

Anti Money Laundering and Counter-Terrorism Financing Part A and Part B program

Transcash International Pty Ltd.

Suite 3, Level 1

49 York Street

Sydney NSW 2000

www.ipayremit.com

Tel: 02 9299 5898, 02 8355 0166

Facsimile: 02 8004 3328

AML CTF Program

1. Contents

2.	Record of adoption of AML/CTF Program	2
3.	Review of program.....	2
4.	Background.....	2
5.	Definitions:	3
6.	Anti-Money Laundering / Counter Terrorism Financing Policy.....	3
Part A – General		8
7.	Risk management.....	8
8.	The Risk Management process.....	9
9.	Controlling the risks	15
10.	Employee due diligence program.....	16
11.	Agent due diligence program	17
12.	Management Oversight.....	18
13.	AML/CTF Compliance officer	18
14.	Independent review.....	19
15.	AUSTRAC feedback	20
16.	On-going Client Due Diligence	20
17.	Enhanced Client Due Diligence.....	21
Part B – Knowing Your Client		22
18.	Purpose	22
19.	Background.....	22
20.	Identifying clients	22
21.	Identifying a Suspicious Transaction.....	23
22.	Reporting a Suspicious Transaction.....	26
23.	Threshold Transaction Report (TTR).....	27
24.	International Funds Transfer Instruction (IFTI)	27
25.	Other reporting requirements	27
26.	Category of service provider	27

2. Record of adoption of AML/CTF Program

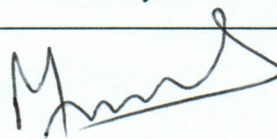
Section 116(2) of the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (Cth) ("the AML/CTF Act") requires a reporting entity to make a record of the adoption of its AML/CTF Program, and to retain that record for a period of 7 years.

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.

Approved by the Board of directors on 28 March 2014.

Certified by Company Secretary 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 reviewed and amended as follows

Date	Activities undertaken	Person responsible
16 Feb 2012	Review of program	Board of directors
10 Feb 2013	Review of program	Board of directors
28 Mar 2014	General review and updates	Board of directors

4. Background

Section 81 and 82 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the Act) 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) (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.
- “**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.
- “**Money Laundering**” is the processing of criminal profits to disguise their illegal origin;
- “**OCDD**” means ongoing client due diligence.
- “**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.

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 +612 9299 5898 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

We will refuse to enter into relationships with shell banks.

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. 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.

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, which enables our employees to understand:

- Transcash International Pty Ltd's obligations under the Act;
- The consequences of non-compliance with the Act;
- The unique ML/TF risks faced by us and
- The specific procedures which are relevant to our employees.

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 serious.

6.5 Roles and responsibilities

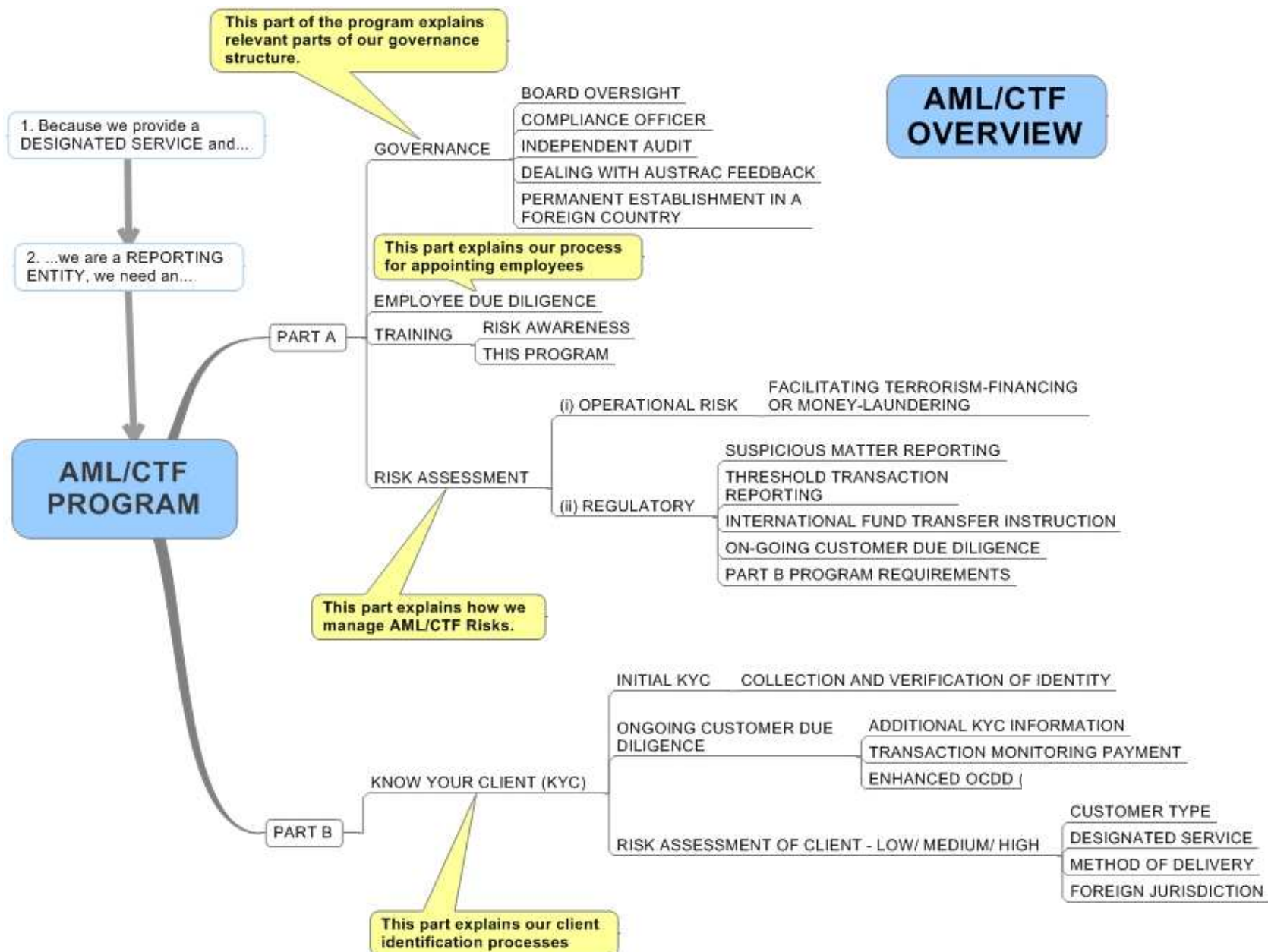
The Board and senior management of Transcash International Pty Ltd have ongoing oversight of the Policy and this Program.

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 Manohar Tiwari. This is the nominated person 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 and AML/CTF is a permanent agenda item of the board.

6.6 AML/CTF Overview

See mind map next page.



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”. The relevant services (known as “designated services”) of TCI are:

- entering into an option contract with a client (eg. Some FX and Derivative trading businesses)¹
- exchanging currency under a spot FX contract, forward FX contract or option contract (eg. FX companies and some derivative trading companies)².
- collecting physical currency, or holding physical currency collected, from or on behalf of a person, where:
 - the service is provided in the course of carrying on a business of collecting or holding physical currency; and
 - the physical currency was not collected by the provider of the service as consideration for the supply of goods (within the meaning of the Trade Practices Act 1974); and
 - the physical currency was not collected by the provider of the service as consideration for the supply of services (within the meaning of the Trade Practices Act 1974) other than the service of collecting or holding physical currency; and
 - the physical currency was not collected as a donation to a charity or charitable institution (eg. Cash carriers).³
- delivering physical currency (including pay-rolls) to a person, where the service is provided in the course of carrying on a business of delivering physical currency (eg. Cash carriers).⁴

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

¹ Item 35, section 6.

² Item 50, section 6.

³ Item 51, section 6.

⁴ Item 53, section 6.

- utilising 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.

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 Licence.

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 (eg, 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 risk⁵ is properly assessed.

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

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

⁵ Rule 4.1.3.

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 Analyse 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 type

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 was being entrusted with prominent public functions. 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.

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>.

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 Transcash International Pty Ltd 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.

8.4 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.

8.4.1 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
- Online Verification Risk
 - when we use online verification, the third party verification provider may provide inaccurate or incomplete verification data.

8.4.2 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

8.5 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** (eg 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.

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

The Risk Management process includes a process to identify and recognize changes in the ML/TF risk on a regular basis. This process to do so shall be as follows:

The AML compliance officer, at least every quarter, during TCI's board meeting or 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 if we are considering offering:

- a new designated service; or
- a new method of delivering a designated service; or
- 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 introduction of new designated service, the new method of delivering the designated service or the implementation of new technology.

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 the 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.

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 PEP.

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 in the placement stage; we generally only accept cash up to AUD 5,000.00. All transfers in excess of this amount have to be routed through the bank accounts.

9.7 Risk awareness training program for employees

TCI ensures that all of its employees who are involved with the provision of the designated services will undergo training. These trainings will be provided to all relevant employees before they commence working and is repeated at least annually. Employees will also be kept updated regarding any changes to the laws and rules. The trainings are designed to cover the following areas:

- the Act and the Rules;
- Policies and procedures as outlined in this Program;
- Identifying client procedures;
- Ongoing due diligence procedures;
- Suspicious transaction reporting;
- Record keeping obligations.

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);
- 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 eg 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 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 and if required, the agreement is terminated.

11.1 Agent screening

TCI shall require the prospective agent to submit a police check of not more than 6 months 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 training

The agents of the TCI shall be provided training on a regular basis. The trainings will aim to make them aware of the risks about the AML/CTF and their prescribed courses of action. In this regard, TCI shall provide training in various areas like TCI's internal policies and procedures, AML/CTF rules and regulations etc.

11.3 Agent rescreening

The agents of TCI shall be rescreened on the recommendation of the AML/CTF Compliance officer. 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 periodic 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 Transcash International Pty Ltd. In addition to the periodic 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
 - 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

14. *Independent review*

The AML/CTF compliance officer will ensure that this Program is independently reviewed regularly, either internally or externally, and a report given to governing board and senior management.

In the independent audit; the auditor will consider:

- the effectiveness of the ML/TF risk management system and controls;
- whether the Program complies with the Act and the Rules; and
- the company's activities in relation to the following reporting requirements:
 - 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 month 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:
 - 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.

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.

16. On-going Client Due Diligence (OCDD)

Under the Act, TCI is obliged to monitor its clients and their transactions on an ongoing basis (ongoing client due diligence or OCDD). OCDD is complementary to the Identifying Clients processes outlined in Part B of this AML/CTF Program and is applicable to all clients; who receive a designated service from us.

OCDD helps us to:

- identify;
- mitigate; and
- manage;

any money-laundering or terrorism financing risks that may arise from providing services to its clients, which arise at any stage after the initial client identification process has been completed.

The difference between client identification and OCDD is that client identification should be undertaken prior to us providing a designated service, and involves collecting and verifying initial KYC information.

16.1 Requirements of OCDD

There are three mandatory components of OCDD:

16.1.1 Collection and verification of additional client identification information:

As set out in the Identifying Clients section, prior to providing a client with one of the designated services, we must collect information about their identity and verify this information. This is known as **initial KYC information**.

TCI has also defined trigger points in its program for collecting **additional** KYC information.

Some examples of trigger points include:

- if a client is designated “High Risk” as set out in the KYC process;
- if a transaction for a significant amount occurs, for example AUD 100,000.00;
- a client makes multiple cash transactions of amounts less than AUD 10,000.00
- if we have doubts regarding a client's identity (such as the use of aliases and/or a variety of addresses)

16.1.2 Transaction monitoring program

TCI has a process which identifies any transaction activity that appears to be suspicious; that is, which have no apparent economic or lawful purpose. This process is set out in detail in the Identifying Suspicious Transaction section in Part B of this program.

16.1.3 Enhanced client due diligence program

Transcash International Pty Ltd has an enhanced client due diligence program in place to assess and collect further client information; in situations where you determine that:

- there is a high ML/TF risk (as determined according to the Identifying Client section in Part B); or
- One of the grounds for reporting a suspicious transaction (paragraph 22) is present.

In either case, we will:

- assess the information that has been already collected and verified about the client - this will involve re-doing the procedure set out in the Appendix;
- then determine which information needs to be clarified, updated or obtained about the client or the nature of their business with us; and
- consider whether additional transaction monitoring procedures should be implemented for this client.

17. Enhanced Client Due Diligence

The enhanced client due diligence system is outlined below in Part B – Know Your Client.

Part B – Knowing Your Client

18. 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

19. Background

This Part sets out procedures for different types of:

- clients;
- services; and
- circumstances⁷

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

See Part A for an assessment of this risk.

20. 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.

20.1 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.

⁶ Section 84.

⁷ Section 88.

⁸ Rule 4.1.2.

⁹ Section 89.

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,
- 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.

20.2 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.

20.3 Documentation

TCI keeps copies of the ID documentation on file for at least 7 years.

21. Identifying a Suspicious Transaction

21.1 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.

21.2 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;
- 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;
- client starts acting out of character and transacting unusual funds flows;
- client performs (or wishes to perform) a transaction that does not appear to be driven by ordinary commercial considerations;
- client seems to be under serious financial stress and normal rules of commerce appear to have been suspended;
- client has businesses that operate in foreign jurisdictions, including "high risk" jurisdictions (eg. Nigeria);
- client has businesses that operate in secret jurisdictions, (eg. Cayman Islands);
- 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);
- client has ID documents that originate from a "high-risk" or "secrecy" jurisdiction (eg. Nigeria);
- 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;
- 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.

21.3 Examples of suspicious activity

21.3.1 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.

21.3.2 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.

21.3.3 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 a number of 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 a number of 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.¹⁰

22. 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.

22.1 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 offence¹¹.

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.

22.2 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;

¹⁰ Examples taken from www.austrac.gov.au

¹¹ Section 123 of the Act

- Collect all relevant KYC information which relates to the client; and
- Verify the KYC information which relates to the client.

23. Threshold Transaction Report (TTR);

We will 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).

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

24. 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 arrangement¹². 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.

25. Other reporting requirements

25.1 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.

25.2 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.

26. 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

¹² Section 45 of the Act

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.