Australian Government

AUSTRAC

A guide to preparing and implementing an AML/CTF program

For your digital currency exchange service business

Introduction

This guide has been prepared for business entities that only provide designated digital currency exchange services. Should your business provide additional/other designated services, you should seek independent advice.

Important: Completion of the 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 ML/TF risks surrounding your business' provision of designated digital currency exchange services.

This guide has been developed in consultation with the Australian Digital Commerce Association (ADCA) and its members to accompany the commencement of the digital currency exchange service sector's AML/CTF compliance obligations effective from 3 April 2018.

AUSTRAC will continue to work closely with the sector to further expand and enhance the guidance based on operational experience and knowledge.

AUSTRAC invites you to submit your feedback and suggestions to Policy_Consultation@austrac.gov.au.

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 both Part A and Part B components (see below). Record keeping is also an important part of your AML/CTF obligations.

Component	Task	Check
AML/CTF program: **Part A**	1. Complete 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 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 ongoing customer due diligence, including transaction monitoring and your enhanced customer due diligence program	☐
	11. Keep records	☐
AML/CTF program: **Part B**	12. Set out your procedures for collecting and verifying 'know your customer' (KYC) information	☐
AUSTRAC – general information	13. How to apply for an exemption	☐
	14. Sanctions	☐

1. Money-laundering and terrorism financing risk assessment

Understanding the money laundering and terrorism financing (ML/TF) risks your business faces is an important step in developing, implementing and maintaining effective and balanced controls, systems and procedures that mitigate and manage these ML/TF risks. Reporting entities may consider adopting the following principles in developing a risk assessment, such as:

- the risk analysis should be solidly founded on reliable research and provide a true reflection of the inherent risks and the way your business mitigates those risks
- the risk criteria and categorisations chosen should be proportionate to the complexity of your business' products and services and be consistent with your risk analysis.

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 a foreign country
    - the nature and purpose of your business relationship with your customers
    - whether any of your customers are likely to be Politically Exposed Persons
- 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.

Services and methods of delivery

What services do you provide to your customers?

☐ Buying digital currency[1]

☐ Selling digital currency

☐ Exchanging digital currency

☐ Hold digital currency (on trust or as custodian)

☐ Other (please describe):

Provide details...

[1] Digital currency means a digital representation of value that functions as a medium of exchange, a store of economic value, or unit of account. Digital currency is not issued by or under the authority of a government. Digital currency is also commonly referred to as cryptocurrency or virtual currency.

List which digital currencies you offer for exchange?

Insert details...

Does your business purchase digital currencies from reliable sources?

Has your business undertaken due diligence on the supply sources of your purchased digital currencies?

Have you determined these digital currency supply sources to be trusted and reliable?

Are these digital currency supply sources contractually committed to backing the types of digital currencies that you are offering to your customers?

Insert details...

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

☐ Yes ☐ No

Note: Where physical cash of AUD10,000 or more (or the foreign currency equivalent) is accepted or paid out by your business for a digital currency transaction, you have threshold transaction reporting obligations.

Do you impose transaction limits?

☐ Yes ☐ No

Insert details...

What tools, including proprietary tools, does your business employ to monitor the blockchain and/or your customer activity?

Insert details...

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 or over-the-counter to customers.

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

- the scope of the exchange's thresholds or acceptable tolerance ranges within a single exchange, daily, weekly, monthly, etc.
- the frequency of a customer's exchange activities
- the amount that the customer exchanges to/from fiat currency (in total and on average)
- the frequency or unusual movement of digital currencies without reasonable explanation

- the situation of the origin of wealth or if the source of funds cannot be easily verified
- the customer is suspected of presenting false identification and verification information
- 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
- the customer is suspected of undertaking gambling activity using an illegal offshore wagering site
- the customer is suspected of being the perpetrator or is the victim of ‘ransomware’
- the customer is undertaking transactions involving the ‘darknet’.

Insert information about your types of customers...

Examples of risks to the digital currency exchange services 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 the *AUSTRAC compliance guide* for detailed guidance on how to conduct a risk assessment.

ML/TF risk indicators	Risk rating			Potential Treatment/Action
	Likelihood	Consequence	Risk score	
Customer provides insufficient, incomplete or suspicious information or information that cannot be verified				• Customer due diligence (CDD) procedures in place to identify and verify all customers • Procedures in place to identify suspicious matters and submit suspicious matter reports (SMR) to AUSTRAC • Employee AML/CTF risk awareness training program implemented
Use of proxies, unverifiable IP address or geographical location, disposable email address or mobile number, ever changing devices used to conduct transactions				• Collect IP addresses and other device identifiers • Ongoing customer due diligence and transaction monitoring program in place • CDD procedures in place to identify and verify all customers • Employee AML/CTF risk awareness training program implemented • Procedures in place to identify suspicious matters and submit SMRs to AUSTRAC • Require the use of one time PINs sent to (Australian) mobile phone number to conduct digital transactions
Customers or transactions in high risk locations (e.g. prescribed foreign countries and the application of sanctions laws)				• Screen customers against the DFAT Consolidated List for sanctions monitoring • Procedures in place 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 in place to identify suspicious matters and submit SMR to AUSTRAC • Employee AML/CTF risk awareness training program implemented

ML/TF risk indicators	Risk rating			Potential Treatment/Action
	Likelihood	Consequence	Risk score	
Unusual patterns of transaction activity (e.g. volumes, velocity, structuring to avoid detection/reporting obligations, source, destination)				• Transaction monitoring program in place • Limit the value of transactions that can be conducted in a day/week/month • Enhanced customer due diligence program in place • Employee AML/CTF risk awareness training program implemented • Procedures in place to identify suspicious matters and submit SMRs to AUSTRAC
Transactions involving known blacklisted addresses such as 'darknet' market place transactions and tumblers				• Transaction monitoring program (including tools to monitor the Blockchain) that screens for interaction with dark-net marketplace • Procedures in place to identify suspicious matters and submit SMR to AUSTRAC
Ransom-ware				• Procedures in place to identify suspicious matters and submit SMR to AUSTRAC • Employee AML/CTF risk awareness training program implemented
Transactions in higher risk or anonymous digital currencies				• Obtain additional customer information • Employee AML/CTF risk awareness training program implemented • Procedures in place to identify suspicious matters and submit SMR to AUSTRAC
Employee collusion				• Procedures in place to identify suspicious matters and submit SMRs to AUSTRAC • Employee due diligence processes in place • Employee AML/CTF risk awareness training program implemented

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, 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
- expanding your services to include additional digital currencies, cash transactions, additional payment or settlement methods, or other designated services
- the use and application of new technologies

After you identify changes in the ML/TF risk environment, you must update your risk assessment register 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.

Name: Enter name…

Title/position: Enter title/position...

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

For example:

- ensure your business' enrolment and registration AUSTRAC Online (see further information below) details are up-to-date to receive updates from AUSTRAC
- subscribe to industry bulletins, attend industry events
- 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.

Insert details...

How will your business 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.

Insert details...

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

Learn more about AUSTRAC Online.

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 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (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.

Who will receive AML/CTF training?

☐ All staff

☐ Other (please describe):

Provide details...

How often will employees receive AML/CTF training?

Provide details...

Who will deliver the training?

For example: the compliance officer, an external service provider.

Provide details...

How will the AML/CTF training be delivered?

For example: on-the-job training, online training and/or interactive seminar.

Provide details...

How will you maintain records of who has completed training and whose training is outstanding?

For example: is this coordinated through Human Resources or the AML/CTF compliance officer?

Provide details...

How will you 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.

Provide details...

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.

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)

☐ Other (please describe):

Provide details...

What checks will you 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 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):

Provide details...

What 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?

Provide details...

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

Provide details...

What will you do if an employee breaches your AML/CTF procedures?

☐ Issue a formal warning

☐ Conduct refresher training

☐ Reassignment of duties

☐ Dismissal

☐ Other (please describe):

Provide details...

Further information: AML/CTF Rules: Part 8.3

4. Adopt the AML/CTF program and ensure ongoing oversight of Part A

When did the board, executives and/or senior management adopt and approve your AML/CTF program? How has this been recorded?

Provide details...

On an ongoing basis, how will your board, executives and/or senior management oversee Part A of the program and ensure it is up-to-date and working?

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 the board, executives and/or senior management.

Provide details...

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.

Who is the AML/CTF compliance officer 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.

Name: Enter name…

Title/position: Enter title/position...

Who is the backup person?

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

Name: Enter name…

Title/position: Enter title/position...

Further information: AML/CTF Rules: Part 8.5

6. Establish regular independent reviews of Part A of your AML/CTF program

Part A of 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.

Who will conduct the independent review?

Provide details...

How often will the review be conducted?

For example: every 12 months, every 24 months, when business practices change, or in response to a major ML/TF event.

Provide details...

How will you 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.

Provide details...

Describe 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?

Provide details...

Describe 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?

Provide details...

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.

Who is responsible for keeping informed of and responding to AUSTRAC feedback? How do they ensure feedback is recorded and responded to in a timely manner, and that the business owner, board or executives, and relevant employees are notified?

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

Provide details...

Further information: AML/CTF Rules: Part 8.7

8. Your reporting procedures

You need to provide AUSTRAC with reports about suspicious matters, 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. A suspicious matter can relate to *any* crime, not just ML/TF.

You must report suspicious matters to AUSTRAC about any digital currency exchange 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.

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.

Scenarios of customer/transactional activity that may warrant the conduct of enhanced customer due diligence and/or raise a suspicion

Scenario 1: Customer provides false identification information

Customer A signs up with Entity A and provides the customer identification information requested on the website. Entity A verifies this information using a Know Your Customer (KYC) service (e.g. the Document Verification Service (DVS)).

Following the on-boarding of the customer, Entity A received a request to conduct an exchange for $3,000 worth of digital currency X. Entity A's transaction monitoring processes include cross checking the location of the customer's IP address with the information supplied at on-boarding.

The IP address indicated that Customer A was not in Australia and this prompted Entity A to put a hold on the transaction and make further inquiries. For example, making a phone call to the customer, sending a letter to the address provided or seeking additional KYC information such as certified photo ID being the customer's passport details.

Following these further inquiries, it was clear that Customer A is not who they claim to be because the letter was returned to sender, the phone number belonged to someone else, the passport number was invalid and/or details of the customer's IP address or device details suggested that the person was not located in Australia.

Having formed doubts about who Customer A claimed to be and whether they were actually based in Australia, the entity submitted an SMR to AUSTRAC and decided for commercial reasons to terminate the transaction and customer relationship.

In addition to the information provided in the “grounds for suspicion” section of the SMR, Entity A also included attachments such as a copy of the passport photo ID and on-boarding documentation provided by the customer.

Scenario 2: Customer interaction with the darknet, tumblers or illegal off-shore wagering websites

Customer B has successfully set up an account with Entity B and has requested it undertake several transactions. As part of its transaction monitoring program, Entity B monitors transactions using a commercially available public blockchain analysis tool. Through this process, Entity B was able to identify several, small interactions by the wallet address provided by Customer B with an illicit marketplace, tumbler or illegal off-shore wagering website.

Entity B submitted an SMR to AUSTRAC (advising in the SMR known customer and recipient identification details, wallet information, transaction details and attachments of transaction history) and terminated any pending transactions and the customer relationship because of the potential ML/TF risk arising from the customer’s activity.

Scenario 3: Ransomware

Customer C is seeking to sign up with Entity C. As part of the online identification process, Entity C asks the customer to confirm whether they have been subject to ransomware. Where the customer indicates that the purchase of digital currency is to pay ransomware, Entity C declines to register the customer and conduct any transactions.

Entity C also checks for known ransomware addresses (this information is often available publicly) to ensure that it does not send digital currency to these addresses.

Entity C reviewed the requested transactions and conducted enhanced customer due diligence. While Entity C recognised that the customer might have been the victim, it resolved on balance to submit an SMR to AUSTRAC in accordance with its internal risk management policy whenever there is any interaction involving ransomware addresses and detail as much as what is known about the ransomware perpetrator and how the victim was ensnared.

Scenario 4: Structuring

Entity D’s customer has requested to purchase digital currency using cash on three occasions in the space of two business days. On all occasions, Customer D seeks to purchase $9,000 worth of digital currency. Entity D believes that this is suspicious because Customer D is aware that a transaction equal to $10,000 or more in cash would require a TTR to be submitted to AUSTRAC. This behaviour – knowingly avoiding the TTR obligations – is known as structuring and is a criminal offence under the AML/CTF Act.

Entity D in reviewing the transaction considered the customer’s transaction history, the timeframes for the use of physical cash and resolved to submit an SMR to AUSTRAC because the behaviour had the characteristics of structuring. In the SMR, Entity D provided a history of their interactions with the customer and any attachments relating to their identity.

Scenario 5: Unable to identify the beneficial owner of a customer

Customer E (ABC Pty Ltd) is a company and is seeking to set up an account with Entity E. Under the beneficial ownership obligations, Entity E must identify the beneficial owners of Customer E.

Entity E asks Customer E to provide additional information regarding the structure and breakdown of shareholdings of the company, the names and addresses and dates of birth of the shareholders and a certificate of incorporation of the company with ASIC or any other supporting documentation.

Despite requests, Customer E could not provide sufficient information about the beneficial ownership and control of the company, and no independent documentation or online check verifying the information was available.

As a result, Entity E refused to proceed with registering the customer and submitted an SMR to AUSTRAC.

Scenario 6: Unusual rapid movement of funds

Customer G was recently on-boarded by Entity G. Customer G wishes to conduct several rapid exchanges between different currencies which differs from their customer profile and is considered unusual trading as it does not appear to have any financial benefit for the customer. Within a short period of time, Customer G then instructs Entity G to transfer all funds to a nominated bank account.

Entity G submits an SMR to AUSTRAC providing a history of the customer's behaviour as it appears to indicate activity such as money laundering, tax evasion or tax avoidance.

Scenario 7: Detection of an unregistered or operation of an illegal exchange

Customer H has made regular purchases of digital currency from Entity H for the past six months. These purchases are always followed by an immediate request to withdraw the digital currency to a particular wallet address.

In conducting routine transaction monitoring, Entity H discovered that Customer H had purchased significant amounts (in excess of $100,000 worth) of digital currency in six months.

As this activity did not reflect the customer's profile, Entity H submitted an SMR to AUSTRAC (advising in the SMR known customer and recipient identification details, wallet information, transaction details and attachments of transaction history) based on the suspicion that Customer H is operating an unregistered or illegal digital currency exchange business.

What do your employees do when they think a customer or matter is suspicious?

For example: inform the AML/CTF compliance officer, complete an SMR.

Provide details...

Who is responsible for submitting SMRs to AUSTRAC?

For example: the AML/CTF compliance officer.

Provide details...

How will you ensure that SMRs are submitted within the required time frames?

For example: daily review of suspicious matter register, providing all team leaders or managers with AUSTRAC Online account access.

Provide details...

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 AUD10,000 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 customer with a digital currency exchange service.

Reports can be submitted electronically via AUSTRAC Online.

What do your employees do when they provide or are paid physical cash of AUD10,000 or more?

For example: inform the AML/CTF compliance officer, complete a TTR form.

Provide details…

Who is responsible for submitting TTRs to AUSTRAC?

For example: the AML/CTF compliance officer.

Provide details...

How will you ensure that TTRs are submitted within the required time frames?

For example: daily review of transaction register, providing all team leaders or managers with AUSTRAC Online account access.

Provide details...

Compliance reporting

Your business must submit a compliance report to AUSTRAC to let us know whether 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.

Who at your business will be responsible for submitting a full and accurate compliance report to AUSTRAC?

For example: the AML/CTF compliance officer.

Provide details...

How will you ensure AML/CTF compliance reports are submitted by the due date?

For example: ensure the business' details are up-to-date to receive AML/CTF compliance report notifications.

Provide details...

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 further requirements to maintain your business enrolment and registration details with AUSTRAC, such as notifying AUSTRAC of any material changes and renewing your business' registration at three yearly intervals.

For information about your business' ongoing enrolment and registration requirements, refer to Chapters 4 and Chapter 5 of the AUSTRAC compliance guide.

Who in your business is responsible for maintaining business and registration details?

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

Insert persons name...

How will this person 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.

Insert details...

Further information: AML/CTF Act: 51F and 76P

10. 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 update, verify and/or re-verify details held about a customer. This is similar to the collection/verification of additional customer information discussed below (see '11. 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.

What circumstances would cause you to update, verify and/or re-verify customer information?

Examples include: you become aware that the customer's address, name, employment situation or circumstance changes, or there is a change in their exchange transaction patterns such as the types of digital currency transacted, frequency, volume, value, source or destination of funds, or you suspect the customer may be involved in suspicious activity.

Provide details...

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 involving a range of digital currencies
- digital currencies that pose a higher ML/TF risk or provide greater anonymity.

Note: Some reporting entities may use proprietary tools to assist in conducting transaction monitoring (for example, a blockchain analysis tool).

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

Action	Purpose	How will monitoring activities/results be recorded?

Action	Purpose	How will monitoring activities/results be recorded?
Develop customer profiles and identify irregular and unusual patterns of transactions	☐ identify customers whose predominant source of funds are derived from cash or cash-equivalent transactions, other digital currency exchanges 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 businesses transacting through digital currency exchanges in a manner expected of individuals (could indicate a front, shell and/or shelf companies ☐ identify non-profit organisations (NPOs) transacting through digital currency exchanges in a manner expected of individuals (this could indicate misappropriation of funds) ☐ identify, where applicable, large purchases, such as real estate, automobiles, and boats ☐ Other: Please specify...	Provide details...
Identify rapid exchange of currencies	☐ identify rapid incoming and outgoing of cash and cash-intensive activity including at digital currency ATM kiosks ☐ identify rapid flow through of funds to external financial institutions, where deposit and outflow appear similar in aggregate value and timeframe ☐ Other: Please specify...	Provide details...
Identify rapid movement of funds	☐ identify the customer undertaking multiple transactions concurrently of varying amounts and in different digital currencies ☐ Other: Please specify...	Provide details...
Identify interactions with known mixers, the use of high-risk counterparties and transactions that use the darknet	☐ Identify customers attempting to obfuscate the movement of funds ☐ Identify customers attempting to obfuscate the movement, source or destination of funds such as through the use of digital currency mixers/tumblers ☐ Identify customers who subsequently transact with higher risk counterparties such as illicit marketplaces and/or illegal offshore gambling websites' ☐ Identify customers who are trying to obfuscate transactions with higher risk counterparties – for example, by transferring funds to a private wallet which then deals with the higher risk counterparty ☐ Identify customers who are trying to obscure the perpetrators of ransomware ☐ Other: Please specify...	Provide details...

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 foreign politically-exposed person (PEP).

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.

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 provided digital currency exchange 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.

What will you do in situations where your enhanced customer due diligence is applied? (tick all boxes that apply)

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

☐ 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 invest or transact in digital currency

Explain how you will undertake this step

☐ Undertake more detailed analysis of the customer’s information and/or transaction history

Explain how you will undertake this step

☐ Verify or re-verify KYC information

Explain how you will undertake this step

☐ Seek senior management approval for processing any future transactions

Explain how you will undertake this step

☐ Other (please describe):

Provide details…

Who is responsible for conducting enhanced customer due diligence?

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.

Name: Enter name…

Title/position: Enter title/position...

Further information: AML/CTF Rules: Parts 15.8 – 15.11

11. Record keeping

Record keeping is an important part of your AML/CTF obligations. Digital currency exchange 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 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.

Provide details...

Describe the procedures your business will follow to record and retain transaction records for at least seven years

Provide details...

Describe the 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.

Provide details...

Further information: AML/CTF Rules: Chapter 20

12. 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 (i.e. by providing these details on a 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 service such as the 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.

What types of customers do you do business with?

Note: you should select check the boxes of customer types that you will do business with. The boxes here 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
- ☐ Domestic companies
- ☐ Registered foreign companies
- ☐ Unregistered foreign companies
- ☐ Trustees of trusts
- ☐ Partnerships
- ☐ Incorporated associations
- ☐ Unincorporated associations
- ☐ Registered co-operatives
- ☐ Government bodies

For individuals, domestic companies and trustees of trusts, 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, domestic companies, or trustees of trusts you need to have additional procedures to identify and verify these customers. You should seek independent advice to support you to develop these procedures.

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.

In addition, you should also ask your customers whether they will be conducting transactions in their capacity as a sole trader (for example, by acquiring digital currency to pay suppliers, exchanging digital currency payments received from customers, and/or operating a digital currency trading business). 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:

- the customer's full name; and
- their date of birth **or** residential address.

How will you verify the identification information of an individual using? (tick one)

☐ 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.

Which identification documents will you verify against?

☐ Drivers licence

☐ Passport

☐ Proof-of-age card

☐ Other government-issued photographic ID:

Provide details...

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:

- customer's name from at least two separate data sources; and
- customer's residential address and/or date of birth from at least two separate data sources.

What reliable and independent electronic data will you rely upon in order to undertake verification of customer information, and how will you determine that the data is reliable and independent?

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 Australian Government's Document Verification

Service (DVS). Other alternatives could include using a commercial provider which may provide access to the DVS, as well as other sources such as Australian electoral roll credit bureau data.

Provide details...

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.

What additional steps will you 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 Document Verification Service)

☐ Other:

Provide details...

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.

What additional information will you collect for individual customers?

☐ Mobile phone number – verified through by sending a one-time password (OTP) 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

☐ Bank account or credit card number – by crediting to or debiting from that account/card a random small amount that the customer must enter

☐ Social media identification – by requiring a user to verify or authenticate their user credentials by using a social login interface.

☐ Other:

Provide details...

In what circumstances will you collect and/or verify this additional information?

You may wish to collect and/or verify this information only in particular circumstances – for example, you require the verification of a bank account or credit card number only when a customer seeks to transact in a significant amount of money (i.e. once they have exchanged $500 or more). Similarly, you might decide to collect both mobile phone and email address, but only require one of these to be verified.

Provide details...

Beneficial owners

For a customer who is an individual, you may assume that the customer and the beneficial owner are one and the same unless you have reasonable grounds to conclude otherwise. Where you form the

view that the beneficial owner is a different person, you must collect and verify the information for that beneficial owner as though they were an individual customer.

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) or the foreign equivalent
- 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 (such as APRA's register of Registrable Superannuation Entity Licensees).

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; and
- the ACN issued to the company

How will you verify this information?

☐ Obtaining a certificate of registration for the company

☐ Manually searching and accessing the information from ASIC Connect

☐ Using a verification service or API that verifies against reliable and independent electronic data

☐ Other:

Provide details...

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.

What additional information will you 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 Service Licensee number) – verified by accessing the website of the registering/licensing authority.

☐ Other:

Provide details...

In what circumstances will you collect and/or verify this additional information?

For example, you may wish to collect the Australian Financial Service Licensee number if they are carrying on a financial services business in Australia.

Provide details...

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.

How will you 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; and/or

☐ using an online identification verification service or API

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).

Trustees

Collection of minimum information

The minimum information that you must collect from a customer who is a trust/trustee of a trust is:

- the full name of the trust;
- full business name (if any) of the trustee in respect of the trust;
- the type of trust;
- country in which the trust was established;
- the name of the settlor, unless:
    - the material asset contribution to the trust by the settlor at the time the trust is established is less than $10,000; or
    - the settlor is deceased; or
    - the trust is verified using the simplified trustee verification procedure outlined below
- the details of the **one** of the trustees who is an individual or company in accordance with the 'individuals' and 'companies' section of this Part B program (i.e. a minimum, name, address and date of birth for an individual);
- *if the trust does **not** meet the requirements to be verified in accordance with the simplified trustee verification procedure below:*
    - the full name and address of each trustee in respect of the trust; and
    - the full name of each beneficiary in respect of the trust; **or** the details of the class of beneficiaries.

Verification of minimum information

Simplified trustee verification procedure

Where the trust is one of the follow types of entities listed below, you may undertake the statutory simplified trustee verification procedure by verifying that the customer is one of those types of entities.

How will you verify each of the following trustee customer types?

Type of entity	Verification procedure
Managed investment scheme registered by ASIC	☐ undertake a search of the ASIC Connect website and record the results of this search (including the entity's Australian Registered Scheme Number). ☐ Other: Provide details...
Managed investment scheme that is not registered by ASIC and that: • only has wholesale clients; and • does not make small scale offerings to which section 1012E of the *Corporations Act 2001* applies	☐ collect from the trust a copy of the Product Disclosure Statement or other offer document in respect of the managed investment scheme. ☐ Other: Provide details...

Type of entity	Verification procedure
Registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust	☐ undertake a search of the relevant regulator's register and record the results of this search – for example, searching APRA's register of Registrable Superannuation Entities (RSEs). ☐ Other: Provide details...
Government superannuation fund established by legislation	☐ obtain a copy of the legislation establishing the government superannuation fund from a government website (such as the Federal Register of Legislation). ☐ Other: Provide details...

Where simplified verification procedures do not apply

For all other trusts, the minimum information that you must verify is:

- full name of the trust;
- full name of the settlor of the trust (unless one of the exceptions outlined in the collection section applies);
- full name of each trustee of the trust; and
- full name of each beneficiary of the trust, or details of the classes of beneficiaries.

You must verify this information by obtaining from the trustee a copy of the trust deed, or a certified copy or certified extract of the trust deed. You must not do business with a person in their capacity as trustee for a trust unless one of these documents is provided (or the customer is verified in accordance with the simplified verification procedure).

In addition to the above, you must also verify the details of the individual or company trustee whose details were collected in accordance with the 'individuals' or 'companies' section of this Part B program. These details must be verified in accordance with the 'individuals' or 'companies' section of this Part B program as appropriate.

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.

What additional information will you collect for trustees of trusts:

☐ Australian Business Number (ABN) – verified by accessing the Australian Business Register's (ABR) ABN Lookup website and/or using the ABN Lookup API.

☐ Other:

Provide details...

In what circumstances will you collect and/or verify this additional information?

For example, you may wish to collect the ABN of a customer if trust is carrying on a business in Australia.

Provide details...

Beneficial owners

If the trustee has been verified using the simplified trustee verification procedure above, you do not need to identify the beneficial owners of the trust

For all other trustees of trusts, you must seek to identify the beneficial owners of that trust by reviewing the trust deed, or certified copy or certified extract of the trust deed to identify any individual who, directly or indirectly, ultimately owns 25% or more of the trust or controls the trust.

Where you cannot identify a beneficial owner after undertaking the above step(s), you must treat as a beneficial owner any individual who holds the power to appoint or remove the trustees of the trust.

For all individuals who are identified as a beneficial owner, you must undertake the same steps to collect and verify information as you would with 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.

How will you determine whether a customer is a PEP?

For example: by conducting an internet search.

Provide details...

How will you determine if a PEP is high risk?

For example: by the number of mentions or severity of media articles.

Provide details...

What steps will you take to mitigate the risk associated with a PEP?

For example: enhanced customer due diligence and monitoring.

Provide details...

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?

Provide details...

What information would you ask for and/or verify in the above situations?

Provide details...

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 demonstrate that you are compliant with AML/CTF Act obligations.

How do you record details of the identification process and verification documents?

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.

Provide details...

13. Exemptions and modifications

Whilst the AML/CTF Act imposes a range of compliance and reporting obligations on reporting entities, the Act does allow for exemptions for some reporting entities from AML/CTF obligations. These exemptions may be brought into effect by the AML/CTF Act or the AML/CTF Rules, or prescribed by an exemption instrument or modification issued by the AUSTRAC CEO. Exemptions may be granted where the reporting entity to demonstrate low or negligible money laundering and terrorism financing risk, while ensuring that the integrity of the AML/CTF regime is maintained.

For information on how to make application for relief via an exemption or modification, refer to Chapter 9 of the AUSTRAC compliance guide.

14. Sanctions

You must comply with the Australian sanctions laws and screen customers against the DFAT Consolidated List of designated persons and entities subject to sanctions. Please refer to the Department of Foreign Affairs and Trade (DFAT) website for further information.

Scenario: Sanctions

Entity F provides digital currency exchange services to customers overseas. Customer F is seeking to sign up with Entity F. Based on the information provided by Customer F (e.g. passport information), the customer is a resident of Zimbabwe. Australia has implemented autonomous sanction laws against 'designated persons' in Zimbabwe. Entity F checks the DFAT Consolidated List (available on the DFAT website) to ensure that Customer F is not listed as a designated person.

Further information: AML/CTF Rules: Chapter 4