Australian Government
AUSTRAC

FIGHTING FINANCIAL CRIME TOGETHER

Preparing and implementing an AML/CTF program

A guide for independent remittance service providers

CONTENTS

Introduction

This guide has been prepared for independent remittance service providers. Should your business provide additional designated services, you should seek independent advice.

Important: Following this guide will not automatically fulfil your business' AML/CTF program obligation. The intention of the guide is to bring to light important considerations for your business in its development of an AML/CTF program, so as to support your identification, mitigation and management of the money laundering and terrorism financing (ML/TF) risks your business faces when providing remittance services.

Your obligations

The guidance focuses on the AML/CTF obligations below, but does not go into comprehensive detail about all obligations. For more detail, refer to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* (No. 1) (AML/CTF Rules) and the AUSTRAC website.

Key terms and concepts

For a list of key terms and concepts discussed in this guide, see the glossary on our website at **austrac.gov.au/glossary**

Are you a remittance service provider?

If your business provides remittance services, under the AML/CTF Act you are required to:

- enrol your business with AUSTRAC
- register your business with AUSTRAC
- adopt and maintain an AML/CTF program that reflects your business' operations to identify, mitigate and manage ML/TF risk
- report suspicious matters, international funds transfer instructions and threshold transactions to AUSTRAC
- keep records relating to customer identification, transactions, and your AML/CTF program, including its adoption.

AUSTRAC Online

AUSTRAC provides an internet-based portal called AUSTRAC Online designed to assist businesses with their regulatory obligations under the AML/CTF Act.

AUSTRAC Online enables you to create your own business account which:

- allows for the electronic submission of transaction reports
- enables you to view and maintain your own information as held by AUSTRAC
- provides a secure system enabling the protection of confidential information
- allows for electronic submission of the AML/CTF compliance report
- assists AUSTRAC to support industry by better understanding the regulated population.

AUSTRAC Online is available if you have AML/CTF Act obligations.

To create an AUSTRAC Online business account see, **austrac.gov.au/enrol-register**

To access the AUSTRAC Online user guide, see **austrac.gov.au/manage-account**

AML/CTF program checklist

You must develop, adopt and maintain an anti-money laundering and counter-terrorism financing (AML/CTF) program that reflects your business' circumstances. Your AML/CTF program needs to set out the ways your business will comply with its AML/CTF obligations and identify, mitigate and manage money laundering and terrorism financing (ML/TF) risks.

An AML/CTF program needs to include the following components (see below). Record keeping is also an important part of your AML/CTF obligations.

Component	Task	Check
AML/CTF program:	1. Complete and review an ML/TF risk assessment of your business	❑
	2. Design and adopt an AML/CTF risk awareness training program	❑
	3. Design and adopt an employee due diligence program	❑
	4. Formally adopt the AML/CTF program and subject it to ongoing oversight by senior management/board	❑
	5. Appoint an AML/CTF compliance officer	❑
	6. Subject your AML/CTF program to regular independent reviews	❑
	7. Describe procedures for responding to AUSTRAC feedback	❑
	8. Describe your reporting procedures	❑
	9. Set out procedures for keeping your AUSTRAC enrolment and registration details current	❑
	10. Set out your procedures for collecting and verifying 'know your customer' (KYC) information	❑
	11. Set out your procedures for ongoing customer due diligence, including transaction monitoring and your enhanced customer due diligence program	❑
	12. Keep records	❑

1.

ML/TF RISK ASSESSMENT

Understanding the money laundering and terrorism financing (ML/TF) risks your business faces is a crucial step in developing, implementing and maintaining controls, systems and procedures that mitigate and manage your ML/TF risks.

Conducting an ML/TF risk assessment

To identify your business' ML/TF risks, you need to consider:

- your customer profiles, including:
  - the types of customers you have and their source of funds
  - customers domiciled in foreign countries
  - the nature and purpose of your business relationship with your customers
  - whether any of your customers are likely to be Politically Exposed Persons (PEP)
- the 'designated services' your business provides and the methods of service delivery
- whether your customers conduct their transactions using physical cash
- the criminal threat environment and possible vulnerabilities of your business
- the foreign jurisdictions in which your business provides services.

Below is a list of examples that you should consider when conducting your risk assessment.

Services and methods of delivery

What services do you provide to your customers?

Transfer money as a result of receiving international fund transfer instructions (IFTIs) where you:

- accept instructions to transfer money or property to a recipient in Australia (incoming)
- accept instructions to transfer money or property to a recipient outside of Australia (outgoing)
- other.

Do you accept cash from or use cash to pay customers?

Note: Where physical cash of AUD 10,000 or more (or the foreign currency equivalent) is accepted or paid out by your business for the transfer of money, you have threshold transaction reporting obligations.

Do you impose transaction limits?

For example: do you limit the amount a customer can transfer per transaction or per day?

Customer profile

Identify the types of customers you deal with and for each customer type, describe known transaction patterns.

Some matters to consider are:

- the types of customers, such as individuals or companies, regular or casual customers
- the physical location of any overseas customers (e.g. whether customers are located in foreign countries that may be considered a higher risk)
- providing services online, by phone or over-the-counter to customers.

For each customer type, describe known or expected transaction patterns. Examples of the usual or unusual customer behaviours or risk factors you may consider including are when:

- there is a higher than normal frequency or unusual movement of funds without reasonable explanation
- the source of funds cannot be easily verified
- a customer structures transactions in an attempt to break up amounts to stay under reporting thresholds
- a transaction is unnecessarily complex with no apparent reason
- the number and value of transactions is inconsistent with the financial standing or occupation, or is outside the normal course of business of the customer
- a customer sends or receives money to or from a higher risk jurisdiction
- a network of customers are using shared contact information such as address and contact telephone numbers
- a customer involved in the transaction appears to have no apparent ties to the destination country and provides no reasonable explanation for transfer
- the customer is suspected of presenting false identification
- there are doubts as to whether a customer is acting on their own behalf or, whether it appears the customer is fronting on behalf of another person and the 'other' person cannot be identified.

Examples of risks to the remittance service provider sector

The following table is a template which may assist you to identify and assess possible ML/TF risks posed to your business.

Important: the following suggested list of ML/TF risk indicators and treatment/actions is not exhaustive and is only to serve as a guide when considering the ML/TF risks that might apply to your business and examples of treatment strategies you should have in place to mitigate those risks.

See **austrac.gov.au/managing-risk** for detailed guidance on how to assess your ML/TF risk.

ML/TF risk indicators	Risk rating			Potential Treatment/Action
	Likelihood	Consequence	Risk score	
Customer provides insufficient, incomplete, false or suspicious information that cannot be verified				• Customer due diligence (CDD) procedures to identify and verify all customers and refuse customers that cannot meet those procedures. • Procedures to identify suspicious matters and submit suspicious matter reports (SMR) to AUSTRAC. • Employee AML/CTF risk awareness training program so staff are aware of requirements.
Customer sending money internationally for reasons such as to claim lottery prize winnings or to someone they have met online.				• CDD procedures to identify and verify all customers and consider refusing customers suspected of being victims of a scam. • Procedures to identify suspicious matters and submit SMRs to AUSTRAC. • Employee AML/CTF risk awareness training program so staff are aware of requirements.
Customers or transactions in high risk locations and sanctioned countries (e.g. prescribed foreign countries and the application of sanctions laws)				• Screen customers using the DFAT Consolidated List for sanctions monitoring. • Procedures to undertake enhanced customer due diligence, in particular, where it determines the ML/TF risk is high or a party is present in a prescribed foreign country. • Procedures to identify suspicious matters and submit SMRs to AUSTRAC. • Employee AML/CTF risk awareness training program so staff are aware of requirements.
Unusual patterns of transaction activity (e.g. volumes, frequency, structuring to avoid detection/ reporting obligations, source, destination)				• Transaction monitoring program. • Limit the value of transactions that can be conducted in a day/week/month. • Procedures to undertake enhanced customer due diligence, in particular, where it determines the ML/TF risk is high or a party is present in a prescribed foreign country. • Procedures to identify suspicious matters and submit SMRs to AUSTRAC. • Employee AML/CTF risk awareness training program so staff are aware of requirements.
Number or value of transactions is inconsistent with financial standing or occupation, or is outside the normal profile of the customer				• Procedures to undertake enhanced customer due diligence, in particular, where it determines the ML/TF risk is high or a party is present in a prescribed foreign country. • Limit the value of transactions that can be conducted in a day/week/month. • Procedures to identify suspicious matters and submit SMRs to AUSTRAC. • Employee AML/CTF risk awareness training program so staff are aware of requirements.
Transactions involving amounts below AUD 10,000 to avoid AUSTRAC threshold reporting requirements (structuring)				• Transaction monitoring program in place • Procedures to identify suspicious matters and submit SMRs to AUSTRAC. • Employee AML/CTF risk awareness training program so staff are aware of requirements.
PEP or his/her family members or close associates; where the beneficial owner of a customer is a PEP				• CDD procedures to identify and verify all customers. • Online website searches to identify possible PEPs. • Procedures to identify suspicious matters and submit SMRs to AUSTRAC. • Employee AML/CTF risk awareness training program so staff are aware of requirements.

Identify changes in ML/TF risk

You must be able to monitor and identify changes in the external ML/TF risk environment. This is so you can respond by adjusting the administration of your services, customers, relationships and delivery methods in order to mitigate new and emerging ML/TF risks.

The risk of your business being used for ML/TF and other serious criminal activity also changes when you start to serve new or different types of customers or jurisdictions, provide new products or services, or change the manner or method in which you provide those services. These ML/TF and other serious criminal activity risks must be assessed before you adopt new services, products or technologies.

Examples of matters you need to consider and assess for ML/TF risk include:

- offering services to new customer types and/or customers located in different foreign jurisdictions
- customers whose identification is difficult to collect or verify
- complex business ownership structures with the potential to conceal underlying beneficial owners or controlling person(s) of a business
- a customer or group of customers making frequent transactions to the same individual/group of individuals
- an individual (or an immediate relative) holding a public position and/or situated in a location which carries a risk of exposure to the possibility of corruption
- customers based in, or conducting business in or through, a high risk jurisdiction, or a jurisdiction with known higher levels of corruption or terrorism, organised crime or drug production/distribution
- a customer's unwillingness to produce evidence of ID or the production of unsatisfactory evidence of ID
- a new customer, particularly one who does not deal face-to-face or wants to carry out a large one-off transaction
- customers that are not local to the business or outside your normal target customer base
- an established customer who begins remitting more often than they usually or normally do
- customers engaged in a business which involves significant amounts of cash
- emergence of crime types within your local community.

After you identify changes in the ML/TF risk environment, you must update your risk assessment accordingly. You should make a record of the changes in risk that you identify, and update your systems and controls to manage the changed risks.

Who in your business is responsible for maintaining awareness of and identifying changes in ML/TF risk.

You might want to identify the specific position in your business, rather than an individual's name. Then, if the person in the position changes, you will not have to update your AML/CTF program if the person leaves the organisation.

- Title or position that will be responsible in your AML/CTF program.
- Name of the person who holds this position.

How this person will maintain awareness of and identify changes in ML/TF risk.

For example:

- ensure your business' enrolment and registration details are up-to-date to receive updates from AUSTRAC. You can do this via AUSTRAC Online (see page 4 for further information).
- subscribe to industry bulletins, attend industry events and undertake relevant training
- attend board meetings/senior management meetings regarding any business changes
- regularly monitor trends/methods in your operating environment (e.g. review transaction monitoring triggers and hits)
- regularly review the AUSTRAC website or follow AUSTRAC on social media.

How your business will respond to changes in ML/TF risk.

For example:

- update the risk assessment
- implement new or updated policies, procedures or systems
- keep records of changes to your business' risk assessment
- keep records of changes to your business' policies, procedures or systems.

Further information: AML/CTF Rules: Parts 8.1.4–8.1.5

2. AML/CTF RISK AWARENESS TRAINING PROGRAM

You need to train your employees about your business' ML/TF risk and your AML/CTF procedures.

Your risk awareness training program needs to include the following elements:

- your business' obligations under the AML/CTF Act and the consequences of non-compliance
- the types of ML/TF risk your business might face and the potential consequences
- the processes and procedures in your AML/CTF program relevant to the work carried out by your employees.

List who will receive AML/CTF training:

- all staff
- specific staff – list which staff.

Describe the following in your program:

- How often employees will receive AML/CTF training.
  For example: frequency, following introduction of new systems, when new staff commence.
- Who will deliver the training.
  For example: the compliance officer, an external service provider.
- How the AML/CTF training will be delivered.
  For example: on-the-job training, online training and/or interactive seminar.
- How you will maintain records of who has completed training and whose training is outstanding.
  For example: is this coordinated through the AML/CTF compliance officer?
- How you will ensure employees are kept up-to-date with new AML/CTF issues.
  For example: AML/CTF issues and compliance is a standing agenda item at staff meetings.

Further information: AML/CTF Rules: Part 8.2

3.

EMPLOYEE DUE DILIGENCE PROGRAM

Your AML/CTF program must have an employee due diligence program that sets out how you will screen employees who might be in a position to facilitate ML/TF.

List which roles in your business could give staff the opportunity to facilitate ML/TF offences:

- customer service personnel
- support/administration, accounts personnel
- any person who can exercise influence, or can make decisions in relation to the operations and conduct of the business (e.g. directors, management and supervision roles)
- any others.

Describe what checks you will perform on prospective employees before you hire them.

Some examples include the following:

- Verify the identity of prospective employees (e.g. request a certified copy of a driver's licence or passport).
- Conduct work history checks and character reference checks.
- Conduct criminal history checks (i.e. National Police Certificate).

Note: National Police Certificates are required as part of your registration obligations for the owner of the business and other key personnel.

- Conduct bankruptcy registry checks.
- Conduct credit reference checks to ensure that the employee is not under undue financial pressure.
- Other (please describe).

Describe any additional checks will you perform on an employee who is transferred or promoted to a position, which could give them the opportunity to facilitate ML/TF.

Describe how you will supervise employees to ensure they follow your AML/CTF procedures and do not collude with customers to facilitate ML/TF.

Describe what you will do if an employee breaches your AML/CTF procedures.

- Issue a formal warning.
- Cconduct refresher training.
- Rreassignment of duties.
- Dismissal.
- Other actions.

Further information: AML/CTF Rules: Part 8.3

4.

ADOPT THE AML/CTF PROGRAM AND ENSURE ONGOING OVERSIGHT OF YOUR PROGRAM

Record the date you adopted, and who approved your AML/CTF program. Include details of how this has been recorded.

List details including dates and names/positions of approvers.

Describe how you and/or senior management will oversee the program and ensure it is up-to-date and working on an ongoing basis.

For example: having AML/CTF as a standing meeting agenda item, regular briefings by the AML/CTF compliance officer, or having the independent reviewer present their findings to you and/or senior management.

Further information: AML/CTF Rules: Part 8.4

5.

AML/CTF COMPLIANCE OFFICER

You must appoint someone at management level to be your AML/CTF compliance officer.

Record who the AML/CTF compliance officer is in your business.

You may want to attach the compliance officer role to a specific position in your business, rather than an individual's name. Then, if the person in the position changes, you will not have to update your AML/CTF program if the person leaves the organisation.

- Title or position that will be responsible in your AML/CTF program.
- Name of the person who holds this position.

Record who the backup person for this role is.

The backup person should assume the AML/CTF compliance officer role when the nominated compliance officer is absent.

- Title or position that will be the backup in your AML/CTF program.
- Name of the person who holds this position.

Further information: AML/CTF Rules: Part 8.5

6.

ESTABLISH REGULAR INDEPENDENT REVIEWS OF YOUR AML/CTF PROGRAM

Your AML/CTF program must be subject to regular independent review.

The review's result, including any report prepared, must be provided to your business' board, executive and/or senior management.

In your program, describe the following:

- Who will conduct the independent review.
- How often the review will be conducted.
  For example: every 12 months, every 24 months, when business practices change, introducing new products and services or in response to a major ML/TF event.
- How you will ensure the reviewer is independent.
  For example: the reviewer is able to conduct the review without being compromised in reaching a conclusion; they did not design, develop, implement, maintain or manage the AML/CTF program; and the reviewer can make enquiries of any employee and access all relevant sources of information.
- The review process
  For example: what documents will the reviewer have access to? Will they come onsite? Will they speak to staff and/or the board, executives and/or senior management?
- How matters arising from the review will be addressed
  For example: what timeframes will you apply? What input will the board, executives and/or senior management have in coming to a solution?

Further information: AML/CTF Rules: Part 8.6

7.

RESPONDING TO AUSTRAC FEEDBACK

You must have procedures in place to ensure you have regard to feedback from AUSTRAC about your AML/CTF obligations, compliance and/or ML/TF risks. This feedback can be specific to your business, or it can be general feedback to the sector or all reporting entities.

Not all feedback requires responding to AUSTRAC. Some of it will be general advice that can be considered and implemented by your business. However, sometimes AUSTRAC will request a response from you. In these circumstances, it is important that responses are received in a timely manner.

Describe who is responsible for keeping informed of and responding to AUSTRAC feedback. Describe how they will ensure feedback is recorded and responded to in a timely manner, and how the business owner, board or executives, and relevant employees will be notified.

For example: the compliance officer as part of their duties.

Further information: AML/CTF Rules: Part 8.7

8.

YOUR REPORTING PROCEDURES

You need to provide AUSTRAC with reports about suspicious matters, international fund transfers, threshold transactions and compliance with your AML/CTF obligations. Refer to section 14 of the AUSTRAC Online user guide.

Suspicious matter reporting

One of the most important ways your business can help fight and disrupt ML/TF is to let AUSTRAC know when you see something suspicious or detect suspicious transactions or activity by completing and submitting an SMR. Prompt and accurate reporting of suspicious customer activity is invaluable in assisting AUSTRAC and partner agencies with the identification of illegal activity. A suspicious matter can relate to any crime, not just ML/TF.

Some common themes or indicators reported in SMRs include:

- customers who undertake transactions that appear inconsistent with their profile
- customers who conduct multiple transactions within a short time frame
- customers who exhibit irregular behaviour or patterns of transactions
- use of currency that is in an unusual condition (for example, dirty, wet, smelly).
- International funds transfers to high-risk countries, where such transactions are inconsistent with the customer's profile. High-risk countries include:
    - countries commonly associated with the production or transport of drugs
    - countries known to be tax havens
    - countries associated with phishing scams and card skimming
    - countries associated with child exploitation.

You must report suspicious matters to AUSTRAC about any remittance service that you provide, propose to provide, or have been asked to provide by a customer. This requirement applies whether you end up providing the service to that customer or not.

It is an offence to tell anyone apart from AUSTRAC that you have formed a suspicion about a customer. Therefore, in some circumstances it might not be appropriate to obtain further information from a customer or a third party when you cannot do so without alerting, or 'tipping off' the customer or third party to your suspicions.

Further information: AML/CTF Act: Section 41 and AML/CTF Rules: Chapter 18

Time frames

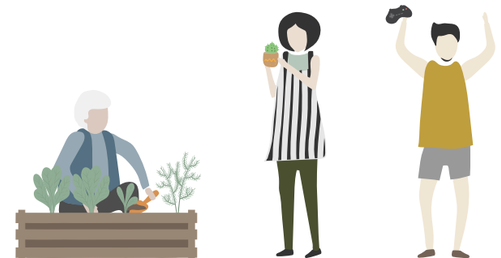
You must complete an SMR and submit it to AUSTRAC within:

- 24 hours if your suspicion relates to terrorism financing.
- 3 business days if your suspicion relates to money laundering, tax evasion or another ground of suspicion other than terrorism financing.
- Reports can be submitted electronically via AUSTRAC Online.

Describe the following in your program:

- What your employees do when they think a customer or matter is suspicious.
  For example: inform the AML/CTF compliance officer, complete an SMR.
- Who is responsible for submitting SMRs to AUSTRAC.
  For example: the AML/CTF compliance officer.
- How you will ensure that SMRs are submitted within the required time frames.
  For example: daily review of suspicious matter register, providing all relevant staff with AUSTRAC Online account access.

Further information: AML/CTF Rules: Part 8.9



International Funds Transfer Instructions

If you receive an instruction to send or receive funds to or from a foreign country, you need to submit an international funds transfer instruction (IFTI) report to AUSTRAC.

Further information: AML/CTF Act: Section 45 AML/CTF Rules: Chapter 17

Time frames

You must submit a completed IFTI report to AUSTRAC within 10 business days after the day on which the instruction was sent or received by you.

Describe the following in your program:

- Who is responsible for submitting an IFTI to AUSTRAC
  For example: the AML/CTF compliance officer.
- How you will ensure that IFTIs are submitted within the required time frames.
  For example: daily review of transaction register, providing all with AUSTRAC Online account access.

Further information: AML/CTF Rules: Part 8.9

Threshold transaction reports

You need to submit a threshold transaction report (TTR) to AUSTRAC if a customer provides you with or is paid with physical cash of AUD 10,000 or more (or foreign currency equivalent).

Further information: AML/CTF Act: Section 43, AML/CTF Rules: Chapter 19

Time frames

You must complete a TTR and submit it to AUSTRAC within 10 business days after you provide the remittance service.

Reports can be submitted electronically via AUSTRAC Online.

Describe the following in your program:

- What your employees do when they provide or are paid physical cash of AUD 10,000 or more.
  For example: inform the AML/CTF compliance officer, complete a TTR form.
- Who is responsible for submitting TTRs to AUSTRAC.
  For example: the AML/CTF compliance officer.
- How you will ensure that TTRs are submitted within the required time frames.
  For example: daily review of transaction register, providing all with AUSTRAC Online account access.

Further information: AML/CTF Rules: Part 8.9

Compliance reporting

Your business may have to submit a compliance report to AUSTRAC to let us know whether and how you are meeting your obligations. AUSTRAC will let you know when the compliance report is due. It is very important that you keep your email address up-to-date so you know when you need to submit your compliance report.

Describe the following in your program:

- Who at your business will be responsible for submitting a full and accurate compliance report to AUSTRAC.
  For example: the AML/CTF compliance officer.
- How you will ensure AML/CTF compliance reports are submitted by the due date.
  For example: ensure the business' details are up-to-date with AUSTRAC to receive AML/CTF compliance report notifications.

Further information: AML/CTF Act: Section 47, AML/CTF Rules: Chapter 11

9. MAINTAINING ENROLMENT AND REGISTRATION DETAILS WITH AUSTRAC

As a registered business, you have requirements to maintain your business enrolment and registration details with AUSTRAC, such as notifying AUSTRAC of any material changes as well as renewing your business' registration at three yearly intervals.

For information about your business' ongoing enrolment and registration requirements, refer to the AUSTRAC website.

Describe who in your business is responsible for maintaining business and registration details.

For example: business owner, company secretary, accountant, office manager, compliance officer.

Describe how this person will identify or be notified of changes to business and registration details.

For example:

- work closely with the business owner or company secretary in relation to business ownership and control changes and/or other registration or licensing requirements with other regulators
- work closely with human resource personnel in relation to staff movements and changes to key personnel details or circumstances.

Further information: AML/CTF Act: Sections 51 and 75

10.

COLLECT AND VERIFY KYC INFORMATION

You need to document the procedures you use to collect and verify (KYC) information about your customers.

Collection of KYC information generally involves asking a customer to state their personal details (e.g. by providing these details on a paper-based or web form).

Verification of KYC information generally involves confirming those details against identification documents such as a driver's licence or passport and/or online identification verification services such as the Australian Government's Document Verification Service (DVS) and other similar third party service providers.

A. Collection and verification of KYC information

You must collect and verify KYC information from a customer prior to providing a designated service to that customer.

The types of information that you must collect and verify will depend on the type of customer that you provide the designated service to.

List the types of customers you do business with.

Note: you should list the customer types that you will do business with in your program. Your customer types should be based on your customer risk assessment (see section 1 of this guide). You may decide that some customer types – i.e. all customer types other than individuals – pose an unacceptable ML/TF risk and therefore choose not to do business with those customer types.

❑	Individuals	❑	Partnerships
❑	Domestic companies	❑	Incorporated associations
❑	Registered foreign companies	❑	Unincorporated associations
❑	Unregistered foreign companies	❑	Registered co-operatives
❑	Trustees of trusts	❑	Government bodies

For individuals and domestic companies, you must undertake the steps outlined in the relevant section below prior to providing a designated service to the customer.

Note: If you provide designated services to customer types other than individuals and domestic companies you need to have additional procedures to identify and verify these customers. You can refer to the AUSTRAC website for further information relating to these customers.

Individuals

Collection of minimum information	
The minimum information you must collect from a customer who is an individual is:	Full name
	Residential address
	Date of birth
Where a customer is operating as a sole trader, you must collect the following additional information:	The full business name under which the customer carries on their business; and
	Any Australian Business Number (ABN) issued to the customer

Verification of minimum information	
The minimum identification information that needs to be verified for an individual is:	Full name
	Date of birth **or** residential address
Describe how you will verify the identification information of an individual.	Reliable and independent documentation
	Reliable and independent electronic data
	A combination of the above

Documentation-based verification	
If you have chosen to use the document-based verification process, you need to verify the minimum identification information against one or more government-issued identification documents. **List which identification documents you will verify against.**	Drivers licence
	Passport
	Proof-of-age card
	Other government-issued photographic ID
You must only accept an identification document that has not expired (the exception to this is an Australian passport that has expired within the preceding two years).	

Electronic-based verification	
If you have chosen to use an electronic-based verification process, you must verify the following using reliable and independent electronic data: **Describe what reliable and independent electronic data you will rely upon in order to undertake verification of customer information, and how you will determine that the data is reliable and independent.**	Customer's name from at least two separate data sources
	Customer's residential address and/or date of birth from at least two separate data sources
For example: you may require a customer to enter a driver's licence and passport number and use these to verify the customer's details using the DVS. Alternatives could include using a commercial provider which may provide access to the DVS, as well as other sources such as Australian electoral roll or credit bureau data.	

High ML/TF risk	
Where you assess that the ML/TF risk associated with a customer, or the provision of a designated service to a customer, is high you must undertake additional steps to verify their identity. **Describe what additional steps you will take to verify the identity of a customer whose ML/TF risk is high.**	Undertake both electronic-based and document-based verification
	Require verification against additional electronic sources
	Authenticate/verify identification documentation provided by the customer (for example, by contacting the issuing authority or using the DVS)
	Other

Collection and verification of additional information	
In addition to the minimum information outlined above, you need to have systems and controls to determine whether and in what circumstances additional KYC information should be collected. **Describe what additional information you will collect for individual customers.**	Mobile phone number – verified through sending a one-time password to the number that the customer must enter
	Email address – verified by sending an activation link or one-time password to the email address that the customer must click or enter
	Other
Describe the circumstances when you will collect and/or verify this additional information. You may wish to collect and/or verify this information only in particular circumstances – for example, only when a customer seeks to transfer a significant amount of money (e.g. when they want to transfer $500 or more). Similarly, you might decide to collect both mobile phone and email address, but only require one of these to be verified.	

Companies – domestic

Collection of minimum information	
The minimum information you must collect from a customer who is a domestic company is:	Full legal name, being the name that it has registered with the Australian Securities and Investments Commission (ASIC)
	Full address of the entity (a principal place of business address, registered office address or both)
	Australian Company Number (ACN) issued to the company
	Whether the company is a proprietary or public company
	If the company is registered as a proprietary company, the name of each director of the company

Verification of minimum information	
Simplified verification procedures	
You may rely upon the simplified company verification procedure if the company is:	A domestic listed public company
	A majority owned subsidiary of a domestic listed public company **or**
	Licenced and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company
In the above circumstances, you may verify the company by obtaining and documenting:	A record of the company from the website of the relevant domestic stock exchange (i.e. the Australian Stock Exchange)
	A public document issued by the company (such as an annual financial report)
	A search of the ASIC Connect website **or**
	A search of the licence or other records of the relevant records of a relevant regulator

Where simplified verification procedures do not apply	
For all other domestic companies, you must verify the following information:	The full legal name of the company
	Whether the company is registered as a proprietary or public company
	The ACN issued to the company

Describe how you will verify this information.	Obtaining a certificate of registration for the company
	Manually searching and accessing the information from ASIC Connect
	Using a verification service that verifies against reliable and independent electronic data
	Other

Collection and verification of additional information	
In addition to the minimum information outlined above, you need to have systems and controls to determine whether and in what circumstances additional KYC information should be collected. **Describe what additional information you will collect for domestic company customers.**	Australian Business Number (ABN) – verified by accessing the Australian Business Register's (ABR) ABN Lookup website (https://abr.business.gov.au/) and/or using the ABN Lookup API
	Industry type classification – verified by accessing the website of the company or a business directory
	Professional registration/licensing numbers (such as an Australian Financial Services Licensee number) – verified by accessing the website of the registering/licensing authority
	Other
Describe the circumstances when you will collect and/or verify this additional information. ***For example:*** you may wish to collect the Australian Financial Services Licensee number if they are carrying on a financial services business in Australia.	

Beneficial owners	
If the domestic company customer has been verified using the simplified company verification procedure above, you do not need to identify the beneficial owners of the company. **For all other domestic company customers, you must seek to identify the beneficial owners of that company.** **Describe how you will seek to identify the beneficial owners of a domestic company customer.**	Collecting this information from the customer
	Obtaining a current and historical company extract from ASIC or an ASIC Information Broker
	Using an online identification verification service
Where you cannot identify a beneficial owner after undertaking the above step(s), you must treat as a beneficial owner any individuals who:	Are entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including a power of veto **or**
	Hold the position of senior managing official or equivalent
For all individuals who are identified as a beneficial owner, you must undertake the same steps to collect and verify information from them as you would from an individual customer (see section above).	

B. Politically exposed persons

When you collect and verify the identity of a customer in the circumstances set out above, you must also determine whether the customer is a PEP.

Describe the following in your program:

- How you will determine whether a customer is a PEP.
  For example: by conducting an internet search.
- How you will determine if a PEP is high risk.
  For example: by the number of mentions or severity of media articles. Foreign PEPs are automatically considered high-risk under AML/CTF legislation.
- The steps will you take to mitigate the risk associated with a PEP.
  For example: enhanced customer due diligence and monitoring.

Further information: AML/CTF Rules: Part 4.13

C. Responding to discrepancies

You need to establish a risk-based system to respond to any discrepancy that arises in the course of verifying information about a customer so that you can be certain that the customer exists and is who they claim to be.

Describe what you would do if you identified a discrepancy in the course of verifying information about a customer.

For example: you suspect that the identification documentation is false or the customer is not who they claim to be. Would you request additional information? Would you require that a senior officer (such as the Compliance Officer) reviews the customer information to make a decision about whether to commence a business relationship with the customer? Would you undertake Enhanced Customer Due Diligence?

Record the information you would ask for and/or verify in the above situations.

Further information: AML/CTF Rules: Part 4.2.5

D. Recording KYC information

You need to keep records of all customer identification that you undertake. This allows you to meet your legislative obligations, and provides useful information for transaction monitoring, enhanced customer due diligence and/or suspicious matter reporting, and demonstrates that you are compliant with AML/CTF Act obligations.

Describe how you record details of the identification process and verification documents in your program.

For example: writing down the driver's licence number, scanning and/or saving identification documents, retaining verification confirmations from the DVS or similar service providers.

11.

ONGOING CUSTOMER DUE DILIGENCE & TRANSACTION MONITORING

A. Updating, verifying and re-verifying customer information

You need to establish risk-based systems and controls to help you determine whether—in certain circumstances—you will need to update, verify and/or re-verify details held about a customer. This is similar to the collection/verification of additional customer information discussed above (see '10. Collect and verify KYC information'). However, ongoing customer due diligence occurs after the relationship with the customer has been established, not when it is being established.

Describe what circumstances would cause you to update, verify and/or re-verify customer information.

For example: you become aware that the customer's address, name, employment situation or circumstance changes, or there is a change in their transaction patterns such as the countries they are sending money to, frequency, volume, value, source or destination of funds, or you suspect the customer may be involved in suspicious activity.

Further information: AML/CTF Rules: Parts 15.2–15.3

B. Monitoring your customers' transactions

You need to establish and maintain a transaction monitoring program to identify any transactions that appear to be suspicious and therefore reportable to AUSTRAC. This includes:

- complex transactions
- unusual and large transactions
- unusual patterns of transactions
- multiple transactions to avoid reporting thresholds
- transactions with no apparent economic or visibly lawful purpose.

The table below sets out some examples of the processes you could put in place to monitor transactions.

Action	Purpose	
Develop customer profiles and identify irregular and unusual patterns of transactions	❑	identify customers whose main source of funds are derived from cash or cash-equivalent transactions and third-party payment processes that provide anonymity to the source of funds
	❑	identify transactional activity that appears excessive for the customer, given their known source of funds
	❑	identify non-profit organisations (NPOs) transacting through remittance services in a manner expected of individuals (this could indicate misappropriation of funds)
	❑	identify transactions that do not fit the customer's normal profile
	❑	identify where multiple customers or agents are transferring funds to similar recipients/ countries
	❑	other
Describe how monitoring activities/results will be recorded.		
Develop transaction profiles and identify irregular transactions	❑	identify transactions that are structured below reporting thresholds
	❑	identify transaction patterns to high risk jurisdictions
	❑	identify transactions that are unusual or involving large amounts of funds/cash
	❑	identify transactions that send funds overseas and the customer receives approximate equivalent funds in return
	❑	other
Describe how monitoring activities/results will be recorded.		
Identify rapid movement of funds	❑	identify customers undertaking multiple transactions concurrently of varying amounts
	❑	other
Describe how monitoring activities/results will be recorded.		

Further information: AML/CTF Rules: Parts 15.4 – 15.7

C. 'Enhanced customer due diligence' procedures

You must have an enhanced customer due diligence program in place. This sets out your procedures for situations where there is a high ML/TF risk, when a suspicious matter reporting obligation arises, or where your customer is a PEP.

Your enhanced customer due diligence program must be applied when:

- your business has determined (under its risk-based systems and controls) that the ML/TF risk is high **or**
- your business is providing remittance services to a customer who is, or who has a beneficial owner who is, a PEP **or**
- your business has formed a suspicion regarding the transaction (see section 8 above for further information) **or**
- a party to the transaction (that your business has entered in or is proposing to enter into) is physically located in a prescribed foreign country.

Describe what you will do in situations where your enhanced customer due diligence is applied.

Appropriate to those circumstances outlined previously, a reporting entity must take the following measures.

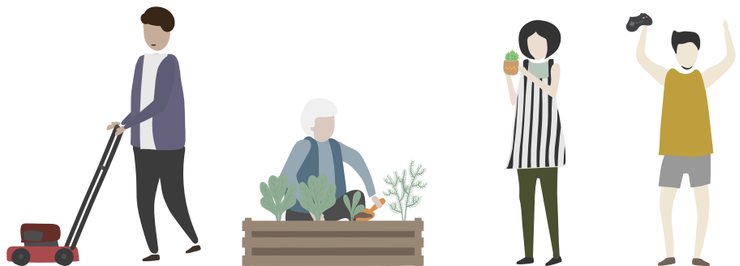
For each of the following, explain how you will undertake the required step.

- Seek further information from the customers or third party sources to:
  - clarify/update the customer's information
  - obtain further information about the customer
  - obtain information about the source of wealth or funds the customer is using to transfer
  - obtain information about the source of wealth or funds the customer is receiving
- Undertake more detailed analysis of the customer's information and/or transaction history.
- Verify or re-verify KYC information.
- Seek senior management approval for processing any future transactions.
- Other.

Describe who is responsible for conducting enhanced customer due diligence (ECDD).

You may want to attach the role to a specific position in your business, rather than an individual's name. Then, if the person in the position changes, you will not have to update your AML/CTF program if the person leaves the organisation.

- Title or position that will be responsible in your AML/CTF program.
- Name of the person who holds this position.



12.
RECORD KEEPING

Record keeping is an important part of your AML/CTF obligations. Remittance service providers must:

- retain records of customer identification for seven years after the date they last provided a service to the customer
- keep any transaction records for seven years after the transaction is conducted
- retain a copy of their AML/CTF program (and record of the adoption of the program) for seven years after the program ceases to have effect. If the AML/CTF program is modified, a copy of the old program must be kept for seven years from the date it is superseded by the new program.

Describe the following in your program:

- procedures your business will follow to ensure that records of customer identification documents will be retained for at least seven years.

  For example: photocopy, scan and save copies of identity documentation electronically.
- procedures your business will follow to record and retain transaction records for at least seven years.

  For example: save and backup records of transactions electronically.
- procedures your business will follow to retain records of current and superseded AML/CTF programs for at least seven years.

  For example: saving time-stamped electronic versions of each new program.

Australian Government

AUSTRAC