AML CTF Program

1. Contents

2. Record of adoption of AML/CTF Program

Section 116(2) of the *Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth)* ("the AML/CTF Act") requires a reporting entity to make a record of the adoption of its AML/CTF Program, and to retain that record for a period of 7 years.

History of adoption of AML/CTF Program:

- Transcash International Pty Ltd formally adopted and approved its AML/CTF Program on 1 September 2011. The approval and adoption of the AML/CTF Program was authorised by Director and compliance officer Manohar Tiwari.
- This program was revised on 28 March 2014. This variation has been adopted and approved by the board of directors of Transcash International Pty Ltd.
- This program was revised and updated on 28 March 2016. This variation has been adopted and approved by the board of directors of Transcash International Pty. Ltd.
- This program has been revised & updated on 28 February 2019. This variation has been adopted and approved by the board of directors of Transcash International Pty Ltd.
- This program has been revised on 28 February 2022. This variation has been adopted and approved by the board of directors of Transcash International Pty. Ltd.

Adopted and Approved by the Board of directors on 1 September 2011.

Certified by then Company Secretary Mr. Manohar Tiwari

3. Review of program

This program will be subject to formal review by the board once a year; or when there is a material change to Transcash International Pty Ltd.'s business.

The program shall also be subjected to annual external review. The recommendations of this review shall be incorporated in the next review, wherever necessary.

The AML/CTF program was first adopted and approved on 1 September 2011; and has since been amended as follows

Date	General nature of changes	Person Responsible	Approved By
28 Mar 2014	General review and updates	Manohar Tiwari	Board of directors
28 Mar 2016	Policy & program update	Akriti Lamichhane	Board of Directors
28 Feb 2019	Policy & program update	Akriti Lamichhane	Board of Directors
28 Feb 2022	Policy & program update	Akriti Lamichhane	Board of Directors

4. Background

Section 81 and 82 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the Act) and all amendments up to 2022 require Transcash International Pty Ltd to document an anti-money laundering and counter-terrorism financing program (divided into Parts A and B for its

Australian operations) and to comply with that program. The Act and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Compilation No. 54)* (the Rules) set out what must be included in each Part of the program.

Note: Where parts of this program derive directly from the Act or Rules, this is identified in footnotes by reference to a section number (and, where relevant, an item or sub-section number) or Rule number respectively.

5. Definitions:

In this Program:

- "**The Act**" means the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- **"AUSTRAC"** means the Australian Transaction Reports and Analysis Centre, which is Australia's anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit.
- **"SMR"** means suspicious matter report.
- **"Designated Services"** means the services set out in section 6 of the Act;
- **"FTR Act"** means the *Financial Transaction Reports Act* (Cth) 1988
- **"KYC"** means know your client.
- **"CDD"** means client due diligence.
- **"Money Laundering"** is the processing of criminal profits to disguise their illegal origin;
- **"OCDD"** means ongoing client due diligence.
- **"Customer"** means the individual or corporate entity who directly engages Transcash International Pty Ltd for services.
- "**PEP**" means a person entrusted with prominent public functions in a *foreign* country (for example, Heads of State, government, senior politicians or senior executives of state owned companies). A PEP is not usually a middle rank or more junior official.
- "**The Rules**" means the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*; "MT/TF risk" means the risk that Transcash International Pty Ltd may reasonably face that, in providing the designated services, it is involved in or facilitates money laundering or terrorism financing;
- "**Representative"** refers to an employee of Transcash International Pty Ltd or an Authorised Representative of Transcash International Pty Ltd, as defined by the *Corporations Act 2001*;
- "**Terrorism financing**" refers to the financing of terrorist acts, and also of terrorists and terrorist organisations;
- "**We/our/us/TCI**" means "Transcash International Pty Ltd", incorporated in Australia.
- Data filtration etc.

6. Anti-Money Laundering / Counter Terrorism Financing Policy

6.1 Purpose

Transcash International Pty Ltd has developed the Anti-Money Laundering and Counter Terrorism Financing Policy ("the Policy"), in order to ensure that the designated services offered by us incorporate sufficient safeguards to detect and prevent money laundering and terrorism financing.

TCI will ensure that it has, in place adequate and appropriate risk mitigation procedures by:

- Complying with the Policy;
- Monitoring compliance with the Policy;
- Assessing, evaluating and approving transactions and clients in accordance with the Policy; and
- Regular review and reporting on relevant clients and/or transactions.

6.2 Commitment

TCI is committed to maintaining high standards of AML/CTF compliance and requires all of its employees, contractors and any other persons representing us to adhere to these standards to prevent the use of our services for illegal purposes.

The Act and the Rules require TCI to develop and maintain an AML/CTF Program to identify and materially mitigate the risks that the provision of a designated service might involve; or facilitate a transaction that is connected with the commission of money laundering or terrorism financing offence.

Non-compliance with the Policy or the AML/CTF Program shall be treated as serious misconduct, and may result in further training, termination of employment, removal of authorisation, or other punitive action. It may also result in disciplinary action and/or civil or criminal proceedings by AUSTRAC.

6.3 Objectives

TCI management and staff will ensure that reasonable measures (including internal controls) are in place to counter attempts to use its services to launder money or finance terrorism.

If an employee, agent or representative becomes aware of any instances of money laundering and terrorism financing activities, or has reasonable grounds to suspect that those activities are taking place or contemplated, they are required to report this occurrence or suspicion to TCI's compliance officer on +61 2 8833 1426 immediately.]

TCI will take immediate action in the event that we become aware of any individual or group engaging in or attempting to engage in money laundering or terrorism financing activities through the provision of our services. This action will include informing AUSTRAC as required pursuant to this Program, the Act and the Rules.

6.4 Principles

The principles governing our approach to money laundering and terrorism financing are:

6.4.1 We will maintain an AML/CTF program as required by the AML/CTF Act

This means we will:

- Comply with this AML/CTF Program;
- Implement and maintain processes designed to identify, mitigate and manage the risk we may reasonably have
    - that the provision of designated services by us, might (whether inadvertently or otherwise) involve or
    - facilitate money laundering or financing of terrorism; and
- Implement and maintain applicable client identification procedures for our clients.

6.4.2 We comply with the law and aim for best practice

We comply with national AML/CTF laws in the countries in which we operate, and have regard to international best practice as detailed, for example in the recommendations of the Financial Action Task Force (FATF).

We work in conjunction with the Australian Government, and the governments of any country in which we operate, and support these governments' objectives in relation to prevention, detection and control of financial crime.

6.4.3 We will not deal with Shell Banks and Shell Entities

We will not enter into relationships with shell banks and shell entities.

6.4.4 We take a risk-based approach

We assess the risks of our products using a risk-based approach. This assessment is mandatorily carried out before the introduction of new products and on a periodic basis.

We identify clients in accordance with the current legislative requirements in the countries in which we operate. Due diligence processes for clients are tailored according to our analysis of the AML or CTF risk associated with those clients (or client groupings) and the designated services, geographies or channels involved. We also continuously monitor the activity of our clients using a risk-based approach.

6.4.5 We act on our suspicions:

We report any suspicious matters or activity to the appropriate authorities in a timely and comprehensive manner, as required by local laws or our own policy, whichever provides the greater standard.

We shall not enter into business relationships where we suspect that our products or services might be used for illegitimate purposes and submit a suspicious matter report to the concerned authorities and AUSTRAC. TCI shall ensure not to disclose the reason to avoid tipping off the client.

If, during the provision of a product or service the matter arouses our suspicion, we will take necessary action. This action will include copying identification offered, noting physical descriptors of the customer and transaction details. At no stage will we inform the customer of our suspicions or intention to submit a suspicious matter report. We will then submit a suspicious matter report to the concerned authorities and AUSTRAC.

6.4.6 We maintain a high standard of record keeping

We keep meticulous records to assist in the investigation of money laundering and terrorism financing. Records include transaction records, client correspondence, notifications of changes to our services/products, and documents given to us by clients or their agents, relating to the designated services we provide. We retain the records for 7 year in order to:

- meeting our record-keeping requirements under the Act and the Rules;
- assessment of the effectiveness of our AML/CTF Program by external parties;
- identification of clients;
- reconstruction of client transactions (if required);
- identification of all investigations and evaluation of potential suspicious matters;
- identification of all suspicious matter reports, threshold transaction reports and IFTI reports;
- provision of documentation to satisfy any inquiries for AUSTRAC, notices from AUSTRAC or any other parties, agencies or court orders and seeking disclosure of information.

6.4.7 We provide our employees with regular risk awareness training in relation to the AML/CTF Program

We provide our employees with regular risk awareness training in relation to the AML/CTF Program, the training includes all level of employees within TCI to ensure equal understanding of the AML/CTF obligations related to the roles and responsibilities of the employees in providing designated services on behalf of TCI.

The training aims to enable our employees to understand:

- Transcash International Pty Ltd's obligations under the Act and commitment to the AML/CTF compliance as stated in the Act;
- TCI's internal policies and procedures in daily business operations
- The consequences of non-compliance with the Act;
- The unique ML/TF risks faced by us and the consequences of those risks and
- The specific procedures which are relevant to the work carried out by our employees.

The training must be delivered to all newly employed personnel and existing employees with job rotation within TCI as part of the induction training for the role. TCI may conduct the training internally or engage external professional training providers to carry out the training, which will be regularly reviewed to ensure the trainings are up to date and relevant to the latest changes of ML/TF risks. TCI will also ensure open on-going communication within internal functions in relation to updates of internal policies, procedures, controls and various systems. The training is compulsory for TCI employees who:

- are in a position which has been assessed as posing a high ML/TF risk
- are customer facing personnel
- in authority to approve customers' transactions
- in authority to manage and handle TCI's cash and funds
- responsible to report suspicious matters to AUSTRAC
- responsible to oversee and implement the AML/CTF program within TCI

The risk awareness training is provided to our employees at least annually and is recorded in our training register.

6.4.8 Consequences of breaching the AML/CTF Program

Every employee of TCI has compliance and operational obligations that vary according to their job. Non-compliance with the obligations set out in the AML/CTF Program may result in disciplinary action and could include dismissal if the instance of non-compliance is severe.

6.5 Roles and responsibilities

The Board and senior management of Transcash International Pty Ltd have ongoing oversight of the Policy and this Program.

Representatives and contractors must comply with the AML/CTF policy and procedures, report suspicious matters or behaviors and attend training as required for their role.

We have also appointed an AML/ CTF compliance officer. This is the nominated person at management level who will support and coordinate senior management focus on managing the money-laundering / terrorist financing risk in our business. The AML/ CTF compliance officer will report to Transcash International Pty Ltd's board regularly on the effectiveness of the AML/CTF program, cases of non-compliance, summary conclusion of third-party independent review and various feedbacks and dialog with authorities in regard to the AML/CTF program of TCI. TCI will also conduct regular review of the ML/TF risks TCI is facing and ensure the risk-based procedures and controls are sufficient and adequate to address the risks and AML/CTF is a permanent agenda item of the board.

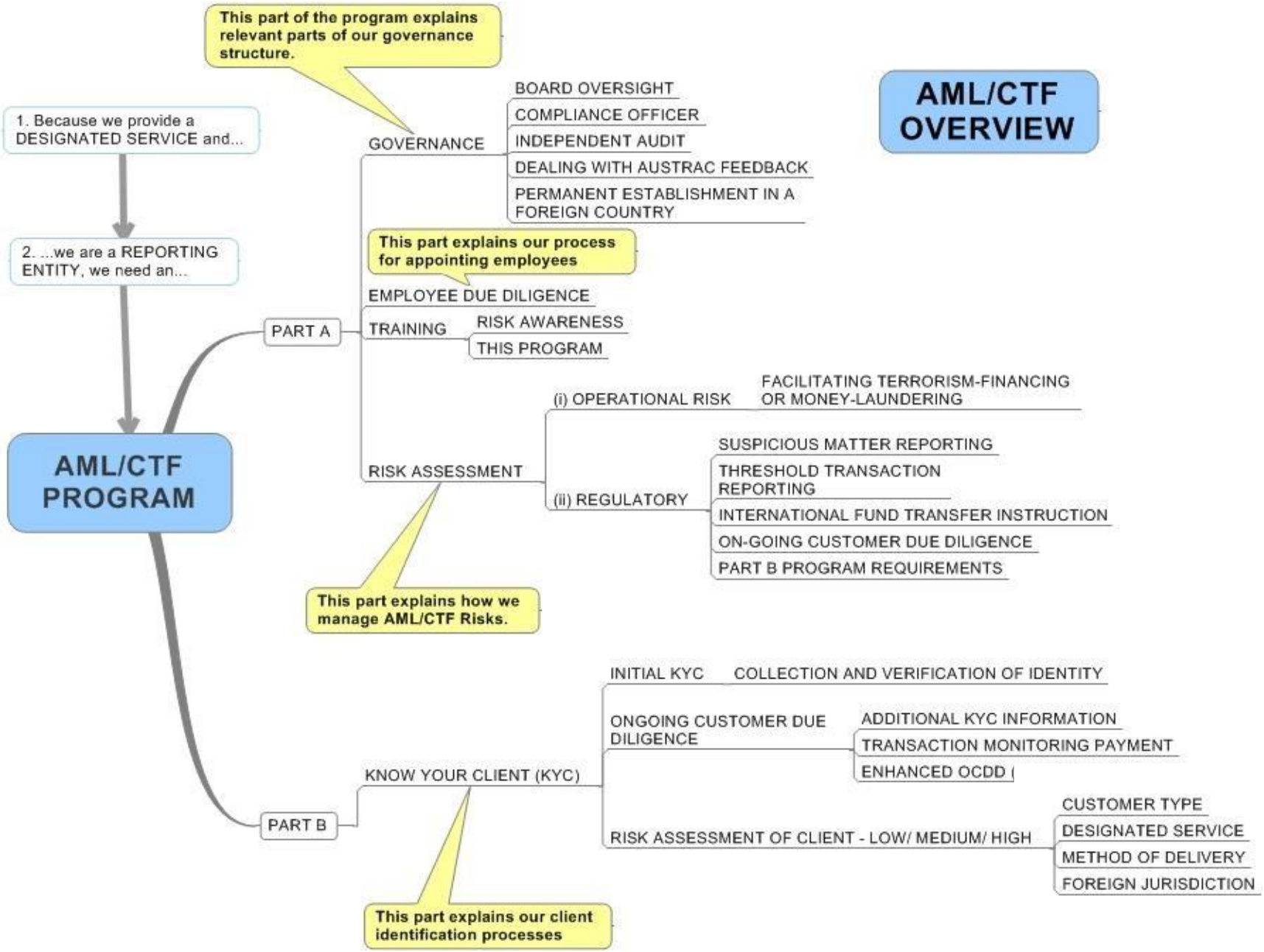
Role and responsibilities of compliance officer:

- Ensure TCI's compliance under the obligations of the Act and the Rules
- Implementation and maintenance of internal AML/CTF compliance policies, procedures, controls, manuals and systems.
- Oversee daily business operations to be compliant with the internal AML/CTF program
- Regular reporting to the board and senior management on all compliance matters
- Become the point of contact to AUSTRAC's feedback in regard to TCI's AML/CTF compliance program
- Reporting suspicious matters to AUSTRAC and acting as contact officer for the SMR

- Acting as contact person for compliance audits, urgent internal compliance reporting and escalations, liaise with documents or information requests from authority, international fund transfer instructions and threshold transactions
- Delegate compliance responsibilities appropriately to certain employees as part of the AML/CTF compliance program.

6.6 AML/CTF Overview

See mind map next page.


AML/CTF OVERVIEW
1. Because we provide a DESIGNATED SERVICE and...
2. ...we are a REPORTING ENTITY, we need an...
AML/CTF PROGRAM
PART A
PART B
This part of the program explains relevant parts of our governance structure.
GOVERNANCE
BOARD OVERSIGHT
COMPLIANCE OFFICER
INDEPENDENT AUDIT
DEALING WITH AUSTRAC FEEDBACK
PERMANENT ESTABLISHMENT IN A FOREIGN COUNTRY
This part explains our process for appointing employees
EMPLOYEE DUE DILIGENCE
TRAINING
RISK AWARENESS
THIS PROGRAM
RISK ASSESSMENT
(i) OPERATIONAL RISK
FACILITATING TERRORISM-FINANCING OR MONEY-LAUNDERING
(ii) REGULATORY
SUSPICIOUS MATTER REPORTING
THRESHOLD TRANSACTION REPORTING
INTERNATIONAL FUND TRANSFER INSTRUCTION
ON-GOING CUSTOMER DUE DILIGENCE
PART B PROGRAM REQUIREMENTS
This part explains how we manage AML/CTF Risks.
KNOW YOUR CLIENT (KYC)
INITIAL KYC
COLLECTION AND VERIFICATION OF IDENTITY
ONGOING CUSTOMER DUE DILIGENCE
ADDITIONAL KYC INFORMATION
TRANSACTION MONITORING PAYMENT
ENHANCED OCDD (
RISK ASSESSMENT OF CLIENT - LOW/ MEDIUM/ HIGH
CUSTOMER TYPE
DESIGNATED SERVICE
METHOD OF DELIVERY
FOREIGN JURISDICTION
This part explains our client identification processes

Part A – General

7. Risk management

7.1 Purpose

The primary purpose of this Part is to identify, mitigate and manage the risks that Transcash International Pty Ltd may be involved in or facilitate money laundering or terrorism financing. This is known as “ML/TF risk”.

This Part is also designed to meet any requirements set out under the Rules. The Act requires TCI to:

- enable the identification of significant changes in ML/TF risks, when providing the designated services, and when identifying clients (see Part B); and
- assess the ML/TF risk when:
    - providing new designated services;
    - providing new methods of service delivery; and
    - utilizing new technology when providing a designated service.

7.2 Responsibility

The risk management assessment is conducted regularly by our AML/CTF compliance officer. It is undertaken every year or sooner if new risks are identified. Where major compliance breach is identified, an independent auditor is engaged to review the procedure. The board of TCI must sign off on all risk management measures.

Transcash International Pty Ltd (***Transcash***) is registered on the Remittance Sector Register as a remittance network provider (***RNP***).

A RNP is a non-financier who operates a network of persons/ company by providing a platform or operating system where the persons in the network are also non-financiers and provide a designated remittance service (***affiliates***) to general public/ customers. As an RNP, the company has management and oversight obligations with respect to its affiliates, as outlined in this paragraph 7.2.

As an independent remittance dealer, Transcash provides remittance services directly to end-user customers.

As an RNP, we provide a systems platform to a network of affiliates. Our RNP business operates so that the direct interactions (of the company) are with the affiliate agent network, with end-customer contact being facilitated by the affiliate agents themselves (with the guidance and direction of Transcash’s policies and procedures).

When operating as an RNP, the company’s customer is the affiliate. However, when the company is operating as an independent remittance dealer, the customer is the ordering party (i.e. the sender of the funds). This has an impact on our ML/TF risk and on our KYC procedures.

A separate customised AML/CTF program has also been prepared by use for Transcash affiliate agents, which is to be made available for all affiliate agents, unless other consistent procedures satisfactory to us are in place. All affiliates are also obliged to comply with the RNP-agent agreement, which is prepared by us, and sets out the rules, rights, and obligations of affiliates in the context of the affiliate relationship.

Our RNP obligations are as follows:

- complying with all KYC procedures for affiliates as customers (see Part B)
- providing affiliates with an AML/CTF Affiliate Program;
- affiliate due diligence;
- providing affiliates with training;
- reporting TTRs, IFTIs, SMRs on behalf of affiliates;
- enrolment on the Reporting Entities Roll and registration on the Remittance Sector Register; and
- compliance review of Australia affiliate operations.

7.2.1 AML/CTF Program for affiliates

We have made available a standard AML/CTF Affiliate Program for our affiliates, a copy of which is kept at our offices.

Affiliates can choose to adopt the standard AML/CTF Affiliate Program as their AML/CTF Program. However, affiliates may also already have their own AML/CTF Program which can be retained, providing that we have advised in writing that we are satisfied that it is consistent with the company's policies and procedures, particularly with respect to Part B.

7.2.2 Due Diligence – affiliates

We conduct due diligence checks of affiliates as part of the application process to join the remittance network as an affiliate. We then determine the ML/TF risk associated with the affiliate, depending on:

- the affiliate's business model, including (for example) whether the affiliate's core business is foreign exchange and remittance, or whether the affiliate is operating a convenience store; and
- the customer base of the affiliate.

Depending on the ML/TF risk assessment assigned to the affiliate, as part of our affiliate recruitment processes, we carry out the following investigations in relation to the affiliates, prior to appointing them as affiliates or after their appointment, if, in the view of the AML/CFT compliance officer, these checks need to be conducted:

- identity verification of the affiliate (if it is a non-individual), in accordance with standard KYC procedures;
- electronic verification of identity using third party ID verification system;
- identity verification of all key personnel (as determined by Transcash);
- Criminal history check (National Police Check) of all key personnel;
- Right to work in Australia via Department of Immigration and Citizenship;
- Disqualified directors & other company officials check via ASIC website www.asic.gov.au;

- Enforceable Undertaking check via the ASIC website www.asic.gov.au; and
- Search engine check.
- Bank account validation of the entity

Records of the results of the screening processes are created, and the AML/CTF compliance officer reviews the results of the screening process, to consider whether the report includes any AML/CTF-related matters about the affiliate, which could be of concern to us. The AML/CTF compliance officer will review the reports with the Director for information and monitoring purposes.

Re-screening affiliates

Every year, we re-screen our affiliates, and again carry out the following checks and investigations:

- identity verification of the affiliate (if it is a non-individual), in accordance with standard KYC procedures;
- identity verification of all key personnel;
- criminal history check (National Police Check); and
- ASIC check, checking the disqualified register (ASIC).

The AML/CTF compliance officer maintains a record of the screening and investigations for the AML/CTF compliance requirements, in accordance to this policy. The compliance officer will re-screen on annual basis since the last screening process took place, and for trigger events requirements to re-screen the relevant affiliates (all records are retained by us).

Records of the results of the re-screening processes are created, and the AML/CTF compliance officer reviews the results of the re-screening process, to consider whether they name any AML/CTF-related matters about the employee, which could be of concern to us. The compliance officer will review the reports with the Director for information and monitoring purposes.

We also conduct KYC identification and verification procedures on our affiliates, as they are our customer for the purposes of providing designated service item 32A (see Part B of this Program).

7.2.3 Affiliate training

We provide the affiliates with training in relation to:

- our system and/or platform;
- the Act and the Rules;
- our obligations under the Act and the Rules;
- our policies and procedures as outlined in this Program;
- the consequences of non-compliance with our obligations;
- the nature and consequences of the ML/TF risks we may reasonably face;
- identifying customer procedures;
- ongoing due diligence procedures;
- suspicious transaction reporting; and
- record keeping obligations.

Training will be provided to all affiliates before they are appointed as affiliates. The training will be repeated annually. Affiliates will also be kept updated and trained in any changes to the law affecting their obligations.

Training methods are diverse, and include induction, on-the-job, e-learning (via austrac.gov.au and third party training providers), face-to-face training, and assessment quizzes.

Training varies depending on the person's role. For example, training provided to senior management is different to training for the customer-facing staff.

Evidence of training is recorded on our training register.

7.2.4 Reporting obligations: TTRs, IFTIs and SMRs for affiliates

As an RNP, we must report Threshold Transactions (***TTRs***) and International Funds Transfer Instructions (***IFTIs***) on behalf of affiliates. We have eliminated cash payments (starting from February 2022) meaning we do not accept any cash payments from the customers or affiliates so **Threshold Transactions Reporting** no more imply on us.

We upload all IFTI reports for affiliates.

We have in place a Suspicious Matter Report (SMR) process for affiliates.

The SMR procedure for affiliates sets out the affiliates' obligation to submit advice of all unusual matters which may constitute a suspicious matter directly to us. We then evaluate the report and if it is determined to be a suspicious matter, we assume the responsibility of submitting the SMR to AUSTRAC within the required time frames.

Although there are confidentiality requirements in place for suspicious matter reporting, network providers (like us) and our affiliates can communicate about such matters between ourselves.

We will submit the affiliates' Annual Compliance Reports on behalf of each affiliate.

7.2.5 Enrolment of affiliates on the Reporting Entities Roll and registration on the Remittance Sector Register

As a remittance network provider, we will apply for registration on the Remittance Sector Register, and enrolment on the AUSTRAC Reporting Entities Roll on behalf of our affiliates. We are obliged to ensure that the registration and enrolment details remain up to date.

7.2.6 Compliance review of affiliates

We conduct periodic reviews of the affiliates' operations annually.

The review process involves conducting an on-site visit of the affiliate at their business premises and includes a review of:

- the affiliate's KYC procedures and KYC records;
- the enhanced customer due diligence and transaction monitoring records; and

- the affiliate's compliance with the AML/CTF Affiliate Program.

The AML/CTF compliance officer will present the results of the review in a report to senior management, which will:

- identify any issues in relation to the affiliate's operations which arise from the review; and

- suggest strategies to manage any issues, which may include further AML/CTF training, additional supervision by us as the RNP and in some cases, reassessment of the affiliate's inclusion in the remittance network.

8. The Risk Management process

Transcash International Pty Ltd has implemented a risk management process as part of our Compliance Manual, which was created and is maintained to assist us to comply with the requirements of our Australian Financial Services License.

The risk management process which forms part of this AML/CTF Program is conducted in the same way as set out in our Compliance Manual (this document is available from our registered office upon request). The risk management process of TCI comprises of the following steps:

8.1 Identify the ML/TF risk

In identifying its ML/TF risk, Transcash International Pty Ltd. Considers:

- The **operational** or business risk, which includes the following considerations:
    - nature, size and complexity of our business;
    - types of clients to whom we provide the designated services (e.g., companies, trusts, partnerships, Politically Exposed Persons (PEPs);
    - types of designated services that we provide;
    - delivery methods of the designated services;
    - foreign jurisdictions we deal with; and
- the **regulatory** risk, which includes:
    - risk of enforcement or punitive action from AUSTRAC.

We, then, consider how each of the above factors impacts on the likelihood and consequences of ML/TF risk materialising. The considerations are made by deliberately ignoring controls in place to manage ML/TF risk; to ensure that inherent ML/TF risk[1] is properly assessed.

When these risks are identified, we ask the following questions:

- What can happen?
- When and where can it happen?

[1] Rule 4.1.3.

- How can it happen?
- Why can it happen?

Having identified the sources of risk, causes and scenarios are considered. We record the risks that we identify in the AML/CTF section of our Risk Register.

In this phase, TCI aims to generate a comprehensive list of events which may facilitate AML or CTF.

8.2 Analyze the identified risks

Transcash International Pty Ltd will, then look at each of the identified risks and ask: How **likely** is this risk event to occur and what are the **consequences** if it does occur? A qualitative and quantitative description of the size of each identified risk may be achieved. For example, **likelihood** can be scored from 1 (rare) to 5 (everyday event or certain) and **consequence** could be rated from 1 (insignificant) to 5 (extreme).

The **consequence of each identified risk is** considered in terms of the chance that our services could be used to launder money by:

- placing money;
- layering money;
- integrating money; or
- facilitating the transfer of funds to be used for terror financing in Australia or overseas

The **consequences** of each identified risk also include an assessment of these things on our:

- regulatory and legal requirements; and
- reputation and goodwill.

8.3 Evaluate the risks

When evaluating the risk, we give due considerations to the following**:**

8.3.1 The client types

If we reasonably believe that a client has information which could assist in complying with Part A, we can request that information from the client in writing. If the client does not provide the information within the specified period we may cease or restrict the services we provide. The client is, in most circumstances, prohibited from bringing legal proceedings against us for any problems arising from our ceasing or restricting the services to the client.

8.3.2 Politically Exposed Persons (PEP)

PEP is an individual who is or is being entrusted with prominent public functions in a foreign country. For example Heads of State, government, senior politicians, senior executives of state owned companies and important political party officials (not intended to include middle ranking or more junior officials). Because of the risks associated with PEPs, the FATF recommendations require the application of additional AML/CTF measures to business relationships with PEP.

Our KYC process for PEPs includes:

- ascertaining whether an individual customer or a beneficial owner of a non-individual customer is a domestic PEP, a foreign PEP or an international organisation PEP; and

- checking whether an individual customer or a beneficial owner of a non-individual customer is an immediate family member or close associate of a PEP.

- We do not accept PEPs once we have identified them

8.3.3 Consolidated List

The Department of Foreign Affairs and Trade (DFAT) maintains a list known as the Consolidated List; containing list of persons and entities who are subject to financial sanctions. This list is created to comply with Australia's UN commitments to freeze terror-owned funds. It is available on http://www.dfat.gov.au/sanctions/consolidated-list.html. We regularly monitor the Consolidated List. We also screen against UN Security Council List, OFAC, UN sanction lists and control lists issued by local regulator AUSTRAC. We check whether any individual customer or beneficial owner of a non-individual customer identified as a foreign PEP or an international organisation PEP is included in the Consolidated List.

8.3.4 Designated Services:

TCI recognizes that different types of designated services will have different ML/TF risks.

8.3.5 Delivery methods:

The method of delivery of the designated services will pose differing levels of ML/TF risks. For example, face to face transactions would involve a lower risk than remote access over the internet. TCI assesses the risk associated with the various delivery methods and has established mechanisms to mitigate these risks.

8.3.6 Foreign jurisdictions:

As TCI operates in foreign jurisdictions, we are exposed to the risk associated with it. The risk is posed because of

- the different legal frameworks; and
- the different AML/CTF controls.

8.3.7 The remittance network risk

We have considered the risks posed by operating a remittance network.

Examples of **remittance network risks** are:

- reliance on transactions involving cash
- the company has a low level of knowledge and understanding of the affiliate's customers
- affiliates who deal with high risk countries
- difficulty of supervising and standardizing the affiliates' compliance with AML requirements

8.3.8 The affiliate risks

We have considered the risks posed by appointing and supervising affiliates.

Examples of **affiliate risks** are:

- as most affiliates are small businesses, the affiliate's experience and understanding of correct KYC procedures is lower than that of companies who operate in the financial industry
- for affiliates, remittance services usually represents a small proportion of the affiliate's business revenue and thus AML/CTF compliance may be given a lower level of importance
- the company exercises a lower degree of control and influence over the affiliates, by virtue of them being third party organizations as opposed to company employees
- affiliates may not comply with the AML/CTF Affiliate Program
- affiliates may conduct non face-to-face transactions, or transactions on behalf of a third party
- affiliates may disclose may divulge confidential login details to others in order to access the company's system platform

8.4 Step 3: Treating the risks

The final stage of the risk management process is for us to decide in relation to each identified residual risk whether to:

1. **avoid the risk altogether** (e.g. by refusing to deal with the customer, or by only dealing with the customer if the AML/CTF compliance officer has personally assessed the customer); or

2. **control the risk,** that is, changing the likelihood or consequences (e.g. by audit and compliance programs, training, reporting to AUSTRAC, customer identification procedures as contained in Part B of this Program).

Documenting how we treat risks is critical to ensure that the appropriate action is taken.

Controlling the risks

We control our ML/TF risk in a number of ways. Our controls include the following steps:

1. customer data collection forms with in-built 'high risk' triggers;

2. this AML/CTF program;

3. Third Party Reference Checking Software is used

4. We only accept bank transfers.

These are also referred to in the Risk Register.

8.5 Process to identify and recognize changes in our ML/TF risk:

The Risk Management process includes a process to identify and recognize changes in the ML/TF risk. This process is as follows:

The AML compliance officer, at least every quarter, during our senior management meetings, is required to review the list of risks set out in the Risk Register, and to evaluate whether any of the risks have changed, or whether any additional risks should be added to the Risk Register. For example, new risks may need to be added to the Risk Register with review and ML/TF risk assessment must be conducted before TCI operate and implement the service, if TCI were considering offering:

- a new designated service; or
- a new method of delivering a designated service; or
- the implementation of new technology to deliver the company's designated service.

If there are any changes to the risks listed in the Risk Register, or there are any new risks to be added to the Risk Register, then the compliance officer will make the appropriate changes to the Risk Register, and evaluate the risks and controls as set out below, for each amended or inserted risk, before the new designated service, the new method of delivering the designated service, or the new technology is implemented by the Company. Review and ML/TF risk assessment must also be conducted if there are changes to the nature of business relationship, control structure or beneficial ownership of the customers. All review and ML/TC risk assessment must be documented in written and to be revisited at periodic basis.

8.6 Training

We ensure that all our employees who are involved with the provision of the designated services will undergo training in relation to:

- our obligations under the Act and the Rules;
- our policies and procedures as outlined in this Program;
- the consequences of non-compliance with the Act and the Rules;
- the nature and consequences of the ML/TF risks we may reasonably face and the potential consequences of such risk;
- identifying customer procedures;
- ongoing due diligence procedures;
- suspicious transaction reporting; and
- record keeping obligations.

Training will be provided to all relevant employees before they commence working at the Company. The training will be repeated at least annually. Employees will also be kept updated regarding any changes to the laws.

Training methods are diverse, and include induction, on-the-job, e-learning (via austrac.gov.au and third party training providers), and face-to-face training.

Training varies depending on the person's role. For example, training provided to senior management is different to training for the customer-facing staff. Please refer to part 6.4.7. Evidence of training is recorded on our training register.

8.7 Monitoring and reporting

Ongoing monitoring, reporting and documenting identified risks and the effectiveness of their treatment will provide a "paper trail" and assist us in improving processes over time.

For example, a review should include an assessment of risk management resources such as funding and staff allocation and may also identify any future needs relevant to the nature, size and complexity of our business. A review may be undertaken either internally or by an external auditor.

Ongoing review is critical because the context will change, bringing about new risks or diminishing old ones. For example, the possibility that we are not able to obtain professional indemnity insurance would post a major risk to the ongoing function of the organization in Australia.
The company will update NPC for all staffs every 6 months and will update any identification documents which are expired. If there is any issue, we will conduct a meeting with head of the staffs. Perform regular meeting once a month and highlight the compliance issue if there are any. and keep documents and minutes in office files. If there are any issue with staff, then we may need to terminate existing staff.

To effectively conduct on-going monitoring and reporting, TCI will include:

- Transaction monitoring program
- Enhanced customer due diligence program

Please refer to part 16.

8.8 Examples of risks to be evaluated:

The following risks are examples of AML/CTF risks which are included in the Transcash International Pty Ltd Risk Register. These risks are evaluated in accordance with the TCI's procedure.

8.8.1 Operational risk:

- Client type:
    - the client is an individual
    - the client is a company
    - the client is a trustee
    - the client is a partnership
    - the client is an incorporated association
    - the client is an unincorporated association
    - the client is a co-operative
    - the client is a government body
    - the client is involved in a complex business ownership structure with no legitimate commercial rationale
    - the non-individual client (for example a trust, company or partnership) has a complex business structure with little commercial justification, which hides the identity of the ultimate beneficiary of the client

- the client is involved in a business which involves significant amounts of cash
- the beneficial owners of a corporate client are hard to verify
- the client has income which is not from employment or from a regular known source
- the client has different levels of risk when using different designated services
- the client is in a position which may expose them to the possibility of corruption (a PEP)
- the client is new
- the client's business is primarily of a money remittance service nature
- the client's business is an unregistered charity, foundation or cultural association
- the client is represented by another person, such as under a power of attorney
- irregular client contact
- business activities of the client are inconsistent with the value of physical currency being collected or delivered

- Designated service
  - there is no clear commercial rationale for the client seeking the designated service
  - the designated service could be used for ML or TF
  - the client requests an undue level of secrecy regarding the designated service
  - the designated services are primarily of a private banking or wealth management kind
  - entering into an option contract with a client, which enables clients to move funds across jurisdictions
  - exchanging currency under a spot FX contract, forward FX contract or option contract, which enables clients to move funds across jurisdictions
- Method of delivery
  - the source of funds is difficult to verify
  - the transaction is a "one-off"
  - the client makes or receives payments to and from offshore accounts (eg electronically)
  - the client has access to offshore funds (eg cash withdrawal or electronic funds transfer)
  - the client makes withdrawal, transfer or drawdown instructions by phone or fax
  - the client makes withdrawal, transfer or drawdown instructions via the internet
  - wide variation in the value of physical currency collected or delivered
  - inconsistent pattern of denominations in physical currency collected or delivered
  - changes in frequency of collections or deliveries

- Foreign jurisdiction
    - the client is based in, or conducts business in a high risk jurisdiction
    - the client's business is registered in a foreign jurisdiction with no local operations
    - the client is making transactions involving known tax and secrecy havens
    - the client is making transactions with countries on an official sanctions list
    - the client orders a transfer in favor of foreign beneficiaries via an overseas bank account in the beneficiary's name

8.8.2 Regulatory risk:

- Failure to comply with the Act and/or the Rules
- Failure to obtain TCI's Board approval of the AML/CTF Program
- Insufficient or inappropriate employee due diligence
- Changes in Transcash International Pty Ltd's business functions which are not reflected in the AML/CTF program (for example, a new product or a new distribution channel)
- Failure to consider feedback from AUSTRAC
- Failure to conduct the 12 monthly review of the company's reporting obligations which includes a review of the following reporting requirements:
    - identifying suspicious transactions;
    - reporting threshold transactions;
    - reporting International Funds Transfer Instructions; and
    - submitting AML/CTF Compliance reports
- Failure to undertake an independent review of our AML/CTF program
- Implementing client identification procedures that fail to prompt requirement for ongoing client due diligence such as;
    - failing to detect where a client has not been sufficiently identified and prevent the client from receiving the designated service
    - failing to take appropriate action when a client provides insufficient or suspicious information in an identification check
    - failing to take appropriate action when identification document is neither an original nor a certified copy
    - failing to recognize foreign identification documents issued by a high risk jurisdiction
    - failing to record comprehensive details of identification documents like date of issue
    - failing to identify when old or expired identification documents have been used
    - failing to collect any other names by which the client is known

- Lack of access by TCI to information sources which identify high risk clients such as PEPs, terrorists and narcotics traffickers
- Lack of ability by TCI to train staff in client identification and transaction reporting procedures

8.9 Treating the risks

The final stage of the risk management process is for us to decide in relation to each identified residual risk whether to:

- **avoid the risk altogether** (e.g. by refusing to deal with the client, or by only dealing with the client if the AML/CTF compliance officer has assessed the client); or
- **manage the risk,** that is, changing the likelihood or consequences (eg by audit and compliance programs, training, reporting to AUSTRAC, client identification procedures as contained in Part B of this Program).

Documenting treatment of the residual risks is critical to ensure that the appropriate action is taken. We shall follow the steps set out in our Compliance Manual; which can be accessed at our registered office upon request.

9. Controlling the risks

Transcash International Pty Ltd mitigates its ML/TF risk through the establishment of control features. These are also referred to in the Risk Register; available from our office upon request. Some of the controls to the specified nature of risk are explained below.

9.1 Clients

We have a detailed client identification (initial and ongoing) process, explained in detail in Part B of this program. This Part B is designed to control the risks arising out of nature of the client. Through a prudent implementation and periodical review of the controls specified in Part B, we expect to minimize the associated risks.

9.2 Politically exposed persons (PEP)

TCI shall ask the customer to “self-identify” themselves as a politically exposed person. We shall also Endeavor to make use of other available resources like the internet, as far as possible, to determine the level of threat posed by these PEPS.

9.3 Consolidated List

TCI has integrated the consolidated list issued by DFAT in the system; which is updated on a regular basis. The details of the transfer are automatically screened against the fields in the consolidated list to ensure that such transactions, if any, are identified timely and accurately. In case of any such transfers arise, TCI is committed to file the suspicious transaction report to Austrac and freeze the corresponding funds.

9.4 Designated Services

To control this risk, TCI ensures that the unique ML/TF risks involved in the proposed designated service is appropriately assessed; prior to introducing a new designated service

9.5 Delivery methods:

TCI shall ensure that the customer conducts the transactions in person by visiting its office or our agent outlets. A repeat customer might not be required to visit in person, but it is mandatory for them to be present in person with the necessary documents; at least during the initial transfer.

9.6 Delivery method-funds

To minimize the threat of our designated services being used for money laundering and terrorism financing; we generally only accept up to AUD 7,500.00. All transfers in excess to this amount must be processed after collecting and verifying the proof of income such as payslips and bank statements of the customer.

10. Employee due diligence program

10.1 Employee Screening

To control ML/TF risk internally, TCI will ensure, as part of its employment processes that it carries out the investigations in relation to each employee, prior to commencing employment and if, in the view of the AML/CTF compliance officer such check is warranted. The compliance officer shall decide on the relevant type of the checks that need to be carried out. Some of the checks that may be required are:

- Criminal History Check (National Police Check);
- Previous disciplinary action by regulator or legal action taken for any matters before a court of law
- Taken advantage of the laws relating to bankruptcy
- Lived in high-risk countries (such as countries sanctioned by Australia)
- Right to work in Australia via Department of Immigration and Citizenship;
- Address verification/ Basic I.D. Check via Electoral Roll and Telephone Registry Searches;
- Employment References;
- Academic Qualification Check (all tertiary qualifications should be checked);
- Professional Recognition Check e.g., CPA, CA, AHRI etc.;

Records of the results of the screening processes are created, and the compliance officer reviews the results of the screening process, to consider whether the report includes any AML/CTF-related findings about the employee, which could be of concern to us. The compliance officer will report the findings to the board.

10.2 Re-screening employees

TCI may re-screen its employees after 2 years; based on the recommendation of the AML/CTF compliance officer.

In this process, the Criminal History Check (National Police Check) will be carried out.

Records of the results of the re-screening processes are documented, and the compliance officer reviews the results of the re-screening process, to consider whether the report includes any causes for concern. The compliance officer will report the findings to the board.

10.3 Transfer / Promotion Re-screening

Employees that are transferred or promoted into a role where she/he can facilitate money laundering or terrorism financing may be re-screened, at the discretion of the AML/CTF compliance officer.

10.4 Failure to comply with the AML / CTF Program

Any failures to comply with the AML/CTF Program must be reported to board by the AML / CTF compliance officer.

Any employee who fails, without reasonable excuse, to comply with any system, control, or procedure within this AML / CTF Program must, as a minimum, recomplete the AML /CTF Training Program. The board may also impose additional requirements after considering the failure, such as further training, termination of employment, removal of authorisation, or other punitive action.

11. Agent/Affiliate due diligence program

TCI uses agents to perform some of the tasks that is essential for the proper implementation of this AML/CTF program; mainly towards the ongoing customer due diligence program. So, it is equally important that the agents are appropriately screened, trained, monitored. If TCI's screening, training and monitoring reveals concerns, the agreement will be terminated.

11.1 Agent/Affiliate screening

TCI shall require the prospective agent to submit a police check no older than 6 months old for each of its key personnel before commencing the business. The police check is reviewed by the Compliance officer to ensure if there are any issues concerning our potential business especially regarding money laundering risk.

11.2 Agent/Affiliate training

The agents of the TCI shall be provided training on a regular basis. The training will make agents of TCI aware of the AML/CTF they face, and the appropriate course of action to address these risks. The training will cover:

TCI's internal policies and procedures;

The AML/CTF rules and regulations.

11.3 Agent/Affiliate rescreening

The agents of TCI shall be rescreened on the recommendation of the AML/CTF Compliance officer and in any event, at least every two years. During this process, the agent shall have to provide fresh police check report for all persons identified by the Compliance officer. The report shall be reviewed, and any relevant issues shall be reported to the board.

11.4 Failure to comply with the program

The performance of the agent shall be reviewed by the AML/CTF compliance officer with regards to AML/CTF risks, on a quarterly basis. If a threat is detected, the agent shall be immediately advised to take a specified course of action. If the agent is unable or unwilling to mitigate the risk as per the guidance of TCI, the Compliance Officer may recommend actions including terminating the relationship of the specified agent to the board.

12. Management Oversight

This program is approved by the board of TCI. In addition to period independent review, the AML/CTF Program is reviewed as a regular agenda item in board meetings.

13. AML/CTF Compliance officer

TCI shall appoint an AML/CTF compliance officer. This person must have independence, seniority, accountability, reporting lines, access to the executive or board, and relevant skills and experience.

13.1 Role of the compliance officer

The role of the compliance officer includes the following duties and responsibilities:

- ensuring continuing compliance with the obligations of the Act and the Rules, subject to the ongoing oversight of the Board, including:
    - AML/CTF risk awareness training for staff members;
    - the employee and agent due diligence program (and screening and re-screening programs);
    - liaison with senior management and/or board on AML/CTF issues and regularly reporting to the board and senior management on all compliance matters; and
    - ensuring that the processes and procedures set out in the AML/CTF Program are absolutely complied with by TCI
- acting as the contact officer for AUSTRAC matters such as reporting suspicious matters, international funds transfer instructions and threshold transactions, urgent reporting, compliance audits, or requests for information or documents;

- contributing to the design, implementation and maintenance of internal AML/CTF compliance manuals, policies, procedures and systems, including:
    - procedure for granting approvals for new designated services or delivery channels;
    - ensuring AML/CTF compliance is measured and if applicable, rewarded in the performance review process for employees and agents;
    - processes to allow staff and agents to report violations of the AML/CTF program confidentially to the AML/CTF compliance officer, with alternative arrangements undertaken if the AML/CTF compliance officer is implicated;
- updating core knowledge on ML/TF risks TCI may reasonably face, including any relevant legislative developments and AML/CTF publications, for example from the Financial Action Task Force (www.fatf-gafi.org) or AUSTRAC;
- providing leadership and contributing to a culture of AML/CTF compliance within TCI;
- conducting initial due diligence on and ongoing evaluation of any third-party AML/CTF compliance-related service providers;
- keeping relevant records in accordance with Part 10 of the Act; and
- amending and updating the AML/CTF Program and the Risk Management process and Risk Register, in conjunction with recommendations from its external compliance consultants and with the Board.
- obtaining disclosures from employees regarding potential suspicious matters or OCDD related queries;
- arranging for the employee's initial and ongoing training to take place;
- arranging for screening and rescreening of new and existing employee/agent respectively;
- monitor the performance of the staff and agents with respect to AML/CTF risks;
- coordinating the periodic independent audit of the Program
- review of AML policy/ Program of Business correspondent partner's regular intervals as integral part of compliance process.
- Compliance team shall engage in random transaction sampling on daily basis to check and ensure that proper AML/ KYC policy & program is adopted across.
- To prepare checklist for any new business relationship and clearance on document and/ or their AML/ KYC policy program.

14. Independent review

The AML/CTF compliance officer will ensure that this Programs independently reviewed regularly, and in any event at least on annual basis, either internally or externally by an independent reviewer who was not involved in the functions or measures being reviewed, and a report given to governing board and senior management.

In the independent audit; the auditor will consider:

- the effectiveness and adequacy of the ML/TF risk management system and controls;
- the changes of TCI's practices and policies in accordance to the changes of ML/TF risk profile
- the adequacy of the response to previous recommendations and post-implementation review
- the effectiveness of staff training
- the seniority and authority of the compliance officer in discharging his roles and responsibilities
- the source of issue for potential breaches or deficiencies and mitigation plan
- the effectiveness of AML/CTF compliance program implementation of other branches or subsidiaries
- whether the Program complies with the Act and the Rules; and
- the company's activities in relation to the following reporting requirements:
    - effectiveness of transaction monitoring systems in identifying suspicious transactions;
    - reporting threshold transactions;
    - reporting International Funds Transfer Instructions; and
    - submitting AML/CTF Compliance reports.
- In relation to all reports submitted to AUSTRAC during the 12 months period, the auditor will assess:
    - the number and details of all suspicious matter reports;
    - the number and details of all threshold transaction reports;
    - the number and details of all International Funds Transfer Instructions; and
    - the details of each AML/CTF Compliance Report.
- The Compliance Officer will present the results of the review in a report to the Board/senior management, which will:
    - elaborate the method and the scope of the testing
    - the size of the sample
    - identify any issues which arise from the review; and
    - suggest strategies to manage any issues, which may include further AML/CTF training, and/or an amendment to this Program.

Additional factors that could warrant more frequent independent review:

- Organisational changes, such as merger and acquisitions
- Changes of Company's ML/TF risk profile
- Significant changes of value and volume of transactions
- Significant changes to PART A of the Company's AML/CTF program
- Changes of the outsourcing partial of the Company's function
- New addition to the designated services/products, delivery channels, customer type

- Compliance deficiencies
- Enforcement actions by regulator
- Any other material triggers

15. AUSTRAC feedback

The AML/CTF compliance officer is responsible for reporting any feedback received from AUSTRAC to the board; and ensuring that appropriate follow up action occurs. And Compliance Officer shall keep proper record and reporting on the follow up action, if any.

16. On-going Customer Due Diligence

Under the Act, we are obliged to monitor our customers and their **transactions on an ongoing basis** (ongoing customer due diligence, or OCDD). OCDD is complementary to the Identifying Customers processes outlined in Part B of this Program.

OCDD helps us to:

- identify;
- mitigate; and
- manage;

any money-laundering or terrorism financing risks that may arise from providing services to our customers, which arise at any stage **after the initial customer identification process has been completed**.
The difference between customer identification and OCDD is that customer identification should be undertaken prior to us providing a designated service, and involves collecting and verifying initial KYC information.

16.1 What are the requirements of OCDD?

There are three mandatory components of OCDD:

Collection and verification of additional customer identification information:

As set out in the Identifying Customers section in *Working Document 1: Customer Risk Assessment*, prior to providing a customer with one of the designated services, we must collect information about their identity and verify this information. This is known as **initial KYC information**.

We have also defined trigger points in our program for collecting **additional** KYC information after the initial customer identification process is completed.

Some examples of trigger points include:

- if a customer or a beneficial owner is designated “High Risk” as set out in the KYC process above;
- if a customer or beneficial owner is a PEP;
- if we enter into a transaction with a party physically present in a foreign country or is a corporation incorporated in a foreign country;
- if a transaction for a significant amount occurs for example. AUD200,000;
- a customer makes multiple cash transactions of amounts less than AUD10,000;

- if a customer makes a significant change to the way that their account has operated in the past for example, if the customer's account details move off-shore to a "non-compliant" jurisdiction, or significant increase in the value or volume of transactions– amend as appropriate for your business;
- if we have doubts regarding a customer's identity (such as the use of aliases and/or a variety of addresses);
- if there are changes in the nature of the business relationship between a customer and its customers;
- if one of the triggers for the transaction monitoring program has been flagged; or
- if a suspicious transaction involving a customer has been reported to AUSTRAC.

All additional KYC information collected in accordance with this procedure is dealt with in accordance with our record-keeping obligations.

Transaction monitoring program

We have in place a transaction monitoring program to ensure that any discrepancies, anomalies and unusual or suspicious transactions are identified, and if yes, the appropriate monitoring and supervision measures are implemented in relation to that customer.

The transaction monitoring program highlights the transactions that might present an increased risk that ML/TF, tax evasion or fraudulent activities are taking place, and implements policies and procedures designed to manage and mitigate that increased risk.

Our transaction monitoring program includes the following procedures:

1. With appropriate risk-based approach, we monitor the transaction behavior of all customers, to identify whether any of the trigger points in the collection and verification of additional customer identification information section above are present

2. As part of our monitoring program, we also check whether any of the indicators of suspicious activity are present. Example: unusually large transactions and unusual patterns of transaction with no economic or visible lawful purpose.

3. If, as a result of the above procedures, the transaction monitoring program identifies a customer or transaction where a red flag has been triggered, we will implement the following controls:

    - collect and verify additional KYC information (see paragraph 13.1 above);
    - seek the approval of the AML/CTF compliance officer as to whether to continue with a specific transaction and whether to continue the business relationship with the customer;
    - Impose transaction limits on the customer, so that all transactions over 7500 are barred and processed only after justifying source of income is established.
    - place a hold on the customer's account until the red flag has been investigated and an acceptable explanation for the behavior is ascertained;

- only allow the customer access to our services if each transaction is reviewed and signed off by the AML/CTF compliance officer.

4. The transaction controls referred to above will remain in place for a minimum of 3 months and will only be removed with the approval of the AML/CTF compliance officer. If a customer is the subject of the transaction monitoring program more than twice in a 12-month period, then the customer will be barred from receiving our services.

.

Enhanced customer due diligence program

We have an enhanced customer due diligence program in place to assess and collect further customer information in situations where we determine that:

- there is a HIGH ML/TF RISK (as determined according to the Identifying Customer section in Part B);
- we are providing a service to an individual customer or a beneficial owner foreign PEP, or an immediate family member or a close associate of a foreign PEP;
- one of the grounds for reporting a suspicious transaction is present; or
- we enter into or intend to enter into a transaction and a party to the transaction is physically present in, or is a company incorporated in, a proscribed foreign country[2].

If any of the above triggers occur, we will:

- analyse the information that we have already collected and verified about the customer (including information about the beneficial owner, if applicable) - this will involve re-doing the procedure set out in *Working Document 1: Customer Risk Assessment*;
- then determine which information needs to be clarified, updated or obtained about the customer or the nature of their business with us;
- consider whether additional transaction monitoring procedures should be implemented for this customer;
- obtain further KYC information or beneficial owner information (if applicable), including identifying the source of the customer's wealth and funds;
- clarify the nature of the customer's business relationship with us;
- verify or re-verify beneficial owner information;
- undertake more detailed analysis of the customer's transactions in the past and in the future, including the purpose of the transactions, and the nature and level of transaction behavior (see transactions monitoring program above).
- seek senior management's approval whether TCI should continue the business relationship with customer, process the transaction and continue to provide the designated service to customer.

16.2 Who does this requirement apply to?

OCDD obligations apply to all customers who receive a designated service from us.

[2]AUSTRAC may declare a country to be a 'proscribed foreign country' in accordance with the AML/CTF Regulations. To date, AUSTRAC has declared that Iran is a proscribed foreign country.

17. Identifying a Suspicious Transaction

17.1 What will TCI look out for?

A suspicious transaction may arise during business dealings between TCI and the client. So, TCI shall look out for information about the client that maybe related to the following:

- tax evasion; or
- criminal activity; or
- money laundering; or
- financing of terrorists.

As a general rule, we will report any transaction that causes us or our employees to have a feeling of apprehension or mistrust about the transaction considering:

- its unusual nature or circumstances;
- the person or group that we are dealing with;
- all the other things that we know about that client; and/or
- the behavior (verbally or physically) of that person.

17.2 Indicators of Suspicious Transactions

Some of the indicators of the suspicious transactions are:

- becoming aware that false ID has been used;
- people who are unwilling to meet the ID requirements;
- false names on accounts;
- aliases and/or a variety of addresses;
- comments by the client about tax evasion or other illegal activity;
- unusual business dealings, particularly where significant amounts of money are involved in circumstances that are difficult to explain. For example, a client who transacts large amounts of cash which is inconsistent with the type of occupation or business in which the client is involved;
- activities of corporate clients, such as:
    - the use of the resources of a public company to further the private interests of the company's officers;
    - the payment of secret commissions;
    - skimming of profits to executive directors;
    - payment of large management fees to entities associated with directors or management;
    - directors or management fraudulently acting against the interests of their company;

- a client starts acting out of character and transacting unusual funds flows;
- a client performs (or wishes to perform) a transaction that does not appear to be driven by ordinary commercial considerations;
- a client seems to be under serious financial stress and normal rules of commerce appear to have been suspended;
- a client has businesses that operate in foreign jurisdictions, including “high risk” jurisdictions (eg. countries classified by fATF);
- a client has businesses that operate in secret jurisdictions, (eg. Cayman Islands);
- a client has businesses that operate in jurisdictions which have targeted financial sanctions and/or travel bans imposed by the United Nations Security Council (eg Iran, Libya, Syria or Zimbabwe);
- a client has ID documents that originate from a “high-risk” or “secrecy” jurisdiction (eg. Nigeria);
- a client’s background is unknown, or his/her reputation is suspicious;
- an element of disguise is involved in the client’s dealings;
- the client is known to be aligned or loyal to a cause whose objects are themselves suspicious;
- the identity and/or location of any beneficiary to the service is unknown or suspicious;
- customer appears to be attempting to transact unexplained wealth based on customer profile recorded;
- customer exhibits unusual concern and government reporting requirements and this Program, including any of our other related policies and procedures;
- customer is reluctant to provide information regarding business activities, or identification and business documents provided are vague or difficult to verify;
- upon request, the customer fails to indicate any legitimate source for their funds or wealth;
- customer opens accounts in the name of family members or nominees;
- customer is involved in unusually complex legal structures with no economic or logistical rationale;
- funds are received directly from high-risk jurisdictions or the transaction involves a bank account in a high-risk jurisdiction;
- customer’s account has unexplained or sudden transaction activity, particularly in accounts that had little or no previous activity;
- wide variation in the value of physical currency collected or delivered;
- inconsistent pattern of denominations in physical currency collected or delivered [for cash carriers;
- changes in frequency of collections or deliveries;
- large ‘one-off’ services;
- gaps in know your client (KYC) information;
- irregular contact with the client; or

- business activities of the client inconsistent with the value of physical currency being collected or delivered.

17.3 Examples of suspicious activity

17.3.1 Evasion or attempted evasion of tax

An individual made numerous international funds transfers to a tax haven in amounts just below the AUD$10,000.00 reporting threshold. The number of transfers sometimes exceeded 3 per day, from different bank branches. AUSTRAC established that more than AUD$800,000.00 was sent off shore over a 2.5 year period.

17.3.2 Supply of illicit drugs

An individual made daily cash withdrawals of AUD$4,500.00, over a three week period – a total of AUD$60,000.00 was withdrawn. The reports provided to AUSTRAC enabled law enforcement officers to connect a known drug dealer to the same client.

17.3.3 Money Laundering by the Retail Industry

A chain of department stores contracted a cash carrier to undertake prime count and cash register reconciliation activities. Each evening, road crews called at each of the client's retail locations to collect the cash and cash register records, which were transported to the carrier's depot where the cash was processed. The following morning, the cash carrier lodged the processed funds into its own bank account and credited the client's bank account with a single electronic payment. Over several months, the value of funds collected fluctuated widely. Cash carrier staff became concerned as there were several unexplained large transactions which appeared to be inconsistent with the client's retail business. The cash carrier submitted a suspect transaction report to the financial intelligence unit and a subsequent investigation by authorities identified several instances where the funds were the proceeds of criminal activity.

The examples in this section are set out for illustration purposes only and should be used as a general guide for determining a basis for TCI to report suspect transactions.[3]

18. Reporting a Suspicious Transaction

If at any time when dealing with a client we form a suspicion that an offence, tax evasion or other criminal activity may be taking place, a report must be provided to AUSTRAC **within 3 business days**. If our suspicion relates to the financing of terrorism, the Suspicious Matter Report must be submitted to AUSTRAC within 24 hours of forming the suspicion.

Paper versions of this report can be obtained from the Compliance Officer or by contacting Austrac on 1300 021 037.

[3] Examples taken from www.austrac.gov.au

18.1 Who is to be notified

The AML/CTF compliance officer is the liaison for submitting all suspicious transaction reports. All employees and officers of TCI will notify the AML/CTF compliance officer of their suspicions within **4 hours** of forming the suspicion.

We will **not** notify the client who is demonstrating suspicious activity and will **not** disclose to anyone outside the business any information about the existence or contents of the report. The prevailing rules stipulate that informing the same to the concerned client or to other party shall be an offence[4].

We understand that, we might be in breach of duty of confidentiality to the client, when informing the matter to AUSTRAC. However, the Act and the *Corporations Act* protect individuals and companies from any breaches of confidentiality in these situations. And failure to report a suspicion may constitute an offence.

18.2 Where must the report be sent to?

If the report is not completed electronically, the report must be sent to:

The Director (AUSTRAC)

PO Box 5516

West Chatswood, NSW 1515

If the amount of money involved is substantial; or if we know that the suspect will be leaving the country quickly, we will report urgent suspicious activity by phone on 1300 021 037, and then send the written report in the mail.

Transcash International Pty Ltd will do one of the following; to assist AUSTRAC's investigation within 2 days of the suspicion being formed

- Complete client identification if this has not already been done;
- Collect all relevant KYC information which relates to the client; and
- Verify the KYC information which relates to the client.

19. Threshold Transaction Report (TTR);

We understand that we must report all physical cash transactions (including e-currency transactions) where the total amount is at least AUD 10,000.00 ("threshold transactions"). The TTR must be submitted **within 10 business days** of the transaction taking place and must include details of the individual conducting the transaction (i.e. the agent of the client or the third-party depositor).

Since we have discontinued accepting cash payments (as from February 2022) Threshold Transaction Report (TTR) submission is not applicable for us.

[4] Section 123 of the Act

20. International Funds Transfer Instruction (IFTI):

Regardless of transfer value, we will report all client instructions to transfer money into or out of Australia, either electronically or through a remittance arrangement[5].The IFTI report must be submitted **within 10 business days** of receiving the IFTI.

Paper versions of this report can be obtained from the Compliance Officer or by contacting Austrac on 1300 021 037.

21. Other reporting requirements

21.1 AML/CTF compliance report

We are required to provide AUSTRAC with an AML/CTF compliance report, which sets out information about our compliance with the Act and the Rules. This will be submitted by paper document report or lodged electronically by the due dates.

21.2 Registration requirements

Transcash International Pty Ltd is registered with AUSTRAC as an independent remittance dealer as well as a remittance network provider. Because of this registration, TCI has the requirement to regularly update various information related to our business with Austrac; via Austrac online or paper based applications on specific periods/events.

22. Category of service provider

Transcash International Pty Ltd has been registered as an “independent remittance dealer” and a “remittance network provider” with Austrac.

As a remittance network provider, TCI is authorized to make the relevant application to AUSTRAC for the affiliate’s registration and discharge some of their affiliates’ obligations like reporting. TCI will also make available to their affiliates a standard AML/CTF program for their use. However, affiliates will be at liberty to adopt a different program for their own use, if desired.

Although there are confidentiality requirements in place for suspicious matter reporting, network providers and their affiliates will be able to communicate about such matters; between themselves.

Registration under this section will last for three years, after which it will require renewal via an application process.

23. Maintaining our enrolment requirements

We are required to enroll with AUSTRAC and provide the prescribed enrolment details via the AUSTRAC Online form.

[5] Section 45 of the Act

We must inform AUSTRAC within 14 days of any change in our enrolment details, including changes in:

- our business details, including:
    - business name
    - contact details;
    - primary place of business;
    - the foreign countries in which we have offices; and
    - the type of business we operate;
- our corporate structure, including:
    - changes to our ACN, ARBN or ABN;
    - changes in the legal structure through which we operate; and
    - our parent companies or subsidiaries (including those entities' contact details);
- our AFSL or ACL number;
- details of any foreign registrations or licenses;
- the business contact details, names and positions of any authorized individuals (including beneficial owners and officers of our business) or key personnel (including the AML/CTF Compliance Officer);
- whether any key personnel have been disciplined under the AML/CTF Act, or have been the subject of proceedings or enforcement actions, that reflected upon the person's competence, diligence, judgment, honesty or integrity;
- our annual earnings figure (where we have to provide earnings details to AUSTRAC) including any changes to our annual earnings figure within 14 days of finalizing and publishing our annual financial reports or statements.

We can notify AUSTRAC of these changes via AUSTRAC Online.

We are also required to be registered on AUSTRAC's Remittance Sector Register. We are currently registered as an independent remittance dealer and a remittance network provider.

We must inform AUSTRAC within 14 days of any change in our circumstances that could materially affect our registration, including changes in:

- our business details, including:
    - business name
    - contact details;
    - primary place of business; and
    - the type of business we operate;
- our corporate structure, including:
    - changes to our ACN, ARBN or ABN; and
    - our parent companies or subsidiaries (including those entities' contact details);
- our AFSL or ACL number;
- details of any foreign registrations or licenses;
- the business contact details, names and positions of any authorized individuals (including beneficial owners and officers of our business) or key personnel; and
- whether any key personnel have been disciplined under the AML/CTF Act or have been the subject of proceedings or enforcement actions, that reflected upon the person's competence, diligence, judgment, honesty or integrity.

We can notify AUSTRAC of these changes via AUSTRAC Online.

Registration on the Remittance Sector Register is valid for three years. The AML/CTF compliance officer is responsible for ensuring that we reapply within 90 days before the cessation of our registration and will also ensure that the registration of the affiliates remains current.

Remittance Network Provider

As a remittance network provider, we can apply to AUSTRAC for our affiliates' registration and we can discharge many of our affiliates' obligations, including KYC, suspicious matter reports and international funds transfer instruction reports and threshold transaction reports. Where an affiliate informs us of a change in their circumstances, we must inform AUSTRAC within 7 days. We must also apply for renewal of registration of our affiliates.

24. Designated Business Group

Transcash is not currently part of a Designated Business Group ('DBG') for the purposes of Chapter 2 of the Rules. A DBG is defined in section 5 of the Act as: "a group of 2 or more persons, where:

A. Each member of the group has elected, in writing, to be a member of the group, and the election is in force; and
B. Each election was made in accordance with the AML/CTF Rules; and
C. No members of the group are a member of another designated business group; and
D. The group is not of a kind, under the AML/CTF Rules, is ineligible to be a designated business group."

Another entity, should it wish to join Transcash to form a DBG, must be:

A. Related to Transcash within the meaning of section 50 of the Corporations Act 2001; and either

a) A reporting entity; or
b) A company in a foreign country which if it were resident in Australia would be a reporting entity; or

B. Providing a designated service pursuant to a joint venture agreement, to which each member of the group is a party; or
C. Otherwise permitted as per Chapter 2 of the AML/CTF Rules.

Transcash DBG's AMLCO ('Nominated Contact Officer') must notify the AUSTRAC CEO, in writing, in the approved form, of any of the following:

a) A withdrawal of a member from the designated business group; or
b) An election of a new member; or
c) The termination of the designated business group; or
d) Any other changes the details previously notified to the AUSTRAC CEO in respect of the Nominated Contact Officer or the designated business group
e) No later than 14 business days from the date on which the withdrawal, election of the new member, termination or changes takes effect.

Part B– Knowing Your Client

25. Purpose

The primary purpose of this Part is to set out the client identification procedures for different types of clients. This Part is also designed to meet any requirements set out under the Act and the Rules.[6]

TCI must reasonably identify and verify the clients by conducting Client Due Diligence (CDD) to ensure that:

- for individual clients, the clients are who they claim to be
- for non-individual clients, necessary measures are to be applied to identify and verify the beneficial owners and the existence of the business

In principles, CDD measures must include:

- Identification and verification of clients' identification information
- Identification and verification of beneficial owner(s) of non-individual clients
- Identification and verification for PEP clients (or related to PEP) and identify the source of funds for the transaction
- Purpose and intended nature of the transaction and business relationship

The above CDD measures must be conducted before on-boarding a new client and providing designated service of the Company.

26. Background

This Part sets out procedures for different types of:

- clients;
- services; and
- circumstances[7]

This procedure consists of risk-based systems and controls appropriate to the nature, size and complexity of our business and prepared in light of the risk that TCI's services may be used to facilitate money laundering or terrorism financing.[8] Some factors that could affect TCI's risk-based approach:

[6] Section 84.
[7] Section 88.
[8] Rule 4.1.2.

- Client types, whether the clients and its beneficial owners are PEP or related to PEP
- Source of funds of clients
- Purpose and intended nature of the transaction and business relationship
- Control structure of non-individuals clients
- Types of designated services that TCI provides
- Method of provision of the designated services
- Foreign jurisdictions from where the clients are originated from

See Part A for an assessment of this risk.

27. Identifying clients

Clients include individuals, companies, trusts and partnerships. A client may also be represented by an agent.[9] TCI follows the procedure as laid down in the *Working Document 1 Categorise, Identify, verify* **before** we provide a designated service to the client for the first time.

Working Document 1 Categorise, Identify, Verify is enclosed in the Appendix of this program.

27.1 For Individual Clients (Other than a sole trader)

As part of TCI's CDD measures, TCI will collect and take reasonable measures to verify:

i. Client's full name
ii. Client's date of birth
iii. Client's residential address
iv. Whether the client is PEP or related to PEP

The above information will be verified by requesting client to provide original or certified copy of primary photographic identification document from client. Where client is not able to provide the requested documentation, TCI may accept an original or certified copy of a secondary identification document, under the circumstances where a client is rated as medium or low ML/TF risk. All documents provided must not exceed the expiry date, if applicable. TCI may assume that the beneficial owner is the same person with the client unless there are reasonable grounds to consider otherwise.

27.2 For Individual Clients (Acting as a sole trader)

As part of TCI's CDD measures, TCI will collect and take reasonable measures to verify:

i. Client's full name
ii. Client's date of birth
iii. Client's full business name
iv. Client's full business address or residential address
v. Whether the client is PEP or related to PEP
vi. Australian Business Number (ABN) issued to client

[9] Section 89.

The above information will be verified by requesting client to provide original or certified copy of primary photographic identification document and a copy of business profile from client. Where client is not able to provide the requested documentation, TCI may accept an original or certified copy of a secondary identification document, under the circumstances where a client is rated as medium or low ML/TF risk. All documents provided must not exceed the expiry date, if applicable. TCI may assume that the beneficial owner is the same person with the client unless there are reasonable grounds to consider otherwise.

27.3 For Company (Domestic Company, Registered Foreign Company and Unregistered Foreign Company)

TCI will apply the necessary measures to verify the existence of the company and identification of its beneficial owners.

Domestic Company

As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

i. full name of the company as registered by Australian Securities and Investments Commission (ASIC)
ii. full address of the company's registered office and principal place of business, if any
iii. Australian Company Number (ACN) issued to the company
iv. whether the company is registered by ASIC as a proprietary or public company
v. if the company is registered by ASIC as a proprietary company, obtain the name of each director of the company
vi. the beneficial owners of the company
vii. whether the beneficial owner or director of the company is PEP or related to PEP
viii. if other than UBO/ Director, then matching authority of the person siging the transfer request
ix. principle business activity

The above information will be verified by requesting client to provide a reliable and independent documentation or electronic data, which includes the disclosure that verifies the information of all beneficial owners of the company. Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body. (Example: ASIC registration or other equivalent registration)

Registered Foreign Company

As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

i. full name of the company as registered by Australian Securities and Investments Commission (ASIC)
ii. full address of the company's registered office in Australia and principal place of business in Australia, if any
iii. Australian Registered Body Number (ARBN) issued to the company
iv. the country in which the company was formed, incorporated or originated
v. whether the company is registered by the relevant foreign registration body. If yes, the type of company (public company, private company, etc.)
vi. if company is registered as private company, obtain the name of each director of the company
vii. the beneficial owners of the company
viii. whether the beneficial owner or director of the company is PEP or related to PEP

ix. if the company is registered as foreign listed public company, identification and verification of the beneficial owner(s) is not required, which is subject to 'transparency of beneficial owner' disclosure requirements (whether by stock exchange rules or by law or enforceable means) which are, or are comparable to, the requirements in Australia
x. matching authority for business undertaking
xi. principle nature of business
xii. ID of authorized personal/ official

The above information will be verified by requesting client to provide a reliable and independent documentation or electronic data, which includes the disclosure that verifies the information of all beneficial owners of the company. Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body. (Example: ASIC registration or other equivalent registration)

Unregistered Foreign Company (Registered by relevant foreign registration body)
As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

i. full name of the company as registered with the relevant foreign registration body
ii. the country in which the company was formed, incorporated or originated
iii. identification number of the company issued by the relevant foreign registration body upon the company's formation, incorporation or registration
iv. full address of the company's registered office in the country of formation, incorporation or registration
v. the type of company which is registered with the relevant foreign registration body
vi. if company is registered as private company, obtain the name of each director of the company
vii. if the company is not registered by the relevant foreign registration body, full address of the principal place of business of the company in its country of formation or incorporation
viii. the beneficial owners of the company
ix. whether the beneficial owner or director of the company is PEP or related to PEP
x. if the company is registered as foreign listed public company, identification and verification of the beneficial owner(s) is not required, which is subject to 'transparency of beneficial owner' disclosure requirements (whether by stock exchange rules or by law or enforceable means) which are, or are comparable to, the requirements in Australia

The above information will be verified by requesting client to provide a reliable and independent documentation or electronic data, which includes the disclosure that verifies the information of all beneficial owners of the company. Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body.

27.4 For Partnership

TCI will apply the necessary measures to verify the existence of the partnership and identification of each of the partners.

As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

i. full name of the partnership and full business name as registered under any State or Territory
ii. country of which the partnership was established
iii. identify and verify the identity of one of the partners, including full name and residential address as per the CDD for individual clients, refer to part 26.1

iv. collect the full name and residential address of each partner. (not required if the regulated status of the partnership is confirmed by referring to a current membership directory of the relevant professional association)
v. the beneficial owners of each partner
vi. whether the beneficial owner or partner of the company is PEP or related to PEP

The above information will be verified by requesting client to provide a reliable and independent documentation and electronic data relating to the partnership, such as:

- a certified copy/extract of a partnership agreement
- a certified copy/extract of minutes of a partnership meeting

Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body.

27.5 For Trustee

TCI will apply the necessary measures to verify:

- the existence of the trust; and
- the name of each trustee and beneficiary, with description of each class of beneficiary of the trust has been provided.

Existence of the trust, TCI will collect and verify:

i. full name of the trust
ii. full business name of the trustee
iii. the type of trust
iv. country of which the trust was established
v. full name of the settlor, unless:
    a. the material asset contribution to the trust by the settlor at the time the trust is established is lesser than AUD$10,000
    b. settlor has deceased
vi. if any of the trustee is an individual, identify and verify the trustee including full name and residential address as per the CDD for individual clients, refer to part 26.1
vii. if any of the trustee is a company, identify and verify the company as per the CDD for company, refer to part 26.3
viii. if the trustees are a combination of individual and company, apply the necessary CDD measures for individual clients and company as per part 26.1 and 26.3

Beneficiaries, TCI will collect and verify one of the following:

- full name of each beneficiary of the trust
- details of the class, if the trust identifies the beneficiaries by reference to the membership of a class

Beneficial owner(s) of the trust, TCI will take reasonable measures to identify and verify:

i. the beneficial owners of the trust
ii. beneficial owner's full name and one of either the beneficial owner's date of birth or full residential address
iii. whether the beneficial owner(s) or related parties of the trust is PEP or related to PEP

The above information will be verified by requesting client to provide a reliable and independent documentation or electronic data, which includes the disclosure that verifies the information of the trust. Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body. (Example: certified copy/extract of the trust deed).

27.6 For Association (Incorporated and Unincorporated)

TCI will apply the necessary measures to verify:

- the existence of the association; and
- the name of any member of the governing committee of the association.

As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

For incorporated association:

i. full name of the association
ii. full address of the association's principal place of administration or registered office; or
iii. the residential address of the association's public officer (president, secretary or treasurer)
iv. identification number of the association, issued by the body responsible for the incorporation of the association (domestic or overseas)
v. full name of the chairman, secretary and treasurer or equivalent officer in the association

For unincorporated association:

i. full name of the association
ii. full address of the association's principal place of administration or registered office
iii. full name of the chairman, secretary and treasurer or equivalent officer in the association
iv. for the member(s), information required as per the CDD for individual clients, part 26.1

Beneficial owner(s) of the association, TCI will take reasonable measures to identify and verify:

i. the beneficial owners of the association
ii. whether the beneficial owner(s) or officer(s) of the association is PEP or related to PEP

The above information will be verified by requesting client to provide a reliable and independent documentation and electronic data relating to the association, such as:

- a certified copy/extract of the constitution or rules of the association
- a certified copy/extract of minutes of the association's meeting
- for incorporated association, ASIC registration or equivalent registration issued by relevant government body

Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body.

27.7 For Registered Co-operative

TCI will apply the necessary measures to verify:

- the existence of the co-operative; and
- the name of chairman, secretary or equivalent officer in the co-operation.

As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

i. full name of the co-operative
ii. full address of the co-operative's registered office or principal place of operations; or
iii. the residential address of the co-operation's secretary or other officer if no secretary within the co-operative (president or treasurer)
iv. identification number of the co-operative, issued by the body responsible for the incorporation of the association (domestic or overseas)
v. full name of the chairman, secretary and treasurer or equivalent officer in the co-operative
vi. the beneficial owners of the co-operative
vii. whether the beneficial owner(s) or officer(s) of the co-operative is PEP or related to PEP

The above information will be verified by requesting client to provide a reliable and independent documentation and electronic data relating to the co-operative, such as:

- a certified copy/extract of any register maintained by the co-operative
- a certified copy/extract of minutes of the co-operative's meeting
- information provided by the State, Territory or overseas body responsible for the registration of the co-operative

Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body.

27.8 For Government Body

TCI will apply the necessary measures to verify:

- the existence of the government body; and
- information about the beneficial owners of the government body, for certain kinds of government bodies.

As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

i. full name of the government body
ii. full address of the government body's principal place of operations
iii. whether the government body is an entity or emanation, or is established under legislation of the Commonwealth
iv. whether the government body is an entity or emanation, or is established under legislation of a State, Territory or a foreign country and the name of that State, Territory or country
v. Identification and verification of the beneficial owner(s) of a foreign government body. (Not required for an Australian Government entity).
vi. Determine whether each beneficial owner of the foreign government body is a PEP

The above information will be verified by requesting client to provide a reliable and independent documentation or electronic data, which includes the disclosure that verifies the information of the government entity. Such document or electronic data must be accurate, up to date, maintained and issued by the relevant government body.

27.9 For Agent (of and Individual Client, of a non-individual client and verifying officer)

Agents of clients who are individuals and non-individuals
TCI will collect:

- the full name of each agent acting on the customer's behalf regarding the provision of the designated service(s)
- evidence of the authorisation of the agent to act on behalf of the customer

TCI will apply risk-based approach to identify and verify the agent who are the agent of individual clients. TCI shall take additional measures to identify the agent based on the ML/TF risks posed.

Verifying officer
As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify:

i. full name of the agent
ii. the title of the position or role held by the agent with the customer
iii. copy of the signature of the agent
iv. evidence of the authorisation of the agent to act on behalf of the customer
v. the information of the verifying officer as per the CDD measures for individual clients, part 26.1
vi. the verifying officer to make and for the customer to retain, a record of all matters collected from point (i) to (iv) above

27.10 For Beneficial Owners

As part of TCI's CDD measures, TCI will collect and take reasonable measures to identify and verify the beneficial owner(s)'s:

i. full name
ii. date of birth
iii. full residential address

However, the above need not be applied, if:

- an Australian Government Entity; or
- a foreign listed public company, or a majority-owned subsidiary of such a company, subject to disclosure requirements (whether by stock exchange rules or through law or enforceable means) that ensure transparency of beneficial ownership

For clients who are individual, TCI may assume that the beneficial owner is the same person, unless there are reasonable grounds to consider otherwise.

28. Discrepancy

If we identify a discrepancy during the validation of KYC information, we will not provide services to the client and the AML/CTF Compliance officer will be notified immediately. An example of a discrepancy may include that the identification provided by the client appears to be forged, tampered with, cancelled or stolen.

If a discrepancy arises in the course of identifying and verifying a client's identity, we will not provide any of the designated services to the client until the discrepancy has been resolved.

Depending of the nature of the discrepancy, AML/CTF Compliance officer will require any or all of the following documents to establish the client's identity.

- Citizenship Certificate / Passport
- Birth Certificate,
- Change of name certificate;
- Electronic verification identity check;
- Proof of incorporation certificate; and/or
- Other documents relevant to the particular situation.

Following the review of these extra identity verification procedures, if the compliance officer still suspects that the client is not the person the client is claiming to be, the compliance officer must then report the discrepancy to the relevant authorities.

29. Re-verification

Where one or more of the client's material details have changed, e.g. name, place of address, etc., TCI will update our KYC information by going through the processes set out in the attached working document, titled "*Working Document 1 Categorise, Identify, Verify*".

Also, where the ID documents relied on to verify a client, have expired, we shall not provide any new service to them, until they have been re-verified using current documents.

30. Documentation

TCI keeps copies of the ID documentation on file for at least 7 years. All documents and information provided by clients must be in English. If clients provide documents in a language other than English, we will require clients to obtain a translated document by an accredited translator.

In the circumstances where TCI personnel understands the documents provided by clients in foreign language, TCI must ensure to facilitate the reference by all employees and able to demonstrate to AUSTRAC that verification has been conducted.