AML/CTF Program (Item 54 only)
Insight Investment Partners

Version	Date updated	Responsibility	Review period
4	27 February 2026	**Anthony Lyon**	12 months

Table of Contents

1. Introduction

1.1 Introduction and scope

We have developed and implemented our **AML/CTF Program** to ensure that we:

- comply with our **AML/CTF Obligations**, and
- appropriately identify, manage and mitigate the money laundering (**ML**), Terrorism Financing (**TF**) and Proliferation Financing (**PF**) risks that we reasonably face when providing our **Designated Services**, which in our **AML/CTF Program** we refer to as our **ML/TF Risk**.

Our **AML/CTF Program** includes:

- our **AML/CTF Policies**
- our **ML/TF Risk Register** (which includes our **ML/TF Risk Assessment**)
- other supporting tools, registers and checklists,

which are appropriate to the nature, size and complexity of our business.

Commitment

Our Compliance Committee is committed to maintaining high standards of AML/CTF compliance, and we require our **Personnel** to adhere to these standards, in order to manage the risk that our services may be used for **ML** activity.

Application

Our **AML/CTF Program** applies to all areas of our business that are involved in providing a **Designated Service**, including in relation to any function provided by a **Third Party**. Our **Personnel** are required to comply with our **AML/CTF Program**.

1.2 Background

Money laundering[1]

Money laundering (ML) includes two main elements the:

- process by which illegally obtained funds are given the appearance of having been legitimately obtained, and
- use of funds (either illegally obtained or legitimate) as an instrument of crime.

ML is a major component of virtually all criminal activity and adversely affects the Australian community in numerous ways. It perpetuates **Serious Crime** by enabling criminals to reinvest in further crime. It diminishes tax revenue and weakens government control over the economy. Money laundering also undermines the integrity of Australia's financial system and other industry sectors and has the potential to damage the credibility and reputation of Australia's regulatory and law enforcement agencies.

The **ML** cycle describes the typical process criminals may use to conceal the source of illicit funds and make funds appear legitimate. It consists of the three stages of placement, layering and integration:

Placement – illegal funds or assets are introduced into the formal financial system. Some common placement techniques include structuring deposits into bank accounts and using cash to purchase assets.

Layering – illegal funds or assets are moved, dispersed or disguised to conceal their true origin. Funds are sometimes layered using a web of complex transactions. Some common layering techniques include using multiple banks and accounts, having professionals act as intermediaries and transacting through corporations and trusts.

Integration – after funds or assets are distanced from their origins, they are made available for investment in further criminal activity, legitimate business or to purchase high-value assets and luxury goods. At this stage the illegal money has achieved the appearance of legitimacy.

Businesses can be knowingly or unwittingly co-opted into facilitating **ML** at any one or more of these stages.

Terrorism financing[2]

Under Australian law, a terrorist act is defined in the **Criminal Code** and includes:

- acts or threats of violence that are done to advance a political, ideological or religious cause, either in Australia or overseas
- acts or threats of violence intended to coerce or influence through intimidation a part of government, either in Australia or overseas
- acts or threats of violence that are done to intimidate the public or a section of the public.

Terrorism financing is defined in section 5 of the **AML/CTF Act**. It is a terrorism financing offence under the **Criminal Code** and the *Charter of the United Nations Act 1945* to provide funds to a terrorist organisation or individual, or to make an asset available to a person or entity who is subject to relevant sanctions.

The terrorism financing process generally involves three distinct stages:

- raising funds through donations, self-funding, legitimate business or criminal activity
- moving funds to a terrorist network, organisation, cell or individual, or between such entities, and
- using funds for direct (operational) and indirect (organisational) costs associated with terrorist activity.

Direct costs are required to fund terrorist attacks. Examples include expenses for travel, training, explosive materials, weapons and vehicles. Indirect costs are required to maintain a terrorist network, organisation or cell, for example funds used to promote a group's ideology, fundraising events, living or legal expenses for members, or support for deceased members' family.

Funds also need to be stored during the terrorism financing process. Storage methods might include hiding cash, depositing funds in a bank account or maintaining some other financial product.

Proliferation financing[3]

Proliferation financing is when a **Person**:

- makes available an asset, or
- provides a financial service, or
- conducts a financial transaction, and

the **Person** knows that, or is reckless as to whether, the asset, financial service or financial transaction is intended to, in whole or in part, facilitate the proliferation of weapons of mass destruction (**WMD**), regardless of whether the activity occurs or is attempted.

Proliferation financing can also occur when entities or individuals who are the subject of **Targeted Financial Sanctions** (**TFS**) attempt to evade sanctions and procure materials for **WMD** programs, for example by using shell or front companies, joint ventures, dummy accounts, middlemen and other fraudulent/sham intermediaries.

The specified activities that comprise **WMD** programs include:

- the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, transhipment or use of:
    - nuclear weapons
    - chemical weapons, or
    - biological weapons
- materials related to nuclear weapons, chemical weapons or biological weapons that are prescribed by regulations, or
- the provision of technical training, advice, service, brokering or assistance related to any of the activities described above.

1.3 Our risk-based approach and the designated services we provide

Overview of Business Activities

The Licensee is an Australian Financial Services Licensee (AFSL) that provides financial services through authorised representatives and Corporate Authorised Representatives (CARs). The business primarily delivers personal and general financial product advice and related dealing services to retail and wholesale clients in relation to investment, superannuation, managed funds, securities, cash management accounts, and related financial products.

The Licensee does not manufacture financial products and generally facilitates client investments through third-party regulated product issuers and investment platforms.

All designated services are delivered through authorised advisers operating under the Licensee's supervision and compliance framework.

Services and Products Relevant for AML/CTF Purposes

Services include:

- Provision of financial product advice
- Arranging and dealing in financial products
- Facilitating establishment of investment and superannuation platform accounts
- Managed account and portfolio services (where applicable)
- Ongoing advice services and portfolio reviews
- Referrals to regulated product issuers and platforms

Products involved typically include:

- Managed funds
- Wrap and investment platforms
- Superannuation and SMSF investments
- Cash management accounts (held with product issuers)
- Securities and listed investments
- Portfolio and managed account services

The Licensee does not provide remittance services or operate money transfer businesses.

Usual Transactions (Value and Frequency)

Typical client transactions involve:

- Initial investments ranging from approximately AUD $20,000 to AUD $2,000,000+ depending on client profile
- Ongoing contributions or portfolio adjustments periodically (monthly, quarterly, or ad hoc)
- Investment switches and rebalancing transactions
- Superannuation rollovers and consolidations

Transaction frequency is generally low to moderate and consistent with long-term investment strategies rather than high-velocity fund movements.

Online Platform / Website

The business maintains a public website for marketing and informational purposes. Advice services are not fully automated or anonymous. Client onboarding and advice delivery occurs through adviser interaction.

Client investments are typically implemented through regulated third-party investment and superannuation platforms that maintain their own AML/CTF controls.

Electronic identity verification and secure digital document collection tools may be used as part of the onboarding process.

Acceptance of Cash

The Licensee and its representatives **do not accept cash payments** from customers for investment purposes or fees.

All client funds are transferred directly to regulated product issuers or platforms via bank transfer or platform payment mechanisms.

ML/TF Risk Assessment Process

Each customer undergoes a documented AML/CTF risk assessment at onboarding using the Licensee's approved KYC and AML risk assessment tools. This includes:

- Identity verification
- Sanctions and PEP screening
- Source of funds and source of wealth review
- Jurisdiction risk assessment
- Customer risk scoring methodology
- Enhanced Due Diligence where higher risk indicators exist

Risk ratings determine whether additional verification or Licensee approval is required before services proceed.

Ongoing monitoring and periodic reviews are conducted.

How Customers Transfer Funds

Customers transfer funds:

- Directly to regulated product issuers and investment platforms
- Via Australian bank transfers
- Via superannuation rollover processes
- Via platform contribution facilities

Funds are **not typically paid to the Licensee or advisers directly** for investment purposes.

Advice fees are generally deducted by product platforms under client authority.

How Customers Receive Funds

Customers receive funds:

- Directly from investment platforms or product issuers
- Via redemption payments to their nominated bank accounts
- Via superannuation benefit payments processed by trustees

The Licensee does not generally disburse client investment funds.

Overseas Fund Transfers

The Licensee does not send funds overseas on behalf of customers.

Customers may invest in products with international exposure through regulated investment products, but fund transfers are handled by the product issuer or platform, not the Licensee.

International transfers initiated by customers are subject to platform and banking controls.

Customer Beneficiaries

Typical beneficiaries include:

- The customer themselves
- Superannuation member accounts
- Investment account holders
- Estate beneficiaries under regulated trustee arrangements

Third-party beneficiary payments are not normally facilitated by the Licensee.

Third-Party Transfers

The Licensee does not generally allow customers to transfer investment funds to unrelated third parties.

Where third-party payment instructions arise, they are subject to:

- Additional verification
- Platform controls
- Enhanced scrutiny
- Compliance approval

Usual Source of Wealth and Source of Funds

Typical customer source of wealth and funds includes:

- Employment and salary income
- Business income

- Sale of property or assets
- Inheritance
- Superannuation balances
- Investment portfolio accumulation
- Retirement savings

Higher-risk or unexplained wealth sources trigger enhanced due diligence.

Outside Risk Appetite

The Licensee's risk appetite excludes or restricts:

- Anonymous or pseudonymous clients
- Clients unwilling to provide identification documents
- Sanctioned or designated persons
- High-risk foreign politically exposed persons without enhanced controls
- Clients primarily dealing in cash
- Complex opaque ownership structures without transparency
- Unverified source of funds situations
- Transactions inconsistent with client profile
- Requests to move funds through unrelated third parties

Such clients or transactions require senior compliance approval or are declined.

Insight Investment Partners is a financial planning practice who holds an Australian Financial Services (AFS) licence operating in Sydney, Australia only. We only provide item 54 designated services. In summary:

- we will not provide **Designated Services** to customers in high risk Jurisdictions
- all clients are individuals based in Australia
- we do not operate an online platform for the delivery of our **Designated Services**, and
- most of our services are delivered in person, via email or phone.

The Financial Services sector has an inherent **ML/TF Risk** rating of low to medium and given our Designated Services we offer, our types of customers we service and our geographic location, we have determined that our overall ML/TF Risk is also low-medium. This is the approach we take when managing our ML/TF Risk and aligns with our overall risk appetite.

Full details of the **Designated Services** (products) we provide, our customer types, delivery channels we use to provide our **Designated Services** and the countries we deal with when providing our **Designated Services** are documented in the ***Business Specific Data Tool (Tool 2A).***

We ensure that we have in place adequate and appropriate **ML/TF** risk mitigation procedures by:

- complying with our **AML/CTF Program**, and monitoring our compliance
- assessing, evaluating and approving customers and transactions in accordance with our **AML/CTF Program**
- regularly reviewing and updating our **AML/CTF Program** and **ML/TF Risk Assessment**, and
- reporting to **AUSTRAC** where appropriate, in relation to customers and transactions.

1.4 Core responsibilities

Chapter	Core Responsibilities addressed
1. Introduction	Develop, maintain and comply with an **AML/CTF Program** which incorporates our **AML/CTF Obligations**, and is appropriate to the nature size and complexity of business.
2. **ML/TF Risk Assessment**	Conduct an assessment of the **ML/TF Risk** we face when providing our **Designated Services** and review and update as required.
3. **Personnel** and Governance	Implement Governance policies and procedures to manage and mitigate our **ML/TF Risk** which include **Personnel** due diligence and AML/CTF training
4. Customer Due Diligence (CDD)	Conduct risk-based **CDD Procedures** on our customers, including **Enhanced CDD**.
5. **AUSTRAC** Enrolment and Reporting	Ensure that we lodge all required reports such as **Suspicious Matter Reports** (SMRs) with **AUSTRAC** and maintain our **AUSTRAC** enrolment requirements.
6. Program Maintenance and Review	Update our **AML/CTF Program**, **ML/TF Risk Assessment** and supporting procedures and tools and maintain records of our compliance.

2. ML/TF Risk Assessment

2.1 Introduction and scope

This policy sets out how we conduct our **ML/TF Risk Assessment**, that is, how we identify, assess and evaluate the **ML/TF Risk** that our business faces when providing our **Designated Services**.

Our **ML/TF Risk Assessment** is based on our risk-based systems and controls, which we consider are appropriate for our business, having regard to its nature, size and complexity, and the type of **ML/TF Risks** our business is exposed to when providing our **Designated Services.**

Our **ML/TF Risk Assessment** Methodology is outlined in section 2.4 below and includes separate supporting tools. The results of our **ML/TF Risk Assessment** are recorded in our ***ML/TF Risk Register (Tool 2B).***

In this policy, we refer to our **ML/TF Risk Assessment** Methodology and our **ML/TF Risk Register**, collectively as our '**ML/TF Risk Assessment'**.

We ensure that our **ML/TF Risk Assessment** is up to date before we commence to provide a **Designated Service**.

2.2 Proliferation financing risk

We have considered the **PF** risk which is relevant to the **Designated Services** we provide, using the criteria in our ***Assessment of PF Risks faced by our Business* (*Tool 2D)***, and have determined that the level of risk that our business could be involved in **PF** activity **low**.

Accordingly, we have formed the view that our **AML/CTF Policies** appropriately manage our **PF** risk, and at this time we do not need to create or implement any **PF**-specific policies.

Our **Senior Manager** will reassess the level of **PF** risk annually, or when any of the factors that form the basis of our assessment change.

2.3 What risk categories do we consider?

We consider the following risk categories:

- **Product:** the nature of the **Designated Services** we provide
- **Customer:** our customer types
- **Channel:** the delivery channels by which our **Designated Services** are provided
- **Jurisdiction:** the countries or other jurisdictions that we deal with when providing our **Designated Services**, or that our customers are connected to ***(Jurisdiction Risk Data (Tool 2C))***
- Other **–** broad risks associated with running an **AML/CTF Program**

2.4 ML/TF Risk Assessment Methodology

At a high level, our **ML/TF Risk Assessment** consists of 3 stages:

- Identify our **ML/TF Risks**
- Assess each **ML/TF risk**, so that we understand when and where this risk can occur, and the likelihood and impact of it occurring
- Evaluate the **ML/TF Risks**, to provide us with a framework for addressing each risk.

Step 1 – Identify

We have considered the following to identify **ML/TF Risks** relevant to our business:

- industry specific risks as identified in **AUSTRAC**'s:
    - Industry Specific Typologies
    - Other guidance ***(refer to AUSTRAC Guidance Register (Tool 6A))***
- business specific risks, broken down by:
    - **Products/services:** the **Designated Services** we provide, including the value of the revenue that each **Designated Service** derives annually, to help us assess the impact and consequences of associated **ML/TF Risks**
    - **Customer:** our different customer types, including high-risk customers, to help us assess the impact and consequences of associated **ML/TF Risks**
    - **Channel:** the channels we use to deliver our **Designated Services**
    - **Jurisdiction:** the countries and other jurisdictions we deal with when providing **Designated Services**, or that our customers are connected to.

The complete list of risks identified for our business is contained in our ***Business Specific Data (Tool 2A)***, and also in our ***ML/TF Risk Register (Tool 2B).***

Step 2 – Assess

For each risk, we have assessed the likelihood and consequence of the **ML/TF Risk** materialising to determine the inherent risk, that is, the level of risk if no controls where in place to mitigate and/or manage the **ML/TF Risk.**

We have used the following table to assess the likelihood of an **ML/TF Risk** occurring.

Likelihood rating	Likelihood of ML/TF risk occurring
1. **Rare**	Highly unlikely, but not impossible
2. **Unlikely**	Could occur, but is unexpected
3. **Possible**	May occur at some time
4. **Likely**	Will probably occur in most circumstances
5. **Almost Certain**	Expected to occur in most circumstances

We have used the following table to assess the impact or consequence of an **ML/TF Risk** occurring.

Consequence rating	Consequence of ML/TF risk occurring
1. **Insignificant**	Negligible ML/TF event or impact
2. **Minor**	Isolated, low-level ML/TF event or impact
3. **Moderate**	Moderate ML/TF event or impact
4. **Major**	Significant ML/TF event or impact
5. **Extreme**	Severe ML/TF event or impact

Combining the above tables produces the following matrix we use to assess the inherent **ML/TF Risk**:

Likelihood ↑						
	Almost Certain	Significant	High	High	High	High
	Likely	Significant	Significant	Significant	High	High
	Possible	Medium	Medium	Significant	Significant	High
	Unlikely	Low	Low	Medium	Significant	Significant
	Rare	Low	Low	Low	Medium	Significant
		Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
		Consequence →				

The resulting overall inherent **ML/TF Risks** used in our **ML/TF Risk Assessment** are defined as follows:

Inherent risk rating	Risk rating description
Low	Insignificant to low inherent **ML/TF Risk** that needs to be appropriately mitigated by our systems and controls

Medium	Medium inherent **ML/TF Risk** that needs to be appropriately mitigated by our systems and controls
Significant	Significant inherent **ML/TF Risk** that requires systems and controls to mitigate and monitor the risk
High	High inherent **ML/TF Risk** that requires additional systems and controls to mitigate and monitor the risk

Our ***ML/TF Risk Register (Tool 2B)*** contains an assessment of each risk based on the methodology above.

Step 3 – Evaluate

A master list of controls and our evaluation of their effectiveness can be found our ***ML/TF Risk Register (Tool 2B).***

To evaluate the effectiveness of each control, referred to as the control effectiveness, we assess if the control meets any of the following factors:

- Design:
  - if it complies with the requirements of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* ('the **AML/CTF Act**') and **AML/CTF Rules**
  - if it adequately addresses the **ML/TF Risk**
  - is it appropriate to the nature, size and complexity of our business.
- Operation:
  - how effective the control is in mitigating and/or managing the risk.

We use the following table to evaluate the overall effectiveness of a control.

Rating	Description
Not effective	Satisfies none or one of the evaluating factors
Partially effective	Satisfies two or three of the evaluating factors
Effective	Satisfies all evaluating factors

Residual risk rating methodology

The residual risk is the **ML/TF Risk** that remains after applying one or more of our identified controls.

It is assessed by evaluating the effectiveness of the control mitigating or managing the inherent **ML/TF Risk**, using the following matrix:

Inherent risk rating ↑				
	High	Medium	Significant	High
	Significant	Low	Medium	Significant

	Medium	Low	Medium	Medium
	Low	Low	Low	Low
		Effective	**Partially effective**	**Not effective**
		Control effectiveness →		

Testing of controls

Once implemented, our controls will be re-assessed after either a period of three months or once sufficient **Designated Services** have been provided to make a reasonable assessment of both the design and operational effectiveness of the control.

Any change in the assessment, will be updated in our Control Library, which forms part of the ***ML/TF Risk Register (Tool 2B)***. Where a control is rated 'Not effective', it will be reviewed and updated or replaced.

Controls will be reassessed in accordance with ***Chapter 6 – Program Maintenance and Review***.

2.5 References

Related policies and tools

Policies	Chapter 6 Program Maintenance & Review
Tools	2A Business Specific Data 2B **ML/TF Risk Register** 2C Jurisdiction Risk Data 2D Assessment of **PF** Risks Faced by our Business

Legislative requirements and references

Law	**AML/CTF Act**
Regulations	**AML/CTF Rules**
Regulatory guidance	**AUSTRAC** guidance – Step 2: Identify and assess your risks: risk assessment (Reform)

3. Personnel and Governance

3.1 Introduction and scope

As an item 54 only provider we are not required to appoint all specific AML/CTF governance roles and undertake Personnel due diligence and training. However, we are committed to ensure we maintain high standards of AML/CTF compliance in order to manage the risk that our services may be used for **ML/TF** activity. As such, we :

- appoint our governance roles, and their respective obligations as part of our broader obligation to ensure we undertake appropriate measures to mitigate and manage our **ML/TF Risk**, and
- undertake initial, ongoing and trigger-based **Personnel** due diligence, by assessing – both before and during their employment or engagement – the skills, knowledge and expertise of our **Personnel** relevant to their responsibilities under our **AML/CTF Policies**, as well as their integrity., and
- provide initial and ongoing **Personnel** AML/CTF training, to ensure our **Personnel** understand our **ML/TF Risk**, obligations, and the processes and procedures they must follow to manage and mitigate our **ML/TF Risk**.

3.2 Identifying relevant and high-risk Personnel

Identifying relevant Personnel

Personnel includes individuals or non-individual persons that we (or that we may):

- employ
- otherwise engage, such as contractors, consultants, volunteers, interns (paid and unpaid) and people employed by service providers that we engage.

The ***Personnel Due Diligence and Training Register (Tool 3A)*** identifies and maps our **Personnel** roles and responsibilities to the functions that are relevant to our AML obligations.

Identifying higher-risk Personnel

Our ***Personnel Due Diligence and Training Register (Tool 3A)*** also identifies roles that pose a higher **ML/TF Risk**.

To identify higher-risk roles, we assess whether the role:

- increases the risk that **Personnel** is or becomes a target for collusion or coercion by criminals
- could pose a serious **ML/TF Risk**, or non-compliance risk if fulfilled by **Personnel** without adequate competence or integrity, or
- enables **Personnel** to, or have the authority to, authorise, override or bypass a range of high-risk activities, as documented in our ***Personnel Due Diligence and Training Register (Tool 3A* column E)**.

3.3 Governance roles

We have appointed the following persons to our governance roles, responsible for:

- implementing and overseeing our **AML/CTF Policies**, and
- ensuring we undertake appropriate measures to mitigate and manage our **ML/TF Risk**.

Role	Requirements	Appointed
Senior Manager(s)	Responsible for making decisions that affect the whole, or a substantial part, of the business of our **Reporting Entity**	Christopher Fellas

Reporting Entity Status

The Licensee is registered with AUSTRAC as a Reporting Entity for AML/CTF purposes.

The Licensee is **not part of a Reporting Group** and has not been appointed as a Lead Entity of a Reporting Group.

Corporate Authorised Representatives, Authorised Representatives, and service providers operate under the Licensee's AML/CTF Program and supervision framework but are not separate Reporting Entities for AUSTRAC reporting group purposes.

Governing Body

Our **Compliance Committee** meets every month and at each meeting, considers the AML/CTF matters set out in the standing agenda ***AML/CTF Standing Meeting Agenda (Tool 3B)*** to ensure that it is provided with the information it requires to fulfil its obligations as detailed below.

Obligations

Our **Governing Body**'s obligations include:

- exercising ongoing oversight by taking reasonable steps to ensure we are complying with our AML obligations, including compliance with the **AML/CTF Act**, regulations and **AML/CTF Rules**
- exercising ongoing oversight by taking reasonable steps to ensure we are appropriately identifying, assessing, managing and mitigating our **ML/TF Risk** relevant to the **Designated Services** we provide

Senior Manager(s)

Obligations

The **Senior Manager** is responsible for considering, and, if appropriate, approving the following:

- our **ML/TF Risk Assessment**, including any updates or changes (refer to ***AML/CTF Program Review and Update Register (Tool 6B)***)
- our **AML/CTF Policies**, including any updates or changes (***AML/CTF Program Review and Update Register (Tool 6B***)
- entering into or continuing, a **Business Relationship** with a **Foreign Politically Exposed Person** (**PEP**) or high risk domestic or international **PEP**, or where the **Beneficial Owner** of the customer or any **Person** on whose behalf the customer is receiving the service, is or becomes a **Foreign PEP** or high risk domestic or international **PEP.**
- commencing or continuing a **Business Relationship** with a customer, as part of undertaking **Enhanced CDD**
- entering into an outsourcing arrangement with a third-party service provider to assist us to comply with our **AML/CTF Obligations**, including due diligence checks, and maintaining ongoing oversight of the external service provider's performance (see ***Chapter 3 – Personnel and Governance)***
- entering into a reliance arrangement with a **Third Party** whereby we rely on the **Know Your Customer (KYC)** information collected about a customer by a **Third Party Reporting Entity** (refer to ***Chapter 4 - Customer Due Diligence***)

3.4 Outsourcing

When or if we appoint an external service provider, for the purpose of outsourcing some of our **AML/CTF Obligations** we:

- assess the **ML/TF Risk** which arises from entering into an outsourcing arrangement
- recognise that regardless of appointing an external service provider to comply with some of our **AML/CTF Obligations**, we retain responsibility for our statutory responsibilities under the **AML/CTF Act**, including ensuring that the identities of our customers are verified, and that suspicious matters are reported, and
- undertake pro-active monitoring and testing of the AML/CTF systems and processes provided by the external service provider, both at the commencement of the appointment and during the period of the appointment.

Prior to appointing an external service provider, the **Senior Manager** is responsible for conducting due diligence on the external service provider, in order to ensure that the service provider:

- has the appropriate experience, qualifications and expertise to deliver the services, and
- provides us with all requested information about their performance of the outsourced **AML/CTF Obligations**

External Service Provider Appointment Assessment Template (Tool 3J) sets out in detail of the due diligence procedures we implement when appointing an external service provider to conduct the outsourced AML Obligations.

Performance targets

We design performance targets for each external service provider, to ensure that the outsourced **AML/CTF Obligations** are performed to our specifications, depending on the nature of the service provided.

The **Senior Manager** monitors the external service provider's performance of the outsourced services, by requiring the service provider to provide a quarterly report which summarises the nature of the services provided and how they were performed.

The **Senior Manager** also implements performance targets and conducts an annual assessment of whether the external service provider is complying with the performance targets (refer to ***External Service Provider Ongoing Assessment Template (Tool 3K)).*** This procedure is implemented earlier, if there is a breach of the outsourcing agreement.

Outsourcing agreement

We enter into an outsourcing agreement with each external service provider. The **Senior Manager** ensures that each outsourcing agreement sets out:

- the services provided (whether one-off or ongoing)
- expected service standards and performance targets
- performance audits and other oversight, monitoring and review measures
- the term of the agreement, and termination provisions
- treatment of data about our business which is held or controlled by the external service provider, both during and at the end of the relationship, and
- the external service provider's obligations in relation to notifying us of any actual or potential breaches of our **AML/CTF Obligations**.

Ongoing management oversight

The **Senior Manager**

- is responsible for implementing controls to manage the **ML/TF Risk** associated with outsourcing
- receiving reports from the external service provider's compliance with the outsourced **AML/CTF Obligations**, and managing any issues of non-compliance by the external service provider
- notifying the **Governing Body** of any issues of non-compliance with performance targets by the external service provider (refer to ***External Service Provider Ongoing Assessment Template (Tool 3K)***).

3.5 Personnel due diligence

Initial Personnel due diligence

As we do not employ or engage any **Personnel** / do not have any **Personnel** involved in the provision of **Designated Services** other than ourselves, we do not currently undertake **Personnel** due diligence. However, if we decide to employ or engage **Personnel** who will be involved in the provision of **Designated Services**, the following process will be followed to assess their skills, knowledge, expertise and integrity.

Before any **Personnel** begins performing any AML/CTF-related functions, we assess whether they are suitable, with respect to their:

- skills, knowledge and expertise, and
- integrity.

Skills, knowledge and expertise

To assess whether **Personnel** have the appropriate skills, knowledge and expertise for their AML/CTF responsibilities, we assess whether they:

- understand our **AML/CTF Obligations**
- are aware of the **ML/TF Risks** relevant to their role and responsibilities outlined in our **AML/CTF Program**
- can apply and implement our **AML/CTF Policies** effectively for their respective role, and
- have adequate AML/CTF training or are otherwise competent to receive such training to close any identified knowledge gaps.

We do this by:

- comparing their application or CV against the position description for the role
- conducting interviews for the role
- requiring them to complete training with knowledge-based assessments
- considering prior AML/CTF experience
- verifying their academic or professional qualifications, memberships or certifications
- considering evidence of their previous performance (including reference checks)
- checking their website (if relevant) and any material on it, and

We may, following our initial assessment, determine that a **Personnel** is generally suitable for a role, but also identify that they have some gaps relevant to the **Designated Services** we provide to our customers. In such circumstances, we may still decide to employ or otherwise engage the **Personnel**, on the basis that:

- if there is a significant risk of ML/TF or non-compliance caused by such gaps, we will delay assigning some or all AML/CTF responsibilities to them until they have undertaken general and/or targeted AML/CTF training as appropriate and in line with this policy, and
- we will reassess their skills, knowledge and expertise (and suitability for the role) once any such training is completed.

Integrity

To assess whether **Personnel** will uphold ethical standards and will not pose an undue risk to compliance with our **AML/CTF Obligations**, we implement the measures set out in the following table.

All Personnel	**Additional measures for higher-risk Personnel**

• Verification of identity:
  ○ Individuals: name, date of birth, place of birth and citizenship via Government-issued identification documents
  ○ Non-individuals: certificate of business or company registration (or equivalent)
• Verification of address (residential address for individuals, business address for non-individuals)
• Nationally Coordinated Criminal History Check
• Foreign jurisdiction criminal history check (for **Personnel** who have been a resident of a foreign jurisdiction during the past 5 years)
• **Visa Entitlement Verification Online ('VEVO')** check, for verification of right to work in Australia for non-Australian or New Zealand citizens
• Confirmation of academic or professional qualifications, memberships or certifications
• Reference checks from previous employers (or persons who have otherwise engaged them)
	• Credit history check
	• **TFS** check
	• **PEP** check
	• Bankruptcy or insolvency check (as applicable)
	• Current and historical **ASIC** register searches for company officer and shareholder roles
	• Relevant integrity regulatory or professional tests, e.g. licences, registrations or memberships (relevant to the role)

• Open-source searches for relevant regulatory (civil or administrative) action, including:
  ○ Public search engines, including checking for adverse media
  ○ [**ASIC** Banned & Disqualified Persons Register]
  ○ [**ASIC** Banned Bodies Corporate Register]
  ○ [**ASIC** Infringement Notices Register]
  ○ [**ASIC** Court Enforceable Undertaking Register]
• Requirement to self-disclose whether they have:
  ○ been the subject of adverse findings, or found to have engaged in serious misconduct, by a law enforcement agency or regulatory body in Australia or a foreign jurisdiction, and
  ○ any conflict of interest that will create a material risk that they will fail to properly perform their duties.	

Ongoing Personnel due diligence

Because our risks, roles and processes evolve over time, we have implemented a range of ongoing **Personnel** due diligence measures to:

- assess whether our **Personnel** continue to be suitable for their role and possess the knowledge to carry out their AML/CTF responsibilities effectively, and
- identify when **Personnel** require additional training.

We do this by:

- conducting periodic checks, reviews and assessments at regular intervals, proportionate to the associated risks, and
- requiring **Personnel** to self-report certain matters and meet certain performance targets.

Our periodic checks, reviews and assessments, and their frequency, are set out in the following table:

Check, review or assessment	**Frequency**	
	Minimum for all Personnel	**Additional measures for higher-risk Personnel**
• Updated integrity checks, as follows:	None	Every 2 years

Check, review or assessment	Frequency	
	Minimum for all Personnel	**Additional measures for higher-risk Personnel**
○ a Nationally Coordinated Criminal History Check, and/or foreign jurisdiction criminal history check (for **Personnel** who have been a resident of a foreign jurisdiction during the past 5 years) (as applicable) ○ adverse media checks via [public search engines or subscription service] and ○ all additional measures for higher-risk **Personnel**.		
• Updated integrity check, requiring **Personnel** to re-attest whether they have: ○ been the subject of adverse findings, or found to have engaged in serious misconduct, by a law enforcement agency or regulatory body in Australia or a foreign country or ○ any conflict of interest that will create a material risk that they will fail to properly perform their duties.	Bi-annually	Annually
• Review the Governance & **Personnel** roles and responsibilities and processes, as part of our internal annual review of our ***Chapter 6 - Program Maintenance & Review***	Annually	Annually
• Assess whether **Personnel** are effectively implementing our **AML/CTF Program**, as part of our annual AML/CTF Compliance Reports (see ***Chapter 5 - AUSTRAC Enrolment, Registration & Reporting***)	Annually	Annually
• Assess **Personnel** knowledge following any updated AML/CTF risk awareness training, following any material changes to **AML/CTF Legislation** or our **AML/CTF Program**	As needed	As needed

In addition, we require our **Personnel** to:

- at all times, notify us whether they have:
    - been the subject of adverse findings, or found to have engaged in serious misconduct, by a law enforcement agency or regulatory body in Australia or a foreign jurisdiction
    - any conflict of interest that will create a material risk that they will fail to properly perform their duties, or
    - observed any suspicious behaviour by other **Personnel** that may indicate that the other **Personnel** may be colluding with, or coerced by, one or more criminals, and
- as part of our performance management process, meet performance targets that demonstrate that they have undertaken all required AML/CTF risk awareness training, and are applying **AML/CTF Policies** effectively.

This obligation is captured in ***AML/CTF Personnel Due Diligence Declaration (Tool 3F)***, which all **Personnel** must complete.

Trigger-based Personnel due diligence or other action

We undertake **Personnel** due diligence or other actions in response to certain trigger events, including AML/CTF compliance breaches or other incidents, as set out in the following table:

Trigger	Due diligence or other action
The Personnel's role changes, either through a transfer, promotion or an expansion of responsibilities, such that their role now carries new or higher **ML/TF Risks**	The due diligence measures set out in this section, as appropriate for the **ML/TF Risk** level of the Personnel's new role, and where those measures have not been conducted during the preceding 12 months.
We commence providing new or amended **Designated Services**, such that there has been a significant increase in our **ML/TF Risk**, and the Personnel's role, therefore, carries higher **ML/TF Risk**	The due diligence measures set out in this section, as appropriate for the **ML/TF Risk** level of the Personnel's new role, and where those measures have not been conducted during the preceding 12 months.
Personnel's change in circumstances gives rise to lower-risk integrity concerns, which may include the following: • being under formal investigation by a law enforcement agency or regulatory body in Australia or a foreign jurisdiction • becoming an undischarged bankrupt under the law of Australia or a foreign country or • entering into a personal insolvency agreement under Part X of the Bankruptcy *Act 1966* (Cth) or a similar law of a foreign country.	Monitor the **Personnel** more closely and more frequently and reassign to a role with lower **ML/TF Risk**, unless and until the lower-risk integrity concerns are resolved satisfactorily.
Personnel's change in circumstances gives rise to higher-risk integrity concerns, including, but not limited to: • being the subject of adverse findings, or found to have engaged in serious misconduct, by a law enforcement agency or regulatory body in Australia or a foreign jurisdiction • possessing any conflict of interest that will create a material risk that they will fail to properly perform their duties • having been observed to have engaged in any suspicious behaviour by other Personnel, that may indicate that they may be colluding with, or coerced by, one or more criminals or • being the subject of adverse media indicating any of the above.	Removal from all roles related to our **AML/CTF Obligations**, unless and until such higher-risk integrity concerns are resolved satisfactorily.
Personnel is suspected to have breached our **AML/CTF Policies**	**Personnel** must report suspected breaches to the **Senior Manager**.

Trigger	Due diligence or other action
	The **Senior Manager** must: • assess the suspected breach, determine whether a breach has occurred, assess its severity, and ensure that the appropriate consequences are implemented (as outlined in the table below named 'Consequences for Personnel Breaches of **AML/CTF Policies'**) • include details of the suspected breach in the relevant **Personnel's** file • review the **Personnel's** compliance with the appropriate consequences after a reasonable period following the imposition of the consequences and • determine whether the matter must be reported to AUSTRAC, and if so, ensure that the report is submitted (for example, lodging a **SMR**.
Personnel demonstrates they have insufficient skills or knowledge to enable them to perform their role	Either: • temporarily suspend their duties relating to complying with our AML/CTF Obligations, and require them to complete AML/CTF training, to ensure they have now obtained the skills and knowledge to enable them to perform their role or (if this is not possible) • remove them from their role and replace them with **Personnel** who have the required skills and knowledge.

Consequences for Personnel Breaches of AML/CTF Policies		
Materiality	**Description of breach**	**Minimum consequences**
Low	A breach that, in the opinion of the [amend as appropriate: **Senior Manager]**, does not involve a material **ML/TF Risk**	• Formal meeting with Personnel's manager and **Senior Manager** to discuss the incident and • Further AML/CTF training.
Medium	One or more breaches that, in the opinion of the Senior Manager involve a material **ML/TF Risk**	In addition to the consequences for Level 1: • formal written warning

		• the **Senior Manager**) reports the breach to the [amend as appropriate: **Governing Body]** • restriction of duties or reassignment to a role with lower **ML/TF Risk**, and/or • increased monitoring and supervision of duties.
High	One or more breaches that, in the opinion of the Senior Manager involve a serious **ML/TF Risk**	The **Senior Manager** reports the breach to the [amend as appropriate: **Governing Body]** and either: • removal from duties relevant to our AML/CTF Obligations, or • termination of employment or engagement.

Response to adverse assessments

If unsatisfactory or adverse information is obtained with respect to initial, ongoing or trigger-based **Personnel** due diligence, the **Senior Manager** will assess the available information and determine, in light of the **ML/TF Risk** involved and as appropriate, whether to:

- obtain and assess further due diligence information regarding the **Personnel**
- not to employ or otherwise engage the **Personnel**
- terminate the employment or engagement of the **Personnel**, or
- remove or restrict the **Personnel** duties that are relevant to our **AML/CTF Obligations**.

3.6 AML/CTF Training

We ensure that all **Personnel** undergo training relevant to their roles, by:

- developing and maintaining a training plan to provide tailored training to different roles and their relevant **ML/TF Risk**
- maintaining a Register to record **Personnel** training completion dates and track when further training is due
- reviewing and monitoring the effectiveness of the training we provide, to assess whether our **Personnel** retain and apply the training, and
- updating the training plan in response to changes in **AML/CTF Legislation**, our **AML/CTF Policies**, or **ML/TF Risk**.

Personnel Training Plans and our Training Register is recorded in ***Personnel Due Diligence and Training Register (Tool 3A)***.

Training plan

This section contains our training plan, which we have developed and maintain and sets out the training that our **Personnel** must complete, in relation to:

- our **AML/CTF Obligations** and our **AML/CTF Policies**
- the nature and consequences of our **ML/TF Risks** and the potential consequences of such risks, including:
    - trends, methodologies and techniques of ML/TF activity, which are relevant for the nature and scale of our business, our sector, and the **Designated Services** we provide and
    - insights into our **ML/TF Risk Assessment**, including the vulnerabilities related to our services, and
- the consequences of non-compliance with our **AML/CTF Obligations** and our **AML/CTF Policies**.

The training methods we use are diverse [amend this sentence as appropriate: and include online learning modules (including via **Third Party** training providers), online training delivered in real time online, and face-to-face training. In addition, **Personnel** are kept updated regarding any changes to **AML/CTF Legislation** or our **ML/TF Risk** through updates from the [amend as appropriate: **Senior Manager]**, which may be delivered over email, online or face-to-face meetings].

The type(s) of formal training that **Personnel** must complete consists of:

- general AML/CTF risk awareness training (for all **Personnel**), and
- tailored training relevant to the Personnel's role.

The particular targeted training required to be completed by relevant **Personnel** is tailored, depending on the Personnel's role and how it relates to our **AML/CTF Obligations**.

Our Senior Managermaintains our training schedule, which forms part of our ***Personnel Due Diligence and Training Register (Tool 3A)*****,** that sets out the type(s) of training each **Personnel** (or group of **Personnel**) is required to complete, and when, pursuant to the training plan.

As set out in the training schedule, all **Personnel** must complete general AML/CTF risk awareness training:

- Initial: within [insert number, e.g. 30] days of commencing their role, and
- Refresher: on an [insert frequency, e.g. annual] basis.

All relevant **Personnel** must complete targeted training relevant to their role within [insert number, e.g. 30] days of when they commence their role, as well as refresher training at the following frequencies:

Personnel role	**Targeted training frequency**
Senior Manager **Governing Body**	Every 12 months

Customer-facing roles	Every 12 months
Transaction-related roles	Every 6 months
Third Party service provider	At least every 12 months, as well as when new **Personnel** perform the tasks, or when their contract is renewed or changed.

Training register

The Senior Manager is responsible for monitoring other **Personnel's** completion of required AML/CTF training. The training register is the tool used for monitoring the satisfactory completion of each **Personnel's** AML/CTF training, as per their training plan.

Reviewing and monitoring training

[Insert a description of how you monitor and supervise your **Personnel** training, and to ensure that they have the skills and knowledge to be able to comply with this Program.

Set out an explanation of:

- how your processes are part of **Personnel** annual reviews
- how **Personnel** are reviewed, including back-office and front-office **Personnel**
- how results of reviews are captured, reported and followed up, and
- an assessment of the adequacy of the AML/CTF training provided to **Personnel**.

Example: As part of our **Personnel** annual performance reviews, we assess our Personnel's:

- comprehension of AML/CTF concepts, and a high-level understanding of the **AML/CTF Legislation**
- knowledge of our **AML/CTF Policies** to conduct risk-based **KYC** checks on customers, and
- understanding our AML/CTF reporting obligations (in particular, the obligation to report suspicious matters), and the procedure that must be followed.]

Updating training

We review and update, as appropriate, our AML/CTF training, in response to:

- changes to **AML/CTF Legislation**
- new and emerging **ML/TF Risks**
- changes to our **AML/CTF Program**
- findings from **AML/CTF Program Independent Evaluations**, or regulatory or internal compliance reviews, that indicate AML/CTF training gaps

- significant instances of non-compliance or breaches of **AML/CTF Obligations** (potential or actual), and
- **AUSTRAC** guidance or other action, such as enforcement action.

3.7 References

Related policies and tools

Policies	Chapter 2 - **ML/TF Risk Assessment** Chapter 5 -**AUSTRAC** Enrolment, Registration and Reporting Chapter 6 - Program Maintenance and Review
Tools	3F. AML/CTF **Personnel** Due Diligence Declaration Template 3G. **Reporting Group** Member Procedure 3H. **Reporting Group** Member Register 3I. **Reporting Group** Member Information Sharing Request Template 3J. External Service Provider Appointment Assessment Template 3K. External Service Provider Ongoing Assessment Template

Legislative requirements and references

Law	**AML/CTF Act**
Regulations	AML/CTF Regulations
Regulatory guidance	**AUSTRAC** Guidance – Personnel due diligence and training (Reform)

4. Customer Due Diligence (CDD)

4.1 Introduction and scope

This Policy sets out how we conduct our **Initial CDD**, that is, how we:

- identity our customers, and **Persons** acting on their behalf
- collect and verify appropriate information about our customers, and
- assess the **ML/TF Risk** associated with providing **Designated Services** to each of our customers' **CRR** and apply Simplified, Standard or **Enhanced CDD** to manage and mitigate those risks.

Compliance with our Privacy Obligations[4]

We comply with our **Privacy Obligations** when undertaking CDD on our customers Privacy Policy, and ensure that:

- we limit our collection of **Personal Information** (including **Sensitive Information**) to what is reasonably necessary to comply with our **AML/CTF Obligations** and as required for our business functions, and
- we do not keep copies of full identification documents such as drivers licences and passports – instead, we keep records of **Personal Information** derived from the identification document which directly relates to our AML/CTF record keeping requirements (***Chapter 6 - Program Maintenance and Review***)

4.2 Initial CDD

We conduct **Initial CDD** before we commence to provide a customer with a **Designated Service**.

In some cases, we are not required to complete **Initial CDD** before providing a customer with a **Designated Service** where our customer is eligible for delayed **Initial CDD**.

CDD Steps

We conduct **Initial CDD** by establishing the following matters (**KYC information**) on reasonable grounds:

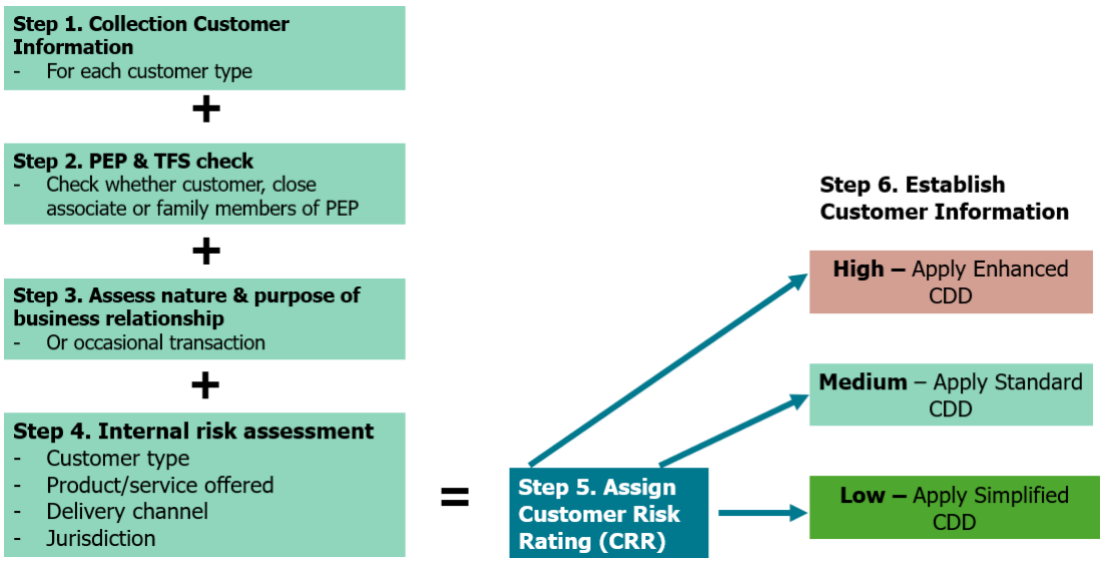
- the identity of our customer
- the identity of any **Person** on whose behalf the customer is receiving a **Designated Service** (such as a beneficiary of a **Trust** or foreign equivalent)
- the identity of any **Person** acting on behalf of the customer, and their authority to act
- if the customer isn't an individual, the identity of any **Beneficial Owners** of the customer

- whether our 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 domestic, international organisation or **Foreign PEP** (or a **Close Associate** or family member of a **PEP**), or is designated for **TFS**
- the nature and purpose of our **Business Relationship** with the customer or of an occasional transaction
- the source of funds and source of wealth of **Foreign PEPs**, high-risk domestic or **International organisation PEPs**
- if we are required to conduct **Enhanced CDD**, the customer's source of funds and source of wealth, if this is relevant to the nature of the customer's **ML/TF Risk**.

If we are unable to establish the above matters on reasonable grounds, we will not provide the customer with a **Designated Service**.

Our **Initial CDD** procedure includes the following steps, which are also summarised in the diagram below:

- collect **KYC Information** from the customer using an onboarding form, using the forms for each customer type set out in our ***AML-CTF KYC Tool (Tool 4A)***. If the customer is an individual, **Beneficial Owner**, or a **Person** acting on behalf of the customer, we take reasonable steps to establish that they are who they claim to be
- identify the customer's **ML/TF Risk** and assign a **CRR**, based on the customer information collected
- determine if the customer is a **PEP** or designated for **TFS**
- determine if we need to apply **Enhanced CDD**, including collecting information on the Customer's source of funds and source of wealth
- determine if we can apply **Simplified CDD**, or use deemed compliance provisions (e.g. for Pre-Commencement Customers or other existing customers
- collect additional **KYC Information** as appropriate to the customer's **CRR**, and to mitigate and manage level of **ML/TF Risk** posed by the customer, and
- verify **KYC Information** using reliable and independent data which is appropriate to the **CRR**, as outlined in our ***AML-CTF KYC Tool (Tool 4A).***



We may be able to complete some of these steps at the same time. For example, the information we collect about the customer's identity and why they are using our **Designated Services** can help us establish their **CRR**.

In some cases, we may need to collect more **KYC Information** than usual to be able to establish a matter on reasonable grounds. For example, where an individual has a common name and personal details, we may need to collect further information to distinguish them from other individuals.

The tool we use to complete initial CDD is our ***AML/CTF KYC Tool (Tool 4A)***

Step 1 – Collect customer information

Different customer types pose different ML/TF Risks. Before we obtain **Personal Information** about the customer (for example, name, date of birth or address), we ensure that the customer has received our privacy statement.

Step 2 – PEP and TFS checks

Identifying PEPs

Our CDD process includes checking whether an individual customer, **Beneficial Owner**, **Person** representing a customer or **Person** on whose behalf the customer is receiving a **Designated Service** is:

- a current or former **PEP**
- is an immediate family member or **Close Associate** of a **PEP** or of a former **PEP**, or
- becomes a **PEP** during the course of our relationship with the customer.

PEPs are individuals entrusted with significant public responsibilities and power and include individuals who have a connection to those that have significant public responsibilities and power. **PEPs** include **Domestic PEPs**, **Foreign PEPs** and **International organisation PEPs**.

A **PEP** may be a target for bribery or corruption, because they hold positions of power or influence or have close associations with such people. For example, a **PEP** may be able to influence any of the following:

- government spending and budgets
- procurement processes, or
- development approvals and grants.

The processes we use to establish if a **Person** is a **PEP** include:

- asking a **Person** if they, a family member or a **Close Associate** is a **PEP** during onboarding and throughout our relationship with the customer
- checking the **Person**'s background on the internet, including sanctions lists and other government lists, and on social media, and
- using databases and reports from **Third Party** providers that specialise in analysing corruption risks.

The following lists can also help us to identify if a **Person** is a **Domestic PEP**:

- **Australian Government Directory** Commonwealth entities and companies, and

- the Department of Foreign Affairs and Trade publishes a list of individuals in senior Australian diplomatic appointments.

We may use a specialist **PEP** database or reports from external third-party providers to identify if a **Person** is a **PEP**.

Former PEPs

When a **Person** leaves their position, they are classified as a former **PEP**, however their status as a former **PEP** can increase the **ML/TF Risk** to our business.

When assessing the **ML/TF Risk** of a former **PEP**, we take into account:

- if the **Person** retains influence over public policy or expenditure decisions, and
- the time that has elapsed since the **Person** was a **PEP**.

Assessing the ML/TF Risk of PEPs

A copy of our **PEP** Risk Assessment is included in our **ML/TF Risk Register**. This includes current and former **PEPs.**

Our **Senior Manager** is responsible for considering and if appropriate, approving the provision of our services to a **Foreign PEP** or high risk domestic or international **PEP**, or where the **Beneficial Owner** of the customer or any **Person** on whose behalf the customer is receiving the service, is or becomes a **Foreign PEP** or high risk domestic or international **PEP** (***Chapter 3 - Personnel and Governance***).

If we identify an individual as a **PEP**, we conduct **Enhanced CDD**, and our **Senior Manager** must approve the commencement and our relationship with the customer.

*Identifying **Persons** designated for TFS*

Sanctions are measures that a government or the United Nations Security Council imposes in response to a situation of international concern. The Department of Foreign Affairs and Trade (DFAT) maintains a Consolidated List of all persons and entities designated for **TFS** under Australian sanctions laws.

If we identify a client as High Risk, we use DFAT's Consolidated List to search for all persons and entities designated for **TFS** under Australian sanctions laws OR We engage an external service provider to conduct electronic screening checks against a comprehensive database of global sanctions laws, to determine whether an individual is designated for **TFS**.

We may also ask the Australian Federal Police for help to determine if an asset is owned or controlled by a designated **Person** or entity.

We are prohibited from dealing with assets owned or controlled by a **Person** designated for **TFS** and are also prohibited from making assets available to them.

If a **Person** is designated for **TFS**, the assets they own or **Control** are frozen. This means we cannot deal with their assets without a sanctions permit. We do not make any assets available to them or allow or facilitate others to make assets available to them, without a sanctions permit.

It may not be appropriate to continue our **Business Relationship** with the customer. We do not return to the customer any assets we hold without a sanctions permit.

If we are, or think we may be holding an asset that is frozen, we will:

- contact the Australian Sanctions Office,(**ASO**) and
- report this to the Australian Federal Police as soon as practicable.

If we suspect on reasonable grounds that we have information relevant to a contravention of Australia's sanctions laws, we submit an SMR with **AUSTRAC**.

Step 3 – Assess nature and purpose of the Business Relationship or occasional transaction

Our **Initial CDD** includes establishing the nature and purpose of our **Business Relationship** or occasional transaction.

Sometimes the nature of the **Business Relationship** or transaction will be evident from the transaction itself and from our normal interactions with our customers. Other times we may need to ask our customer questions to understand the nature of our relationship.

Information that might be relevant includes:

- what they will be using our **Designated Services** for
- their expected transaction frequency and volume
- how they plan to have our **Designated Services** delivered to them, such as online or face-to-face
- whether they will use our **Designated Services** for business or personal transactions
- nature and details of an individual's occupation and employment
- the individual's date of birth (for example, is the customer a child or likely to be a retiree)
- record of changes of address
- the nature of the relationships between a customer and the **Person** acting for them
- the source of the customer's wealth and funds for the **Designated Service**.

In accordance with our record keeping obligations in ***Chapter 6 - Program Maintenance and Review***, we keep records on how we establish if a **Person** is a **PEP** for each of our customers. We also record any high-risk customers, such as **Foreign PEPs**, in ***High Risk Customer and ECDD Register (Tool 4B)***.

Step 4 – Internal Risk Assessment

Once we understand who the customer is and the nature and purpose of the relationship, we review and assess any additional risks that have been identified in our overall **ML/TF Risk Assessment** that are specifically relevant to this customer ***(refer to our ML/TF Risk Register (Tool 2B).*** These risks are based on:

- customer type
- delivery channel
- product/ services, and
- jurisdiction.

We also identify any red flags that may be relevant to the customer. These red flags are based on the criteria above, together with flags that have been specifically identified by **AUSTRAC**.

Step 5 – Assign Customer Risk Rating (CRR)

Each risk in our **ML/TF Risk Register** has been assigned a risk indicator of low, medium or high.

Once we have collected the information in Steps 1-4, we assign an overall initial **CRR** to each customer of low, medium or high.

We apply the following methodology to achieve the **CRR**.

Initial assessment	**Overall CRR**	**Type of CDD to implement**
One or more high risk indicators	High	**Enhanced CDD**
At least 3 medium risk indicators	High	**Enhanced CDD**
A maximum of 2 medium risk indicators	Medium	Standard CDD
No identified risk indicators, or only low risk indicators	Low	**Simplified CDD**

We do this using our ***AML/CTF KYC Assessment Tool (Tool 4A)*** or using an external service provider.

Step 6 - Establish customer information

Once we have assigned a **CRR** of low, medium or high to a customer, we collect the appropriate **KYC Information** for that risk level and establish, on reasonable grounds, the identity of the customer. We have determined that it is appropriate to verify:

- more information collected from a medium and high risk customer than from a low risk customer
- more information about **Persons** associated with a high risk customer (such as a **Beneficial Owner**) than those associated with a low risk customer
- information through additional sources, such as through a **Document Verification Service (DVS),** if we are concerned a document might not be legitimate, and
- the source of a customer's funds, or the recipient of a transaction to help us establish the nature and purpose of a transaction.

Reasonable grounds

Reasonable grounds is an objective standard, meaning that a reasonable person in our position would consider that a matter is established for the purpose of **Initial CDD**, based on the facts, circumstances and information that we know or could reasonably be expected to have known at the time.

A reasonable person is a legal term and describes a hypothetical person who displays reasonable or ordinary behaviour or judgment in the circumstances. Those circumstances include where the reasonable person had:

- reviewed the same material, and
- similar knowledge, experience or training.

Once we have collected **KYC Information** to identify the customer, we take steps to verify this information. We do this by one or both of two methods:

- traditional or document-based verification, or
- online or electronic verification.

If by using online verification we cannot verify the identity of the customer, we use the traditional or document-based processes, or a combination of both.

In accordance with our record keeping obligations in ***Chapter 6 - Program Maintenance and Review***, we keep records on how we establish each matter on reasonable grounds, when conducting CDD on each of our customers.

Traditional or document-based verification of KYC information

We review reliable and independent documents from the customer and other sources as set out in the ***AML-CTF KYC Tool (Tool 4A)***.

We sight the original documents and record the details of the **Personal Information** derived from the identification document, as required for each customer type in the ***AML-CTF KYC Tool (Tool 4A)***.

Online or electronic verification of KYC information

We verify the **KYC Information** we collect about our customers and other **Persons** against independent and reliable data. We consider that data is reliable and independent if it is provided by:

- an Australian government body
- a foreign government, where the document is an official document such as a passport, or
- a well-known and established Australian company.

Electronic verification service provider

We have appointed, or may in the future appoint external service providers who conduct electronic verification services on our customers. Our **Senior Manager** is responsible for considering and if appropriate, approving the appointment of an external service provider (Refer to ***Chapter 3 – Personnel and Governance*** for details on Outsourcing).

In appointing an external service provider, we recognise that we retain responsibility for our statutory responsibilities under the **AML/CTF Act**, including ensuring that the identities of our customers are verified, and that suspicious matters are reported.

At the time of appointing the external service provider, we assess whether the external service provider has the appropriate knowledge of our business and our industry sector, as well as the service provider's prior experience in providing the services. Our procedure for appointing an external service provider is set out in ***External Service Provider Appointment Assessment Template (Tool 3J).***

We also consider whether the data used by the external service provider is reliable and independent by considering:

- how accurate the data is

- how comprehensive the data is, such as the range of persons or information included in the data and when the time period the data was collected
- how the data is kept up to date
- who is responsible for maintaining the data, such as a government body
- the sources the electronic verification service uses to verify the data, and
- whether the system is secure and kept up to date.

To complete this assessment, we use our ***External Service Provider Appointment Assessment Template (Tool 3J)***.

After we have appointed an external service provider, we undertake pro-active monitoring and testing of the AML/CTF systems and processes provided by the service provider during the period of the appointment. Our procedure for maintaining ongoing oversight of the services provided by an external service provider is set out in our ***External Service Provider Ongoing Assessment Template (Tool 3K).***

Our **Senior Manager** ensures that the integrity of the online verification data is tested at least annually by using different authentication methods on a sample of customer files.

Inconsistencies or discrepancies in KYC information

If we find inconsistencies or discrepancies in the **KYC Information**, we:

- identify and document the reason for the inconsistency
- ask the customer to explain the discrepancies, such as differences in name spelling or address history, and requesting supporting evidence if appropriate
- review the reason for the inconsistency, such as if there is a minor administrative error or a potential indicator of **ML/TF Risk** like the use of fraudulent documents
- re-assess the **CRR** and as appropriate, implement Ongoing and **Enhanced CDD**, and
- re- verify the information with independent and reliable third parties or contacting issuing authorities to confirm the validity of documents or to request certified copies.

If we cannot verify a **Person's** identity because of inconsistent information, and reasonably suspect that the **Person** is not who they say they are, we will not provide our **Designated Services** to the customer and must lodge an **SMR** (***Chapter 5 - AUSTRAC Enrolment, Registration and Reporting***).

4.3 Simplified CDD during Initial CDD

Simplified CDD refers to the reduced customer identification and verification processes, which we apply when:

- the **CRR** is low, based on **KYC Information** we have collected about the customer
- we are not required to conduct **Enhanced CDD**
- we follow our processes for applying **Simplified CDD**

- if the customer is an individual – we have taken reasonable steps to establish that the customer is the **Person** they claim to be
- if we have established on reasonable grounds that the customer is or is controlled by:
    a. a government body
    b. an entity that is subject to oversight by a prudential, insurance, or investor protection regulator through registration or licensing requirements, or
    c. a corporation or association of homeowners in a strata title or community title scheme.

If the above conditions apply, and there are no reasonable grounds for us to doubt the adequacy or veracity of the **KYC Information**, we are not required to verify (and will be taken to have established, on reasonable grounds) the identity of:

- any **Person** on whose behalf the customer is receiving the **Designated Service**
- any **Person** acting on behalf of the customer and their authority to act
- any **Beneficial Owners** of the customer (if the customer is not an individual)

If we apply **Simplified CDD**, we are not exempt from our **Initial CDD** obligations.

We remain required to collect and verify **KYC Information** that is sufficient to:

- assign a **CRR** to the customer and
- establish certain matters on reasonable grounds.

4.4 Delaying Initial CDD

We may be able to start providing a **Designated Service** to a customer before we complete **Initial CDD**, provided the **Designated Service** is provided at or through a permanent establishment in Australia and it would disrupt the ordinary course of business.

The parts of **Initial CDD** that we can delay (and how long we can delay them for) are different in each of the above situations, as set out under the subheadings in this section.

In all the above circumstances, before we start providing the **Designated Service**, we demonstrate on reasonable grounds that both:

- it is essential to delay **Initial CDD** to avoid interrupting the 'ordinary course of business' (explained under the following subheading), and
- there is a low **ML/TF Risk** associated with delaying **Initial CDD**.

For each of the above circumstances, we have determined that there is a low **ML/TF Risk** associated with delaying **Initial CDD** if the customer is assessed as posing a low **ML/TF Risk**.

We do not delay parts of **Initial CDD** where:

- we are unlikely to later be able to collect information from the customer that we need for **Initial CDD**, or
- the customer could exploit our service for **ML/TF** or other illegal activity, before we establish their identity on reasonable grounds

When we delay **Initial CDD**, we:

- complete **Initial CDD** as soon as reasonably practicable (taking reasonable steps to do so at the earliest possible time) after starting to provide the **Designated Service** to the customer, and no later than the timeframes set out in each of situations below, and
- mitigate and manage any associated risks of delaying **Initial CDD**.
- Our procedures to mitigate and manage the risk of delaying **Initial CDD** include :
- if, once we have completed **Initial CDD** after starting to provide the **Designated Service**, the customer asks us to return funds transferred to us, we avoid converting or otherwise legitimising funds that may otherwise have been illegitimate, such as by avoiding a payment of cash or a bank cheque, and instead only returning electronic deposits to the same originating bank account, or
- if the customer tries to prove their identity with other service providers by demonstrating that we are providing **Designated Services** to them, we withhold our correspondence or statements that would otherwise be issued to the customer, or clearly mark it as relating to an unverified account. Interrupting the ordinary course of our business

We do not delay **Initial CDD** because it would be inconvenient for us or the customer to complete **Initial CDD** before we provide them with a **Designated Service**.

It may be essential for us to delay **Initial CDD** to avoid an interruption to the ordinary course of our business where:

- allowing a customer to open an account remotely or online (but not allowing any transactions on the account), where we can't immediately verify their identity at the time using electronic data
- for customers in an emergency, such as family and domestic violence or natural disasters who don't have access to identity documents, or
- time-critical services where for commercial reasons we need to lock in an exchange rate, interest rate or other rapidly fluctuating aspect of the service on the day the customer requested the **Designated Service**.

Designated Services provided in Australia

We may delay verifying some **KYC Information** as part of **Initial CDD** if we are providing a **Designated Service** at or through a permanent establishment in Australia.

If we delay verification, we complete **Initial CDD** on the customer before we:

- transfer, or allow or facilitate the transfer of money, property or virtual assets for or on behalf of the customer or
- otherwise make money, property or virtual assets available to the customer (other than holding it in an account or on deposit from the customer).

In these circumstances, we can start providing a **Designated Service** after we have collected but not before we verify the **KYC Information** about:

- the identity of any **Person** on whose behalf the customer is receiving the **Designated Service**
- the identity of any **Beneficial Owners** of the customer
- whether the customer, any **Beneficial Owners**, 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 **Person** designated for **TFS**, and
- the nature and purpose of the **Business Relationship** or occasional transaction (where **Enhanced CDD** applies).

If we delay **Initial CDD** in these circumstances, we verify the **KYC Information**, including confirming if the customer is a **PEP** or designated for **TFS**, as soon as reasonably practicable and within 20 business days of starting to provide the customer with the **Designated Service**.

Certain financial market transactions that must occur rapidly

We may start providing a **Designated Service** to a customer before we complete **Initial CDD** if all the following apply:

- the **Designated Service** is acquiring or disposing of a security, derivative or foreign exchange contract on a declared financial market (within the meaning of the *Corporations Act 2001*)
- the **Designated Service** is provided at or through our permanent establishment in Australia, and
- this must occur quickly because of financial market conditions relevant to the transaction.

However, the service must not involve the acquisition of an interest in a managed investment scheme to which section 1019B of the Corporations Act 2001 applies.

We will not do any of the following:

- accept physical currency or virtual assets to fund the **Designated Service**
- permit the customer to transfer, or otherwise part with, proceeds from a disposal of an asset to which the **Designated Service** relates
- resell, transfer, or otherwise part with an asset related to the **Designated Service** that has been acquired on the customer's behalf, or
- allow the customer to be recredited with or obtain a refund of the purchase price.

If we delay **Initial CDD** in these circumstances, we complete **Initial CDD** as soon as reasonably practicable, and within 5 business days of starting to provide the customer with the **Designated Service**.

4.5 Identifying individuals who do not have standard identification documents

When providing **Designated Services** to customers and complying with our CDD obligations, we:

- apply a flexible, sensitive and compassionate approach to support individuals
- consider the barriers individuals may face obtaining and providing identification
- have designed procedures that balance meeting the needs of these individuals with meeting our CDD obligations, and
- provide tailored training to staff to ensure they are aware of and are able to implement the alternative identification procedures, exercising discretion as needed.

When we conduct CDD on individuals, some individuals may:

- experience barriers obtaining standard identification, which may be ongoing, temporary or because of their situation
- be unable to access standard identification because of circumstances outside their control

- have inconsistent personal details across identification documents, such as their name or date of birth.

Where we are required to conduct CDD on individuals who do not have standard identification documents, we complete ***Identification of individuals without standard identification documents Form* (*Tool 4C)***. A list of individuals who may not have standard identification documents is included in this form.

We have considered, mitigated and managed the additional risk posed by an individual who cannot provide standard identification information in our ***ML/TF Risk Register (Tool 2B)***.

We may use additional data sources to proactively identify communities and locations where individuals are more likely to need a flexible approach.

4.6 Reliance on CDD conducted by a third party

There may be instances where we provide our customer with a **Designated Service**, whilst at the same time, our customer is receiving a **Designated Service** from another **Reporting Entity**. For example, this may occur where our customer holds accounts with multiple **Financial Institutions** or is receiving services from both a financial adviser and an investment platform.

In order to minimise inconvenience to our customers, rather than requiring our customers to provide us with the CDD information which has already been provided to another **Reporting Entity**, we may rely on the CDD checks conducted by the **Third Party** on our customer, who is either a:

- **Reporting Entity**, or
- **Person** regulated under laws in a foreign country that give effect to **FATF** recommendations relating to CDD and record keeping.

This type of reliance arrangement is referred to in the **AML/CTF Act** as a **CDD Arrangement**, and may be entered into:

- under an ongoing agreement or arrangement, or
- on a case-by-case basis.

When disclosing our customers' **Personal Information** to the **Third Party**, we ensure that we comply with our **Privacy Obligations** and also ensure that the **Third Party** has policies and procedures in place which ensure that they comply with their **Privacy Obligations**.

Entering into a CDD Arrangement

We ensure that when we enter into a **CDD Arrangement**, it is appropriate to the **ML/TF Risks** we may reasonably face in providing our **Designated Services** (**CDD Risk Assessment**).

As set out in ***CDD Arrangement: Appointment and Ongoing Monitoring Procedure (Tool 4D)***, when appointing the **Third Party**, we require the **Third Party** to provide us with the documents and information about their AML/CTF systems and controls (including their record keeping procedures), as well as independent evaluation reports, adverse media reports and any regulator action which relates to the **Third Party**.

We then assess the **ML/TF Risk** associated with relying on the CDD checks conducted by the **Third Party** using the procedure set out in ***CDD Arrangement - CDD Risk Assessment (Tool 4E)***, taking into account:

- nature, size and complexity of the third party's business
- products and services the **Third Party** provides
- delivery channels the **Third Party** uses to provide services
- kinds of customers they provide services to, and
- countries where they operate or are a resident.

As part of the **CDD Risk Assessment**, we consider whether the **Third Party**:

- has appropriate measures in place to comply with its **AML/CTF Obligations**, and
- implements these measures in practice.

Documenting CDD Arrangements

Our **CDD Arrangement** is documented in a written **CDD Agreement**, which sets out the responsibilities of each party, including:

- the nature of the **CDD Procedures** to be conducted by the **Third Party**
- the third party's obligation to provide us with all the **KYC Information** it has collected before we begin to provide a **Designated Service**
- how records of the **CDD Procedures** are kept, and the manner and time frames within which we can access those records (including records of the independent and reliable data the other party used to verify the customer's **KYC Information**)

If customers can rapidly conduct several higher-risk transactions, it may be appropriate for information to be available:

- immediately (such as under IT systems permitting real-time access)
- within minutes of a request.

We ensure that all **CDD Agreements** are reviewed and approved by the **Senior Manager**.

Assessment of CDD Arrangement

As outlined in ***CDD Arrangement: Appointment and Ongoing Monitoring Procedure (Tool 4D)***, we:

- conduct regular assessments of the **CDD Arrangement** (**CDD Risk Assessment**), and
- prepare a written record within 10 business days after the day we complete each **CDD Risk Assessment**.

We conduct our own **Initial CDD** on a customer if, after completing an assessment, we are not satisfied that the agreement or arrangement complies with the **AML/CTF Rules**.

We conduct **CDD Risk Assessments**:

- at least every 2 years or more regularly as appropriate, considering our **ML/TF Risk**, and
- if there's a significant change in circumstances that may affect whether the **CDD Arrangement** meets the requirements of the **AML/CTF Legislation**.

Information which may indicate a significant change to the **CDD Risk Assessment** include:

- publication of adverse regulatory findings against the **Third Party**
- adverse media searches
- any significant changes to the third party's **ML/TF Risk** profile
- the outcomes of a recent **Independent Evaluation** of the third party's **AML/CTF Program**
- failure to complete remedial action on CDD issues
- open-source information indicating a significant change in the domestic **ML/TF** or other **Serious Crime** environment in the country where the **Third Party** is based, and
- changes in ownership or **Control** of the **Third Party** that may affect its risk profile (for example, whether the **Person** representing the **Third Party** or a **Beneficial Owner** is a **Foreign PEP** or is designated for **TFS**).

In accordance with our record keeping obligations in ***Chapter 6 - Program Maintenance and Review***, we keep records of the **CDD Arrangement** with each **Third Party**, as well as the **CDD Risk Assessment Materials** and the **CDD Risk Assessments**.

Entering into a CDD Arrangement with a third party in a foreign country

If we intend to enter into a **CDD Arrangement** with a **Third Party** that is located overseas and is not a **Reporting Entity** under the **AML/CTF Act**:

- the **Third Party** must be regulated under laws in a foreign country that give effect to the **FATF** recommendations relating to CDD and record keeping (equivalent obligations), and
- we consider the country where the **Third Party** operates or is a resident, and assess the risk level associated with the country, using the procedure set out in ***Jurisdiction Risk Data (Tool 2C)***.

As we review the risk rating of each jurisdiction annually, this enables us to identify any changes in the country profile using the data sources outlined in the above Tool, which include:

- **Basel Institute on Governance**: Basel AML Index Scores
- List of **FATF** member countries
- UN Security Council and Australian Government Sanctions lists
- **FATF** list of deficient jurisdictions
- EU list of non-co-operative tax jurisdictions.

4.7 Enhanced Customer Due Diligence (Enhanced CDD)

We implement **Enhanced CDD** measures in order to understand the **ML/TF Risk** posed by our customers, and to assist us to appropriately manage and mitigate those risks.

We conduct **Enhanced CDD** on:

- our customer
- any **Beneficial Owner** of the customer
- any **Person** on whose behalf the customer is receiving the **Designated Service**, such as a beneficiary of a **Trust** or foreign equivalent
- any **Person** acting on behalf of the customer,

in the following circumstances:

- if the customer's **CRR** is high as assessed during **Initial CDD** or increases to high while undertaking **Ongoing CDD**
- we are required to submit a **SMR** in relation to the customer, and we intend to continue to provide a **Designated Service** to the customer.
- if a customer requests a designated service in circumstances:
    - where the service does not have a clear economic or legal purpose
    - it involves unusually complex or large transactions
    - it involves an unusual pattern of transactions
- if an individual associated with a customer is a **Foreign PEP**, or a high risk domestic or **International organisation PEP**
- if an individual is physically present in, or formed in, a high-risk jurisdiction (refer to ***2C Jurisdiction Risk Data***), which includes jurisdictions that the **FATF** has called for **Enhanced CDD** to be applied.

We maintain a list of our high risk customers and document the **Enhanced CDD** triggers and measures that we have implemented for each high risk customer in our ***High Risk Customer and ECDD Register (Tool 4B)***.

The Adviser completes the **Enhanced CDD** Form in the ECDD Form Tab 2 of our ***High Risk Customer and ECDD Register (Tool 4B)*** to record the **Enhanced CDD** triggers and measures implemented each time we conduct **Enhanced CDD**.

Our **Senior Manager** reviews each completed **Enhanced CDD** Form, including the recommendations for next steps.

Enhanced CDD measures

We determine which of the **Enhanced CDD** measures listed in this section (and set out in the **Enhanced CDD** Form in Tab of ***High Risk Customer and ECDD Register (Tool 4B)*** are to be applied to the customer, depending on which **Enhanced CDD** trigger is present, including the reason why the **CRR** is high, and taking into account the measures required to manage and mitigate that **ML/TF Risk**.

When an **Enhanced CDD** red flag is triggered, we apply one or more of the following **Enhanced CDD** measures:

- collect and/or verify more **KYC Information** about the customer
- obtain the reason for certain transactions or services
- collect and/or verify information about the customer or **Beneficial Owner's** source of funds or source of wealth (see below)
- take additional measures to better understand the background, ownership (if relevant) and financial situation of the customer, and other parties to the transaction
- conduct more in-depth customer monitoring and analysis of transactions and behaviours.
- increase the frequency of reviews of the **Business Relationship**, to assess whether the customer's risk has changed and whether the risk remains manageable
- update the customer's **KYC Information** more frequently than we would for other customers.

Our ***AML-CTF KYC Tool (Tool 4A)*** sets out examples of additional **KYC Information** we may collect and verify about our high risk customers.

When carrying out **Enhanced CDD**, we take active steps to manage and mitigate any **ML/TF Risks**, and where appropriate elect not to provide a **Designated Service** where this falls outside our business's risk appetite.

After completing **Enhanced CDD**, we may urgently escalate the matter for further decision by our **Senior Manager** in accordance with our **AML/CTF Policies**. This is an important way of making sure our **Senior Manager**:

- maintain oversight of our business's **ML/TF Risks**, and
- determine whether any changes are required to the **AML/CTF Program** or **ML/TF Risk Assessment**.

Additional KYC information

We collect additional **KYC Information** when undertaking **Enhanced CDD** in order to:

- 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** (**CRR**)
- 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, for the purpose of managing and mitigating our **ML/TF Risk**.

We verify additional **KYC Information** during **Enhanced CDD** in order to establish the accuracy of the **KYC Information** collected and verified during **Initial CDD**. We may also re-verify **KYC Information** using different sources.

For example, 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 **CRR** 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.

Responding to Enhanced CDD findings

As noted above, we document the **Enhanced CDD** triggers which arise in our business and also document the **Enhanced CDD** measures that we have implemented in each instance in our ***High Risk Customer and ECDD Register (Tool 4B)***.

The Senior Manager completes the **Enhanced CDD** Form Tab 2 of our ***High Risk Customer and ECDD Register (Tool 4B)*** to record the **Enhanced CDD** triggers and measures implemented each time we conduct **Enhanced CDD**.

The **Enhanced CDD** Form also sets out the next steps for the customer how we respond to the **Enhanced CDD** findings, and includes each of the following options:

- urgently escalate the matter to the **Senior Manager** or The Compliance Committee.
- implement the **SMR** assessment procedure (***Chapter 5 - AUSTRAC Enrolment, Registration and Reporting)***
- implement additional monitoring
- considering whether to continue or terminate the customer relationship
- diarise the next **Enhanced CDD** review to be conducted before before the end of the next quarter

In some situations, as determined by the **Senior Manager**, we may continue to provide **Designated Services** to customers requiring **Enhanced CDD**.

In accordance with our record keeping obligations in ***Chapter 6 - Program Maintenance and Review***, we keep records to document the **Enhanced CDD** measures we apply to a customer.

4.8 Source of funds and source of wealth

We conduct source of funds and source of wealth checks:

- as part of Enhanced CDD
- where a customer is a Foreign PEP, or a high ML/TF Risk domestic or International organisation PEP
- has transaction activity or behaviour which does not align with the information we collected
- has funds or wealth which come from sources that are less common or may be more open to criminal exploitation

The steps we take to establish a customer's source of funds and source of wealth are:

- proportionate to the customer's CRR
- effective at managing and mitigating the ML/TF Risk

- appropriate to the duration of the risk.

When establishing the customer's source of funds and source of wealth, we implement one or more of the following procedures:

- review information we already hold about the customer, such as information obtained in our onboarding process
- collect, where appropriate, additional information to identify how the customer obtained the funds for the **Designated Service** or accumulated their wealth
- verify, where appropriate, any of the information using reliable and independent sources.

We collect information in order to establish, on reasonable grounds, a high **ML/TF Risk** customer's source of funds and source of wealth, including in the following situations:

- customers involved with high-risk jurisdictions (refer *to **Jurisdiction Risk Data (Tool 2C***))
- use of shell companies or complex **Trust** or corporate structures that have obfuscated 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 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 (including high risk jurisdictions)
- there are inconsistencies between the information the customer provided and other information available to you related to their income or wealth
- adverse media reporting or other reliable information about the customer's business or commercial activities, and
- there has been a material change in the customer's financial circumstances or position.

When collecting and verifying this information, we aim to establish if:

- there is a legitimate source for the customer's funds or wealth, and
- whether the customer's funds or wealth could be sourced from unlawful activity.

We consider the information we obtain from independent sources and assess whether it is consistent with the customer's explanation or raises further questions.

If an explanation is consistent with the customer's risk profile and we don't have other concerns about the transaction, we document the explanation and monitor the customer to confirm that future activity is consistent with the explanation provided.

Questions we consider when establishing the source of funds and source of wealth

When collecting and verifying information about a customer's source of funds and source of wealth, we consider the following questions:

- Why and how does the customer have the amount of assets they do?

- Can we easily explain the customer's source of wealth or source of funds, such as through their occupation, inheritance or investments?
- Is there a reasonable explanation for the customer to conduct this transaction or request this **Designated Service**, particularly if it involves the use of cash?
- Are there any indicators that the customer derived their funds or wealth from the proceeds of crime?
- Is the customer's background consistent with what we know about their former, current or planned business activity, their business' turnover (if applicable), the source of funds and source of wealth?
- Are we able to confirm that the information and documentation obtained as part of the source of funds and source of wealth checks are consistent with what we know about the customer from our due diligence, including open-source checks?

Collecting and verifying information on source of funds and source of wealth

When establishing the source of funds and source of wealth of a customer we:

- use information we collect and establish on reasonable grounds during **Initial CDD**
- use information we collected about or from the customer for other purposes, e.g., when we provide another service (whether or not it is a **Designated Service**)
- request that the customer make a formal declaration about their source of funds or source of wealth, or
- use secondary sources – such as internet searches, media reporting, published lists of prominent persons, commercial databases.

When verifying the source of funds, we:

- confirm where those funds came from
- how the customer obtained them,
- if this is consistent with what we expect of the customer.

We may use evidence to verify the customer's source of wealth to verify the source of funds, when we have questions about the information provided.

Verifying a customer's source of wealth can be more challenging, as their wealth may include funds or assets that we do not hold on behalf of the customer.

We consider the source and type of evidence we collect and determine if it's sufficient to support the information the customer has provided about their source of wealth.

Customers using cash for transactions

Where a customer can't or won't produce any documentation to verify where the funds came from, we also consider if:

- the transaction or behaviour is consistent with what we know about the customer, and
- we have information that suggests the funds could be proceeds of criminal activity.

If the customer's funds or wealth don't align with what we know about the customer and don't have a clear explanation, we:

- review the **CRR**, and
- submit an **SMR** to **AUSTRAC** (see ***Chapter 5 - AUSTRAC Compliance and Reporting***).

Documents and data to verify the source of funds and source of wealth

Examples of documents and data we use to identify the source of funds or source of wealth may include:

- bank statements
- payslips
- tax returns
- a probated will
- court order (such as a divorce settlement)
- loan agreements
- 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
- gambling winnings
- property or land registers
- business and company registers
- audited financial accounts or statements
- written confirmation from a legal practitioner or accountant, and
- formal and witnessed declarations (using a statutory declaration in the absence of any other supporting information).

Responding to a customer behaviour or transaction monitoring red flag

When we detect a red flag, we:

- review and, if appropriate, update our assessment of the customer's **ML/TF Risk** (**CRR**)
- review and, if appropriate, update and re-verify the **KYC** information relating to the *c*ustomer
- review whether the customer has become a **PEP** or has ceased to be a **PEP** since the commencement of the relationship

- determine whether there is a legitimate explanation for the red flag
- decide whether to conduct **Enhanced CDD**, and
- decide whether to implement the **SMR** assessment procedure.

4.9 Transitioning existing customers

Other existing customers – Initial CDD

We do not need to conduct **Initial CDD** on a customer if, before 31 March 2026, we conducted the then applicable customer identification procedure (**ACIP**), on:

- a customer, or
- the trustee of a customer.

Customer is a transferred pre-commencement customer

We do not need to conduct **Initial CDD** on a customer where:

- we have taken over all or part of another Reporting Entity's business, or
- all or part of another Reporting Entity's assets and liabilities have become ours because of a voluntary or compulsory transfer, and
- we have received copies of all Initial and **Ongoing CDD** records, as well as transaction records for the **Designated Services** for the customer.

If we do not have all records required for CDD and transactions for the customer as required under the AML/CTF regime, we conduct **Initial CDD** before we provide a **Designated Service** to the customer.

We also conduct **Initial CDD** for a customer before we provide a **Designated Service** if any of the following circumstances occur:

- any unusual transactions or behaviours that may give rise to an **SMR** obligation, or
- there is a significant change in the nature and purpose of the **Business Relationship**, which results in the **CRR** being medium or high.

4.10 References

Related policies and tools

Policies	Chapter 2 **ML/TF Risk Assessment** Chapter 5 **AUSTRAC** Enrolment, Registration and Reporting Chapter 6 Program Maintenance and Review

Tools	4A. AML/CTF **KYC** Tool 4B. High Risk Customer and ECDD Register 4C. Identification of individuals without standard identification documents Form 4D. **CDD Arrangement** Appointment and Ongoing Monitoring 4E. **CDD Arrangement** – **CDD Risk Assessment**

Legislative requirements and references

Law	**AML/CTF Act**
Regulations	AML/CTF Regulations
Regulatory guidance	**AUSTRAC** Guidance: Customer due diligence (Reform)

5. AUSTRAC Enrolment and Reporting

5.1 Introduction and scope

This Policy outlines our obligations and procedures to ensure that we comply with our **AML/CTF Obligations** to:

- enrol with **AUSTRAC** as a **Reporting Entity**, and ensure our enrolment information is current at all times
- report certain matters to **AUSTRAC**.

5.2 AUSTRAC Enrolment Policy

As a business that provides **Designated Services** and has as a geographical link to Australia, we have enrolled with **AUSTRAC** as a **Reporting Entity**.

The information we have provided to **AUSTRAC** is recorded in ***AUSTRAC Enrolment Information (Tool 5A)*** and includes:

- general information about our business, including its legal form
- **AUSTRAC** contact person details
- information about our **Designated Services**, and
- if we are part of a **Reporting Group**.

We ensure that all information provided as part of our enrolment is true and correct.

The Responsible Manager is responsible for lodging our enrolment through **AUSTRAC Online** within 28 days of our **Reporting Entity** first providing a **Designated Service**.

Changes in enrolment details

Once enrolled, we keep our enrolment information current, including information about the **Designated Services** we provide or intend to provide.

Any changes to the information in ***AUSTRAC Enrolment Information (Tool 5A)*** are notified to **AUSTRAC** within 14 days of the change occurring by The Responsible Manager using **AUSTRAC Online**.

If we cease providing Designated Services

If our business ceases to provide **Designated Services**, we will submit a request to **AUSTRAC** to be removed from the **Reporting Entities Roll** and provide the following information:

- name of the person submitting the request
- the date which we ceased providing **Designated Services**

- if we intend to provide **Designated Services** in the financial year following our request to be removed from the **Reporting Entities Roll**, and
- if we, as a business, have any outstanding obligations to report on the following matters, and if so, the information on the outstanding obligations:

5.3 AUSTRAC Reporting Obligations - Overview

As a **Reporting Entity**, we report the following matters to **AUSTRAC**, including:

- Suspicious Matters, and
- Notices and requests for information or documents regarding AML/CTF reports.

The purpose of our **AUSTRAC** reporting obligations is to help **AUSTRAC** detect and disrupt criminal and terrorist activities, so we ensure that our reports are accurate and submitted on time. **AUSTRAC** uses the information we report to:

- find patterns of criminal or terrorist activity, and risks to national security, and
- help its partners in Australia and overseas to investigate and fight crime.

5.4 Suspicious Matter Reports (SMRs)

The steps we follow for our **SMRs** are as follows:

1. identify and escalate potential suspicious matters
2. assess and determine whether we have 'reasonable grounds for suspicion', and
3. where required, submit an **SMR** within the required timeframes.

Step 1 – Identify and escalate potential suspicious matters

Personnel training

In accordance with ***Chapter 3 - Personnel and Governance***, we train our **Personnel** as appropriate, to monitor for and identify potential suspicious matters, and to follow our escalation, assessment and reporting processes, as set out in this policy.

What is a suspicious matter?

The obligation to report a **Suspicious Matter** arises where:

- either:
  - we provide, or propose to provide, one of our **Designated Services** to a **Person**, or
  - a **Person** asks us to provide one of our **Designated Services** to them, or enquires whether we can provide one of our **Designated Services** to them, and
- we form a suspicion on reasonable grounds that:

- the **Person**, or their agent, is not the **Person** they claim to be
- information we have may be relevant to the investigation, prosecution or other enforcement action related to a contravention of a law of the Commonwealth, State or Territory, including tax evasion, **ML**, terrorism financing, proliferation financing, or any other **Serious Crime**, or
- our provision, or potential provision, of **Designated Services** is preparatory to **ML** or **TF**.

Monitor for suspicious activity

Where we provide, or a **Person** makes enquiries about whether we can provide, a **Designated Service** to a customer, we monitor for information that may indicate potential suspicious activity. Our processes for doing so are set out in ***Chapter 4 Customer Due Diligence*.**

Indicators of suspicious activity

The following are common indicators of suspicious activity, which fall into three broad categories. The presence of one indicator alone may not provide reasonable grounds to suspect an offence is being committed, rather multiple indicators may be required depending on the circumstances.

1. Suspicious customer behaviour includes but is not limited to:

- requests to be anonymous
- appearing to be acting under the direction of a third party
- appearing nervous, overly defensive, in doubt or evasive when asked for further information
- refusing to provide reasons for requesting a **Designated Service**, or provides vague information, or
- enquiring about whether we report to Federal, State or Territory government bodies such as **AUSTRAC**, the **ATO**, Services Australia or law enforcement agencies (e.g. police).

2. Suspicious customer identification includes but is not limited to:

- customer is identified in adverse media as being the subject of law enforcement enquiries
- documents appear to be forged or tampered with
- information on identification documents differ from payment information provided by the customer
- customer displays a pattern of name variations or uses aliases from one transaction to another
- customer refuses, or is reluctant, to provide the identification information required, or
- any party to a transaction appears on a sanctions list.

3. Suspicious (including unusual or complex) transactions includes but is not limited to:

- transactions that are unusually large for the customer
- transaction activity that does not appear to be consistent with the customer's profile
- requests for transactions with higher-risk countries and jurisdictions
- sudden changes in the nature or frequency of transactions for the customer
- transactions conducted in an overly complex way for no apparent purpose

- rapid domestic transfers between third parties that do not appear to have a legitimate purpose
- 'U-turn' transactions where funds are transferred out of Australia and a portion of the funds returned to Australia
- reporting structuring', whereby larger transactions are split into a number of smaller transactions under the **TTR** threshold of AUD$10,000, with no apparent purpose other than to avoid reaching that threshold, or
- purchases and sales of high-value goods and assets that are inconsistent with our information about the source of the customer's funds and wealth, such as bullion, luxury goods and investments.

A comprehensive list of indicators of suspicious activity specific to our business are documented in our ***ML/TF Risk Register (Tool 2B***) (refer to Red Flags column on ML TF Risk Assessment tab and the Additional Red Flags Tab).

Escalate suspicious activity

To comply with our **SMR** obligations:

- all **Personnel** are required to monitor for suspicious activity
- if any **Personnel** are unsure whether information may be indicative of suspicious activity, they will promptly inform, and discuss it with, their direct manager.
- if any **Personnel** becomes aware of suspicious activity, they will promptly inform The Senior Manager, initially orally, and then in writing via our ***Suspicious Activity Report (Tool 5C)***, and
- if the Senior Manager becomes aware of suspicious activity, including via a Suspicious Activity Report, they will promptly assess the matter and determine if there are reasonable grounds for suspicion, as detailed in the following section.

Step 2 - Assess reasonable grounds for suspicion

Initial assessment

If the **Senior Manager** becomes aware of suspicious activity, including via a Suspicious Activity Report, they will promptly (and at any rate within 1-3 business days), assess the level of priority of the matter, based on the information received, so that where information that initially indicates higher risks or greater consequences is dealt with more urgently than other potential suspicious activity.

Where the available information indicates higher risks or greater consequences, the **Senior Manager** informs the Compliance Committee in accordance with ***Chapter 3 - Personnel and Governance***, and records the suspicious activity in the ***Suspicious Activity Register (Tool 5B)***.

The **Senior Manager** then assesses the suspicious activity by completing the ***Assessment of Suspicious Activity Form (Tool 5F)***, which requires them to:

- collect or access all relevant and available information concerning the customer, including their identity, **CRR**, source of funds, and source of wealth
- collect or access all of the relevant and available information regarding the suspicious activity, such as information referred to in the Suspicious Activity Report, transaction information or records, call recordings or surveillance images, as well as by speaking to relevant **Personnel**
- collect or access alerts or reports generated by our transaction monitoring system(s)

- consider whether the customer's behaviour is unusual or their activity is not consistent with their profile
- consider whether the customer appears to be under the influence or instructions of a third party
- consider whether there could be legitimate reasons for the unusual activity, and
- consider the indicators of suspicious activity set out earlier in this section.

The **Senior Manager** records the progress of the assessment of the suspicious activity in the ***Suspicious Activity Register (Tool 5B)***.

Determine reasonable grounds for suspicion

The **Senior Manager**] then promptly determines whether there are 'reasonable grounds' for a suspicion, that is, whether a **Suspicious Matter** exists that must be reported in an **SMR** (refer to ***Assessment of Suspicious Activity Form (Tool 5F)***).

'Reasonable grounds' is an objective standard and means that a 'reasonable person' considering all of the circumstances and information that they know, or could reasonably be expected to know at the time, would conclude that there is a relevant suspicion.

A 'reasonable person' refers to a hypothetical person who displays reasonable or ordinary behaviour or judgment in the circumstances.

Additional information we consider when determining whether a suspicion exists includes:

- who are the **Person**(s) (individual and non-individual) involved and their involvement in the matter
- what are the types and purpose of the **Designated Service**(s) involved and suspicious activity
- where the activity took place
- when the activity took place (specific times and dates, in chronological order)
- why we formed our suspicion (our reasons and the crime type we believe may be involved), and
- how we believe the activity is, has been, or will be, conducted.

The **Senior Manager** then promptly takes appropriate action as set out in the following table and records the outcome in the ***Suspicious Activity Register (Tool 5B*)]**:

Outcome	**Action**
The **Senior Manager** determines that **there are no reasonable grounds** for a suspicion	• Record the reasons for this determination in writing and records the fact and date of this outcome in the ***Suspicious Activity Register (Tool 5B)***.
The **Senior Manager cannot determine if there are reasonable grounds** for a suspicion, or does not have enough information to do so	• Conduct a further assessment or other measures (which may include undertaking **Enhanced CDD** in accordance with ***Chapter 4 Customer Due Diligence*** where appropriate) to establish whether there are reasonable grounds for a suspicion (refer to ***Assessment of Suspicious Activity Form (Tool 5F***))

Outcome	Action
	• Apply additional monitoring measures to the relevant Customer(s), to identify any additional indicators of suspicious activity and • Record the fact and date(s) of these actions in the ***Suspicious Activity Register (Tool 5B)***.
The **Senior Manager** determines that **there are reasonable grounds** for a suspicion	• Record the reasons for determination in writing, and record the fact and date of this outcome in the ***Suspicious Activity Register (Tool 5B)*** • Prepare and submit an **SMR** via **AUSTRAC Online** within the required timeframes • Report the matter to the Compliance Committee. • If we intend to continue providing a **Designated Service** to the Customer, undertake **Enhanced CDD** in accordance with ***Chapter 4 Customer Due Diligence***

Step 3 – Where required, submit SMRs

Once The **Senior Manager** has formed a suspicion on reasonable grounds, they submit an **SMR** via **AUSTRAC Online** within:

a) **24 hours** if the **Suspicious Matter** relates to terrorism financing

b) **3 business days** for other suspicious matters or

The **Senior Manager** records the submission of the **SMR** in the ***Suspicious Activity Register (Tool 5B)***.

For the avoidance of doubt, The **Senior Manager** will not delay in submitting an **SMR** (for example, to complete **Enhanced CDD**), if they have already formed a suspicion on reasonable grounds.

To ensure we are submitting **SMRs** within the required timeframes, The **Senior Manager** records the fact and date that they determined that there are reasonable grounds for a suspicion.

*What we include in our **SMRs***

To ensure that our **SMRs** are effective, each **SMR** is prepared and submitted via **AUSTRAC Online** using the prescribed form and includes full and complete details as described in ***Suspicious Matter Report Content Requirements (Tool 5D)***.

Each **SMR** to be submitted is checked by at least two **Personnel**, the **Senior Manager** and a representative of the **Compliance Committee** to ensure its completeness and accuracy.

Ending/continuing the Customer relationship following an SMR

When we submit an **SMR** to **AUSTRAC**, we do not necessarily need to stop providing **Designated Services** to that customer or end our **Business Relationship**.

However, if we submit an **SMR** and decide to continue our **Business Relationship** with the customer, we continue to appropriately manage and mitigate the **ML/TF Risk** involved in engaging with that customer, including by applying **Enhanced CDD**.

This may in some circumstances, require us to end our **Business Relationship**, where we conclude we must do so to comply with our **Ongoing CDD** obligations.

If we decide to end our **Business Relationship** with a customer following submission of an **SMR**, we ensure that we do not commit the criminal offence of 'Tipping Off' by informing them or implying to them that we have done so because we have formed a suspicion or submitted an **SMR**.

5.5 Prevention of Tipping Off

What is Tipping Off?

Tipping Off is an offence[5]. It includes the disclosure by us or by our **Personnel**, to any **Person**, that:

- we have submitted, are required to submit, or have prepared for submission, an **SMR** to **AUSTRAC**, or
- we have been required by a notice under sections 49(1) or 49B(2) of the **AML/CTF Act** to give information or produce a document, or we have given such information or produced such a document,

where such disclosure would or could reasonably be expected to prejudice an investigation of a crime.

In considering whether disclosure would or could reasonably be expected to prejudice an investigation, it does not matter whether we know or believe an investigation has started. We consider the consequences that disclosing information could have on an investigation, if there was one now, or in the future. This consideration depends on a combination of:

- what information is disclosed
- who the disclosure is made to
- how the disclosure is made, and
- when the disclosure is made.

Generally, if an investigation is complete or finalised, it is unlikely that the disclosure of information would or could prejudice that completed investigation.

How we prevent Tipping Off

We have implemented the following measures in order to prevent **Tipping Off**:

- implementing specific controls on **SMR**-related data, strictly restricting access to authorised **Personnel**, including in relation to Suspicious Activity Reports**,** the ***Suspicious Activity Register (Tool 5B)***, ***Suspicious Activity Report (Tool 5C), Assessment of Suspicious Activity Form (Tool 5F)*** and draft or actual **SMRs**.

Types of information protected by the Tipping Off offence

Information about SMRs

This includes the following, to the extent they identify the subject matter of an **SMR** (such as the **Person** to whom the **SMR** relates):

- copies or extracts of **SMRs** that we have submitted to **AUSTRAC**
- information that establishes that we have submitted an **SMR**, or that a requirement to submit an **SMR** has been triggered (e.g. documents including emails setting out that we have formed a suspicion on reasonable grounds), and
- any document purporting to set out information contained in an **SMR** (e.g. Board or committee meeting agendas/minutes).

Information about notices given to us under sections 49 and 49B of the AML/CTF Act

This includes:

- that we are or were required to give information or produce a document in response to such a notice, or
- that we have given information or produced a document in response to such a notice.

Examples of disclosures that may be Tipping Off

The following disclosures would or could reasonably be expected to prejudice an investigation if we or our **Personnel**:

- tell a customer or their known associate that we have provided, or need to provide, an **SMR** or further information to **AUSTRAC** in relation to their activities
- tell a customer that we suspect they are using our services to engage in criminal conduct, or give them enough information that they can understand that we have formed such a suspicion, requiring us to report to **AUSTRAC**
- inadvertently disclose information publicly, for example if our **Personnel** publishes the information on our website, or
- disclose information to a third party who may share it more widely, e.g., disclosing information to another customer, or a journalist, about suspicions we hold about a **Person's** criminal conduct or the activities we have reported in **SMRs**.

In these examples, the customer or an associate could be 'tipped off' that we are suspicious of their conduct, and that we are required to submit an **SMR** or respond to a notice. This may prompt them to change their behaviour to avoid detection by law enforcement and make investigations more difficult.

Disclosures that are not likely to be considered Tipping Off

We will not have engaged in **Tipping Off** if we merely disclose protected information in the following situations:

- to comply with requirements in or made under Commonwealth, State or Territory laws, e.g., laws to prevent scams, such as the Scams Prevention Framework, or state-based gambling laws
- to appropriately manage **ML/TF Risk** in our business, e.g., disclosures to **Personnel** including employees or senior management, an entity in our **Reporting Group**, or external service providers for this purpose (applying appropriate controls – see below **Outsourcing to external service providers**)
- in the process of supporting due diligence in a merger or acquisition involving our business (applying appropriate controls)
- to meet our **AML/CTF Obligations** or manage our **ML/TF Risk**, e.g., to consultants supporting us with **AML/CTF** remediation and uplift, or to our lawyers to seek legal advice on our **AML/CTF Obligations** (applying appropriate controls see below on Outsourcing to external service providers)
- to participate in activities of the Fintel Alliance, including through disclosures made between reporting entities engaging in these activities
- if our **SMR** obligation has not been triggered, and we are asking a customer reasonable questions or conducting **Enhanced CDD**, or
- to Australian law enforcement, intelligence or regulatory agencies (e.g. State or Federal police, the **ATO**, the National Anti-Corruption Commission, Australian Border Force, or the Australian Criminal Intelligence Commission).

Controls to reduce the risk of Tipping Off

We have implemented the following controls to reduce the risk of **Tipping Off**:

- restrict access to information that is protected by the **Tipping Off** offence to those with a genuine need to know, including third party service providers with access to our systems
- de-identify any such information that is distributed more widely across our business, e.g., redacting names or other identifying information in copies or extracts of **SMRs**
- when discussing **SMR** trends and insights, disclose generally identified patterns of behaviour rather than mentioning specific customers or transactions
- implement and review audit trails of who accesses such information and when, and
- use a legally enforceable agreement to ensure that such information is kept confidential by our **Personnel** and any third parties, e.g., external service providers we engage.

We also maintain adequate information security practices, such as:

- secure physical and electronic document storage
- password protection of electronic documents or systems, and
- secure physical document destruction.

When sharing information that is protected by the **Tipping Off** offence with third parties, e.g., external service providers, we:

- only disclose such information to people that have a genuine ‘need to know’
- consider what legal obligations apply to third parties in foreign countries that we are sharing the information with, to ensure they are consistent with our **AML/CTF Obligations**
- consider whether third parties we may share information with have adopted suitable systems and controls to prevent **Tipping Off**, such as those we have implemented and outlined above, and
- impose legally enforceable conditions on the further use of information we provide to third parties to prevent the information being disclosed to a **Person** the subject of an **SMR**.

Managing our customers to reduce the risk of Tipping Off

Where risks of Tipping Off may arise

Tipping Off risks may arise when managing our customer relationships, for example when engaging with them by:

- requesting further information from a customer, including when assessing a potential **Suspicious Matter**, and/or applying our **Enhanced CDD** pursuant to ***Chapter 4 Customer Due Diligence****, or*
- deciding to end the **Business Relationship**, where the reason for doing so is a **Suspicious Matter**, and we need to communicate an explanation to the customer.

When we engage with a customer in relation to any information protected by the **Tipping Off** offence, or any suspicious activity, we must document our engagement and any steps we took to reduce the risk of **Tipping Off** (see ***Chapter 6 - Program Review and Maintenance***).

Making enquiries into customer activity

We may do the following, without necessarily engaging in **Tipping Off**:

- make reasonable enquiries into customer activity that may be unusual, or
- tell a customer that we need to collect further information to comply with our **AML/CTF Obligations**, such as **KYC**.

However, when making enquiries into customer activity, we do not disclose information if it would or could be likely to prejudice an investigation.

Where possible, we provide the customer with genuine reasons for engaging with them that do not mention their suspicious conduct (or indicate that we are suspicious of their activity).

For example, we are permitted to say that we are required to take relevant steps to:

- comply with **AML/CTF Legislation** or other legal obligations to, for example, know our customer (**KYC**)
- make sure we have the most up to date customer details on file
- collect additional information as part of our standard processes and procedures in certain situations, or
- resolve issues with customer information or identification documents that require additional verification.

To further reduce the risk of **Tipping Off**, we may develop standardised communications and forms for such circumstances, including 'scripts' for **Personnel** to use when engaging with customers to make further enquiries.

*Choosing to end a **Business Relationship** with a customer*

If we decide to end a **Business Relationship** with a customer, where possible we provide genuine reasons for doing so that do not indicate we are suspicious of their conduct.

For example, our reasons include:

- the general nature of the customer's activities fall outside our risk appetite
- the customer has failed to respond to our requests that they provide further details within a reasonable timeframe, or in a satisfactory way
- we have decided not to implement the additional systems and controls that would be required to manage regulatory obligations associated with the customer's account, or
- other reasons that demonstrate we have a commercial basis to end the **Business Relationship** with the customer.

Outsourcing to external service providers

We may need to disclose information protected by the **Tipping Off** offence to external service providers, e.g., to help us review or uplift our AML/CTF reporting, transaction monitoring, or record-keeping functions.

This disclosure will not necessarily result in **Tipping Off**, however, we do not disclose information to external service providers if it would or could reasonably be expected to prejudice an investigation.

One way in which we manage this risk is to conduct due diligence on our external service providers, to verify that they have appropriate controls in place to reduce the risk of **Tipping Off** (see ***Chapter 3 - Personnel and Governance***).

Where we engage an external service provider who operates in a foreign jurisdiction, we will consider whether the laws of that jurisdiction are consistent with our **AML/CTF Obligations**. For example:

- we may submit to **AUSTRAC** an **SMR** about a **Foreign PEP** from a particular jurisdiction country
- we may disclose information to an external service provider based in that country
- the laws and processes in that country may mean that there is a substantial known risk that the **Foreign PEP** will obtain this information from the external service provider
- in this scenario, we will select a different external service provider who does not carry the same risks.

Disclosure to courts or tribunals

We may be requested to provide information protected by the **Tipping Off** offence in court or tribunal proceedings, e.g., following our decision to:

- stop providing services to a customer due to forming a suspicion, or
- dismiss **Personnel** because of their high **ML/TF Risk**.

In these circumstances, we will seek external legal advice before disclosing such information.

Providing **Personnel** and customers with genuine reasons for such decisions, that do not disclose that we are suspicious of their conduct, can help reduce the likelihood that we may be asked or required to produce such information in court or tribunal proceedings.

Under the **AML/CTF Act**, we cannot be required to disclose information protected by the **Tipping Off** offence to a court or tribunal, unless it is in a proceeding to give effect to the **AML/CTF Act**, e.g., proceedings brought by **AUSTRAC**.

We are unlikely to be **Tipping Off** if we merely simply state (or provide documents showing) that particular transactions occurred.

5.6 Threshold Transaction Reports (TTRs)

We are not required to submit a **TTR** where we provide **Designated Services** involving a threshold transaction (AUD$10,000 or more in cash) as we hold an Australian Financial Services licence and are arranging for a **Person** to receive a **Designated Service**.

5.7 Notices and requests for information or documents regarding AML/CTF reports

We may receive a notice requiring us to, under s49, 49A, 49B or 49C of the **AML/CTF Act**, provide documents or other information to **AUSTRAC** or another government authority, regulator or law enforcement agency. This may include further information or documents in relation to the reports we have submitted to **AUSTRAC** outlined elsewhere in this Policy.

If we receive any such notice, we must:

- seek and obtain internal and/or external legal advice regarding the notice, and
- comply with the requirements of the notice.

5.8 References

Related policies and tools

Policies	Chapter 2 **ML/TF Risk Assessment** Chapter 3 **Personnel** and Governance Chapter 4 Customer Due Diligence Chapter 6 Program Maintenance and Review
Tools	5A **AUSTRAC** Enrolment Information 5B Suspicious Activity Register 5C Suspicious Activity Report

	5D **Suspicious Matter** Content Requirements 5F Assessment of Suspicious Activity Form

Legislative requirements and references

Law	**AML/CTF Act**
Regulations	AML/CTF Regulations
Regulatory guidance	**AUSTRAC** Guidance – Enrol with us (Reform)

6. Program Maintenance & Review

6.1 Introduction and scope

This Policy sets out how we meet our obligation to maintain and review our **AML/CTF Program** including:

- when we will review and update our **ML/TF Risk Assessment**
- when we will update our **AML/CTF Policies** to ensure they continue to appropriately manage and mitigate our **ML/TF Risk**
- the records we will retain to document our compliance with our obligations, including how we will protect them from unauthorised access, loss or tampering, and
- the procedures we have implemented to ensure that our **AML/CTF Program** is independently evaluated as required by the **AML/CTF Act** and the **AML/CTF Rules**.

6.2 Reviewing our ML/TF Risk Assessment

We will review and update our **ML/TF Risk Assessment** in order to meet our obligation to identify and assess our **ML/TF Risks** as they change over time.

The **Senior Manager** is responsible for the review and update of our **ML/TF Risk Assessment**, for the purpose of identifying and assessing any new or changed risks of **ML**, **TF** or **PF** that we, as a business, may reasonably face when providing our **Designated Services**.

The review of our **ML/TF Risk Assessment** is appropriate for the nature, size and complexity of our business.

When a review is conducted

The due dates by which The Senior Manager reviews and if required, amends our **ML/TF Risk Assessment** are set out in the following table.

Reason for review of our ML/TF Risk Assessment	**When we review and, if required, update our ML/TF Risk Assessment**
Initial review	**Review:** Three months after **AML/CTF Program** is operationalised or once sufficient **Designated Services** have been provided. **Update:** As soon as practicable after our review is completed

Reason for review of our ML/TF Risk Assessment	When we review and, if required, update our ML/TF Risk Assessment
Periodic review	**Review:** At least every 3 years **Update:** As soon as practicable after our review is completed.
A significant change that is within our control	**Review:** Before the significant change occurs. **Update**: Before the significant change occurs.
A significant change that is not within our control	**Review**: As soon as practicable after we become aware that the significant change occurs. **Update**: As soon as practicable after our review is completed.
AUSTRAC communicates information identifying or assessing risks in relation to our provision of **Designated Services**, e.g.: • **AUSTRAC** guidance (including sector-specific guidance), or newsletters or • Direct communication from **AUSTRAC** to our business.	**Review**: As soon as practicable after **AUSTRAC** communicates the information to us. **Update**: As soon as practicable after our review is completed.

What is a 'significant change'?

A 'significant change' with respect to certain trigger events, will include changes to any of the risk categories outlined in our **ML/TF Risk Assessment** that could have a significant impact on our **ML/TF Risk**. Such changes may be within or outside of our control.

Examples of significant changes to our risk categories within our control include:

- offering a new **Designated Service** to our customers
- providing our **Designated Services** through new channels – such as expanding from in-person service to online services

- introducing a new technology to deliver our **Designated Services**
- providing our **Designated Services** to new customer types – such as to corporations when we previously only served individuals, and
- providing our **Designated Service** that involves dealing with a new country.

Examples of significant changes outside of our control include changes in the **ML/TF Risk** rating of a country or individual citizens of that country with which we deal, such as those affected by **TFS**.

Where there is a change to our business that is not a significant change and does not have a significant impact on our **ML/TF Risk** as outlined above, we do not need to review or update our **ML/TF Risk Assessment** outside of our periodic review.

6.3 Updating and approving our ML/TF Risk Assessment

The Senior Manager updates our **ML/TF Risk Assessment** as soon as practicable after they identify any issues in their review.

For example, if they identify new or changed **ML/TF Risk**, they update the **ML/TF Risk Assessment** to adequately identify, assess and evaluate those new or changed **ML/TF Risk**.

6.4 Reviewing and approving our AML/CTF Policies

Reviewing our AML/CTF Policies

The time by which The Senior Manager reviews and, if required, updates our **AML/CTF Policies** is set out in the following table.

Reason for review of our AML/CTF Policies	**When we review and, if required, update our AML/CTF Policies**
Periodic review: All of our **AML/CTF Policies**	**Review:** At **least every 3 years.** **Update:** As soon as practicable after our review is completed.
Updates made to our **ML/TF Risk Assessment**	**Review**: At least every 3 years **Update**: As soon as practicable after our review is completed.

We consider that these frequencies of periodic review are appropriate after considering the nature, size and complexity of our business, and the type of **ML/TF Risk** we face.

Scope of review following trigger events

The scope and priority areas of the review of our **AML/CTF Policies** will depend on the reason for conducting the review, as follows:

- for a review triggered by updates to our **ML/TF Risk Assessment**, the review prioritises those parts of our **AML/CTF Policies** which are affected by those updates

  e.g., if the updates relate to new or emerging **ML/TF Risk**, the review will prioritise the systems and controls within our **AML/CTF Policies** that are designed to mitigate or manage those particular risks, and

6.5 Record keeping

We keep records that document our compliance with our **AML/CTF Obligations**. This section details:

- the records we have identified that we keep to meet our **AML/CTF Obligations**
- the format and systems to be used for storing records
- how long each type of record is kept (retention periods)
- who has responsibility for maintaining, reviewing and securely storing each type of record, and
- how we protect records from unauthorised access, loss or tampering.

General record-keeping requirements

Proper record keeping involves:

- creating accurate and complete records
- keeping records for a specific period, usually 7 years (see ***Document Destruction Schedule (Tool 6C)***).

The records we are required to retain include, but are not limited to:

- contracts and agreements
- relevant details of identification documents (including **PEP** checks) (this does not need to include copies of the identification documents themselves)
- emails and other correspondence
- **Senior Manager** approvals or notifications
- audio and video files
- reports

- transaction details
- meeting minutes
- logs and databases, and
- software code.

The precise types of records we keep depends on how our business operates and the services we provide. However, at a minimum, we keep records that are:

- reasonably necessary to show we are meeting our **AML/CTF Program** obligations, including our CDD obligations, and
- sufficient to reconstruct individual transactions.

We use our professional judgement to decide what records we need to demonstrate this.

We can meet our record keeping obligations by making or keeping records ourselves or using an external or third-party provider.

Form, storage and backup of records

Form of records

Our records may be:

- hard copy and/or electronic, and
- stored at our premises and/or offsite, including with a third-party provider.

However, we endeavour to keep our records in their original format, or the format we usually use, to avoid unnecessarily changing the document's structure or usability.

Records relating to our **AML/CTF Program** are in the English language, or in a format easily accessed and translated into English.

Storage of records

We store our AML/CTF related records to make them easily retrievable, particularly if records include text and chat messages across multiple apps and smartphones.

However, we also store such records securely, in accordance with our **Reporting Entity** to reference its general document storage and security policy, and disaster recovery and business continuity plan, as applicable

In addition, we store sensitive AML/CTF related records with additional security, outlined below. Sensitive records may include records such as details of customer identification, internal suspicious activity reports, and **SMRs** lodged with **AUSTRAC**. We do this to mitigate the risk of non-compliance with our obligations to:

- avoid committing the offence of **Tipping Off** (see ***Chapter 5 - AUSTRAC Enrolment, Registration and Reporting***) and
- comply with the *Privacy Act 1988* (Cth) in relation to managing **Personal Information**.

The additional security we apply to storing sensitive records includes :

- limiting access to authorised **Personnel**, on a “need to know” basis
- implementing electronic records security measures such as encryption, password protection and/or restricted access
- securely storing paper records in locked cabinets or restricted-access areas
- avoiding security risks by refraining from making or printing unnecessary copies, and
- disposing of records securely.

Back up of electronic records

In accordance with our

- regularly back up AML/CTF-related records to a secure, offsite location or encrypted cloud storage
- ensure backup systems protect data from tampering or unauthorised access, and
- have a data recovery plan for data loss or cyber incidents.

Training our Personnel

In accordance with ***Chapter 3 - Personnel and Governance***, we provide all **Personnel** with training about our record-keeping obligations, system and processes, outlined in this Policy.

Specific records we must keep

The **AML/CTF Records** we keep are those in the following categories:

- records relating to developing and maintaining our **AML/CTF Program**
- records demonstrating governance and oversight of our **AML/CTF Program**
- records demonstrating compliance with our reporting obligations
- records demonstrating compliance with our CDD obligations (including initial, simplified and **Enhanced CDD**), and
- transaction records related to a **Designated Service**, including customer-provided transaction records, sufficient to reconstruct the transaction.

Full details of the records we keep and how long we keep them for can be found in our ***AML/CTF Document Destruction Schedule (Tool 6C)***.

6.6 References

Related policies and tools

Policies	Chapter 1 Introduction Chapter 2 **ML/TF Risk Assessment** Chapter 3 **Personnel** and Governance Chapter 4 Customer Due Diligence Chapter 5 **AUSTRAC** Enrolment, Registration and Reporting
Tools	6A. **AUSTRAC** Guidance Register 6B. AML-CTF Program Review and Update Register 6C. AML CTF Document Destruction Schedule

Legislative requirements and references

Law	**AML/CTF Act**
Regulations	AML/CTF Regulations
Regulatory guidance	**AUSTRAC** Guidance

Endnotes

[1] National Risk Assessment: Money Laundering in Australia, July 2024, page 10
[2] National Risk Assessment: Terrorism Financing in Australia July 2024, page 12
3 Proliferation Financing in Australia 2022, page 11
4 Australian Government: Office of the Australian Information Commissioner: Privacy guidance for reporting entities under the AML/CTF Act (January 2026)
5 Section 123(1) of the Act