AML Program – Part A

January 2023

Contents

Revision Header

This policy is to be reviewed on an annual basis. In particular, Aliro's services and their designation (under section 6 of the Act) is required to be annually reviewed.

Revision No.	Revision Date	Revision Comments	Prepared By:	Approved By:
1	August 2018	Initial Version	Compliance Officer	Board
2	October 2020	Periodic review	Compliance Officer	Board
3	June 2021	Periodic review	Compliance Officer	Board
4	January 2023	Periodic review	Compliance Officer	Board

In addition, this policy is to be reviewed by an independent reviewer, at least once every 3 years. The review should be conducted in accordance with the risk-based approach and must assess and test the following four areas:

- Part A's effectiveness in addressing the ML/TF risk of the reporting entity or each reporting entity in a designated business group;
- whether Part A complies with the requirements outlined in the AML/CTF Rules;
- whether Part A has been effectively implemented;
- whether the reporting entity, or each reporting entity in a DBG, complied with the procedures outlined in Part A.

The independent reviewer must review how the policy has been implemented in practice, with the outcome of the review provided to the Board.

General

1. Description

This Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Program Part A outlines the policies in place to ensure Aliro Group Pty Limited ("Aliro") meets its obligations in relation to AML/CTF. "Know your client" requirements are set out separately in Aliro's AML/CTF Program Part B.

2. Regulatory references

- Anti - Money Laundering and Counter Terrorism Financing Act 2006 ("Act")

3. Tools and references

- Attachment 1: AML/CTF Risk Assessment
- AML/CTF Program Part B
- Customer identification forms

4. Policy breaches

All material or repeated breaches of this Policy will be escalated to the Compliance Manager and will be recorded and reported through Aliro's Breach, incident and escalation policy.

5. Consequences of non-compliance

Consequences of non-compliance with this policy may include:

a) Criminal or civil penalties. The penalties for criminal offences include imprisonment for up to ten years and fines of up to $1.1 million.

b) Breaches of the civil penalty provisions in the Act can attract a pecuniary penalty of up to $11 million for a body corporate and $2.2 million for individuals. Contraventions of the following obligations may give rise to application of civil penalty orders:

   i. providing a Designated Service to a Customer before carrying out an applicable Customer identification procedure.

   ii. not carrying out ongoing transaction monitoring and Customer due diligence.

   iii. failure to report Suspicious Matters, Threshold Transactions or International Fund Transfer Instructions.

   iv. providing a designated service without having adopted a Program under the Act.

   v. failure to keep records in relation to compliance with the Act including the performance of Customer Identification and Verification Procedures.

c) In responding to instances of detected non-compliance with the Act, AUSTRAC has a broad range of enforcement powers which include undertaking criminal prosecutions, seeking injunctions and civil penalty orders, negotiating enforceable undertakings and issuing mandatory remedial directions against reporting entities.

Non-compliance with this Policy by Aliro staff or agents may result in performance management up to and including termination of employment or termination of an agreement with the Aliro.

6. Monitoring

Compliance with this policy will be monitored through a number of different methods including:

- Internal reporting.
- Training with the aim of educating all persons to identify and report breaches.
- Records management.

7. Protections

Any employee who discloses a potential breach under this policy will be protected from reprisal or disadvantage provided that the reports are made in good faith and the employee has not recklessly or intentionally caused the breach.

Policy

1. Overview

Aliro is the holder of Australian Financial Services License Number 502179 ("AFSL"). Aliro uses its AFSL to operate and act as trustee for wholesale unregistered property related trust structures ("Schemes").

This Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Program Part A outlines the policies in place to ensure Aliro meets its obligations in relation to AML/CTF. "Know your client" requirements are set out separately in Aliro's AML/CTF Program Part B.

The object of this program is that Aliro identify, mitigate and manage money laundering and terrorism financing risk ("ML/TF Risk") - the risk that the designated services provided by Aliro might be used in the furtherance of money laundering or the financing of terrorism.

2. What is money laundering and terror financing?

Money laundering

Money laundering is the process by which persons engaged in criminal activities attempt to conceal the true origin and ownership of the proceeds of their activities. If money laundering is successful, those proceeds can lose their apparent criminal identity and appear legitimate.

When criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying source of those funds. Criminals do this by disguising the sources of funds they control, typically by converting such funds into other assets forms in the legitimate financial system.

In summary, the money launderer seeks to:

- place money into the legitimate financial system or retail economy, without arousing suspicion (a stage often referred to as 'placement');
- move the money around, often in a series of transactions so it becomes more difficult to identify its original source (a stage referred to as 'layering'); and
- reintroduce the money into the legitimate economy as if derived from an apparently clean source (a stage referred to as 'integration').

Businesses such as ours can be knowingly or unwittingly co-opted into facilitating money laundering at any one or more of these stages. For this reason, the law requires we have processes to either frustrate money laundering activity or failing that at the very least track and record the verified identity of the Customers of our Designated Services so that law enforcement agencies can later access that information.

Terrorism financing

The United Nations 1999 International Convention for the Suppression of the Financing of Terrorism explains terrorist financing as an offence whereby a person:

'....by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex to the Convention; or

(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.'

Whilst engaging in terrorism financing activity is of itself an offence, the Act is also concerned to ensure that legitimate businesses are not knowingly or unwittingly used in facilitating the commission of such offences. For this reason, we are required to maintain processes designed to identify and report suspected terrorism financing activity or, at the very least, track and record the verified identity of the Customers of our Designated Services so that law enforcement agencies may later be able to later access that information.

3. How is AML/CTF relevant to us?

The following is a table which shows what activities we currently provide that constitute Designated Services under the Act:

Item	Designated Service	Customer of the designated service	Example in Aliro
35	issuing or selling a security or derivative to a person, where: (a) the issue or sale is in the course of carrying on a business of issuing or selling securities or derivatives.	The person – ie the investor	Issuing units in a scheme operated by Aliro
46	providing a custodial or depository service, where: (a) the service is provided in the course of carrying on a business of providing custodial or depository services; and (b) the service is not an exempt legal practitioner service.	The client of the service	Providing self-custody in relation to wholesale unregistered managed investment schemes

The designated services are applicable only to unlisted managed investment schemes where there is the issue, transfer or redemption of units in these schemes.

A full list of Designated Services is set out in section 6 of the Act.

Aliro's clients may only be:

- wholesale clients who satisfy the "sophisticated investor" test as set out in regulation 6D.2.03 Corporations Regulations 2001 (Cth); and
- wholesale clients, including financial institutions such as banks, insurance companies, superannuation schemes, managed investment schemes and other asset managers.

4. How can our business facilitate money laundering?

- Investors may invest funds derived from illegal activities (referred to as 'proceeds of crime') in the Schemes in order to legitimise the funds.
- Criminal organisations may invest proceeds of crime in the Scheme by using false identity documents or through a third party such as a relative or an unwitting participant recruited by the criminal organisation as a 'money mule'.
- By having procedures to more effectively identify the Customers of our Designated Services, and a Program to manage and mitigate ML risk, we provide both a deterrent to persons considering the misuse of our services but also generate records that provide an audit trail that may be relied upon by law enforcement agencies entitled to access the information.

5. How can our business facilitate terrorism financing?

- Terrorist organisations derive income from a variety of means, often combining both lawful and unlawful funding sources. The forms of financing are typically grouped into the following categories:
    - financial support – in the form of donations, community solicitation and other fundraising initiatives; or
    - revenue generating activities – income may be derived from criminal activities but also from legitimate economic activities such as real estate and securities investments or generated via normal business activity.
- When acting on directions from Customers to disburse funds in accordance with instructions received we need to be aware of circumstances where those funds may be intended for TF activity or are paid in a manner in which it may later be difficult to trace the ultimate destination of those funds. By limiting the manner in which we are permitted to disburse funds and ensuring that the immediate destination of payments by us are therefore more readily traceable we will be able to better manage and mitigate the risk of misuse of our services to facilitate TF activity.

6. AML/CTF compliance officer

Aliro has appointed Rupert Smoker from Evolution Fund Services Pty Ltd as its designated Anti-Money Laundering/Counter Terrorism Financing Compliance Officer ("AML Officer"). The responsibilities of the AML Officer include:

- maintaining and implementing this AML/CTF Program;
- overseeing the establishment, maintenance and review of effective AML/CTF systems and controls;
- reporting to the board of directors of Aliro on compliance with this AML/CTF Program and the AML/CTF Regulations;
- making recommendations to the Board on changes to this AML/CTF Program, in light of changes to the AML/CTF Regulations, the nature of Aliro's business and/or clients;
- ensuring Aliro staff and contractors receive appropriate training on their obligations in relation to AML/CTF;
- monitoring AUSTRAC's publicly issued guidance and assessing its relevance to this AML/CTF Program;
- Responding to information requests from AUSTRAC;
- filing reports with AUSTRAC in accordance with the AML/CTF Regulations; and
- if applicable, managing the relationship of each DBG member with AUSTRAC.

The AML Officer may delegate certain duties to other employees of Aliro but must retain responsibility for implementing and assessing this AML/CTF Program.

7. Risk assessment approach

- In developing and updating our Program, we must conduct an assessment of risks that we may reasonably face that the provision by us of Designated Services might involve or facilitate ML or TF activity.
- Our Program is intended to identify, mitigate and manage such risks. The Risk Management Framework is reviewed and updated on a periodic basis, reflecting changes to the risk environment.

Main types of risks

The main categories of risk are:

Regulatory risk: A Reporting Entity must manage regulatory risks associated with breaches of relevant provisions of the Act and the Rules. This requires implementation of a robust program that encompasses relevant obligations and defines the control and review mechanisms needed to ensure compliance. Aliro is committed to implementing and maintaining AML/CTF policies and procedures that meet the regulatory requirements applicable to it.

Business risk: Business risk is the risk that designated services may be used to facilitate ML or TF. These are categorised as inherent risks (prior to controls being implemented) and residual risks (post controls).

Reputational risk: the risk associated with damage to the Reporting Entity's reputation as a result of non-compliance with the Act or Rules which may give rise to a perception that the Reporting Entity has facilitated ML or TF activity.

ML/CTF risk assessment

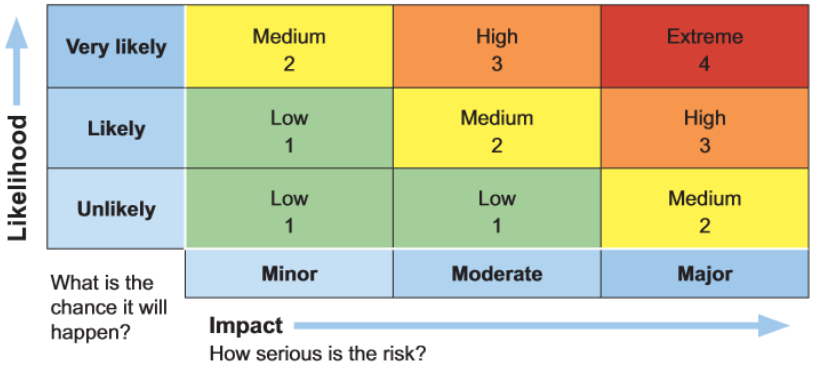
Aliro assesses this risk and assigns a level of risk to the provision of each new client service, having regard to:

- designated services.
- customer types.
- the nature and purpose of the business relationship with customers, including, as appropriate, the collection of information relevant to that consideration.
- delivery methods.
- Jurisdiction of clients

Attachment 1 to this Program identifies, assesses and evaluates our exposure to each of the ML and TF risk categories in the context of the designated services we provide.

Our categorisation of relevant ML/TF risks as either a low, medium or high risk will be based upon the risk matrix illustrated below.

Threat level for ML/TF risk



8. Employee due diligence

Employee due diligence is carried out by performing checks during the recruitment phase for new Employees, and on an ongoing basis for continuing Employees. The purpose of Employee due diligence is to reduce the risk of Employees being involved in the facilitation of ML or TF activity in connection with the provision of our Designated Services.

The AMF/CTF compliance officer is responsible for overseeing employee due diligence.

Aliro undertakes background checks on all new employees regardless of their position, these checks include performing searches to ensure that the prospective employee:

- has not been convicted of any offences involving dishonesty, money laundering or terrorism financing by obtaining a National Criminal History Check (or equivalent in other jurisdictions);
- has not been the subject of disciplinary action by ASIC or APRA (or any equivalent regulator);
- is not bankrupt and has not taken advantage of the laws relating to bankruptcy; and
- querying if the employee has lived in a "high-risk" country, such as a country that is subject to international trade sanctions or unilateral Australian sanctions.

In addition, where an employee has been promoted or their role has changed so that they are involved in any money handling, cash payments, accounting, human resources or customer interactions a refreshed employee due diligence process will be conducted.

9. Outsourcing

Aliro may elect to outsource its AML/CTF obligations where the designated services are provided by an external entity. In these circumstances, external organisations will be appointed to provide these services. Aliro remains ultimately responsible for outsourced services in accordance with the Act and the outsourced services provider must have an AML/CTF Program that is sufficiently equivalent to this program. In this document, references to Aliro includes references to appointed service providers.

Aliro has an Outsourcing Policy which includes various requirements to perform initial and ongoing due diligence on external service providers. The key obligations Aliro imposes under this policy in order for it to meet its AML/CTF obligations when services are outsourced are:

- an assessment of the operational competency of the proposed service provider prior to their appointment;
- contractual documentation imposing obligations on the service provider the ensure they can comply with the Act;
- a requirement that the outsourced service provider provides regular compliance certificates attesting to their compliance;
- a monitoring program whereby the Company may come and inspect the service provides operating environment to test compliance with obligations.
- periodic review (at least every two years) of the outsourcing agreements.

10. AML/CTF risk awareness training

Aliro has a risk awareness training program to provide its employees appropriate training in identifying transactions or clients which may be using our Designated Services to launder money or finance terrorism.

This risk awareness program is conducted at the following intervals:

- All new employees on induction.
- Annually, for other employees that are involved in any money handling, cash payments, accounting, human resources or customer interactions.
- Where an employee's role has changed to fit the description of Paragraph 8 above, when this change occurs.

Under the training program, Employees need to be made aware of:

- Our obligations as a Reporting Entity under the Act and Rules including, but not limited to the requirement to report Suspicious Matters (this could include making a list of the 'Red Flags' and distributing them to Employees), Threshold Transactions and other compliance matters;
- procedures and processes which must be carried out by the Employee in accordance with this Program including, but not limited to the Customer Identification and Verification Procedures;
- the consequences of non-compliance with this Program; and
- the type of ML/TF risks that we face and the consequences of failing to address these risks.

Aliro may determine that it is appropriate for AML/CTF training to be provided within a reasonable period after commencement of their role. No new employee may undertake an unsupervised role or a role with medium or higher ML/TF Risk without obtaining the appropriate AML/CTF training.

Aliro maintains records of training provided to employees. The AML/CTF compliance officer is responsible for ensuring the training program is appropriate and up to date.

11. Enhanced Due Diligence

Enhanced Due Diligence (EDD) is the process of undertaking additional identification and verification measures in certain circumstances deemed to be high risk.

Customers

We proceed on the assumption that the substantial majority, if not all, of our Customers should generally be assessed as low to medium risk. This assumption is based upon our assessment of the ML and TF risks which Aliro is exposed to.

Customer identification and verification procedures will be conducted on all prospective customers without exemption.

ECDD will be conducted where we suspect a particular Customer may be of 'higher risk' of engagement in ML or TF activity. The ECDD procedures are set out in Part B to this AML/CTF program.

The 'red flag' indicators considered to identify if a particular customer will be identified as 'high risk' are set out in Appendix A to this document.

Employees

Employees may be subject to EDD if they are found not to comply with this AML/CTF program. EDD for employees may include:

- Undergoing mandatory training to refresh their knowledge of the AML/CTF program
- Being subject to disciplinary actions, ranging from formal warnings to instant dismissal, or reconsideration of role suitability, depending on the seriousness of the breach.

12. Ongoing customer due diligence and transaction monitoring

We will monitor transactional activity by our Customers on an ongoing basis in order to detect activity or behaviour that may be indicative of Suspicious Matters (which may give rise to a Suspicious Matter Reporting Obligation) or other abnormal or atypical activity that may be suggestive of any of the following:

- circumstances that indicate the Customer may not be who they initially had claimed to be;
- circumstances that directly indicate the Customer may be seeking the delivery of our services:
    - in connection with the commission of a ML or TF offence;

- in connection with the commission of any other offence against any laws of the Commonwealth, States or Territories of Australia;
- the existence in relation to a prospective Customer of one or more of the 'Red Flag' risk indicators set out in Appendix A to this document.

Customers that are subject to transaction monitoring may:

- be required to provide additional KYC information (see Part B to this program)
- be subject to enhanced due diligence
- result in a Suspicious Matter Reporting Obligation
- be subject to termination of the Customer's relationship.

If at any time, we have reasonable grounds to doubt whether an Existing Customer is the person they claim to be, we must within 14 days of formation of that opinion, take appropriate and reasonable steps to satisfy ourselves as to the true identity of the Customer including undertaking Customer Identification and Verification Procedures. Failure to satisfy ourselves as to the true identity of a Customer will give rise to a Suspicious Matter Reporting Obligation.

13. Reporting

Suspicious matters

Section 41 of the Act provides that, we are required to report to AUSTRAC 'Suspicious Matters' that fit any of the descriptions set out in Appendix A of this Program. The Act also imposes prescribed time frames for us to complete that reporting.

For the purpose of this Program, a 'Suspicious Matter' will be deemed to have occurred when there are reasonable grounds for us to suspect:

- That a Customer, or an agent purporting to act on their behalf, is not who they claim to be;
- We have information that may be relevant to the investigation of an evasion of tax law, or the prosecution of a person for an offence against the laws of the Commonwealth, States or Territories of Australia, or may be of assistance in the enforcement of the Proceeds of Crimes Act 2002 (Cth) (or equivalent State or Territory legislation);
- The provision by us of a Designated Service has been used or may be used to assist the financing of a ML or TF offence; or
- The provision by us of a Designated Service may be relevant to the investigation or prosecution of a person for a ML or TF offence.

How do we determine and report suspicious matters?

Each Employee who forms a belief, or becomes aware of information to indicate that a Suspicious Matter may have occurred must notify the AML/CTF Compliance Officer of that belief.

Within 2 hours of receipt of a notification from an Employee, or if otherwise becoming aware of a possible Suspicious Matter the AML/CTF Compliance Officer must:

- Review and investigate the issue in order to decide whether or not a Suspicious Matter Reporting Obligation has been triggered within the meaning of the Act and Rules
- Consider whether it is appropriate to make the Customer subject to the enhanced due diligence procedures
- ensure that any further enquiries:
    - are conducted in a prudent manner using common sense, tact and discretion; and
    - do not give rise to a 'tipping off' offence (see section 14 for further details);
- seek guidance from AUSTRAC or professional legal advice if unsure; and
- keep a written record of any review and investigation undertaken.

Threshold transactions

Section 43 of the Act provides that, we are required to report to AUSTRAC all 'Threshold Transactions'. A Threshold Transaction is a transaction involving the transfer of $10,000 or more in physical currency or e-currency.

Each Employee who handles a Threshold Transaction must notify the AML/CTF Compliance Officer of that fact.

The AML/CTF Compliance Officer must:

- report all Threshold Transactions to the AUSTRAC CEO within ten Business Days after the transaction takes place using the AUSTRAC prescribed form.
- report to the Board at the next scheduled board meeting that a Threshold Transaction has occurred.

International funds transfer instruction (IFTI) reports

Aliro does not provide a registrable designated remittance service or conducts electronic funds transfer. Therefore, Aliro does not have any obligations with respect to reporting IFTIs.

Compliance reporting to AUSTRAC

- As a part the requirements under the Act, an AML/CTF compliance report must be provided to AUSTRAC with information about our compliance with the Act.
- The Company's AML/CTF compliance report must be lodged online at https://online.austrac.gov.au.
- The AML/CTF Compliance Officer must provide AUSTRAC with information about the Company's compliance with the Act.

Business changes

Should Aliro substantially change its business operations it is obliged to report this to AUSTRAC within 14 days of that change occurring.

Compliance with reporting obligations

The AML/CTF Compliance Officer will be responsible for:

- Overseeing all Employees compliance with our reporting obligations.
- Arranging training for all Employees in relation to our reporting obligations.
- Undertaking an audit of an appropriate sample of Customer files randomly selected every year and reviewing whether our reporting obligations have been complied with.
- Prior to lodging the annual compliance report with AUSTRAC notifying the Board of any circumstances brought to the attention of the AML/CTF Compliance Officer which would lead them to believe that we have not complied with the Act or this Program.
- The AML/CTF Compliance Officer must provide confirmation to the Board that the compliance report has been submitted to AUSTRAC including a summary of its contents and any matters relevant for noting as soon as possible after the report has been lodged with AUSTRAC.

14. Tipping off offences

What is tipping off?

A Reporting Entity, its directors, employees or agents must not disclose to anyone other than AUSTRAC that it has:

- reported, or is required to report information about a Suspicious Matter Reporting Obligation or Threshold Transaction; or
- formed a suspicion about a Suspicious Matter.

Failure to comply with this obligation is an offence under section 123 of the Act. In particular, the Company its Directors, Employees or agents must not do anything that would lead a Customer or anyone else (other than AUSTRAC) to believe that a suspicion has been formed or that information has been communicated to AUSTRAC.

In some circumstances, enhanced due diligence procedures may lead a Customer to suspect that they are being investigated. It is AUSTRAC's view that the mere act of asking a Customer for additional information about their identity or source or destination of their funds, for example, would not constitute an unlawful disclosure of information under the tipping off provisions of the Act.

Exceptions

If required, a Reporting Entity may disclose the matter to:

- A lawyer or accountant for the purpose of dissuading the Customer from engaging in conduct that constitutes, or could constitute, evasion of a taxation law, evasion of a law of a State or Territory that deals with taxation or an offence against a law of the Commonwealth or a State or Territory;
- Its lawyers for the purpose of obtaining legal advice;
- An Australian Government Agency that has responsibility for law enforcement (i.e. Australian Capital Territory Police or the Australian Federal Police);
- Another Reporting Entity within its designated business group for the purpose of informing the other Reporting Entity about the risks involved when dealing with a Customer;
- External auditors; or
- Foreign members of the same corporate or designated business group with which you have a shared customer but only if the foreign members are regulated by laws of a foreign country that give effect to some or all of the FATF recommendations.

15. Record keeping

Record keeping involves creating full and accurate records and the storage and management of them. Keeping records:

- Demonstrates to AUSTRAC that Aliro (or its agenets) are fulfilling its AML/CTF obligations
- Helps manage the risks of the business being exploited for ML/TF
- Assists the regulators in understanding the circumstances in the event the business is exploited by criminals.

Aliro (or its agents) will keep records relating to AML/CTF matters for 7 years, in accordance with the following table.

Document	Form
A record made by Aliro of information relating the provision of a designated service to the customer	original, copy or an extract from the record
A document given to Aliro by the customer (or someone on behalf of the customer) relating to the provision or prospective provision of a designated service by us to the customer (if Aliro provides a designated service to that customer)	original or copy
A record of the applicable identification procedure carried out in respect of a customer (if Aliro provide a designated service to that customer) (The record must allow Aliro to demonstrate to an investigator that the procedure has been carried out, and the information and documents collected in the course of the procedure)	original or copy
Information obtained in the course of carrying out the applicable customer identification procedure (if we provide a designated service to that customer)	original or copy
The record of our adoption of this Anti-Money Laundering and Counter-Terrorism Financing Program	original or copy

This Anti-Money Laundering and Counter-Terrorism Financing Program or any variation or copy of the variation	original or copy
Employee records	Original or copy

16. Review of AML/CTF Program

This AML/CTF Program is subject to regular independent review by either external auditor or compliance specialist or by someone internal to Aliro that is not involved in the provision of designated services. The purpose of this review is to:

- assess the effectiveness of this AML/CTF Program, having regard to the ML/TF Risks faced by Aliro;
- assess whether this AML/CTF Program complies with the AML/CTF Regulations;
- assess whether this AML/CTF Program has been effectively implemented; and
- assess whether Aliro has complied with this AML/CTF Program.

The results of any independent review, including any report prepared will be provided to the Board, and senior management of Aliro. The AML Officer may address any recommendations on behalf of and under advisement from senior management and the Board or its delegate.

Where appropriate, this AML/CTF Program may be amended as a result of the review.

We must have in place a procedure that allows us to receive and have regard to feedback from AUSTRAC in respect of our performance on managing the ML/TF risk.

The AML/CTF Compliance Officer must:

- amend the Program (for adoption by the Board) to take into account any deficiencies identified in feedback provided by AUSTRAC;
- develop a plan (with appropriate training) for implementation of the amendments incorporating the AUSTRAC feedback of the Program; and
- manage the conduct of the developed plan.

Appendix A – Red Flag Indicators

Transaction monitoring

- The Customer engages, or seeks to engage, in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 reporting Threshold Transactions, especially if the cash or monetary instruments are in an amount just below the reporting or recording Threshold Transactions.
- The Customer requests to pay or be paid in cash or cash equivalents.
- The Customer's account has a large number of ingoing or outgoing or electronic transfers that have no apparent business purpose.
- Receiving five or more applications from the same Customer during the same Quarter.
- Receiving three or more applications and three or more redemptions from the same Customer during the Quarter.
- A Customer exercising the Scheme's cooling-off period for an application more than once during a six-month period.
- A Customer changing bank account details more than once during a six-month period.
- The Customer maintaining multiple accounts or maintaining accounts in the names of family members or corporate entities, for no apparent purpose.

Suspicious matter reporting obligation

- Information arises that:
- indicates that the Customer may not be who they claim to be.
- might be relevant to the investigation of an evasion of tax law or the prosecution of a person for an offence against a Commonwealth, State or Territory law, or may be of assistance in enforcement of the Proceeds of Crime Act 2002 (Cth) (or criminal and State or Territory legislation).
- indicates that the provision of the designated service may be preparatory to the commission of a terrorism financing or money laundering offence.
- may be relevant to the investigation of or prosecution of a person for a terrorism financing or money laundering offence.

Other suspicious behavior

- The Customer showing unusual concern about our compliance with reporting requirements and the processes and procedures contained in the Program.
- The Customer engaging in transactions that lack business sense or apparent investment strategy, or are inconsistent with the Customer's stated investment objectives.
- The information provided by the Customer that purports to identify a legitimate source for funds is suspected to be false, misleading or substantially incorrect.
- The Customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person's identity.
- The Customer has difficulty describing the nature of their business or lacks general knowledge of their industry.

- The Customer (or in the case of a corporate entity, persons representing or purporting to act on behalf of the Customer) exhibits unusual concern, reluctance or refusal regarding compliance with our Program.
- The Customer (or a person publicly associated with the Customer) is known to have a criminal, or otherwise questionable, background or is the subject of news reports indicating involvement in possible criminal, civil, or regulatory violations.

Foreign customers

- The Customer is revealed to have a substantial personal or business connection with, or makes payment from, or requests payment to, a financial institution account or provides an address in a Non-compliant Jurisdiction.
- The Customer is identified as a Politically Exposed Person. In addition, we will Verify or re-verify beneficial owner information in accordance with the identification requirements specified in Chapter 4 of the AML/CTF Rules, and seek senior management approval for:
    - continuing a business relationship with the customer;
    - whether a transaction on an account should be processes; and
    - whether the designated service should continue to be provided to the customer.
- The Customer is a person physically located in or a corporation incorporated in a prescribed foreign country.

AML Program Part B

March 2023

Contents

Revision Header

Revision No.	Revision Date	Revision Comments	Prepared By:	Approved By:
1	August 2018	Initial Version	Compliance Officer	Board
2	March 2023	Periodic Review	Compliance Officer	N/A

This Program should be reviewed every 2 years. This Program can only be amended with the approval of Senior Management, with the exception of minor amendments that do not affect the nature, substance or intent of the document.

General

This Policy is Part B to Aliro's AML / CTF program and sets out the customer identification procedures including enhanced customer due diligence required under the Know Your Customer ("KYC") requirements.

Program

1. Overview

- Section 32 of the Anti-Money and Counter Terrorism Financing Act 2006 ("The Act") requires that we identify Customers before we provide a Designated Service to them.
- The Rules provide that we need to both collect certain information in relation to Customers and verify that information against primary or secondary documentation. By this means we aim to form a reasonable belief as to the true identity of the Customer and retain some record of the process by which we sought to verify their identity. We will be able to use information collected to check against databases and other records and assign to particular Customers a low, medium or high risk of participation in ML or TF activity.

2. How do we identify a customer?

- Whenever we receive a request for the provision of a Designated Service from a prospective Customer, we must first establish the Customer type that seeks delivery of the Designated Service.
- Aliro has Customer Identification Forms that apply different Customer Identification and Verification Procedures depending on type of Customer which must be completed by the Customer (together with associated verification documentation) the type of Customer.
- After we have ascertained Customer type, we must then:
    - Ensure we have collected the information in relation to the Customer required under the relevant form pertaining to that Customer type
    - Verify the documentary information received in relation to the Customer
- Where multiple Customers are acting jointly (for example applications received from a husband and wife) we must separately identify and verify each Customer.
- Unless the required Customer Identification and Verification Procedure and, where applicable, any heightened procedures in relation to high-risk Customers set out in this Program, have been completed in relation to a Customer, we must not proceed to deliver a Designated Service to the Customer.
- In limited circumstances, we will permit the provision of KYC documentation up to 5 days post the provision of the designated services, in once off scenarios and subject to the discretion of Senior Management who will make a risk based assessment.

3. Determine the identity of the beneficial owner

We are required to ascertain a beneficial owner of all 'non-individual' customers, this includes taking reasonable measures to verify:

- For a company or a partnership, any individual who:
    - is entitled (either directly or indirectly) to exercise 25% of more of the voting rights, including a power to veto, or
    - holds the position of senior managing official (or equivalent);

- For a trust, any individual who holds the power to appoint or remove trustees of the trust;
- For an association or a registered co-operative, any individual who:
    - Is entitled (either directly or indirectly) to exercise 25% or more of the voting rights including a power to veto, or
    - Would be entitled on dissolution to 25% or more of the property of the association or registered co-operative, or
    - Holds the position of senior managing official (or equivalent)
- Aliro's Customer Identification Forms request details on beneficial ownership. Where details or documentation provision in relation to a chain of beneficial ownership is unclear, Aliro's AML/CTF Compliance Officer will assess the documentation provided and may request additional information or documentation from the Customer.

4. Verification procedures

- Designated services offered by Aliro are medium or lower risk.
- The Customer Identification Forms used by Aliro set out the documentation requirements that Aliro has identified is acceptable for verification purposes.
- Aliro will assess all the information obtained through the identification forms for consistency. Should there be any issues with the consistency of information collated, the AML/CTF Officer must be consulted, who may then either elect to contact the potential customer, or conduct Enhanced Customer Due Diligence (identified below).
- Where a foreign customer is not subject to Enhanced Customer Due Diligence, Aliro will accept legal document certification applicable in the customers home geography, noting that this may not provide Aliro with the 'Safe Harbour' protections in accordance with the Act. In all other cases, certification must occur in accordance with Appendix A to this document.

5. Enhanced Customer Due Diligence

- In the event that any of the red flags in Part A of this program are identified enhanced due diligence procedures will be conducted. Aliro's Client Risk Assessment is provided at Attachment 1 for the purpose of documenting the review of red flags.
- There is no obligation on reporting entities to carry out enhanced due diligence procedures in relation to Australian Politically Exposed Persons unless required to do so under some other process and procedure contained in the Program (for example, a Suspicious Matter Reporting Obligation).
- Where a red flag has been identified, the AML/CTF Compliance Officer must be immediately notified. The AML/CTF Compliance Officer will then seek additional information in respect to the prospective customer, which will include, but will not be limited to the following:
    - The Customer's occupation, business activities or functions
    - Formal confirmation of the Customer's purpose and intention in requesting the relevant Designated Service including where appropriate the purpose of specific transactions, or the expected nature and level of transactions to be undertaken by the Customer
    - Any other name the Customer is known by (other than that already provided)
    - The Customer's country(ies) of citizenship and residence.
    - The Customer's financial position and other information regarding the income or assets available to the Customer.

- The Customer's source of funds, including where appropriate, confirmation of the origin of funds.
- Details in respect of the ownership and control structure of the Customer.
- The beneficial ownership of the funds used by the Customer with respect to the Designated Service.
- Confirmation of the intended beneficiaries of the proposed transactions including, where appropriate, the destination of funds.
- Where the Customer is not a natural person, further particulars relevant to the identity of natural persons who exercise ultimate control over the affairs of the Customer.
- Verify or re-verify KYC information in accordance with the customer identification program. To the extent that KYC information has not pervious
- undertake more detailed analysis and monitoring of the Customer's transactions

- For all Politically Exposed Persons ("PEP") identified the AML/CTF Officer must:
  - Perform a risk assessment of the PEP
  - Obtain Senior Management approval prior to establishing the business relationship and providing the Designated Services
  - Take measures to establish the customer's source of wealth or funds
  - Conduct transaction monitoring on this account, and any for high risk PEPs that are accepted as customers, obtain senior management approval prior to accepting any instructions from them.
- In conducting enhanced Customer Due Diligence, the AML/CTF officer should consider verification of KYC information from independent 3rd party sources, such as online databases.
- Depending on outcome of the above, the AML/CTF will assess whether a "Suspicious Matter" should be reported in accordance with Part A of this program.

AML Program – Part A

January 2023

Contents

Revision Header

This policy is to be reviewed on an annual basis. In particular, Aliro's services and their designation (under section 6 of the Act) is required to be annually reviewed.

Revision No.	Revision Date	Revision Comments	Prepared By:	Approved By:
1	August 2018	Initial Version	Compliance Officer	Board
2	October 2020	Periodic review	Compliance Officer	Board
3	June 2021	Periodic review	Compliance Officer	Board
4	January 2023	Periodic review	Compliance Officer	Board

In addition, this policy is to be reviewed by an independent reviewer, at least once every 3 years. The review should be conducted in accordance with the risk-based approach and must assess and test the following four areas:

- Part A's effectiveness in addressing the ML/TF risk of the reporting entity or each reporting entity in a designated business group;
- whether Part A complies with the requirements outlined in the AML/CTF Rules;
- whether Part A has been effectively implemented;
- whether the reporting entity, or each reporting entity in a DBG, complied with the procedures outlined in Part A.

The independent reviewer must review how the policy has been implemented in practice, with the outcome of the review provided to the Board.

General

1. Description

This Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Program Part A outlines the policies in place to ensure Aliro Group Pty Limited ("Aliro") meets its obligations in relation to AML/CTF. "Know your client" requirements are set out separately in Aliro's AML/CTF Program Part B.

2. Regulatory references

- Anti - Money Laundering and Counter Terrorism Financing Act 2006 ("Act")

3. Tools and references

- Attachment 1: AML/CTF Risk Assessment
- AML/CTF Program Part B
- Customer identification forms

4. Policy breaches

All material or repeated breaches of this Policy will be escalated to the Compliance Manager and will be recorded and reported through Aliro's Breach, incident and escalation policy.

5. Consequences of non-compliance

Consequences of non-compliance with this policy may include:

a) Criminal or civil penalties. The penalties for criminal offences include imprisonment for up to ten years and fines of up to $1.1 million.

b) Breaches of the civil penalty provisions in the Act can attract a pecuniary penalty of up to $11 million for a body corporate and $2.2 million for individuals. Contraventions of the following obligations may give rise to application of civil penalty orders:

   i. providing a Designated Service to a Customer before carrying out an applicable Customer identification procedure.

   ii. not carrying out ongoing transaction monitoring and Customer due diligence.

   iii. failure to report Suspicious Matters, Threshold Transactions or International Fund Transfer Instructions.

   iv. providing a designated service without having adopted a Program under the Act.

   v. failure to keep records in relation to compliance with the Act including the performance of Customer Identification and Verification Procedures.

c) In responding to instances of detected non-compliance with the Act, AUSTRAC has a broad range of enforcement powers which include undertaking criminal prosecutions, seeking injunctions and civil penalty orders, negotiating enforceable undertakings and issuing mandatory remedial directions against reporting entities.

Non-compliance with this Policy by Aliro staff or agents may result in performance management up to and including termination of employment or termination of an agreement with the Aliro.

6. Monitoring

Compliance with this policy will be monitored through a number of different methods including:

- Internal reporting.
- Training with the aim of educating all persons to identify and report breaches.
- Records management.

7. Protections

Any employee who discloses a potential breach under this policy will be protected from reprisal or disadvantage provided that the reports are made in good faith and the employee has not recklessly or intentionally caused the breach.

Policy

1. Overview

Aliro is the holder of Australian Financial Services License Number 502179 ("AFSL"). Aliro uses its AFSL to operate and act as trustee for wholesale unregistered property related trust structures ("Schemes").

This Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Program Part A outlines the policies in place to ensure Aliro meets its obligations in relation to AML/CTF. "Know your client" requirements are set out separately in Aliro's AML/CTF Program Part B.

The object of this program is that Aliro identify, mitigate and manage money laundering and terrorism financing risk ("ML/TF Risk") - the risk that the designated services provided by Aliro might be used in the furtherance of money laundering or the financing of terrorism.

2. What is money laundering and terror financing?

Money laundering

Money laundering is the process by which persons engaged in criminal activities attempt to conceal the true origin and ownership of the proceeds of their activities. If money laundering is successful, those proceeds can lose their apparent criminal identity and appear legitimate.

When criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying source of those funds. Criminals do this by disguising the sources of funds they control, typically by converting such funds into other assets forms in the legitimate financial system.

In summary, the money launderer seeks to:

- place money into the legitimate financial system or retail economy, without arousing suspicion (a stage often referred to as 'placement');
- move the money around, often in a series of transactions so it becomes more difficult to identify its original source (a stage referred to as 'layering'); and
- reintroduce the money into the legitimate economy as if derived from an apparently clean source (a stage referred to as 'integration').

Businesses such as ours can be knowingly or unwittingly co-opted into facilitating money laundering at any one or more of these stages. For this reason, the law requires we have processes to either frustrate money laundering activity or failing that at the very least track and record the verified identity of the Customers of our Designated Services so that law enforcement agencies can later access that information.

Terrorism financing

The United Nations 1999 International Convention for the Suppression of the Financing of Terrorism explains terrorist financing as an offence whereby a person:

'....by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex to the Convention; or

(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.'

Whilst engaging in terrorism financing activity is of itself an offence, the Act is also concerned to ensure that legitimate businesses are not knowingly or unwittingly used in facilitating the commission of such offences. For this reason, we are required to maintain processes designed to identify and report suspected terrorism financing activity or, at the very least, track and record the verified identity of the Customers of our Designated Services so that law enforcement agencies may later be able to later access that information.

3. How is AML/CTF relevant to us?

The following is a table which shows what activities we currently provide that constitute Designated Services under the Act:

Item	Designated Service	Customer of the designated service	Example in Aliro
35	issuing or selling a security or derivative to a person, where: (a) the issue or sale is in the course of carrying on a business of issuing or selling securities or derivatives.	The person – ie the investor	Issuing units in a scheme operated by Aliro
46	providing a custodial or depository service, where: (a) the service is provided in the course of carrying on a business of providing custodial or depository services; and (b) the service is not an exempt legal practitioner service.	The client of the service	Providing self-custody in relation to wholesale unregistered managed investment schemes

The designated services are applicable only to unlisted managed investment schemes where there is the issue, transfer or redemption of units in these schemes.

A full list of Designated Services is set out in section 6 of the Act.

Aliro's clients may only be:

- wholesale clients who satisfy the "sophisticated investor" test as set out in regulation 6D.2.03 Corporations Regulations 2001 (Cth); and
- wholesale clients, including financial institutions such as banks, insurance companies, superannuation schemes, managed investment schemes and other asset managers.

4. How can our business facilitate money laundering?

- Investors may invest funds derived from illegal activities (referred to as 'proceeds of crime') in the Schemes in order to legitimise the funds.
- Criminal organisations may invest proceeds of crime in the Scheme by using false identity documents or through a third party such as a relative or an unwitting participant recruited by the criminal organisation as a 'money mule'.
- By having procedures to more effectively identify the Customers of our Designated Services, and a Program to manage and mitigate ML risk, we provide both a deterrent to persons considering the misuse of our services but also generate records that provide an audit trail that may be relied upon by law enforcement agencies entitled to access the information.

5. How can our business facilitate terrorism financing?

- Terrorist organisations derive income from a variety of means, often combining both lawful and unlawful funding sources. The forms of financing are typically grouped into the following categories:
    - financial support – in the form of donations, community solicitation and other fundraising initiatives; or
    - revenue generating activities – income may be derived from criminal activities but also from legitimate economic activities such as real estate and securities investments or generated via normal business activity.
- When acting on directions from Customers to disburse funds in accordance with instructions received we need to be aware of circumstances where those funds may be intended for TF activity or are paid in a manner in which it may later be difficult to trace the ultimate destination of those funds. By limiting the manner in which we are permitted to disburse funds and ensuring that the immediate destination of payments by us are therefore more readily traceable we will be able to better manage and mitigate the risk of misuse of our services to facilitate TF activity.

6. AML/CTF compliance officer

Aliro has appointed Rupert Smoker from Evolution Fund Services Pty Ltd as its designated Anti-Money Laundering/Counter Terrorism Financing Compliance Officer ("AML Officer"). The responsibilities of the AML Officer include:

- maintaining and implementing this AML/CTF Program;
- overseeing the establishment, maintenance and review of effective AML/CTF systems and controls;
- reporting to the board of directors of Aliro on compliance with this AML/CTF Program and the AML/CTF Regulations;
- making recommendations to the Board on changes to this AML/CTF Program, in light of changes to the AML/CTF Regulations, the nature of Aliro's business and/or clients;
- ensuring Aliro staff and contractors receive appropriate training on their obligations in relation to AML/CTF;
- monitoring AUSTRAC's publicly issued guidance and assessing its relevance to this AML/CTF Program;
- Responding to information requests from AUSTRAC;
- filing reports with AUSTRAC in accordance with the AML/CTF Regulations; and
- if applicable, managing the relationship of each DBG member with AUSTRAC.

The AML Officer may delegate certain duties to other employees of Aliro but must retain responsibility for implementing and assessing this AML/CTF Program.

7. Risk assessment approach

- In developing and updating our Program, we must conduct an assessment of risks that we may reasonably face that the provision by us of Designated Services might involve or facilitate ML or TF activity.
- Our Program is intended to identify, mitigate and manage such risks. The Risk Management Framework is reviewed and updated on a periodic basis, reflecting changes to the risk environment.

Main types of risks

The main categories of risk are:

Regulatory risk: A Reporting Entity must manage regulatory risks associated with breaches of relevant provisions of the Act and the Rules. This requires implementation of a robust program that encompasses relevant obligations and defines the control and review mechanisms needed to ensure compliance. Aliro is committed to implementing and maintaining AML/CTF policies and procedures that meet the regulatory requirements applicable to it.

Business risk: Business risk is the risk that designated services may be used to facilitate ML or TF. These are categorised as inherent risks (prior to controls being implemented) and residual risks (post controls).

Reputational risk: the risk associated with damage to the Reporting Entity's reputation as a result of non-compliance with the Act or Rules which may give rise to a perception that the Reporting Entity has facilitated ML or TF activity.

ML/CTF risk assessment

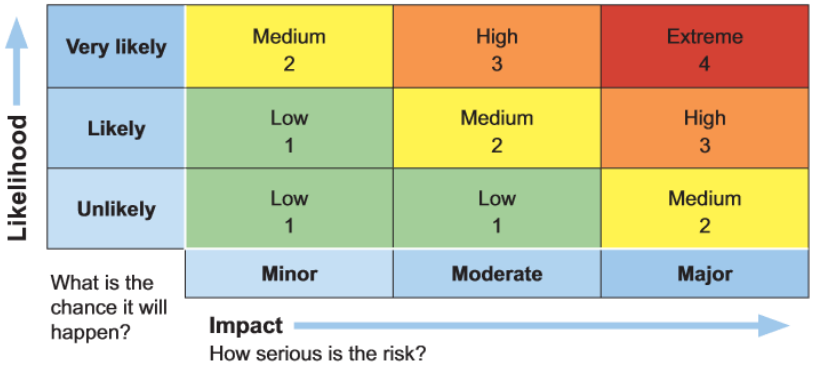
Aliro assesses this risk and assigns a level of risk to the provision of each new client service, having regard to:

- designated services.
- customer types.
- the nature and purpose of the business relationship with customers, including, as appropriate, the collection of information relevant to that consideration.
- delivery methods.
- Jurisdiction of clients

Attachment 1 to this Program identifies, assesses and evaluates our exposure to each of the ML and TF risk categories in the context of the designated services we provide.

Our categorisation of relevant ML/TF risks as either a low, medium or high risk will be based upon the risk matrix illustrated below.

Threat level for ML/TF risk



8. Employee due diligence

Employee due diligence is carried out by performing checks during the recruitment phase for new Employees, and on an ongoing basis for continuing Employees. The purpose of Employee due diligence is to reduce the risk of Employees being involved in the facilitation of ML or TF activity in connection with the provision of our Designated Services.

The AMF/CTF compliance officer is responsible for overseeing employee due diligence.

Aliro undertakes background checks on all new employees regardless of their position, these checks include performing searches to ensure that the prospective employee:

- has not been convicted of any offences involving dishonesty, money laundering or terrorism financing by obtaining a National Criminal History Check (or equivalent in other jurisdictions);
- has not been the subject of disciplinary action by ASIC or APRA (or any equivalent regulator);
- is not bankrupt and has not taken advantage of the laws relating to bankruptcy; and
- querying if the employee has lived in a "high-risk" country, such as a country that is subject to international trade sanctions or unilateral Australian sanctions.

In addition, where an employee has been promoted or their role has changed so that they are involved in any money handling, cash payments, accounting, human resources or customer interactions a refreshed employee due diligence process will be conducted.

9. Outsourcing

Aliro may elect to outsource its AML/CTF obligations where the designated services are provided by an external entity. In these circumstances, external organisations will be appointed to provide these services. Aliro remains ultimately responsible for outsourced services in accordance with the Act and the outsourced services provider must have an AML/CTF Program that is sufficiently equivalent to this program. In this document, references to Aliro includes references to appointed service providers.

Aliro has an Outsourcing Policy which includes various requirements to perform initial and ongoing due diligence on external service providers. The key obligations Aliro imposes under this policy in order for it to meet its AML/CTF obligations when services are outsourced are:

- an assessment of the operational competency of the proposed service provider prior to their appointment;
- contractual documentation imposing obligations on the service provider the ensure they can comply with the Act;
- a requirement that the outsourced service provider provides regular compliance certificates attesting to their compliance;
- a monitoring program whereby the Company may come and inspect the service provides operating environment to test compliance with obligations.
- periodic review (at least every two years) of the outsourcing agreements.

10. AML/CTF risk awareness training

Aliro has a risk awareness training program to provide its employees appropriate training in identifying transactions or clients which may be using our Designated Services to launder money or finance terrorism.

This risk awareness program is conducted at the following intervals:

- All new employees on induction.
- Annually, for other employees that are involved in any money handling, cash payments, accounting, human resources or customer interactions.
- Where an employee's role has changed to fit the description of Paragraph 8 above, when this change occurs.

Under the training program, Employees need to be made aware of:

- Our obligations as a Reporting Entity under the Act and Rules including, but not limited to the requirement to report Suspicious Matters (this could include making a list of the 'Red Flags' and distributing them to Employees), Threshold Transactions and other compliance matters;
- procedures and processes which must be carried out by the Employee in accordance with this Program including, but not limited to the Customer Identification and Verification Procedures;
- the consequences of non-compliance with this Program; and
- the type of ML/TF risks that we face and the consequences of failing to address these risks.

Aliro may determine that it is appropriate for AML/CTF training to be provided within a reasonable period after commencement of their role. No new employee may undertake an unsupervised role or a role with medium or higher ML/TF Risk without obtaining the appropriate AML/CTF training.

Aliro maintains records of training provided to employees. The AML/CTF compliance officer is responsible for ensuring the training program is appropriate and up to date.

11. Enhanced Due Diligence

Enhanced Due Diligence (EDD) is the process of undertaking additional identification and verification measures in certain circumstances deemed to be high risk.

Customers

We proceed on the assumption that the substantial majority, if not all, of our Customers should generally be assessed as low to medium risk. This assumption is based upon our assessment of the ML and TF risks which Aliro is exposed to.

Customer identification and verification procedures will be conducted on all prospective customers without exemption.

ECDD will be conducted where we suspect a particular Customer may be of 'higher risk' of engagement in ML or TF activity. The ECDD procedures are set out in Part B to this AML/CTF program.

The 'red flag' indicators considered to identify if a particular customer will be identified as 'high risk' are set out in Appendix A to this document.

Employees

Employees may be subject to EDD if they are found not to comply with this AML/CTF program. EDD for employees may include:

- Undergoing mandatory training to refresh their knowledge of the AML/CTF program
- Being subject to disciplinary actions, ranging from formal warnings to instant dismissal, or reconsideration of role suitability, depending on the seriousness of the breach.

12. Ongoing customer due diligence and transaction monitoring

We will monitor transactional activity by our Customers on an ongoing basis in order to detect activity or behaviour that may be indicative of Suspicious Matters (which may give rise to a Suspicious Matter Reporting Obligation) or other abnormal or atypical activity that may be suggestive of any of the following:

- circumstances that indicate the Customer may not be who they initially had claimed to be;
- circumstances that directly indicate the Customer may be seeking the delivery of our services:
    - in connection with the commission of a ML or TF offence;

- in connection with the commission of any other offence against any laws of the Commonwealth, States or Territories of Australia;
- the existence in relation to a prospective Customer of one or more of the 'Red Flag' risk indicators set out in Appendix A to this document.

Customers that are subject to transaction monitoring may:

- be required to provide additional KYC information (see Part B to this program)
- be subject to enhanced due diligence
- result in a Suspicious Matter Reporting Obligation
- be subject to termination of the Customer's relationship.

If at any time, we have reasonable grounds to doubt whether an Existing Customer is the person they claim to be, we must within 14 days of formation of that opinion, take appropriate and reasonable steps to satisfy ourselves as to the true identity of the Customer including undertaking Customer Identification and Verification Procedures. Failure to satisfy ourselves as to the true identity of a Customer will give rise to a Suspicious Matter Reporting Obligation.

13. Reporting

Suspicious matters

Section 41 of the Act provides that, we are required to report to AUSTRAC 'Suspicious Matters' that fit any of the descriptions set out in Appendix A of this Program. The Act also imposes prescribed time frames for us to complete that reporting.

For the purpose of this Program, a 'Suspicious Matter' will be deemed to have occurred when there are reasonable grounds for us to suspect:

- That a Customer, or an agent purporting to act on their behalf, is not who they claim to be;
- We have information that may be relevant to the investigation of an evasion of tax law, or the prosecution of a person for an offence against the laws of the Commonwealth, States or Territories of Australia, or may be of assistance in the enforcement of the Proceeds of Crimes Act 2002 (Cth) (or equivalent State or Territory legislation);
- The provision by us of a Designated Service has been used or may be used to assist the financing of a ML or TF offence; or
- The provision by us of a Designated Service may be relevant to the investigation or prosecution of a person for a ML or TF offence.

How do we determine and report suspicious matters?

Each Employee who forms a belief, or becomes aware of information to indicate that a Suspicious Matter may have occurred must notify the AML/CTF Compliance Officer of that belief.

Within 2 hours of receipt of a notification from an Employee, or if otherwise becoming aware of a possible Suspicious Matter the AML/CTF Compliance Officer must:

- Review and investigate the issue in order to decide whether or not a Suspicious Matter Reporting Obligation has been triggered within the meaning of the Act and Rules
- Consider whether it is appropriate to make the Customer subject to the enhanced due diligence procedures
- ensure that any further enquiries:
    - are conducted in a prudent manner using common sense, tact and discretion; and
    - do not give rise to a 'tipping off' offence (see section 14 for further details);
- seek guidance from AUSTRAC or professional legal advice if unsure; and
- keep a written record of any review and investigation undertaken.

Threshold transactions

Section 43 of the Act provides that, we are required to report to AUSTRAC all 'Threshold Transactions'. A Threshold Transaction is a transaction involving the transfer of $10,000 or more in physical currency or e-currency.

Each Employee who handles a Threshold Transaction must notify the AML/CTF Compliance Officer of that fact.

The AML/CTF Compliance Officer must:

- report all Threshold Transactions to the AUSTRAC CEO within ten Business Days after the transaction takes place using the AUSTRAC prescribed form.
- report to the Board at the next scheduled board meeting that a Threshold Transaction has occurred.

International funds transfer instruction (IFTI) reports

Aliro does not provide a registrable designated remittance service or conducts electronic funds transfer. Therefore, Aliro does not have any obligations with respect to reporting IFTIs.

Compliance reporting to AUSTRAC

- As a part the requirements under the Act, an AML/CTF compliance report must be provided to AUSTRAC with information about our compliance with the Act.
- The Company's AML/CTF compliance report must be lodged online at https://online.austrac.gov.au.
- The AML/CTF Compliance Officer must provide AUSTRAC with information about the Company's compliance with the Act.

Business changes

Should Aliro substantially change its business operations it is obliged to report this to AUSTRAC within 14 days of that change occurring.

Compliance with reporting obligations

The AML/CTF Compliance Officer will be responsible for:

- Overseeing all Employees compliance with our reporting obligations.
- Arranging training for all Employees in relation to our reporting obligations.
- Undertaking an audit of an appropriate sample of Customer files randomly selected every year and reviewing whether our reporting obligations have been complied with.
- Prior to lodging the annual compliance report with AUSTRAC notifying the Board of any circumstances brought to the attention of the AML/CTF Compliance Officer which would lead them to believe that we have not complied with the Act or this Program.
- The AML/CTF Compliance Officer must provide confirmation to the Board that the compliance report has been submitted to AUSTRAC including a summary of its contents and any matters relevant for noting as soon as possible after the report has been lodged with AUSTRAC.

14. Tipping off offences

What is tipping off?

A Reporting Entity, its directors, employees or agents must not disclose to anyone other than AUSTRAC that it has:

- reported, or is required to report information about a Suspicious Matter Reporting Obligation or Threshold Transaction; or
- formed a suspicion about a Suspicious Matter.

Failure to comply with this obligation is an offence under section 123 of the Act. In particular, the Company its Directors, Employees or agents must not do anything that would lead a Customer or anyone else (other than AUSTRAC) to believe that a suspicion has been formed or that information has been communicated to AUSTRAC.

In some circumstances, enhanced due diligence procedures may lead a Customer to suspect that they are being investigated. It is AUSTRAC's view that the mere act of asking a Customer for additional information about their identity or source or destination of their funds, for example, would not constitute an unlawful disclosure of information under the tipping off provisions of the Act.

Exceptions

If required, a Reporting Entity may disclose the matter to:

- A lawyer or accountant for the purpose of dissuading the Customer from engaging in conduct that constitutes, or could constitute, evasion of a taxation law, evasion of a law of a State or Territory that deals with taxation or an offence against a law of the Commonwealth or a State or Territory;
- Its lawyers for the purpose of obtaining legal advice;
- An Australian Government Agency that has responsibility for law enforcement (i.e. Australian Capital Territory Police or the Australian Federal Police);
- Another Reporting Entity within its designated business group for the purpose of informing the other Reporting Entity about the risks involved when dealing with a Customer;
- External auditors; or
- Foreign members of the same corporate or designated business group with which you have a shared customer but only if the foreign members are regulated by laws of a foreign country that give effect to some or all of the FATF recommendations.

15. Record keeping

Record keeping involves creating full and accurate records and the storage and management of them. Keeping records:

- Demonstrates to AUSTRAC that Aliro (or its agenets) are fulfilling its AML/CTF obligations
- Helps manage the risks of the business being exploited for ML/TF
- Assists the regulators in understanding the circumstances in the event the business is exploited by criminals.

Aliro (or its agents) will keep records relating to AML/CTF matters for 7 years, in accordance with the following table.

Document	Form
A record made by Aliro of information relating the provision of a designated service to the customer	original, copy or an extract from the record
A document given to Aliro by the customer (or someone on behalf of the customer) relating to the provision or prospective provision of a designated service by us to the customer (if Aliro provides a designated service to that customer)	original or copy
A record of the applicable identification procedure carried out in respect of a customer (if Aliro provide a designated service to that customer) (The record must allow Aliro to demonstrate to an investigator that the procedure has been carried out, and the information and documents collected in the course of the procedure)	original or copy
Information obtained in the course of carrying out the applicable customer identification procedure (if we provide a designated service to that customer)	original or copy
The record of our adoption of this Anti-Money Laundering and Counter-Terrorism Financing Program	original or copy

This Anti-Money Laundering and Counter-Terrorism Financing Program or any variation or copy of the variation	original or copy
Employee records	Original or copy

16. Review of AML/CTF Program

This AML/CTF Program is subject to regular independent review by either external auditor or compliance specialist or by someone internal to Aliro that is not involved in the provision of designated services. The purpose of this review is to:

- assess the effectiveness of this AML/CTF Program, having regard to the ML/TF Risks faced by Aliro;
- assess whether this AML/CTF Program complies with the AML/CTF Regulations;
- assess whether this AML/CTF Program has been effectively implemented; and
- assess whether Aliro has complied with this AML/CTF Program.

The results of any independent review, including any report prepared will be provided to the Board, and senior management of Aliro. The AML Officer may address any recommendations on behalf of and under advisement from senior management and the Board or its delegate.

Where appropriate, this AML/CTF Program may be amended as a result of the review.

We must have in place a procedure that allows us to receive and have regard to feedback from AUSTRAC in respect of our performance on managing the ML/TF risk.

The AML/CTF Compliance Officer must:

- amend the Program (for adoption by the Board) to take into account any deficiencies identified in feedback provided by AUSTRAC;
- develop a plan (with appropriate training) for implementation of the amendments incorporating the AUSTRAC feedback of the Program; and
- manage the conduct of the developed plan.

Appendix A – Red Flag Indicators

Transaction monitoring

- The Customer engages, or seeks to engage, in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 reporting Threshold Transactions, especially if the cash or monetary instruments are in an amount just below the reporting or recording Threshold Transactions.
- The Customer requests to pay or be paid in cash or cash equivalents.
- The Customer's account has a large number of ingoing or outgoing or electronic transfers that have no apparent business purpose.
- Receiving five or more applications from the same Customer during the same Quarter.
- Receiving three or more applications and three or more redemptions from the same Customer during the Quarter.
- A Customer exercising the Scheme's cooling-off period for an application more than once during a six-month period.
- A Customer changing bank account details more than once during a six-month period.
- The Customer maintaining multiple accounts or maintaining accounts in the names of family members or corporate entities, for no apparent purpose.

Suspicious matter reporting obligation

- Information arises that:
- indicates that the Customer may not be who they claim to be.
- might be relevant to the investigation of an evasion of tax law or the prosecution of a person for an offence against a Commonwealth, State or Territory law, or may be of assistance in enforcement of the Proceeds of Crime Act 2002 (Cth) (or criminal and State or Territory legislation).
- indicates that the provision of the designated service may be preparatory to the commission of a terrorism financing or money laundering offence.
- may be relevant to the investigation of or prosecution of a person for a terrorism financing or money laundering offence.

Other suspicious behavior

- The Customer showing unusual concern about our compliance with reporting requirements and the processes and procedures contained in the Program.
- The Customer engaging in transactions that lack business sense or apparent investment strategy, or are inconsistent with the Customer's stated investment objectives.
- The information provided by the Customer that purports to identify a legitimate source for funds is suspected to be false, misleading or substantially incorrect.
- The Customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person's identity.
- The Customer has difficulty describing the nature of their business or lacks general knowledge of their industry.

- The Customer (or in the case of a corporate entity, persons representing or purporting to act on behalf of the Customer) exhibits unusual concern, reluctance or refusal regarding compliance with our Program.
- The Customer (or a person publicly associated with the Customer) is known to have a criminal, or otherwise questionable, background or is the subject of news reports indicating involvement in possible criminal, civil, or regulatory violations.

Foreign customers

- The Customer is revealed to have a substantial personal or business connection with, or makes payment from, or requests payment to, a financial institution account or provides an address in a Non-compliant Jurisdiction.
- The Customer is identified as a Politically Exposed Person. In addition, we will Verify or re-verify beneficial owner information in accordance with the identification requirements specified in Chapter 4 of the AML/CTF Rules, and seek senior management approval for:
    - continuing a business relationship with the customer;
    - whether a transaction on an account should be processes; and
    - whether the designated service should continue to be provided to the customer.
- The Customer is a person physically located in or a corporation incorporated in a prescribed foreign country.

Appendix A

Certification definitions and applicable procedure

When applying the verification it is acceptable for 'Certified Copies' or 'Certified Extracts' of original documents to be provided by a Customer in place of originals.

Categories of persons authorised to certify documents

Persons who can certify documents or extracts are:

- (a lawyer) a person who is enrolled on the roll of the Supreme Court of a State or Territory, or High Court of Australia, as a legal practitioner (however described);
- a judge of a court;
- a magistrate;
- a chief executive officer of a Commonwealth court;
- a registrar or deputy registrar of a court;
- a Justice of Peace;
- a notary public (for the purposes of the Statutory Declaration Regulations 1993);
- a police officer;
- (a postal agent) an agent of the Australian Postal Corporation who is in charge of an office supplying postal services to the public;
- (the post office) an permanent employee of The Australian Postal Corporation with 2 or more years of continuous service who is employed in an office supplying postal services to the public;
- an Australian consular officer or an Australian diplomatic officer (within the meaning of the Consular Fees Act 1955);
- an officer with two or more continuous years of service with one or more financial institutions (for the purposes of the Statutory Declaration Regulations 1993);
- a finance company officer with two or more continuous years of service with one or more financial companies (for the purposes of the Statutory Declaration Regulations 1993);
- an officer with, or authorised representative of, a holder of an Australian financial services license, having two or more continuous years of service with one or more licensees; and
- (an accountant) a member of the institute of Chartered Accountants in Australia, CPA Australia or the National Institute of Accountants with two or more years of continuous membership.

Notwithstanding the above, we will always apply a common sense discretion in considering whether to reject a purported certification where we reasonably suspect the person purporting to certify a document may, in fact, not be within the permitted categories of persons capable of certifying documents or where we have reason to believe that certification of the document has not be validly or reliably performed.