reporting entity.

Chapter 7 of the AML/CTF Rules specifies circumstances where certain types of reporting entities may rely on the customer identification procedures carried out by another reporting entity, including circumstances where either:

- the customer identification procedure was conducted by a licensed financial adviser in the process of arranging for a customer to receive a designated service from the other reporting entity
- the two reporting entities are members of the same designated business group.

The reporting entity that did not conduct the identification procedure either obtains a copy of the record (from the other reporting entity) or needs to have access to the other reporting entity's records.

Customer identification record keeping

Under section 113 of the AML/CTF Act records of customer identification must be retained for 7 years.

The AML/CTF Act is principles-based rather than prescriptive legislation. This means it is up to your organisation to determine if you will keep electronic or paper records and how those records will be stored and protected. For example, while it is not always necessary to photocopy documents, you must keep records of the identification details. Again, these practices will vary depending on things such as the size and nature of your organisation, information technology capabilities, available onsite storage and the security procedures you have in place.

Note that under the Privacy Act, storage of personal information must be secure and confidentiality needs to be maintained. Your business should consider the best way to ensure these obligations are met. For example, electronic records may be password protected and restricted to certain individuals for legitimate reasons.

Customers' obligations

It is possible your business may face resistance from some customers who may not be willing to provide identification. This can be particularly difficult when you may have known a client for a long period of time, or where issues of trust and community loyalty come into play. As previously mentioned, identification requirements for customers who were receiving one of your designated services prior to 12 December 2007 may often be less stringent. You may wish to consider an awareness campaign notifying customers through signs, mail-outs, or your website that due to new legislative requirements customer identification procedures have changed. Public knowledge that your business is active in fighting terrorism and money laundering is likely to benefit your overall business through enhancing its reputation, credibility and market competitiveness.

If a reporting entity has reasonable grounds to believe a customer may have information that will help them to comply with their AML/CTF program, section 92 of the AML/CTF Act allows the reporting entity to request in writing such information within a specified time. During that time the AML/CTF Act allows you to restrict or limit designated services to the customer. For reporting entities concerned with any legal action taken against them regarding actions taken in good faith when exercising this power, additional protection from liability may be available under subsection 92(5) of the AML/CTF Act.

Ongoing customer due diligence (OCDD)

From 12 December 2008 reporting entities that provide designated services will be required to monitor customers and their transactions on an ongoing basis. This process is referred to as 'ongoing customer due diligence' (OCDD) and is prescribed under section 36 of the AML/CTF Act.

Your AML/CTF program needs to include systems and procedures for OCDD that reflect the risk-based approach of the legislation. This means that high-risk situations will require more attention than low-risk situations.

Chapter 15 of the AML/CTF Rules sets out the three main components of OCDD:

- a. know your customer (KYC) information
- b. transaction monitoring program
- c. enhanced customer due diligence program.

OCDD obligations only apply to the provision of designated services at or through a reporting entity's permanent establishment(s) in Australia.

OCDD obligations do not apply to a designated service(s) covered by item 54 of table 1 in section 6 of the AML/CTF Act.

OCDD obligations apply in relation to all of a reporting entity's customers who receive designated services including:

- pre-commencement customers (where the reporting entity commenced to provide a designated service before the OCDD obligations came into effect)
- customers of a reporting entity who were identified (and whose entity was verified) by another reporting entity under the deeming provisions of section 38 of the AML/CTF Act.

In the case of designated business groups, ongoing customer due diligence may be carried out by any member of the group for another member.

Know your customer information

Your AML/CTF program will need to address whether and in what circumstances further KYC information about your customers should be updated or existing KYC information verified. Examples of when this may be necessary include when a significant transaction (for example, in amount, size or volume) takes place, or a

material change to how the account has been previously operated by the customer.

Transaction monitoring program

Your AML/CTF program must include a transaction monitoring program to detect suspicious transactions when they occur. A transaction is suspicious if it satisfies one or more of the conditions specified in section 41 of the Act.

To identify apparently suspicious transactions, the transaction monitoring program must have regard to complex or unusual large transactions and all unusual transaction patterns where there is no apparent economic or lawful purpose. Examples of these include:

- significant transactions (in terms of amount or volume) for that customer
- transactions that exceed transaction or amount limits
- very high account turnover inconsistent with the size of the balance
- transactions outside the regular pattern of an account's activity.

Enhanced customer due diligence

Your AML/CTF program must include an enhanced customer due diligence program. This program must be applied where you assess ML/TF risk is high, or when a suspicious matter reporting obligation arises. In applying enhanced customer due diligence you may consider:

- seeking further information from the customer or third-party sources to clarify, update or obtain the customer's KYC information; clarify the nature of the customer's ongoing business with the reporting entity; or consider any suspicion that may be reportable to AUSTRAC
- undertaking more detailed analysis of their KYC information
- verifying or re-verifying KYC information
- analysing the customer's past transactions and possibly monitoring future transactions
- whether a suspicious matter report ought to be lodged with AUSTRAC.

If you lodge a suspicious matter report in relation to a pre-commencement customer, you are required to verify that customer's identity under section 29 of the AML/CTF Act.

AUSTRAC intends to maintain its AML/CTF Programs e-learning application as an evolving resource to reflect changing patterns of behaviour, legislative development and the broader Anti-Money Laundering environment. Should you require further information on the e-learning application, AUSTRAC's operations, the *Financial Transaction Reports Act 1988* (FTR Act) or the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), please contact:

AUSTRAC Help Desk via:

help_desk@austrac.gov.au or Telephone 1300 021 037.

© 2008, Commonwealth of Australia

Each cash dealer, reporting entity or other stakeholder may use this material internally as an educational tool. It may view and use this application solely in the usual operation of its web browser in visiting the AUSTRAC Site ("the Site"). Except for this purpose, the material may not otherwise be used, copied, reproduced, published, altered or transmitted in any form or by any means in whole or part (except where such use constitutes fair dealing under the *Copyright Act 1968* (Cth)) without the prior written approval of the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>, with a copy to AUSTRAC.

The Commonwealth accepts no liability in regard to any loss or damage suffered by you resulting from a loss of service, malfunction, computer viruses, or any other cause connected with your use of the Site.

The information contained in this application is intended only to provide a summary and general overview on these matters. The AML/CTF Programs course is not intended to be comprehensive nor does it constitute legal advice. AUSTRAC may from time to time amend legislative instruments under the legislation it administers and this may impact on the form and content of the AML/CTF Programs course. The AML/CTF Programs course contains statements of policy that reflect AUSTRAC's administration of the legislation in performing its statutory functions. The Commonwealth accepts no liability for any loss suffered as a result of reliance it. AUSTRAC recommends that cash dealers, reporting entities and other stakeholders should obtain their own legal and/or technical advice on matters arising from the AML/CTF Act, the FTR Act, regulations and/or the published Anti-Money Laundering/Counter-Terrorism Financing Rules (AML/CTF Rules) tailored to the cash dealer, reporting entity or other stakeholder's specific circumstances, prior to making any decisions. The information contained in the AML/CTF Programs course is current as at the version date which appears on the AML/CTF Programs course.

Your use of this application does not relieve you of any obligations you may have under any legislation, subordinate legislation, rules, requirements or standards, including but not limited to the AML/CTF Act and the FTR Act.

Cash dealers, reporting entities and other stakeholders using this application should be aware of any obligations they may have under the *Privacy Act 1988* (Cth). These obligations could include a duty of confidentiality to their customers and not using personal information for an improper purpose. Further information regarding privacy obligations can be obtained from the Privacy Commission via www.privacy.gov.au or telephone **1300 363 992**. [Click here for AUSTRAC's privacy statement.](#)