# AML/CTF Customer Due Diligence Policy

TLSC Reporting Group (we, us, our)

## Quick overview

This Policy covers our customer due diligence obligations under the AML/CTF Act and Rules and how we will comply with them including:

- initial and ongoing CDD
- different types of PEPs
- enhanced CDD
- all our CDD procedures

## 1. Purpose

This Policy describes our customer due diligence obligations under the AML/CTF Act and Rules and how we will comply with them.

This Policy forms part of our overall AML/CTF Program.

## 2. Designated services that we provide

In the conduct of our business, we provide the following Designated Services:

- Assisting a person in the planning or execution of a transaction, or otherwise acting for or on behalf of a person in a transaction, to sell, buy or otherwise transfer real estate, where the sale, purchase or other transfer is not pursuant to, or resulting from, an order of a court or tribunal.
- Assisting a person in the planning or execution of a transaction, or otherwise acting for or on behalf of a person in a transaction, to sell, buy or otherwise transfer a body corporate or legal arrangement, where the sale, purchase or other transfer is not pursuant to, or resulting from, an order of a court or tribunal.
- Selling or transferring a shelf company.
- Assisting a person to plan or execute, or otherwise acting on behalf of a person in, the creation or restructuring of: (a) a body corporate (other than a corporation under the Corporations (Aboriginal and Torres Strait Islander) Act 2006); or (b) a legal arrangement.

## 3. Key terms and what they mean in this Policy

**AML/CTF Act** means the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) as amended from time to time.

**AML/CTF Compliance Officer** means the individual designated by our Governing Body to act as the AML/CTF Compliance Officer.

**AML/CTF Personnel** means any individuals who perform or will perform roles relevant to our AML/CTF obligations. This includes people we employ but also people we otherwise engage including contractors or consultants, volunteers or interns (paid and unpaid) and people employed by service providers we use.

**AML/CTF Policies** means our policies, procedures, systems and controls (as amended from time to time) that:

- appropriately manage and mitigate the risks of money laundering, financing of terrorism and proliferation financing that we may reasonably face in providing our Designated Services;
- ensure we comply with our obligations imposed by the AML/CTF Act, AML/CTF Rules and regulations;
- are appropriate to the nature, size and complexity of our business; and
- comply with the requirements of the AML/CTF Rules.

**AML/CTF Program** means our ML/TF Risk Assessment and our AML/CTF Policies.

**AML/CTF Rules** means AML/CTF Rules Instrument 2025 (No.1) as amended from time to time.

**AUSTRAC** means the Australian Transaction Reports and Analysis Centre.

**Beneficial Owner** means an individual who ultimately owns (directly or indirectly) 25% or more or exercises control (directly or indirectly), including through ownership, decision-making rights, or other means.

**CDD** means Customer due diligence.

**Customer** is any individual or entity to whom we provide a Designated Service.

**Designated Services** means the designated services we provide as set out above.

**Governing Body** means the individual or group of individuals with primary responsibility for our governance and executive decisions. As we have formed a Reporting Group, our Governing Body for the purpose of this Policy is the Governing Body of the Lead Entity.

**Lead Entity** means Townsends Business & Corporate Lawyers.

**ML/TF risk** means the risk that our products and/or services may be used to facilitate Money Laundering, Terrorism Financing or Proliferation Financing.

**ML/TF Risk Assessment** means our assessment of the ML/TF risk we face (including all members of our Reporting Group that are Reporting Entities, based on the Designated Services provided) that is undertaken, documented and reviewed in accordance with our AML/CTF Risk Assessment Policy.

**Money Laundering** means the process of hiding the true origin of money or property derived from crime to make it appear legitimate.

**PEP** means a politically exposed person.

**Proliferation financing** is when a person makes available an asset, provides a financial service or conducts a financial transaction that is intended to facilitate the proliferation of weapons of mass destruction, regardless of whether the activity occurs or is attempted.

**Reporting Entity** means an entity that is required to be enrolled with AUSTRAC.

**Reporting Group** means the reporting group known as 'TLSC Reporting Group' Reporting Group.

**Senior Manager** means an individual who makes, or participates in making, decisions that affect the whole or a substantial part of our business who has been designated for approving our ML/TF Risk Assessment and AML/CTF Policies, approving relationships with certain Customers and/or agreements with third parties to collect and verify CDD information on our behalf.

**Suspicious Matter** means a situation where it is suspected on reasonable grounds that:

- information we have may be relevant to a crime;
- a Customer, future Customer or their agent isn't who they claim to be; or
- a person is planning an ML/TF offence using a Designated Service.

This includes where it is suspected on reasonable grounds that we have information that concerns Money Laundering, Terrorism Financing, Proliferation Financing, offences such as tax evasion and any other Commonwealth, state or territory offences.

**SMR** means a report that is required to be submitted to AUSTRAC when a Suspicious Matter occurs.

**Terrorism Financing** means the use of funds to finance the training for, preparation of and carrying out a terrorist activity.

# 4. Who this Policy applies to

This Policy applies to:

- the members of our Governing Body, the Senior Manager(s), the AML/CTF Compliance Officer and all AML/CTF Personnel; and
- any third parties or outsourced providers who perform AML/CTF-related activities on our behalf.

# 5. Overview of obligations

CDD involves understanding who our Customers are before we start providing them with Designated Services and throughout the course of our business relationship with the Customer.

The purpose of CDD is to:

- establish the identity of our Customers and that they are who they claim to be, know whether they're acting on behalf of another person, and determine that there's no legal barrier to providing them with the Designated Service;
- identify and assess the ML/TF risks involved in providing Designated Services to the Customer, so we can appropriately manage and mitigate these risks; and
- obtain the information we require to make reports to AUSTRAC under our reporting obligations.

# 6. Initial CDD

We must complete initial CDD before we start providing a Designated Service to the Customer.

Initial CDD is about identifying our Customers, Beneficial Owners of our Customer, any person on whose behalf the Customer is receiving a Designated Service and the identity of any person acting on behalf of the Customer and their authority to act and identifying their ML/TF risk. It helps us decide what we need to do to manage and mitigate the ML/TF risks involved in providing that Customer with a Designated Service.

We do this by:

- collecting and verifying know your customer (**KYC**) information; and
- assessing the Customer's ML/TF risks

The information we need to collect and verify will be different depending on the type of Customer involved (i.e. whether they are a company, trust or individual) and their ML/TF risk.

## 6.1. What we must establish during initial CDD

We must establish **all** of the following items on reasonable grounds (see more on reasonable grounds below) before we start providing our Customer with a Designated Service:

- the identity of the Customer;
- the identity of any person on whose behalf the Customer is receiving a Designated Service (such as a beneficiary of a trust);
- the identity of any person acting on behalf of the Customer and their authority to act;
- if the Customer isn't an individual, the identity of all Beneficial Owners of the Customer (taking reasonable steps and, after determining which individuals meet the definition of Beneficial Owner, applying any applicable deeming provisions under the AML/CTF Rules);
- whether the Customer, any Beneficial Owners of the Customer, any person on whose behalf the Customer is receiving the Designated Service or any person acting on behalf of the Customer is a PEP or designated for targeted financial sanctions;
- the nature and purpose of the business relationship or transaction;
- the source of funds and source of wealth of foreign PEPs, high-risk domestic or international organisation PEPs; and
- if we are required to apply enhanced CDD (see further on this below), the Customer's source of funds and source of wealth if relevant to the nature of the Customer's ML/TF risk.

All of the above items are referred to below as '**Required Items**'.

## 6.2. Reasonable grounds

Reasonable grounds is an objective standard – meaning that a reasonable person in our position would determine that the Required Items have been established based on the facts, circumstances and information available (all information and circumstances that we could reasonably be expected to have known at the time).

We must explain how each of the Required Items was established in a way that demonstrates that a reasonable person would likely reach the same conclusion if they were to review the same material and have similar knowledge to us.

We must keep records of how we established each of the Required Items on reasonable grounds for each Customer.

## 6.3. How we will establish each required item on reasonable grounds

Establishing the Required Items will consist of the following steps:

- Collect KYC information from the Customer (including Beneficial Owners of the Customer, any person on whose behalf the Customer is receiving a Designated Service and any person acting on behalf of the Customer and evidence of their authority to act).
- Identify Beneficial Owners and understand the ownership and control structure of the Customer.
- Identify the Customer's ML/TF risk based on the KYC information collected (see more on this below).

- Determine if the Customer, Beneficial Owners of the Customer, any person on whose behalf the Customer is receiving a Designated Service and any person acting on behalf of the Customer is a PEP or designated for targeted financial sanctions.
- Determine if we need to apply enhanced CDD.
- Determine if we can apply simplified CDD or use deeming provisions such that a Required Item is taken to have been established.
- Collect additional KYC information as appropriate to the Customer's ML/TF risk and to mitigate and manage that ML/TF risk.
- Verify KYC information using reliable and independent data that is appropriate to the Customer's ML/TF risk.

Note, some of these steps can be completed at the same time where relevant.

The Annexure to this Policy sets out the CDD procedures we will follow for different kinds of Customers to help us establish the Required Items on reasonable grounds.

The information we collect and verify must be sufficient to establish all of the above Required Items on reasonable grounds and appropriate to the Customer's ML/TF risks and the ML/TF risks we may reasonably face in providing Designated Services.

For instance, sometimes the nature of the business relationship or transaction will be clearly evident from the transaction itself or our normal interactions with our Customer. At other times we may need to ask our Customer questions to understand the nature of the relationship, including (where relevant):

- what they will be using our Designated Services for;
- their expected transaction frequency and volume;
- how they plan to have Designated Services delivered i.e. online or face to face;
- whether they will use our Designated Services for business or personal transactions;
- the nature and details of their occupation or employment;
- explanations for changes of address;
- the nature of the relationship between a Customer and the person acting on their behalf; or
- information about their source of wealth and funds.

## 6.4. Customer's ML/TF risk

In addition to assessing the ML/TF risks we face as an overall business, we assess the ML/TF risks associated with each Customer as part of CDD and assign a risk rating to each Customer.

The relevant ML/TF risk rating of each Customer will impact the CDD (both initial and ongoing) that is undertaken with respect to that Customer.

In assigning a risk rating to the Customer, we consider:

- the type of Customer and any ML/TF risks arising from that type of Customer;
- the Designated Services we are providing to the Customer and any ML/TF risks arising from those Designated Services;

- the delivery channels we will use to provide Designated Services to the Customer and any ML/TF risks arising from those delivery channels;
- what country the Customer resides in or is connected to (i.e. via Beneficial Owners);
- any specific risk factors applying to the relevant Customer;
- whether there are any indicators of unusual or criminal activity.

As part of initial CDD, we will balance the nature and scale of all of the above and assign an overall risk rating for the Customer.

The above assessment and Customer's risk rating is documented in the AML/CTF Customer Checklist that is completed for each Customer

The minimum KYC information must be collected for each Customer as set out in the Annexure to this Policy. However, we will collect more information about a Customer that is assessed as high ML/TF risk (including KYC information about people connected with the Customer such as Beneficial Owners or agents) than we will for Customers who have been assessed as low ML/TF risk.

We will also collect more KYC information from a Customer where the request for Designated Services seems unusual or where any red-flags are present (refer to our AML/CTF Red-Flags document for more information on red-flags).

## 6.5. Verifying KYC information using independent and reliable data

Once we have collected KYC information, we need to verify this information (to establish the above required items on reasonable grounds), as appropriate to the ML/TF risk we have assigned to the relevant Customer.

Where the AML/CTF Rules provide that we are taken to have established a Required Item on reasonable grounds, we are not required to separately verify that information.

KYC information must be verified using independent and reliable data.

Independent and reliable data includes original or reliable copies of documents or electronic data that we have assessed as being independent and reliable.

We don't necessarily need to verify every piece of KYC information we have collected (this will depend on the ML/TF risk associated with the Customer). However, in all cases we must verify:

- sufficient KYC information to establish each Required Item on reasonable grounds (this will generally involve verifying at least one key identifier for each Required Item, but may require more extensive verification depending on ML/TF risk); and
- more information about a Customer that is assessed as high ML/TF risk (including KYC information about people connected with the Customer such as Beneficial Owners or agents) than we will for Customers who have been assessed as low ML/TF risk.

We will also verify more KYC information about a Customer where the request for Designated Services seems unusual or where any red-flags are present (refer to our AML/CTF Red-Flags document for more information on red-flags).

We may decide to use third-party digital identity services to verify KYC information. Before making this decision, we need to determine that the data we receive is reliable and independent, including whether the data used by the third-party is independent, reliable and up to date. Any third-parties engaged in our CDD process must be engaged via our outsourcing process as documented in our AML/CTF Governance and Oversight Policy.

## 6.6. Dealing with discrepancies

When we verify KYC information, we may discover inconsistencies with the information we have collected. When this occurs we will take any one or more of the following steps (where relevant to the situation):

- verify the information with independent and reliable data from third parties;
- contact the authority who has issued the relevant document to confirm validity;
- ask the Customer to explain discrepancies (name spelling or address history for example) and request further supporting evidence (such as an updated utilities notice where a change of address has occurred for instance);
- review the reason for the inconsistency (for instance, is it just a minor admin error or potential red-flag?);
- in some circumstances, apply alternative identification procedures (see section 6.8 below).

We must not provide a Designated Service if we can't establish all of the Required Items on reasonable grounds.

## 6.7. Suspicious Matters

Everyone must be on the look-out for Suspicious Matters when undertaking CDD. Refer to our AML/CTF Reporting Obligations Policy on your obligations to escalate all Suspicious Matters to the AML/CTF Compliance Officer.

## 6.8. Alternative identification procedures

Some Customers may not be able to provide standard identification required under our normal CDD procedures. We can use alternative identification procedures for individuals who for a range of reasons (including diverse backgrounds, challenging circumstances or vulnerability):

- can't obtain standard identification information or evidence;
- can't access standard identification information or evidence due to circumstances outside of their control; or
- have inconsistent details across their identification documents.

The AML/CTF Compliance Officer must approve the use of alternative identification procedures. Before applying alternative identification procedures, the AML/CTF Compliance Officer must consider the ML/TF risk of using the alternative procedure in the circumstances and first confirm that the individual cannot:

- provide the standard identification documents needed for the service or transaction; or
- prove their standard identification is correct if the information doesn't match.

In applying alternative verification procedures we must still:

- take reasonable steps to make sure the Customer is who they claim to be using the alternative identification that we have;
- identify the Customer's ML/TF risk based on accepting alternative identification options reasonably available to the Customer;
- collect KYC information that is appropriate to the Customer's ML/TF risk;
- take reasonable steps to verify the KYC information using alternative forms of identification reliable and independent data that is appropriate to their ML/TF risk; and

- mitigate and manage any additional ML/TF risk arising from the lack of standard information or evidence.

As a last resort where we cannot establish the identity of an individual any other way, we may accept an individual's self-attestation of their identity. We must document our reasons for this and must not rely on self-attestation if we know or suspect it is incorrect or misleading.

# 7. Ongoing CDD

After we conduct initial CDD, if we have a business relationship with the Customer, we must continue to monitor our Customers so we can identify, assess and mitigate their ML/TF risks over time.

A business relationship means a relationship between us and our Customer involving the provision of a Designated Service or Designated Services that has, or could reasonably be expected to have, an element of duration.

Ongoing CDD helps us determine whether the KYC information we hold remains accurate and whether the nature or ML/TF risk of the Customer has changed.

We do this by:

- keeping the Customer's KYC information up to date and re-verifying it where appropriate;
- monitoring for unusual transactions and behaviours and any indicators of criminal activity;
- updating the Customer's ML/TF risk as we know more about them and how they use our services; and
- collecting or verifying additional KYC information where appropriate to the Customer's ML/TF risk.

Ongoing CDD must be proportionate to the ML/TF risks associated with each Customer.

## 7.1. What we must monitor for

We must take reasonable steps to monitor our relationship with each Customer to identify:

- inconsistencies between the Customer's transactions or behaviour and what we know about them, their business or their normal transaction patterns;
- unusual, complex or large transactions that do not appear to have a legitimate purpose;
- changes in the Customer's circumstances or ownership structure that may affect their ML/TF risk;
- discrepancies or new information that calls into question the veracity or adequacy of the KYC information we previously collected;
- indicators that the Customer or related parties may be involved in criminal activity; and
- any information that gives rise to reasonable grounds to suspect a Suspicious Matter (refer to our AML/CTF Reporting Obligations Policy).

Customers with a high ML/TF risk are reviewed more often than those with a low ML/TF risk:

- Low ML/TF risk Customers – monitoring will generally occur through periodic reviews and consideration of any new information that becomes available during the normal course of the business relationship.
- Medium ML/TF risk Customers – monitoring will include periodic review of Customer information, reassessment of ML/TF risk where circumstances change, and closer scrutiny of unusual transactions or changes in behaviour.

- High ML/TF risk Customers – monitoring will be more intensive and may include more frequent reviews of KYC information, enhanced transaction monitoring, and periodic reassessment of source of funds or source of wealth where relevant.

The frequency and depth of monitoring will be determined by the Customer's ML/TF risk and the nature of the Designated Services provided.

Our monitoring activities include:

- review at regular intervals whether KYC information remains up to date or whether anything has changed that would impact the Customer's ML/TF risk;
- review whether KYC information remains up to date or whether anything has changed that would impact the Customer's ML/TF risk if something material changes for the Customer (such as adverse news, a large transaction or new structure is established);
- request information from the Customer about any changes in their circumstances or details when we interact with them;
- third party monitoring of changes relating to the Customer.

Where we identify an issue, we must take steps to understand the issue and update our CDD as required – including via enhanced CDD (see section 8 below).

## 7.2. When we must update and re-verify KYC information

We must review, update and where appropriate re-verify KYC information when:

- we identify a discrepancy or new information that indicates a Required Item may no longer be accurate;
- the Customer's ML/TF risk increases, including where new risk indicators or red-flags emerge;
- we identify unusual, large or complex transactions that require further understanding;
- the Customer has a high ML/TF risk and we need to update KYC information as part of our enhanced CDD obligations;
- the Customer becomes a PEP or designated for targeted financial sanctions; or
- we otherwise need additional information to establish a Required Item on reasonable grounds.

The level of updating or re-verification and the information we will collect and verify must be appropriate to the Customer's ML/TF risk rating and the ML/TF risks we have identified.

## 7.3. Identifying when a Customer's ML/TF risk has changed

We must take reasonable steps to determine if the ML/TF risk of a Customer has changed, including where:

- we observe changes in transaction patterns, ownership, control or behaviour;
- we identify adverse media relating to the Customer or related parties;
- the Customer requests new or different Designated Services that may carry a different ML/TF risk;
- the Customer begins to operate in new jurisdictions or sectors; or
- new information arises about the Customer's source of funds or source of wealth.

Where a Customer's ML/TF risk increases, we must apply enhanced CDD as appropriate (see section 8).

## 7.4. Ongoing CDD obligations where PEPs are involved

We must take reasonable steps to identify if our Customer, any Beneficial Owner of the Customer, any person acting on behalf of the Customer or any person on whose behalf the Customer is receiving a Designated Service becomes a PEP during the course of our business relationship.

If a person becomes a PEP, we must:

- review and, where appropriate, update and re-verify the KYC information we hold;
- reassess the Customer's ML/TF risk and determine whether enhanced CDD is required;
- monitor the Customer for behaviours or transactions that may indicate misuse of their position (including indicators of corruption or bribery); and
- obtain Senior Manager approval to continue the business relationship where the Customer is assessed as high ML/TF risk.

## 7.5. When ongoing monitoring will require enhanced CDD

Ongoing monitoring will trigger a requirement to apply enhanced CDD when we identify:

- unusual, large or complex transactions;
- indicators of criminal activity or other red-flags;
- discrepancies in KYC information;
- a Customer becoming a PEP or designated for targeted financial sanctions;
- a Customer's ML/TF risk increasing to high; or
- information giving rise to reasonable grounds to suspect a Suspicious Matter.

Enhanced CDD ensures we take additional steps to establish Required Items on reasonable grounds and to manage and mitigate identified ML/TF risks (see section 8).

If a suspicion arises, we will undertake as much ongoing CDD as we can without alerting the Customer, and escalate to the AML/CTF Compliance Officer in accordance with our AML/CTF Reporting Obligations Policy.

# 8. Enhanced CDD

Enhanced CDD is where we take additional steps to identify our Customer, Beneficial Owners of our Customer, any person on whose behalf the Customer is receiving a Designated Service and the identity of any person acting on behalf of the Customer and their authority to act and to identify, manage and mitigate their ML/TF risks.

## 8.1. When we will apply enhanced CDD

We will apply enhanced CDD:

- for all Customers we have assessed as having a high ML/TF risk (whether this is during initial CDD or during ongoing CDD);

- where we are required to submit a SMR (refer to our AML/CTF Reporting Obligations Policy for more information on SMRs and when they are required);
- for unusual, large or complex transactions;
- where Designated Services are part of a 'nested services' relationship (this will generally not occur for us);
- where our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service is a foreign PEP;
- where our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service are physically present in, or formed in, a high risk jurisdiction that the Financial Action Task Force has called for enhanced CDD to be applied: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html.

Our CDD Procedures in the Annexure to this Policy set out our procedures for enhanced CDD.

Enhanced CDD is not a 'one-size-fits-all' and must be tailored to the ML/TF risks involved with the relevant Customer and/or transaction. Our enhanced CDD procedures include a range of enhanced CDD measures that can be used as appropriate to managing and mitigating our Customer's ML/TF risks.

The enhanced CDD measures applied in each case must be informed by the reason why the Customer was identified as high ML/TF risk and designed to manage and mitigate the ML/TF risk.

## 8.2. Who is responsible for applying enhanced CDD

The AML/CTF Compliance Officer will be responsible for applying enhanced CDD in the above situations.

## 8.3. How we will monitor and review effectiveness of enhanced CDD

We will monitor and review whether our enhanced CDD procedures are being applied and managing ML/TF risks as part of our annual compliance tasks.

## 8.4. Managing tipping off obligations when conducting enhanced CDD

We need to be very careful to manage our tipping off obligations when conducting enhanced CDD. Enhanced CDD needs to be handled sensitively so that the Customer is not tipped off. Refer to our AML/CTF Reporting Obligations Policy for more information in relation to tipping off and how we manage our obligations.

# 9. Politically exposed people (PEPs)

A PEP is an individual who holds a prominent public position. They can be a target for bribery and corruption because they hold positions of power and influence.

We have additional CDD obligations if we are dealing with a PEP. This includes where our Customer, Beneficial Owners of our Customer, any person on whose behalf the Customer is receiving a Designated Service and any person acting on behalf of the Customer is a PEP or an associate of a PEP.

There are 3 types of PEPs:

- a foreign PEP;
- a domestic PEP; and
- an international organisation PEP.

## 9.1. Foreign PEPs

A foreign PEP is an individual who holds a prominent office or position or public function in or for the legislature, executive or judiciary of a foreign company, including any individual who holds any of the following offices or positions:

- head of state or head of government;
- member of the executive council of government;
- member of a legislature;
- minister, deputy minister or equivalent office or position;
- judge of a supreme court, constitutional court or other court of general jurisdiction or last resort;
- ambassador, high commissioner or charge d'affaires;
- high ranking military officer;
- head or board member of a government body;
- head or board member of a state-owned company or a state-owned bank; or
- member of a governing body of a political party represented in a legislature.

A foreign PEP is also a family member of an individual listed above or an individual who is known (based on information that's public or readily available) to have any of the following:

- joint beneficial ownership of a body corporate or legal arrangement with an individual listed in the above positions;
- sole beneficial ownership of a body corporate or legal arrangement on behalf or for the benefit of an individual listed in the above positions; or
- any other close business relations with an individual listed in the above positions.

## 9.2. Domestic PEPs

A domestic PEP is an individual who holds any of the following offices or positions:

- member of the legislature of the Commonwealth or a state or territory;
- member of the governing body of a political party represented in the legislature of the Commonwealth or a state or territory;
- Governor-General;
- Governor of a state;
- Administrator of a territory;
- Justice of the High Court;
- Judge of the Federal Court of Australia;
- Judge of the Supreme Court of a state or territory;

- accountable authority, or member of the accountable authority, of a Commonwealth entity within the meaning of the Public Governance, Performance and Accountability Act 2013 (PGPA Act);
- member of the governing body of a wholly-owned Commonwealth company within the meaning of the PGPA Act;
- Head (however described) of a department of state or territory, or an agency or authority of a state or territory that has a prominent public function;
- Head (however described) of a local government council in a state or territory;
- the chair of the board, chief executive officer or chief financial officer of a company or other incorporated body that's wholly-owned or majority-owned by a state or territory;
- Chief of the Defence Force, Vice Chief of the Defence Force, Chief of Navy, Chief of Army or Chief of Air Force;
- officer of the Navy of the rank of Vice Admiral or a higher rank;
- officer of the Army of the rank of Lieutenant General or a higher rank; or
- officer of the Air Force of the rank of Air Marshal or a higher rank.

It also includes any of the following offices of the Commonwealth in a foreign country, or to a public international organisation, to which appointments are made by the Governor-General:

- Ambassador;
- High Commissioner;
- Consul-General;
- Australian representative;
- Special representative;
- Representative;
- Permanent representative; or
- Chargé d'affaires.

A domestic PEP is also a family member of an individual listed above, or an individual who is known (based on information that's public or readily available) to have any of the following:

- joint beneficial ownership of a body corporate or legal arrangement with an individual listed in the above positions;
- sole beneficial ownership of a body corporate or legal arrangement on behalf or for the benefit of an individual listed in the above positions; or
- any other close business relations with an individual listed in the above positions.

## 9.3. International organisation PEPs

An international organisation PEP is an individual entrusted with a prominent public function, position or office of a public international organisation. This includes a head, deputy head or board member in a public international organisation. For example, a head, deputy head or board member of a United Nations body.

An international organisation PEP is also a family member of one of these individuals, or an individual who is known (based on information that's public or readily available) to have any of the following:

- joint beneficial ownership of a body corporate or legal arrangement with an individual entrusted with a prominent public function, position or office of a public international organisation;
- sole beneficial ownership of a body corporate or legal arrangement on behalf or for the benefit of an individual entrusted with a prominent public function, position or office of a public international organisation; or
- any other close business relations with an individual entrusted with a prominent public function, position or office of a public international organisation.

## 9.4. Establishing if our Customer (or other specified people) are PEPs

As part of our initial CDD, we must establish on reasonable grounds if our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service are a PEP before we provide the Customer with a Designated Service.

We will establish whether any of these people are PEPs by:

- asking the Customer if they, any Beneficial Owner of the Customer, any person acting on behalf of the Customer or any person on whose behalf the Customer is receiving a Designated Service or a family member or a close associate is a PEP during onboarding
- using reports from third-party providers that specialise in conducting PEP and sanctions checks.

We must take reasonable steps to monitor our Customers to determine if our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service becomes a PEP during the course of our business relationship. We do this by:

- asking the Customer if they, any Beneficial Owner of the Customer, any person acting on behalf of the Customer or any person on whose behalf the Customer is receiving a Designated Service or a family member or a close associate is a PEP when KYC information is re-verified in ongoing CDD or during other interactions
- periodically running checks through third-party providers that specialise in conducting PEP and sanctions checks.

When a person leaves their position, they're no longer a PEP, however their former position can still affect their ML/TF risk having regard to:

- if the person still has influence over public policy or expenditure decisions
- the time that has elapsed since the person was a PEP
- if the person is still prominent and politically connected
- other information that suggests the person may still have a high ML/TF risk because of their former PEP status.

# 10. Senior Manager approval

Senior Manager approval is required before we provide a Designated Service to a Customer if:

- we have assessed a Customer's ML/TF risk rating as 'high'; or

- our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service is or was previously a foreign PEP (for instance, a beneficiary of a trust).

Senior Manager approval is also required to continue a business relationship with an existing Customer if our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service becomes a foreign PEP or a domestic or international organisation PEP (where we have assessed the Customer as having a high ML/TF risk).

# 11. Persons designated for targeted financial sanctions

Before we start providing a Customer with a Designated Service, we must establish on reasonable grounds if the Customer, any Beneficial Owners of our Customer, any person on whose behalf the Customer is receiving a Designated Service and any person acting on behalf of the Customer are designated for targeted financial sanctions.

We can't deal with assets owned or controlled by a person designated for targeted financial sanctions. We are also prohibited from making assets available to them.

We will also re-screen where material KYC changes occur, or where the Customer's risk increases, where the re-screen is relevant to our ongoing CDD measures.

# 12. Outsourcing part of the CDD process

Where we engage a service provider to perform any part of the CDD process (such as electronic verification of identity), we must comply with our outsourcing obligations which are set out in our AML/CTF Governance and Oversight Policy.

# 13. Relying on CDD by another Reporting Entity

In limited situations we can rely on KYC information that has been collected and verified by another reporting entity. There are strict requirements for these CDD reliance arrangements which are set out in our AML/CTF Governance and Oversight Policy.

# 14. Training

Refer to our AML/CTF Personnel Due Diligence and Training Policy for training requirements.

# 15. Record Keeping

Refer to our AML/CTF Record Keeping Policy for a description of our record keeping obligations.

# 16. Non-compliance with this Policy

All instances of non-compliance with this Policy will be handled in accordance with our AML/CTF Breach and Incident Policy.

# 17. Review

The AML/CTF Compliance Officer will review this Policy at least annually (all changes must be approved by the Senior Manager).

# 18. Annexure – CDD Procedures

In the tables below, the 'Required Items' refers to the matters we are required to establish on reasonable grounds for each Customer.

Simplified CDD can only be applied where it is appropriate to the Customer's assessed ML/TF risk. The KYC information collection and verification steps set out in Simplified CDD Procedures below are appropriate for a Customer where:

- for individual Customers, we have taken reasonable steps to establish that the Customer is the person they claim to be;
- we have identified the ML/TF risk of the Customer based on the KYC information that is reasonably available to us before commencing to provide a Designated Service and the Customer's ML/TF risk has been assessed as 'low';
- we have collected the KYC information we have prescribed below about each Customer that is appropriate to the ML/TF risk of the Customer, and
- there are no reasonable grounds for us to doubt the adequacy or veracity of the KYC information we have collected.

Simplified CDD cannot be applied where:

- the Customer is assessed as medium or high ML/TF risk;
- enhanced CDD is required for any reason;
- there are discrepancies or doubts about KYC information; or
- a Suspicious Matter has been identified or is suspected.

In any other case, we will be required to take additional steps to collect additional KYC information and verify the KYC information collected (as appropriate to the ML/TF risk) to ensure we have established the Required Item.

## 18.1. Assessing a Customer's ML/TF risk

Each Customer's risk rating is documented in the AML/CTF Customer Checklist that is completed for each Customer

The Customer's ML/TF risk assessment will determine the CDD procedures that are applied to that Customer.

## 18.2. Enhanced CDD

We must undertake enhanced CDD:

- for all Customers we have assessed as having a high ML/TF risk (whether this is during initial CDD or during ongoing CDD);
- where we are required to submit a SMR (refer to our AML/CTF Reporting Obligations Policy for more information on SMRs and when they are required) and we propose to continue to provide a Designated Service or services to the customer;
- for unusual, large or complex transactions;
- where Designated Services are part of a 'nested services' relationship (this will generally not occur for us);

- where our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service is a foreign PEP;
- where our Customer, any Beneficial Owner of our Customer, any person acting on behalf of our Customer or any person on whose behalf the Customer is receiving a Designated Service are physically present in, or formed in, a high risk jurisdiction that the Financial Action Task Force has called for enhanced CDD to be applied: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html.

Refer to our Enhanced CDD procedures later in this document for how we will undertake enhanced CDD.

## 18.3. Simplified CDD Procedures

Where simplified CDD applies under the AML/CTF Rules, we must still establish each Required Item on reasonable grounds.

This means:

- identity of individuals must be established on reasonable grounds, which will usually involve verification using reliable and independent information, proportionate to ML/TF risk;
- not all KYC information collected needs to be independently verified, unless required by the Rules or where there is reason to doubt the information; and
- ownership, control, authority and purpose information may be collected without separate verification where the conditions for simplified CDD are met and documented.

Where the AML/CTF Rules provide that we are taken to have established a Required Item on reasonable grounds, we may rely on those deeming provisions instead of separately verifying KYC information for that Required Item as long as:

- any conditions for the relevant deeming provisions are clearly satisfied;
- there are no reasons to doubt any of the information we have received; and
- the Customer is not assessed as medium or high ML/TF risk (unless otherwise permitted under the AML/CTF Rules).

## 18.4. Individuals

We need to make sure the Customer is the person they claim to be. We can do this by matching appearance against photographic identification (including via a video call) or using biometric technology where we engage a third-party ID verification provider.

In addition to making sure the Customer is who they claim to be, we must collect sufficient KYC information to establish each Required Item on reasonable grounds. Under simplified CDD, only some of this information must be independently verified, as set out below.

| **Required Items** | **KYC information to collect** | **KYC information to verify** | **Independent and reliable data we can use** |
|---|---|---|---|
| Identity of Customer | Enough information to distinguish the Customer from another | Full name and date of birth | Gov-issued primary photographic ID doc. |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| | individual with the same or similar name/details including:<br>• full name<br>• other name(s) commonly known by<br>• date of birth<br>• residential address<br>• unique identifier (if applicable) i.e. driver's licence number or passport number | | Primary non-photographic ID doc and secondary identification doc showing name and address.<br>Reliable and independent electronic data. |
| Identity of any person acting on the Customer's behalf (and their authority to act) | • Enough information to distinguish the individual acting on the Customer's behalf from another individual with the same or similar name/details including:<br>  • full name<br>  • other name(s) commonly known by<br>  • date of birth<br>  • residential address<br>  • unique identifier (if applicable) i.e. driver's licence number or passport number<br>• Information about the nature of their authority and reason for granting the authority. | Independent verification is not required unless there is reason to doubt the authority or identity information provided.<br>If any doubt exists, verify the information to establish identity on reasonable grounds, proportionate to ML/TF risk. | Dependent on the information that needs to be verified (if any). |
| Identity of any person on whose behalf the Customer is receiving the service | If the person who approaches us for a Designated Service is receiving this service for someone else's behalf, that other person will be our Customer and we need to undertake CDD on that person. | N/A | N/A |
| If any of the above people are PEPs or designated for | Whether any of the above people are PEPs and if so, the details of the individual and role. | PEP status and sanctions status must be verified. | PEP check – either manual using PEP Checklist or using third- |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| targeted financial sanctions | | | party provider that provides PEP screening.<br><br>Undertake sanctions check using DFAT's Consolidated List.<br><br>In both cases, ensure search allows for minor discrepancies or errors in names (particularly for non-English names changed into English). |
| The nature and purpose of the business relationship or transaction | • Reasons the Customer is seeking our services and the nature of the service sought.<br><br>• Occupation. | Independent verification is not required unless there is reason to doubt the information provided.<br><br>If any doubt exists, verify the information to establish reasons for seeking service and nature of service sought on reasonable grounds, proportionate to ML/TF risk. | Dependent on the information that needs to be verified (if any). |

## 18.5. Sole traders

You need to make sure the Customer is the person they claim to be. You can do this by matching appearance against photographic identification (including via a video call) or using biometric technology where we engage a third party ID verification provider.

In addition to making sure the Customer is who they claim to be, we must collect sufficient KYC information to establish each Required Item on reasonable grounds. Under simplified CDD, only some of this information must be independently verified, as set out below.

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| Identity of Customer (both the individual and their sole trader business) | **Information on the individual**<br><br>Enough information to distinguish the Customer from another individual with the same or similar name/details including:<br>• full name<br>• other name(s) commonly known by<br>• date of birth<br>• residential address<br>• unique identifier (if applicable) i.e. driver's licence number or passport number.<br><br>**Information on the business**<br>• any business name used for the conduct of the business<br>• any other names the individual and their business are commonly known by<br>• a unique identifier for the business (i.e. ABN) where there is one<br>• address of the principal place of business | • Full name and date of birth for the individual<br>• Business name and unique identifier (ABN) for the business (if there is one) | Gov-issued primary photographic ID doc.<br><br>Primary non-photographic ID doc and secondary identification doc showing name and address.<br><br>Where there is an ABN, Australian Business Register.<br><br>Reliable and independent electronic data. |
| Identity of any person acting on the Customer's behalf (and their authority to act) | • Enough information to distinguish the individual acting on the Customer's behalf from another individual with the same or similar name/details including:<br>  • full name<br>  • other name(s) commonly known by<br>  • date of birth<br>  • residential address | Independent verification is not required unless there is reason to doubt the authority or identity information provided.<br><br>If any doubt exists, verify the information to establish identity on reasonable | Dependent on the information that needs to be verified (if any). |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| | • unique identifier (if applicable) i.e. driver's licence number or passport number<br>• Information about the nature of their authority and reason for granting the authority. | grounds, proportionate to ML/TF risk. | |
| Identity of any person on whose behalf the Customer is receiving the service | If the person who approaches us for a Designated Service is receiving this service for someone else's behalf, that other person will be our Customer and we need to undertake CDD on that person. | N/A | N/A |
| If any of the above people are PEPs or designated for targeted financial sanctions | Whether any of the above people are PEPs and if so, the details of the individual and role. | PEP status and sanctions status must be verified. | PEP check – either manual using PEP Checklist or using third-party provider that provides PEP screening.<br>Undertake sanctions check using DFAT's Consolidated List.<br>In both cases, ensure search allows for minor discrepancies or errors in names (particularly for non-English names changed into English). |
| The nature and purpose of the business relationship or transaction | • Reasons the Customer is seeking our services and the nature of the service sought.<br>• Information about the general commercial activity or sector the Customer operates in and the kinds of products and services they offer. | Independent verification is not required unless there is reason to doubt the information provided.<br>If any doubt exists, verify the information to establish reasons for seeking service and nature of service sought (including | Dependent on the information that needs to be verified (if any). |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| | | information about the Customer's business activities and services) on reasonable grounds, proportionate to ML/TF risk. | |

## 18.6. Bodies corporate (companies), partnerships or unincorporated associations

Whilst bodies corporate, partnerships and unincorporated associations are used for a range of legitimate purposes, they are also commonly used by money launderers to place, layer and integrate the proceeds of crime. AUSTRAC has rated legal structures and bodies corporate as a high national money-laundering risk that has been persistently exploited by criminals to store and move large volumes of criminal proceeds, including offshore. This is why there is more extensive information to collect and verify when our Customer is a body corporate, partnership or unincorporated association.

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| Identity of the Customer | • Customer's full legal name<br>• Any business names of the Customer<br>• Any other names the Customer is commonly known by<br>• Unique identifier for the Customer (if any) – i.e. ABN or ACN<br>• Address of the principal place of business or operations of the Customer<br>• Address of any registered office of the Customer<br>• Evidence of the Customer's existence (i.e. ASIC Connect or Australian Business Register ABN Lookup, certificate of registration, ASIC extract, partnership agreement, certificate of | Verify, using reliable and independent data, such of the collected KYC information as is appropriate to ML/TF risk to establish the Customer's identity. | ASIC search.<br>Certificate of incorporation or registration.<br>ARBN (if a foreign company registered with ASIC).<br>Information on foreign government registers.<br>Original or reliable copy or extract of partnership agreement, company constitution or rules of association.<br>ABN Lookup. |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| | registration from a foreign regulatory body, constitution (for an association) or for a co-operative, an official extract of the co-operatives register from the state or territory of registration)<br>• Powers that bind and govern the Customer (constitution, partnership agreement or rules of association)<br>• Full names (and, for bodies corporate, any director identification numbers) of all individuals responsible for the governance and executive decisions of the Customer | | |
| Identity of any person acting on the Customer's behalf (and their authority to act) – only representatives who engage with us in relation to our Designated Services (not every representative they have) | Where representative is a company, collect the KYC information required for 'Bodies corporate (companies), partnerships or unincorporated associations'. Where the representative is an individual, collect the required KYC information for 'Individuals'.<br>Information regarding authority to act i.e. copy of POA. | Independent verification is not required unless there is reason to doubt the authority or identity information provided.<br>If any doubt exists, verify the information to establish identity on reasonable grounds, proportionate to ML/TF risk. | Dependent on the information that needs to be verified (if any). |
| Identity of any person on whose behalf the Customer is receiving the Designated Service | If a body corporate, partnership or unincorporated association is seeking our services on behalf of another person, that other person is our Customer and we need to identify who they are (applying the relevant CDD procedures depending on Customer type). | N/A | N/A |
| The identity of any Beneficial | Unless Simplified Verification Measures apply to the Customer (see below this table), collect the | Unless Simplified Verification Measures apply to | Original or reliable copy of constitution, charter or rules. |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| Owner(s) of the Customer[a] | following to ascertain the identity of the Beneficial Owners:<br>• information on the ownership of the Customer including any distribution of shares and the kind of shares distributed<br>• duties, rights and entitlements for administering the Customer<br>• control and decision-making processes of the Customer | the Customer (see below this table),<br>• Ownership and control information must be verified unless there is no reason to doubt the information collected.<br>• The identity of any individual Beneficial Owner must still be established on reasonable grounds, applying the CDD procedures for 'Individuals'. | ASIC searches.<br>Annual statements.<br>Member statements.<br>Partnership agreements.<br>Refer to requirements for 'Individuals' for Beneficial Owners. |
| If any of the above people are PEPs or designated for targeted financial sanctions | Whether any of the above people are PEPs and the details of the individual and role if yes. | PEP status (only for individuals) and sanctions status (for all) must be verified for:<br>• the Customer<br>• any representative who engages with us in relation to Designated Services<br>• all Beneficial Owners | PEP check – either manual using PEP Checklist or using third-party provider that provides PEP screening.<br>Undertake sanctions check using DFAT's Consolidated List.<br>In both cases, ensure search allows for minor discrepancies or errors in names (particularly for non-English names changed into English). |
| The nature and purpose of the business relationship or transaction | • Reasons the Customer is seeking our services and the nature of the service sought.<br>• Information about the general commercial activity or sector the Customer operates in and the | Independent verification is not required unless there is reason to doubt the information provided. | Dependent on the information that needs to be verified (if any). |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| | kinds of products and services they offer or, if not engaged in commercial activity, the purpose of the company. | If any doubt exists, verify the information to establish reasons for seeking service and nature of service sought (including information about the Customer's business activities and services) on reasonable grounds, proportionate to ML/TF risk. | |

[a]If we have taken all reasonable steps to establish the identity of Beneficial Owners, recorded the steps we have taken and difficulties encountered when trying to establish this and collected and verified information about the individual who is the CEO (or equivalent) of the Customer based on the ML/TF risk of the Customer, we will be taken to have established this Required Item.

## Simplified Verification Measures for Body Corporate, Partnership or Unincorporated Association

Simplified Verification Measures can be applied to a body corporate, partnership or unincorporated association in the following circumstances so that we are taken to have establish certain Required Items.

We are taken to have established on reasonable grounds the identity of the Customer's Beneficial Owners where the Customer is, or is controlled (directly or indirectly) by:

- a government body; or
- a listed public company subject to public disclosure requirements that ensure transparency regarding the identity of its beneficial owners.

We are taken to have established on reasonable grounds the identity of an individual Beneficial Owner where:

- the Customer is owned in part (directly or indirectly), but not controlled, by a government body or such a listed public company; and
- the individual is a beneficial owner of that entity; and
- the individual is a beneficial owner of the Customer solely by reason of that ownership interest.

(we will still need to establish the identity of any other Beneficial Owners).

Where the Customer is, or is controlled by, an entity subject to appropriate regulatory oversight, or a strata/community title body, and the Customer is assessed as low ML/TF risk (and enhanced CDD is not required), we are not required to verify the identity of Beneficial Owners.

To verify the Customer meets these requirements, obtain reliable and independent data to confirm that the Customer meets the above requirements.

## 18.7. Trusts

Whilst trusts are used for a range of legitimate purposes, they are also commonly used by money launderers to place, layer and integrate the proceeds of crime. AUSTRAC has rated trusts as a high national money laundering risk and assessed the poor transparency of trusts as one of Australia's key national vulnerabilities to criminal exploitation. This is why there is extensive information to collect and verify when our Customer is a trust.

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| Identity of the trust | • Name of trust<br>• Kind of trust (i.e. bare trust, discretionary trust, unit trust, deceased estate, testamentary trust)<br>• Any business names of the trust<br>• Any other names the trust is commonly known by<br>• Unique identifier for the trust, if any (i.e. ABN)<br>• Address of the principal place of business or operations of the trust<br>• Evidence of the trust's existence<br>• Information about the powers that bind and govern the trust (usually in the trust deed)<br>• Full name of the individuals or each member of the group with primary responsibility for governance and executive decisions of the trust (i.e. trustees, appointors, guardians and protectors, for a bare trust, this would be the beneficiaries, for a corporate trustee, it would be the directors of the corporate trustee) | Verify, using reliable and independent data, such of the collected KYC information as is appropriate to ML/TF risk to establish the Customer's identity. | Trust deed and any amendments.<br>Where there is an ABN, Australian Business Register/ABN Lookup.<br>Where items cannot be verified from the above, letters or documents from the trust's professional advisers (who do not play any role in the trust). |
| Identity of any person acting on the Customer's behalf (and their authority to act) – any trustee(s) of the trust or other representative(s) | Where the trustee or representative is a company, collect the KYC information required for 'Bodies corporate (companies), partnerships or unincorporated associations'. Where the trustee or representative is an individual, | Independent verification is not required unless there is reason to doubt the authority or identity information provided. | Dependent on the information that needs to be verified (if any). |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| that engages with us in relation to our Designated Services | collect the required KYC information for 'Individuals'.<br><br>Information regarding authority to act for the trust i.e. copy of trust deed or POA. | If any doubt exists, verify the information to establish identity on reasonable grounds, proportionate to ML/TF risk. | |
| Identity of any person on whose behalf the trust is receiving the Designated Service (this includes all beneficiaries of the trust or if they can't be individually identified, each class of beneficiaries) | If a beneficiary is an individual – collect all KYC information required to be collected about each beneficiary as if that beneficiary was our Customer (refer to CDD procedures for 'Individuals' above).<br><br>If a beneficiary is a company, we will need to collect all KYC information required to be collected about the beneficiary as if that company was our Customer (refer to CDD procedures for 'Bodies corporate (companies), partnerships or unincorporated associations') above.<br><br>If we cannot identify each beneficiary because of the nature of the trust, we must instead collect a description of each class of beneficiary (i.e. where there is an extremely high number of beneficiaries – for example, a managed investment scheme with an extremely large number of investors or no named beneficiaries - some trusts define beneficiaries based on relationships to a primary beneficiary such as a spouse, child etc). | The same verification requirements apply depending on the type of beneficiary i.e. for beneficiaries who are individuals, refer to CDD procedures for 'Individuals' and for beneficiaries who are companies, refer to CDD procedures for 'Bodies corporate (companies), partnerships or unincorporated associations'.<br><br>We need to verify the class of beneficiaries where we cannot identify each beneficiary of the trust. | Refer to 'Individuals' or 'Companies' depending on the type of beneficiary.<br><br>For verification of class of beneficiary, original or reliable copy of trust deed and any amendments. |
| The identity of any Beneficial Owner(s) of the trust – including individual trustees and the Beneficial Owner(s) of corporate trustees, | Unless Simplified Verification Measures apply to the trust (see below this table), collect:<br><br>• Information about the control structure of the trust – including duties, rights and entitlements for administering the trust and | Unless Simplified Verification Measures applies to the trust:<br><br>• Ownership and control structure. | Original or reliable copy of trust deed and amendments.<br><br>Trustee resolutions.<br><br>Letters or documents from trust's professional |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| settlors, appointors, guardians, protectors and any other individual who exercises control over the trust through formal or informal arrangements including in some cases beneficiaries | control and decision-making processes for administering the trust and whether there are any people who control the trust (other than trustee, settlor, appointor, guardian and protector of the trust)<br>• Identity of any settlor, appointor, guardian or protector of the trust | • Identity of any individual(s) who owns or controls the trust – apply same CDD procedures for 'Individuals' to these people. | advisers that are not involved in the trust.<br>Refer to data to be used for 'Individuals' to verify identity of Beneficial Owner(s). |
| If any of the above people are PEPs or designated for targeted financial sanctions | Whether any of the above people are PEPs and the details of the individual and role if yes. | PEP status (only for individuals) and sanctions status (for all) must be verified for:<br>• the trust<br>• all trustees of the trust and any representative who engages with us in relation to Designated Services<br>• all identifiable beneficiaries of the trust<br>• all individual settlors, appointors, guardians, protectors and any other individual who exercises control over the trust. | PEP check – either manual using PEP Checklist or using third-party provider that provides PEP screening.<br>Undertake sanctions check using DFAT's Consolidated List.<br>In both cases, ensure search allows for minor discrepancies or errors in names (particularly for non-English names changed into English). |
| The nature and purpose of the business relationship or transaction | • Reasons the Customer is seeking our services and the nature of the service sought.<br>• Information about the general commercial activity or sector the | Independent verification is not required unless there is reason to doubt the | Dependent on the information that needs to be verified (if any). |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| | Customer operates in and the kinds of products and services they offer or, if not engaged in commercial activity, the purpose of the trust. | information provided.<br><br>If any doubt exists, verify the information to establish reasons for seeking service and nature of service sought (including information about the Customer's business activities and services) on reasonable grounds, proportionate to ML/TF risk. | |

## Simplified Verification Measures for Trusts

Simplified Verification Measures can be applied to a trust in the following circumstances so that we are taken to have establish certain Required Items.

We are taken to have established on reasonable grounds the identity of the Customer's Beneficial Owners where the Customer is, or is controlled (directly or indirectly) by:

- a government body; or
- a listed public company subject to public disclosure requirements that ensure transparency regarding the identity of its beneficial owners.

We are taken to have established on reasonable grounds the identity of an individual Beneficial Owner where:

- the Customer is owned in part (directly or indirectly), but not controlled, by a government body or such a listed public company; and
- the individual is a beneficial owner of that entity; and
- the individual is a beneficial owner of the Customer solely by reason of that ownership interest.

(we will still need to establish the identity of any other Beneficial Owners).

Where the Customer is, or is controlled by, an entity subject to appropriate regulatory oversight, or a strata/community title body, and the Customer is assessed as low ML/TF risk (and enhanced CDD is not required), we are not required to verify the identity of Beneficial Owners.

To verify the Customer meets these requirements, obtain reliable and independent data to confirm that the Customer meets the above requirements.

## 18.8. Government bodies

Government bodies include the government of a country, or part of a country or an agency or authority of such a government.

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| Identity of the government body | • The government body's full name<br>• Any other names the government body is commonly known by<br>• The name of the country or part of a country under which the government body is established<br>• A unique identifier for the government body (if there is one)<br>• The address of the principal place of business or operations of the government body (the main physical location from which they conduct their activities)<br>• Evidence of the government body's existence (e.g. a law or executive decision or order that establishes an agency or an extract from an official government website)<br>• The full name of the individual(s) with primary responsibility for the governance and executive decisions of the government body (e.g. CEO of an agency, Secretary of a department or board of commissioners of an agency) | • Full name of government body<br>• The address of the principal place of business or operations of the government body (the main physical location from which they conduct their activities)<br>• Name of the country or part of a country under which the government body is established | Department of Finance list of Commonwealth entities and companies.<br>ABN Lookup.<br>Reliable and independent publicly available information such as government reports and directories.<br>Reliable publicly available information online such as official government websites.<br>Viewing legislation or executive decisions that establish or regulate the relevant body. |
| Identity of any person acting on the government body's behalf (and their authority to act) – only representatives who engage with us in relation to our Designated Services (not every | Where representative is a company, collect the KYC information required for 'Bodies corporate (companies), partnerships or unincorporated associations'. Where the representative is an individual, collect the required KYC information for 'Individuals'.<br>Information regarding authority to act for the government body (i.e. | Independent verification is not required unless there is reason to doubt the authority or identity information provided.<br>If any doubt exists, verify the | Dependent on the information that needs to be verified (if any). |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| representative they have) | agency agreement, POA, employment contract with appropriate authority to represent the government body) | information to establish identity on reasonable grounds, proportionate to ML/TF risk. | |
| Identity of any person on whose behalf the government body is receiving the Designated Service | If a government body is seeking our services on behalf of another person, that other person is our Customer and we need to identify who they are (applying the relevant CDD procedures depending on Customer type). | N/A | N/A |
| The identity of any Beneficial Owner(s) of the government body | N/A | N/A | N/A |
| If any of the above people are PEPs or designated for targeted financial sanctions | Whether any of the above people are PEPs and the details of the individual and role if yes. | PEP status (only for individuals) and sanctions status (for all) must be verified for:<br>• the government body<br>• any person acting on their behalf in relation to our Designated Services | PEP check – either manual using PEP Checklist or using third-party provider that provides PEP screening.<br>Undertake sanctions check using DFAT's Consolidated List.<br>In both cases, ensure search allows for minor discrepancies or errors in names (particularly for non-English names changed into English). |
| The nature and purpose of the business relationship or transaction | • Reasons the Customer is seeking our services and the nature of the service sought.<br>• Nature of the Customer's business or operations (including the general activity or sector they operate in). | Independent verification is not required unless there is reason to doubt the information provided.<br>If any doubt exists, verify the information to establish reasons | Dependent on the information that needs to be verified (if any). |

| Required Items | KYC information to collect | KYC information to verify | Independent and reliable data we can use |
|---|---|---|---|
| | | for seeking service and nature of service sought (including information about the Customer's business activities and services) on reasonable grounds, proportionate to ML/TF risk. | |

## 18.9. CDD Procedures where we can't use simplified CDD

Where simplified CDD does not apply, we must determine which KYC information needs to be independently verified to establish the relevant Required Item on reasonable grounds, having regard to the ML/TF risk.

What we need to do will depend on the situation and the ML/TF risks involved.

For instance:

- Where the Required Item is the identity of any person acting on the Customer's behalf (and their authority to act), we may verify the KYC information we have collected by obtaining the original or a reliable copy of the document establishing/ proving authority to act (such as a POA, agency agreement, instrument of delegation etc).
- Where the Required Item is the nature and purpose of the business relationship or transaction, we may verify the KYC information we have collected by obtaining original or reliable copies of business activity statements, business records or review publicly available information including reliable third-party (including government) websites, annual reports, information from government sources, official documents approving procurement, evidence of trust activity (such as disbursements to beneficiaries where relevant). We may also collect, or collect and verify source of wealth or source of funds information where this is needed to help establish the nature and purpose of the relationship or transaction.

Work with the AML/CTF Compliance Officer to determine the additional verification that is required for the particular Customer situation and assess whether enhanced CDD is required.

## 18.10. Delaying initial CDD

In limited circumstances, we may delay completing initial CDD until after a Designated Service has commenced where this is permitted under the AML/CTF Act and Rules and the ML/TF risk associated with the Customer and the Designated Service is assessed as low.

Delayed CDD does not remove the requirement to complete CDD. All Required Items must still be established on reasonable grounds as soon as practicable after the Designated Service has commenced and in any event within the applicable specified period (which will depend on the relevant Designated Service involved).

Delayed CDD may only be applied where all of the following conditions are satisfied:

- delaying CDD is necessary to avoid interrupting the normal conduct of business;

- there is no suspicion of money laundering, terrorism financing or proliferation financing;
- the Customer and the Designated Service have been assessed as presenting a low ML/TF risk; and
- appropriate risk mitigation controls are implemented during the delay period.

Delayed CDD must not be applied where:

- the Customer is assessed as medium or high ML/TF risk;
- the Customer is a foreign PEP;
- there are indicators of suspicious activity; or
- the delay would create unacceptable ML/TF risk.

Where initial CDD is delayed, we must implement appropriate controls to manage ML/TF risk until CDD is completed. Depending on the circumstances, this may include:

- limiting the scope or functionality of the Designated Service;
- restricting the value, frequency or type of transactions that can be conducted;
- not permitting transfers of money/property/virtual assets for or on behalf of the Customer, or otherwise making them available to the Customer, until initial CDD is completed, unless approved controls are in place and the ML/TF risk remains low;
- enhanced monitoring of the Customer's transactions or behaviour during the delay period;
- requiring additional internal approvals before certain transactions are processed; or
- escalating unusual activity to the AML/CTF Compliance Officer.

CDD must be completed as soon as practicable after the Designated Service has commenced.

If we are unable to complete initial CDD within a reasonable timeframe, we must:

- cease providing the Designated Service until CDD is completed; and
- consider whether a Suspicious Matter Report (SMR) should be submitted.

The decision to delay initial CDD must be approved by the AML/CTF Compliance Officer and documented, including:

- the reason delayed CDD was necessary;
- the ML/TF risk assessment supporting the decision;
- the controls implemented during the delay period; and
- the expected timeframe for completing CDD.

All staff must consult with the AML/CTF Compliance Officer before applying delayed CDD.

## 18.11. Enhanced CDD Procedures

Enhanced CDD is not a 'one-size-fits-all' and must be tailored to the ML/TF risks involved with the relevant Customer and/or transaction. Our enhanced CDD procedures include a range of enhanced CDD measures that can be used as appropriate to managing and mitigating our Customer's ML/TF risks.

The enhanced CDD measures applied in each case must be informed by the reason why the Customer was identified as high ML/TF risk and designed to manage and mitigate the ML/TF risk.

When carrying out enhanced CDD, we will take active steps to manage and mitigate any ML/TF risks, not just monitor those risks.

This includes escalating issues for further decision by Senior Manager(s) and in some situations, declining to act for the Customer where we are not comfortable with the risks involved (this will be determined by the Senior Manager(s)).

For example, as part of our enhanced CDD, it may be appropriate to apply one or more of the following enhanced CDD measures:

- collecting and/or verifying more KYC information about the Customer;
- obtaining information on the destination of transfers of value;
- obtaining more information on the reason for certain transactions or services;
- collecting and/or verifying information about the Customer or Beneficial Owner's source of funds or source of wealth, where relevant to the nature of their ML/TF risk;
- taking additional measures to better understand the background, ownership (if relevant) and financial situation of the Customer, and other parties to a transaction;
- conducting more in-depth Customer monitoring and analysis of transactions and behaviours
- increasing the frequency of reviews of the business relationship, to assess whether the Customer's risk has changed and whether the risk remains manageable; or
- updating the Customer's KYC information more frequently than you would for other Customers.

## Collecting additional KYC information

Collecting additional KYC information when undertaking enhanced CDD can help us:

- obtain a greater level of confidence in the Customer's identity
- identify additional ML/TF risks;
- update our assessment of the Customer's ML/TF risk;
- make sure information the Customer previously provided to us is accurate;
- clarify or update KYC information relating to the Customer;
- better understand the nature and purpose of the business relationship or transaction with the Customer;
- decide whether to continue providing Designated Services to the Customer or limit the services we provide.

The additional KYC information we choose to collect will depend on the relevant ML/TF risks that we have identified.

Examples of additional KYC information (depending on the relevant situation) include:

- additional identity documents, such as a passport where we had previously collected a driver's licence; or
- photographs of Customers holding their photo identity documents to confirm the documents belong to them;
- the Customer's or Beneficial Owner's source of funds, source of wealth, and overall financial position;
- other people involved in the Designated Service including the counterparty, and their relationship with the Customer;
- why the Customer is seeking a specific Designated Service;
- the Customer's or Beneficial Owner's reputation, such as their past and present business activities;
- the destination of transfers of value; and/or
- information about the Customer available online and from internet searches, including public social media accounts.

## Verifying or re-verifying KYC information

During initial CDD, we must verify KYC information as appropriate to the Customer's ML/TF risk and will usually verify some, but not all, of the KYC information we have collected during initial CDD.

Verifying additional KYC information during enhanced CDD can provide greater certainty about the information's accuracy. We may also choose to re-verify KYC information using different sources to ensure the checks we did previously were accurate, and we can still trust the verification.

For example, as part of enhanced CDD we may:

- re-verify a Customer's KYC information;
- verify KYC information from additional independent and reliable sources;
- verify additional information to make sure their KYC information and ML/TF risk is up to date;
- re-verify information about the Customer's identity if we have doubts about the veracity or adequacy of the information we previously obtained when identifying the Customer.

## Conduct more detailed monitoring and analysis of transactions and behaviours

It may be appropriate to monitor a Customer and their activity in more depth to identify unusual transactions and behaviours.

Some methods we may use for increased monitoring and analysis include:

- reviewing the Customer's past transactions more closely to help better identify and assess their ML/TF risk and understand how they use our Designated Services;
- reviewing the Customer's transactions more frequently;
- manually reviewing unusual, complex or high-value transactions; and/or
- where relevant, updating monitoring triggers to flag additional kinds of transactions.

## Source of funds and source of wealth

In some cases we will need to conduct source of funds or source of wealth checks/verification during enhanced CDD to manage and mitigate the Customer's ML/TF risk or to help us determine if the funds for a transaction come from a legitimate source or illicit activity.

This will not be relevant to all types of ML/TF risk and so the checks we undertake must be tailored to the relevant ML/TF risks involved.

We must establish the Customer's source of funds and source of wealth on reasonable grounds as part of initial CDD if it's relevant to the nature of the Customer's high ML/TF risk – for instance where we identify ML/TF risks related to the Customer's source of funds or source of wealth or where we have a suspicion that the money, property or other assets involved could be derived from criminal activity.

During updating and reverifying KYC information as a part of ongoing CDD, we must also make sure we hold information about the Customer's source of funds and source of wealth if it's relevant to their high ML/TF risk.

There are some types of ML/TF risks which are best managed and mitigated by establishing a Customer's source of funds and source of wealth on reasonable grounds, for example:

- Customers involved with high-risk jurisdictions that have high levels of corruption, weak AML regimes or sanctions laws, or conflict zones;
- use of shell companies or complex trust or corporate structures that have hidden or opaque Beneficial Ownership;
- a Customer that has previously been a PEP, and who remains high ML/TF risk after ceasing to be a PEP due to continuing political influence;
- a Customer who isn't a PEP but holds another position of political influence and Customer monitoring has detected large transactions inconsistent with what we know about the Customer;
- a Customer who wants to conduct unusually large cash transactions, or only transacts in cash;
- high-net-worth individuals whose income sources are unclear, or with complex or opaque wealth structures;
- Customers whose wealth or income comes from multiple jurisdictions;
- there are inconsistencies between the information the Customer provided and other information available to us in relation to their income or wealth;
- there's adverse media reporting or other reliable information about the Customer's business or commercial activities; and/or
- there has been a material change in the Customer's financial circumstances or position.

In these scenarios, it's important to understand where the assets are coming from to finance the Designated Service or which have enabled our Customer to accumulate their wealth.

We do this by:

- reviewing the information we already hold about the Customer;
- collecting additional information to identify how the Customer obtained the funds for a Designated Service or accumulated their wealth in general; and/or
- verifying, where appropriate, any of the information using reliable and independent sources where we can.

In some cases we may be satisfied without having to independently verify the information we collect about source of funds or source of wealth. In which case, we will document our reasons for this. Where we can't be

satisfied without independent verification, we will need to verify the information we have collected using reliable sources.

Documents and data we can use to identify source of funds include:

- bank statements
- payslips
- tax returns
- a probated will
- court order (such as a divorce settlement)
- loan agreements
- evidence of compensation/insurance payouts
- investment/capital gains statements
- a trust deed and trustee distribution minutes
- sale/purchase agreements
- extracts from share registries
- evidence of the receipt of royalties
- records relating to business ownership
- trading receipts
- proof of gifted funds – such as a written document signed by the gifter
- evidence of gambling winnings
- property or land registers
- business and company registers
- audited financial accounts or statements
- written confirmation from a legal practitioner or accountant
- formal and witnessed declarations (using a statutory declaration in the absence of any other supporting information).

## Responding to enhanced CDD findings

Where the findings from our enhanced CDD remove the ML/TF risks we have identified, the AML/CTF Compliance Officer will take detailed notes explaining the reasons for this.

Where the findings from our enhanced CDD donot fully remove the ML/TF risks we have identified, the AML/CTF Compliance Officer will:

- escalate to the Senior Manager(s) to approve any measures to manage and mitigate the residual ML/TF risks and for approval to continue the relationship with the Customer. Where our enhanced CDD measures cannot

manage and mitigate the ML/TF risks we have identified, we will decline to provide (or continue to provide) Designated Services;

- determine if any changes are required to our ML/TF Risk Assessment; and/or
- where a Suspicious Matter arises, a SMR will be submitted in accordance with our AML/CTF Reporting Obligations Policy.

We will record our enhanced CDD measures, findings and outcomes in the AML/CTF Enhanced CDD Checklist.