Anti-Money Laundering and Counter-Terrorism Financing Program

TraderQ operated by Ozifin Tech as authorised representative of AGM Markets Pty Ltd

(ACN 158 706 766)

CONTENTS

1. OVERVIEW

1.[1] The *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (**"AML/CTF Act"**) received Royal Assent on 12 December 2006. The broad purpose of the AML/CTF Act is to regulate financial transactions in a way that will help identify, mitigate and manage Money Laundering (**"ML"**) and Terrorism Financing (**"TF"**) risks.

1.2 The AML/CTF Act provides general principles and obligations while detailed operating rules are covered in Rules made by the Australian Transaction Reports and Analysis Centre (**"AUSTRAC"**). AUSTRAC is the government agency responsible for administering the AML/CTF Act.

1.3 ML involves the injection of funds generated from illegal activities into the legitimate financial system in order to hide or disguise the criminal source of those funds. TF is the use of money, which may or may not be generated from criminal activity, for financing terrorist activities.

1.4 Failure to comply with the AML/CTF laws may carry serious consequences, including both civil and criminal penalties. The maximum civil penalty is 20,000 penalty units ($3.6 million) for individuals and 100,000 penalty units ($18 million) for body corporates1. Penalties for criminal offences may include imprisonment for up to 25 years, fines of up to $1.8 million or both.

2. ABOUT THE AML/CTF ACT

2.1 The AML/CTF Act applies to persons who provide specified services (known as "**designated services**"). Persons providing designated services are called "reporting entities".

2.2 The AML/CTF Act adopts a risk-based approach. This approach means that the reporting entity will decide how best to identify, mitigate and manage the risk of ML and TF through its business. Reporting entities will therefore need to undertake a comprehensive assessment of these risks relative to their businesses. Reporting entities will need to be able to demonstrate to AUSTRAC that they have carried out such an assessment and have a program in place to identify, mitigate and manage the risk of their products or services being used to facilitate ML or TF.

3. SUMMARY OF GENERAL OBLIGATIONS

3.1 From 12 December 2007, reporting entities must:

a. have and carry out prescribed procedures to verify a customer's identity before providing a designated service;

b. adopt and maintain an AML/CTF program; and

c. have an AML/CTF Compliance Officer.

[1] Division 2, Part 15 of the AML/CTF Act

3.2 From 12 December 2008, reporting entities must:

a. report suspicious matters to AUSTRAC's Chief Executive Officer (**"CEO"**); and

b. undertake ongoing customer due diligence.

4. DEFINITIONS

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
AUSTRAC Guidance Note: Risk management and AML/CTF programs.	Part 6.6

4.1 Words and phrases defined in the AML/CTF Act or Rules have the same meaning when used in the AML/CTF Program (**"Program"**) of TRADERQ OPERATED BY OZIFIN TECH ("**OT**"), AS AUTHORISED REPRESENTATIVE OF AGM MARKETS, unless otherwise specified.

4.2 **Politically Exposed Persons** (**"PEP"**): Individual that holds a prominent public position or function in a government body or an international organisation. The definition now captures domestic and international PEPs, and also includes their immediate family members and close associates. Paragraph 1.2.1 of the Rules provides a non-exhaustive list of the positions, family members and close associates. Reporting Entities may decide to treat other individuals as PEPs after considering the associated ML/TF risks.

5. DESIGNATED BUSINESS GROUP

5.1 OT (a **Reporting Entity** (**"RE"**)) does not currently share obligations with another person, for the purposes of forming a Designated Business Group (**"DBG"**) under the AML/CTF Act and Rules.

5.2 Another entity can join with OT to form a DBG if:

a. that entity is:

i. related to each other member of OT DBG within the meaning of section 50 of the *Corporations Act* 2001 (Cth);

ii. either:

A. a RE;

B. a company in a foreign country which if it were resident in Australia would be a RE; or

C. providing a designated service pursuant to a joint venture agreement, to which each member of OT's DBG is a party; and

ii. not a member of another DBG; or

b. otherwise permitted by the AML/CTF Act or Rules.

5.3 In order to join OT 's DBG, a director or officer of the other entity will need to elect in writing (on behalf of that entity) to be a member of OT's DBG by completing the election form as specified by AUSTRAC at the time. The AML/CTF Compliance Officer will provide the completed form to AUSTRAC in the method specified by AUSTRAC.

5.4 When any of the following changes in OT 's DBG occurs, the AML/CTF Compliance Officer must notify AUSTRAC's CEO, in writing, by completing the approved notification form:

a. a withdrawal of a member from OT's DBG;

b. an election of a new member to join OT's DBG;

c. the termination of OT's DBG; or

d. any other change in the details previously notified to AUSTRAC's CEO in respect of the Nominated Contact Officer or OT's DBG.

5.5 Any of the changes listed in Section 5.4 of Anti-Money Laundering and Counter-Terrorism Financing Policy (**"Policy"**) must be approved by the Board of Directors of OT's DBG.

5.6 The AML/CTF Compliance Officer must provide the notification to AUSTRAC no later than fourteen (14) business days from the date the change takes effect.

6. AML/CTF PROGRAM ADOPTION AND REVIEW

6.1 OT adopts Parts A and B of this Policy as its AML/CTF program (**"OT's AML/CTF Program"**) for the purposes of the AML/CTF Act. OT must comply with OT's AML/CTF Program, as varied from time to time

6.2 This AML/CTF Program outlines how OT will meet its AML/CTF obligations.

6.3 This Program is to be reviewed by the AML/CTF Compliance Officer not less than every 12 months.

6.4 A report of the review, together with the recommendations, if any, of the AML/CTF Compliance Officer and any comments of the AML/CTF Compliance Officer, must be tabled at the next meeting of the Internal Compliance Department held after the report is completed.

6.5 In addition, this policy will be reviewed following any substantive changes to AML/CTF legislation or external factors such as regulatory feedback.

7. RECORDS RELATING TO OT 'S AML/CTF PROGRAM

7.1 The AML/CTF Compliance Officer will ensure that the following records are retained for each of OT:

a. AML/CTF Program and each variation;

b. Board of Directors' approval of this Program;

c. AUSTRAC's feedback, correspondence and any actions taken by OT as a result;

d. external, internal AML/CTF review reports and the associated follow-up actions; and

e. correspondence with external lawyers and/or consultants on AML/CTF issues.

7.2 The records referred to in Section 7.1 of this Policy will be retained:

a. in the case of records relating to the adoption of each variation to this Policy and OT's AML/CTF Program, during the period it or any part of it remains in force and for seven (7) years after it ceases to be in force; and

b. for the period of time determined by the AML/CTF Compliance Officer for all other records.

8. AML/CTF REPORTING

8.1 The reporting obligations that apply to OT and its AML/CTF functions, under sections 41, 43, 45 and 47 of the AML/CTF Act, are:

(a) Reports of suspicious matters;

(b) Reports of threshold transactions;

(c) Reports of international funds transfer instructions;

(d) AML/CTF Compliance Reports;

(e) Changes in enrolment details.

PART A

9. INTRODUCTION

9.1 Part A of this Program is designed to identify, mitigate and manage the risk that OT may reasonably face by its provision of its designated services, at or through a permanent establishment of that entity in Australia, might involve or facilitate ML or TF.

10. ANALYSIS AND ASSESSMENT OF ML/TF RISK

10.1 In determining and putting in place appropriate risk-based systems and controls to identify, mitigate and manage ML/TF risks in Part A of this Program, OT has had regard to the following factors:

(a) the nature, size and complexity of its business; and (b) the type of ML/TF risk that it might reasonably face.

10.2 OT has also considered the following factors when identifying OT's exposure to ML and TF, the:

a. customer types (including beneficial owners of customers and PEPs);

b. customers' sources of funds and wealth;

c. nature and purpose of the business relationship with customers;

d. control structure of non-individual customers;

e. types of designated services provided;

f. methods by which those services are delivered; and

g. foreign jurisdictions with which it deals.

Each of these factors are discussed below.

10.3 Customer Types

OT mainly deals with individual customers based in Australia and overseas, with occasional company and trust customers.

Different types of customers may pose different levels of ML/TF risks to the reporting entity. The more complex the structure of a customer, the more potential ML/TF risks a customer may carry. Beneficial ownership and politically exposed persons need to be taken into consideration.

"Beneficial owner" refers to an individual who ultimately owns or controls (directly or indirectly) an entity. Owns means direct or indirect ownership of 25% or more. Control includes control as a result of, or by means of, trust, arrangements, agreements, understanding or practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to determine decisions about financial and operating policies.

Politically Exposed Person ("PEP") refers to an individual that holds a prominent public position or function in a government body or an international organisation. The

definition now captures domestic and international PEPs, and also includes their immediate family members and close associates. Paragraph 1.2.1 of the Rules provides a non-exhaustive list of the positions, family members and close associates. Reporting Entities may decide to treat other individuals as PEPs after considering the associated ML/TF risks.

Individual customers who reside in Australia are relatively easy to identify and verify. Australian based companies and trusts are reasonably easy to identify and verify. However these structures, when domiciled overseas, may bring more challenges to the KYC process. OT considers the ML/TF risks imposed by different types of customers it deals with to be between low and high.

The on-boarding process of non-individual customers also identifies and verifies the beneficial owners of all non-individual entities in order to determine the individuals who ultimately exercises control over these entities.

All prospective customers are subject to PEPs screening. Once OT deems a person as a PEP, they are considered to carry high ML/TF risks and the customer identification procedures for high risk customers will apply. Senior management approval will be obtained before OT can provide any designated service to the customer in this case.

10.4 Customer's Source of Funds and Wealth

Information on a customer's source of funds and wealth provides valuable insights in to the reasonable amount of transactions that the customer is likely to be able to fund. Generally, the higher a customer's transaction amount and the more frequent the transactions, the more information may be required from the customer and more verification could potentially be carried out in order for OT to be reasonably certain that the customer's funds are from legitimate sources.

The vast majority of OT's customers are individual customers who use our services to conduct speculative trading on the currency market in the over the counter environment. A small proportion of clients use their Self Managed Superannuation Fund to trade generally to diversify their investments. OT may collect (and/or verify) financial information from customers in order to be reasonably certain that the sources of the funds used by clients are from legitimate sources. Generally OT considers the ML/TF risks poste by the sources of client funds and wealth to be low to medium.

10.5 Nature and Purpose of Business Relationship with Customers

OT 's core business is to facilitate retail traders to gain exposure to currency market movements through the over-the-counter derivative products. The vast majority of our customers are individuals who wish to make profits from trading on margin FX products. A small portion of customers conduct their trading through their SMSF as a diversification of their portfolios and to achieve tax savings.

OT considers the ML/TF risks posted by the nature and purpose of our business relationship with our customers to be low to medium.

10.6 Control Structure of Non-Individual Customers

OT has a small portion of non-individual customers. The majority of nonindividual customers are SMSF customers that use Margin FX as part of their overall portfolio investment strategies. Typically theses customers will have individual trustees who are also the sole beneficiaries of the trust. Alternatively there may be a private company as a trustee, whose directors are also the beneficiaries of the trust. Complex, multi-layered structures are very rarely used by customers. OT may collect and/or verify financial information from these customers in order to understand their purposes of utilising our services, and to assess the ML/TF risks the customers pose. OT generally considers the control structure of non-individual customers to pose low to medium ML/TF risks.

10.7 Designated Services:

Designated services that OT currently provides include:

a. Item 33 of section 6 of the AML/CTF Act (in the capacity of agent of a person, acquiring or disposing of a security, or derivative or foreign exchange contract on behalf of the person); and

b. Item 35 of section 6 of the AML/CTF Act (issuing or selling a security or derivative to a person)

OT considers the above designated services to carry approximately medium ML/TF risks, which may include but not limited to the following factors:

a. Customer transactions may involve large sums of money;
b. OT's services appeal to a wide range of clients, including retail and wholesale clients, and clients with various backgrounds in various jurisdictions;
c. OT has a large client base, which may bring challenges in terms of customer due diligence and the ongoing monitoring obligations;
d. OT 's services may appeal to PEPs.

10.8 New Offerings

Prior to a new designated service being introduced to the market by OT, the AML/CTF Compliance Officer will thoroughly evaluate the ML/TF risks associated with such offering, establish and implement corresponding risk-based systems and procedures to ensure that offering new designated services will not lead to material increase of OT's ML/TF risks.

10.9 Methods of Delivery

The designated services are delivered electronically through the reporting entity's website and online trading platforms, once the customer identification process has been successfully completed. When a prospective customer wishes to utilise OT's services, they are required to complete an application form on OT's website which collects the required information as set out in Part B of this Program. Document based and/or electronic data sources may be used to verify the customer's identity. If the customer can be successfully identified and verified, OT may provide the customer with the requested designated services. OT considers this method of delivering its designated service to carry medium level of ML/TF risks.

Before any new methods of delivery can be adopted, the AML/CTF Compliance Officer will evaluate the ML/TF risks imposed by the proposed methods of delivery, establish and implement risk-based systems and controls to manage such risks.

10.10 Foreign Jurisdictions

OT provides its designated services in Australia. However it recognises that due to the borderless nature of online trading it may attract customers that are located in foreign jurisdictions. For every jurisdiction that OT transacts with, the AML/CTF Compliance Officer will evaluate the jurisdiction and implement appropriate risk-based systems and controls to manage and mitigate the associated ML/TF risks before it begins to deal with these countries. Factors to be considered include:

(1) Sanctions imposed by Department of Foreign Affairs and the United Nations;

(2) Membership and observer-ship with FATF and the associated regional FATFstyled bodies;

(3) Maturity of the local financial system;

(4) Local AML/CTF frameworks and regulations;
(5) Whether the country is an offshore financial centre;

(6) Any prominent issues such as illicit drugs trafficking, human trafficking, illicit arms trafficking, terrorism groups and activities, and corruption.

Each country will be risk rated as low, medium, high risk or do not deal as a result of the evaluation. The jurisdictions where OT 's customers are located can range from low to high in terms of the ML/TF risks.

10.11 New and Developing Technologies

Prior to the adoption of a new technology used for the provision of a designated service, the AML/CTF Compliance Officer will assess it to determine whether it involves a new or increased ML/TF risk.

10.12 Identification of Significant Changes in ML/TF Risks

The AML/CTF Compliance Officer is responsible for monitoring the ML/TF risk exposures on OT 's behalf. The person will produce a monthly compliance report which will summarise the monitoring activities undertaken during the month, key findings and any recommended actions if applicable. The report will also document the number of SMRs submitted during the reporting period. Any trends that can be identified will be reviewed as they may indicate systematic issues with the AML/CTF policies and procedures, or potentially a change in ML/TF risks faced by the business.

The AML/CTF Compliance Officer is also to conduct the risk assessment every 12 months, and more frequently if deemed necessary, to ensure that any changes in the ML/TF risks can be addressed in a timely manner and that OT's AML/CTF measures remain sufficient and up-to-date. In making this assessment, the Officer will:

i. Take into account the nature, size and complexity of OT's business; and how this will change with the new introduction or adoption;

ii. Take into account the customer type, designated service and jurisdictional ML/TF risks that could be increased or introduced;

iii. Assess the compatibility of OT's AML/CTF Program with the new or increased ML/TF risk;

iv. Produce a report of the AML/CTF Compliance Officer's:

a. findings in relation to new or increased ML/TF risks; and

b. recommendations of appropriate changes to the Program;

v. Present the report to OT's Board, to effect implementation of the recommendations.

vi. A copy of the AML/CTF Compliance Officer's report must be kept on record.

vii. Where it is determined that a new or increased ML/TF risk is involved, the AML/CTF Compliance Officer will recommend amendment of OT's AML/CTF Program and its practices, to reflect the change.

viii. Any risk-based procedure included in Part B will only be appropriate if it takes into account the nature, size and complexity of OT's business, as well as the type of ML/TF risks it might face. The AML/CTF Compliance Officer must abide by this principle when assessing a new or increased ML/TF risk. The AML/CTF Compliance Officer must have regard to the ML/TF risks relevant to OT's provision of designated services.

11. APPLICATION OF PART A

11.1 Part A of this Program applies to OT in relation to all areas of its business that are involved in the provision of a designated service, including any functions carried out by a responsible third party.

11.2 The procedures in Part A apply on and from April 2014.

12. THE AML/CTF COMPLIANCE OFFICER

12.1 OT's Compliance Manager has been appointed as:

(a) The AML/CTF Compliance Officer for the purposes of the AML/CTF Act and Rules; and

(b) Appointed by OT as its Nominated Contact Manager for the purposes of the AML/CTF Rules.

12.2 The AML/CTF Compliance Officer will at all times:

(a) be part of the management of OT;

(b) report directly to the CEO of OT; and

(c) possess sufficient skills and experience to carry out the role of the AML/CTF Compliance Officer.

12.3 The AML/CTF Compliance Officer is responsible for implementing and overseeing OT 's obligations under the AML/CTF Act and Rules in accordance with OT 's compliance procedures. Their main responsibilities include the following:

a) Manage this AML/CTF Compliance Program;

b) Manage the ML/TF risk awareness training for new staff and on an ongoing basis;
c) Facilitate employee due diligence;

d) Produce regular reports regarding OT's compliance with this Program, in particular, any systematic issues identified and the corresponding solutions;

e) Manage OT's reporting obligations to AUSTRAC;

f) Be the point of contact for all AUSTRAC feedback and communication. Facilitate investigations when required by AUSTRAC;

g) Conduct periodic reviews of this Program;

h) Organise independent review of Part A of this Program to be conducted on a regular basis.

12.4 The AML/CTF Compliance Officer is authorised to delegate any of h i s responsibilities under this Program, the AML/CTF Act or Rules to another OT employee, agent or responsible third party provided it is reasonable to do so. The AML/CTF Compliance Officer's responsibilities may be undertaken in conjunction with an external compliance consultant.

13. EMPLOYEE DUE DILIGENCE PROGRAM

13.1 OT has adopted risk-based employee due diligence processes. The higher ML/TF risks a particular job function may carry, the more due diligence is to be conducted on the prospective employee before they are offered employment with the reporting entity.

13.2 New Employees

(a) The AML/CTF Compliance Officer must be informed of all prospective new employees before they are issued with an employment contract.

(b) For all newly created roles, a risk assessment must be undertaken of that role to determine the level of ML/TF risks they carry.

(c) The following procedures are to be carried out for prospective employees before they are offered employment with OT:

(i) Face to face interview(s);

(ii) Obtain a copy of the most up-to-date resume;

(iii) sight the original and make copy of the prospective employee's passport and visa where the employee is not an Australian citizen;

(iv) carry out at least one reference check;

(v) sight the original and make copies of all tertiary educational qualifications or, if none, the person's highest educational qualification;

(v) carry out a criminal history check with the Australian Federal Police (**"AFP"**) (subject to (e) below); and

(vi) carry out a bankruptcy check (where it is a director or senior management role only);

(d) Any other due diligence procedures that the AML/CTF Compliance Officer deems appropriate given the nature of the role and the individual's background.

(e) The procedures in Section 13.2 of this Program will be carried out before an employment offer is made unless the AML/CTF Compliance Officer decides otherwise having regard to the ML/TF risk associated with the position of the prospective employee and any other reason(s) why they cannot be completed beforehand.

(f) If a prospective employee fails, without reasonable excuse, to comply with these procedures, then OT may decide not to offer that person employment.

(g) Employment contracts issued will include a clause stating that employment within OT is conditional on passing the checks outlined in OT's AML/CTF Policy.

(h) If an offer of employment has already been made, and the prospective employee does not co-operate with the above procedures or the results of the checks are not satisfactory, then OT may withdraw the offer.

13.3 Existing Employees

(a) The due diligence procedures outlined in section 13.2(c) are to be repeated for all employees on regular basis.

(b) Where it is proposed that an employee will be transferred or promoted from a role with lower ML/TR risks to a role with higher ML/TF risks further due diligence may be carried out as per AML/CTF Compliance Officer's instruction.

(d) Employees who fail to comply with the procedures above will be reported to OT's Compliance Manager. Appropriate disciplinary action, including termination of employment, will occur where it is deemed necessary.

13.4 Copies of employee checks undertaken in accordance with Sections 13.2 and 13.3 of this Program will be kept in accordance with the OT's Document Retention Policy.

13.5 Managing Non-Compliance

(a) OT will, on an ongoing basis, monitor its employees' compliance with this Program.

(b) The employees' compliance with this Program will be monitored in a number of ways and may include, subject to applicable laws, surveillance of an employee's activities in the workplace.

(c) An employee who fails to comply with this Program will be reported to the AML/CTF Compliance Officer. Appropriate disciplinary action, including official warnings and termination of employment, may occur where it is deemed necessary.

14. RISK AWARENESS TRAINING PROGRAM

14.1 The Risk Awareness Training Program (**"RATP"**) is designed to ensure each employee of OT receives appropriate ongoing training on the ML/TF risks that OT may face and have up-to-date knowledge and tools to manage the ML/TF risks entailed in their job functions.

14.2 The RATP is designed to enable OT 's employees to understand:

(a) OT's obligations under the AML/CTF Act and Rules;

(b) the consequences of non-compliance with the AML/CTF Act and Rules;

(c) the type of ML/TF risk that OT might face and the potential consequences of such risk; and

(d) those processes and procedures provided for by this Program which are relevant to the work carried out by the employees.

14.3 Employee AML/CTF Training

(a) The AML/CTF Compliance Officer is responsible for organising an AML/CTF induction for all new employees within a reasonable period of time from the commencement of their employment.

(b) All staff members are required to attend regular AML/CTF refreshers organised by the AML/CTF Compliance Officer, to ensure that all employees are equipped with adequate knowledge to manage the ML/TF risks in their roles.

(c) Attendance is recorded in the Training Register in accordance with OT's Document Retention Policy.

(d) At the discretion of the AML/CTF Compliance Officer, additional training may be provided to employees whose job functions carry higher ML/TF risks when required. The training requirement may be imposed on third party service providers where appropriate.

(e) Non-attendance at an AML/CTF seminar by an employee, without reasonable excuse, will be reported to the CEO and appropriate disciplinary action will be taken at the request of the AML/CTF Compliance Officer.

14.5 Document Retention Policy

(a) The AML/CTF Compliance Officer will require each:

(i) new employee to read a copy of OT's Document Retention Policy within a reasonable time of commencing their employment; and

(ii) employee to read a copy of OT's Document Retention Policy on a regular basis as determined by the AML/CTF Compliance Officer.

(b) Employees who fail, without reasonable excuse, to read OT's Document Retention Policy will be reported to the CEO. Appropriate disciplinary action will be taken at the request of the AML/CTF Compliance Officer.

15. OUTSOURCING

15.1 Where OT outsources any of its AML/CTF obligations, it will:

a. have an agreement in place with the party to whom the activities are outsourced;

b. where relevant, require the parties to whom the activities are outsourced to implement policies and procedures similar to those outlined in this AML/CTF Program;

c. assess the ML/TF risk associated with the outsourcing of the particular activity;

d. conduct due diligence on the activities outsourced to ensure that outsourcing these activities and services is not materially increasing the ML/TF risk faced by OT;

e. conduct due diligence on the parties to whom the activities are outsourced to ensure that outsourcing activities to these parties is not increasing the ML/TF risk faced by OT;

f. ensure that all parties to whom the activities and services are outsourced understand:

i. OT's obligations under the AML/CTF Act and Rules;

ii. the consequences of non-compliance with the AML/CTF Act and Rules;

iii. the type of ML/TF risk OT might face and the potential consequences of such risk; and

iv. those processes and procedures provided for by this Program that are relevant to the work carried out by the employee.

g. OT is to closely monitor the performance of the service provider to ensure that the service received is satisfactory and will not materially increase the ML/TF risks faced by OT.

16. PROVISION OF DESIGNATED SERVICES THROUGH PERMANENT ESTABLISHMENTS IN FOREIGN COUNTRIES

16.1 OT does not provide designated services through permanent establishments in foreign countries.

16.2 If at any time OT plans to provide designated services at or through permanent establishments in foreign countries, the AML/CTF Compliance Officer will evaluate the ML/TF risks associated with the particular and establish and implement risk-based procedures to ensure that the operations in the foreign jurisdictions comply with the relevant AML/CTF requirements in Australia and in the local country.

17. RECORD KEEPING OBLIGATIONS RELATING TO CUSTOMER IDENTIFICATION AND THE PROVISION OF DESIGNATED SERVICES

A copy of this Program, and a copy of each historical version of this Program are to be kept on file for a minimum of 7 years from the date when the Program ceases to be in use. Other records to be kept for 7 years include:

(1) The Board of Directors' approval of Part A of this Program and any subsequent changes and variations of it;
(2) Compliance reports produced by the AML/CTF Compliance Officer and records of any follow-up actions as a result;
(3) SMRs and the Annual Compliance Reports;
(4) Customer transactions records;
(5) Customer identification and verification records;
(6) Employee due diligence records;
(7) AML/CTF risk awareness training program training materials and the attendance records;
(8) Reports produced as a result of internal or independent reviews of this Program and implementation of any amendments to the AML/CTF compliance policies and procedures;
(9) AUSTRAC communication, feedback and instructions;
(10) Any other records that may be relevant to ensuring OT's compliance with the AML/CTF requirements.

18. SUSPICIOUS MATTER REPORTING

18.1 Unusual Matters and Suspicious Matters Reporting

The AML/CTF Compliance Officer the designated persons authorised to form a suspicion on behalf of OT for the purposes of Section 41 of the AML/CTF Act. Where the AML/CTF Compliance Officer is absent, one of the directors will be designated as a substitute to handle Unusual and Suspicious Matter reporting.

If an employee or representative observes that a prospective or existing customer and/or their agent is behaving unusually given their financial backgrounds, account transaction patterns (if applicable), so that the employee or representative reasonably believes that the individual(s) may not be who they claim to be, may be involved in ML/TF activities, or may be relevant to any offence or proceeds of crime, or any other offences under federal laws, or the laws of the States or Territories, the employee or representative is to notify the AML/CTF Compliance Officer immediately by filing a Unusual Matter Report.

Under no circumstances should an employee or representative who has submitted an Unusual Matter Report or has assisted the AML/CTF Compliance Officer with an investigation into a Unusual Matter Report, discuss any matters associated with such Report with any person other than their AML/CTF Compliance Officer, unless authorised by the AML/CTF Compliance Officer for the purposes of the investigation or otherwise required by law.

If the AML/CTF Compliance Officer receives an Unusual Matter Report from an employee or representative, he or she must assess the information provided and determine whether a reasonable suspicion is to be formed. If after the assessment the AML/CTF Compliance Officer has reasonable grounds to believe that:

(1) A customer or their agent may not be who they claim to be;
(2) Information that OT holds on the provision or prospective provision of its services may be relevant to
    i. The investigation of, or prosecution of a person for an evasion or an attempted evasion of a taxation law at the Commonwealth, State or Territory levels; ii. The investigation of, or prosecution of a person, for an offence against a law of the Commonwealth or of a State or Territory;
    iii. The enforcement of the Proceeds of Crime Act 2002 or regulations under that Act;
    iv. The enforcement of a law of a State or Territory that corresponds to the Proceeds of Crime Act 2002 or regulations under that Act;
(3) The provision or prospective provision of its services is preparatory to the commission of a financing of terrorism offence;

(4) The investigation of, or prosecution of a person for a financing of terrorism offence;

(5) provision or prospective provision of its services is preparatory to the commission of a money laundering offence;

(6) The investigation of, or prosecution of a person for a money laundering offence

The AML/CTF Compliance Officer is to form a suspicion on behalf of OT and submit a Suspicious Matter Report ('SMRs') to AUSTRAC within 3 business days upon forming such a suspicion, or within 24 hours should the suspicion be relevant to financing of terrorism. SMRs are to be submitted electronically through AUSTRAC Online.

Section 123 Offence of Tipping Off

It is prohibited:

(1) If

(a) a suspicious matter reporting obligation arises or has arisen for OT in relation to a person; and

(b) the AML/CTF Compliance Officer (or their substitute) has communicated information to the AUSTRAC CEO under subsection 41(2);

OT must not disclose to someone other than the AUSTRAC CEO or a member of the staff of AUSTRAC that the information has been communicated to the AUSTRAC CEO.

(2) If

(a) a suspicious matter reporting obligation arises or has arisen for OT in relation to a person; and (b) either:

(i) the AML/CTF Compliance Officer (or their substitute) has formed the applicable suspicion mentioned in subsection 41(1); or

(ii) the AML/CTF Compliance Officer (or their substitute) has communicated information to the AUSTRAC CEO under subsection 41(2);

Then

(c) OT must not disclose to someone other than the AUSTRAC CEO or a member of the staff of AUSTRAC:

(i) a suspicion has been formed in accordance with subsection 41(1); or

(ii) any other information from which the person to whom the information is disclosed could reasonably be expected to infer that the suspicion had been formed

(3) If OT is required under subsection 49(1) to give information, or produce a document, to a person, the reporting entity must not disclose to anyone else:

(a) that OT is or has been required to do so; or

(b) that the information has been given or the document has been produced; or

(c) any other information from which the person to whom the information is disclosed could reasonably be expected to infer that:

(i) OT had been required to give the first-mentioned information or produce the document; or

(ii) The first-mentioned information had been given; or (iii) The document had been produced.

A breach of this provision may lead to imprisonment for 2 years, 120 penalty units ($20,600) or both.

19. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER

19.1 Where OT has provided or is to provide a designated service to a customer and the AML/CTF Compliance Officer believes, on reasonable grounds, that a customer has information that may assist OT in the identification, management and mitigation of ML/TF risk, the AML/CTF Compliance Officer may request the customer to provide OT with any such information. The request must be provided in writing and notify the customer that if the request is not complied with, then OT may do any or all of the following until the information, covered by the request, is provided:

(a) refuse to continue to provide a designated service;

(b) refuse to commence to provide a designated service; or

(c) restrict or limit the provision of the designated service to the customer.

19.2 If the customer does not comply with the request within a reasonable time then the AML/CTF Compliance Officer may determine that, until the information covered by the request is provided, OT will:

(a) refuse to continue to provide the designated service;

(b) refuse to commence to provide the designated service; or

(c) restrict or limit the provision of the designated service to the customer.

19.3 In these circumstances, the AML/CTF Compliance Officer will determine whether the matter should be reported to AUSTRAC as a suspicious matter (refer to Section 18 of this Program).

20. ONGOING CUSTOMER DUE DILIGENCE – OVERVIEW

20.1 OT will monitor its customers with a view to identifying, mitigating and managing the risk that the provision of a designated service by a RE at or through a permanent establishment in Australia may involve or facilitate ML or TF.

20.2 OT will monitor its customers by implementing systems to:

(a) collect further KYC Information for ongoing customer due diligence processes;

(b) update and verify KYC Information for ongoing customer due diligence purposes;

(c) monitor the transactions of customers; and

(d) conduct enhanced customer due diligence in respect of high risk customers and customers about whom a suspicion has been formed where possible without triggering section 123.

20.3 As part of implementing systems for ongoing customer due diligence purposes, OT will group its customers according to their level of risk assessed as part of the risk assessment procedures outlined in this Program. The risk grouping will determine:

(a) what further KYC Information needs to be collected for ongoing customer due diligence purposes in respect of a particular customer;

(b) what level of transaction monitoring needs to be conducted in relation to a customer; and

(c) whether the enhanced customer due diligence program needs to be applied.

21. KYC AND BENEFICIAL OWNERSHIP

21.1 OT is required to have risk-based systems and controls in place to keep, update and review the KYC information, and the beneficial owner identification information where it has reasonable grounds to believe that the beneficial owner might not be the customer themselves, especially customers that carry higher ML/TF risks, to ensure the information held by the reporting entity and correct and up to date.

21.2 OT deals with a variety types of customers, including individuals, companies, and trusts. Individual customers are deemed to be the beneficial owners unless the reporting entity has reasons to believe that may not be the case. OT takes reasonable steps to identify and verify the structures of non-individual entities and their beneficial owners.

21.3 Risk-based routine and spot checks on customer records may be conducted by the AML/CTF Compliance Officer based on their ML/TF risk ratings (Low/Medium/High). Higher ML/TF risk ratings will lead to a larger sample to be selected and reviewed. High risk customers or beneficial owners are subject to enhanced due diligence procedures.

21.4 Based on the assessed level of a ML/TF risk involved in the provision of designated services provided by OT on the date that this Section of this

Program was adopted, OT has determined that no additional KYC and/or beneficial ownership Information needs to be collected in relation to low risk customers. The AML/CTF Compliance Officer will determine what additional KYC Information will be collected and verified, in respect of medium and high risk customers, prior to the provision of any designated service to assist OT to undertake ongoing customer due diligence.

21.5 The additional KYC and/or beneficial ownership Information will be collected at the same time as and in the same manner as the KYC Information is required to be collected under Part B. Failure to provide the required Information will be treated in the same way as the failure to provide any other KYC Information collected under Part B.

21.6 OT will update and re-verify KYC and/or beneficial ownership Information in respect of a customer where:

(a) the AML/CTF Compliance Officer considers that Information held in respect of a customer and/or their beneficial owner(s) is likely to be incomplete or unreliable;

(b) a representative of OT becomes aware that KYC Information held in respect of a customer and/or their beneficial owner(s) has or is likely to have changed;

(c) the customer engages in a significant transaction or series of transactions with OT , where a significant transaction occurs if a transaction, or series of transactions conducted within any calendar month exceeds $10,000 in value; or

(d) a significant change occurs in the way the customer conducts transactions, where a significant change occurs if the number of transactions carried out by a customer increases by 100% within a five (5) calendar day period.

21.7 Where one of the above circumstances arises in respect of a customer and the applicable customer identification procedure has not previously been carried out in respect of the customer (i.e. the customer is a precommencement customer), OT will carry out the applicable customer identification procedure in accordance with Part B of this Program and collect and verify the relevant KYC Information and beneficial owner information.

21.8 Where a change in customer information relates to in the case of:

(a) individual customers, the customer's:
  (i) name;
  (ii) date of birth; or
  (iii) residential address

(b) a company:
  (i) the company's name; or
  (ii) the company's registration number;

(c) a trust:

(i) the trustee; or

(ii) the name of the trust; and

(d) in the case of a partnership, the identity of a partner.

OT will seek to verify the updated KYC Information and beneficial ownership using reliable and independent documentation or electronic data in accordance with Section 51 of this Program.

22. TRANSACTION MONITORING PROGRAM

22.1 This Section describes the transaction monitoring program adopted by A G M M which includes risk-based systems and controls to monitor the transactions of customers, for the purpose of identifying any transactions that appear to be suspicious under section 41 of the AML/CTF Act (refer to Section 18 of this Program).

22.2 The AML/CTF Compliance Officer must identify ML/TF risk factors relevant to customers of particular services and products provided by the relevant RE, which may involve the provision of a designated service and to representatives of such customers. Some of the potential red flags are:

(a) value of a transaction where it exceeds ten thousand dollars ($10,000.00);

(b) a customer conducts a series of transaction within a short period of time each of which is marginally below the $10,000 threshold. For the purpose of monitoring 5 calendar days is used as the timeframe and transactions above $8,000 and below $10,000 are used as monetary thresholds.

(c) volume of transactions conducted by a customer within a five (5) calendar day period has increased by more than one hundred percent (100%);

(d) the amount of funds transacted cannot be explained by the income and asset information that OT holds on file about the customer;

(e) the customer is a PEP but did not declare this information;

(f) transaction involves foreign countries, customers or third parties against whom sanctions have been imposed or have been included on any of the lists:

i. maintained by the Department of Foreign Affairs and Trade under the *Charter of United Nations (Terrorism and Dealings with Assets) Regulations* 2002 (Cth); or

ii. maintained by the Office of Foreign Assets Control; or

iii. contained in the *Criminal Code Regulations* 2002 (Cth); or

(d) transaction involves a customer or third party who is a PEP (refer to Section 54 of this Program).

22.3 In addition to the Risk Awareness Training referred to in Section 14 of this Program, the AML/CTF Compliance Officer will ensure that all employees of OT , who have direct contact with customers or their representatives, receive regular training in the identification of relevant ML/TF risk factors and the red flags.

22.4 An employee of OT must immediately inform the AML/CTF Compliance Officer when any red flags are identified in relation to a customer or a customer's representative.

22.5 Where an employee of OT identifies a customer or third party of a kind specified in Section 22.2(c) or 22.2(d) of this Program, the AML/CTF Compliance Officer will take such appropriate action as is necessary, including seeking further information from the customer or their representative or from another source, to determine, with a reasonable degree of certainty, whether the customer or third party is that person.

22.6 If it is determined, as a result of transaction monitoring, that:

a. a customer should be placed in a higher risk grouping, OT will collect and verify (where appropriate) additional KYC Information and beneficial ownership information if required as referred to in Section 21 of this Program;

b. KYC and/or beneficial ownership Information needs to be updated or verified in respect of a customer, OT will update or verify the required information in accordance with Section 21 of this Program;

c. a customer is a high risk customer, OT will apply the enhanced customer due diligence program in accordance with Section 23 of this Program; or

d. a suspicious matter report needs to be lodged in respect of a customer, OT will follow the procedure outlined in Section 18 of this Program.

The AML/CTF Compliance Officer must fully document the above mentioned investigation process, including any evidence and the rationale of their decisions on the course of action to take.

23. ENHANCED CUSTOMER DUE DILIGENCE PROGRAM

23.1 OT is required to have in place an Enhanced Customer Due Diligence Program. Where the AML/CTF Compliance Officer determines that:

(a) the ML/TF risk associated with a particular designated service, customer, delivery method or jurisdiction is high, including but not limited to when the customer:

i. is engaged in business which involves a significant number of cash transactions or amounts of cash;

ii. uses a complex business ownership structure for no apparent commercial or other legitimate reason, especially if the beneficial owners of the legal entity cannot be determined;

iii. cannot provide information to verify the source of funds;

iv. requests an undue level of secrecy in relation to a designated service;

(b) a suspicion has arisen for the purposes of section 41 of the AML/CTF Act (refer to Section 18 of this Program),

(c) Its services is being provided to a customer is a politically exposed person;

(d) A party to a (proposed) transaction involving OT is located or incorporated in a prescribed foreign country;

Should one of the above scenarios take place, OT is to carry out one or more of the following procedures

(e) seek further information from the customer or from third party sources in order to:

i. clarify or update the customer's KYC and/or beneficial ownership Information in accordance with Section 21 of this Program;

ii. obtain any further Information in accordance with Section 21 of this Program;

iii. clarify the nature of the customer's ongoing business with OT ; and

iv. consider any suspicion that may have arisen for the purposes of section 41 of the AML/CTF Act (refer to Section 18 of this Program);

(f) conduct more detailed analysis in respect of the customer's KYC and/or beneficial ownership Information;

(g) verify or re-verify KYC and/or beneficial ownership Information in accordance with the customer identification program outlined in Part B of OT's AML/CTF Program;

(h) conduct more detailed analysis and monitoring in respect of the customer's activities and transactions – both past and future;

(i) consider whether a suspicious matter report ought to be lodged in accordance with section 41 of the AML/CTF Act (refer to Section 18 of this Program);

(j) Consider whether to exit a particular customer and/or cease to provide a particular service to the customer, and to obtain senior management approval before taking the action where appropriate

24. REVIEW OF OT 'S AML/CTF PROGRAM

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTIONS**
AUSTRAC Guidance Note: Risk management and AML/CTF programs.	Parts 4.7 and 8.4

24.1 The AML/CTF Compliance Officer must regularly assess OT 's ML/TF risk and should take steps to have this Program modified appropriately:

(a) where the AML/CTF Compliance Officer identifies that there has been a significant change in the ML/TF risks reasonably faced by OT in the course of providing its designated services;

(b) prior to OT introducing a new designated service to the market;

(c) prior to OT adopting a new method of delivering a designated service; and

(d) prior to OT adopting a new technology or developing technology used for the provision of an existing or new designated service.

24.2 Internal

(a) Due to the small number of staff members at OT , internal reviews will not be carried out unless the AML/CTF Compliance Officer considers it necessary or subject to section 24.2(b) of this Program. However, an internal review must take place at least annually.

(b) Internal reviews may be carried out where required by OT's Board of Directors.

(c) The internal party conducting the review should:

i. have unlimited access to the records, personnel and property of OT within the context of OT 's obligations under the *Privacy Act* 1988; and

ii. be impartial and objective in performing their duties and should not be inappropriately influenced by management of OT .

(d) The AML/CTF Compliance Officer will report the results of the internal review to the Board of Directors.

(e) The internal review will:

i. assess the effectiveness of Part A of this Program having regard to the ML/TF risk of OT ;

ii. assess whether Part A of this Program complies with the AML/CTF Rules;

iii. assess whether Part A of this Program has been effectively implemented;

iv. assess whether OT has complied with Part A of this Program;

v. assess the risk management resources available to OT including, but not limited to:
   a. funding; and
   b. staff allocation;

vi. identify any future needs relevant to the nature, size and complexity of OT ; and

vii. assess the ongoing risk management procedures and controls in order to identify any failures.

(f) When assessing ongoing risk management procedures and controls in order to identify any failures, the internal party conducting the review may have regard to:

(i) any market information relevant to the global AML/CTF environment which may have an impact on the ML/TF risk faced by OT ;

(ii) failure to include all mandatory legislative components in OT 's AML/CTF Policy;

(iii) failure to gain approval from OT 's Board of Directors of this Program;

(iv) insufficient or inappropriate employee due diligence;

(v) frequency and level of risk awareness training not aligned with potential exposure to AML/CTF risk(s);

(vi) changes in business functions which are not reflected in this Program (for example, the introduction of a new product or distribution channel);

(vii) failure to consider feedback from AUSTRAC (for example, advice regarding an emerging AML/CTF risk);

(viii) failure to undertake an independent review (at an appropriate level and frequency) of the content and application of this Program;

(ix) legislation incorrectly interpreted and applied in relation to a customer identification procedure;

(x) customer identification and monitoring systems, policies and procedures that fail to:

a. prompt, if appropriate, for further identification and/or verification to be carried out when the ML/TF risk posed by a customer increases;

b. detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;

c. take appropriate action where a customer provides insufficient or questionable information in relation to an identification check;

d. take appropriate action where the identification document provided is not an independent and reliable document;

e. recognise foreign identification issued by a high-risk jurisdiction;

f. record details of identification documents, for example, the date of issue;

g. consult appropriate resources in order to identify high-risk customers;

h. identify when an expired or old identification document (for example, a driver's licence) has been used;

i. collect any other name(s) by which the customer is known;

j. be subject to regular review;

(xi) lack of access to information sources to assist in identifying and/or verifying higher risk customers (and the jurisdiction in which they may reside), such as PEPs, terrorists and narcotics traffickers;

(xii) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:

A. customer identification policies, procedures and systems; and
B. identifying potential ML/TF risks;

(xiii) assess the acceptance of documentation that may not be readily verifiable.

(g) If the AML/CTF Compliance Officer determines it is appropriate, the internal review may also:

i. assess whether the risk-based procedures and processes adopted in this Program have changed such that alterations need to be made to the AML/CTF Program;

ii. assess whether Part B of this Program is sufficient to cover the ML/TF risks posed by existing and potential customers of OT ; and

iii. assess whether any additional changes need to be made to this Program as a result of changes to AML/CTF regulations and legislation and the AML/CTF environment generally.

24.3 External

(a) The AML/CTF Compliance Officer will arrange for this Program to be reviewed by an external party every 2 years at a minimum or more frequently, subject to changes to the risk profile of OT , legislative developments and market information regarding ML/TF risk. Additional external reviews may be carried out where the AML/CTF Compliance Officer considers it necessary.

(b) The AML/CTF Compliance Officer will report the results of the external review to the Board of Directors for OT .

(c) The external review will:

i. assess the effectiveness of Part A of this Program having regard to the ML/TF risk of OT ;

ii. assess whether Part A of this Program complies with the AML/CTF Rules;

iii. assess whether Part A of this Program has been effectively implemented;

iv. assess whether OT has complied with Part A of this Program;

(d) The AML/CTF Compliance Officer may also require the external party conducting the review to:

i. assess the ongoing risk management procedures and controls to identify any failures including, but not limited to:

A. failure to include all mandatory legislative components in OT's AML/CTF Program;

B. failure to gain approval from OT's Board of Directors for Part A of this

Program;

C. insufficient or inappropriate employee due diligence;

D. frequency and level of risk awareness training not aligned with potential exposure to ML/TF risk(s);

E. changes in business functions which are not reflected in this Program (for example, the introduction of a new product or distribution channel);

F. failure to consider feedback from AUSTRAC (for example, advice regarding an emerging AML/CTF risk);

G. failure to undertake independent review (at an appropriate level and frequency) of the content and application of this Program;

H. legislation incorrectly interpreted and applied in relation to customer identification procedures;

I. customer identification and monitoring systems, policies and procedures that fail to:

    i. prompt, if appropriate, for further identification and/or verification to be carried out when the ML/TF risk posed by a customer increases;

    ii. detect where a customer has not been sufficiently identified and/or verified and prevent the customer from receiving the designated service;

    iii. take appropriate action where a customer provides insufficient or questionable information in relation to an identification check;

    iv. take appropriate action where the identification document provided is not an independent or reliable document;

    v. recognise foreign identification issued by a high-risk jurisdiction;

    vi. record details of identification documents, for example, the date of issue;

    vii. consult appropriate resources in order to identify high-risk customers;

    viii. identify when an expired or old identification document (for example, a driver's licence) has been used;

ix. collect any other name(s) by which the customer is known;

x. be subject to regular review;

J. lack of access to information sources to assist in identifying higher risk customers (and the jurisdiction in which they may reside), such as PEPs, terrorists and narcotics traffickers;

K. lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:

i. customer identification policies, procedures and systems; and

ii. identifying potential AML/CTF risks;

L. assess the acceptance of documentation which may not be readily verifiable;

M. assess the risk management resources available to OT including, but not limited to:

i. funding; and

ii. staff allocation; and

N. identify any future needs relevant to the nature, size and complexity of OT .

(e) If the external reviewer determines it is appropriate, the external review may also:

i. assess whether the risk-based procedures and processes adopted in this Program have changed such that alterations need to be made to this Program;

ii. assess whether Part B of this Program is sufficient to cover the ML/TF risks reasonably faced by OT in the course of providing its designated services; and

iii. assess whether any additional changes need to be made to this Program as a result of changes to the AML/CTF regulations and legislation and the AML/CTF environment generally.

25. AUSTRAC FEEDBACK

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
AUSTRAC Guidance Note: Risk management and AML/CTF programs	Part 8.5

25.1 The AML/CTF Compliance Officer is the designated contact person for all AUSTRAC communication. Where AUSTRAC provides OT with feedback regarding performance on the management of ML/TF risks, the AML/CTF Compliance Officer will assess AUSTRAC's feedback to determine if any changes to this Program are required and implement any such changes as soon as reasonably practicable, subject to complying with the procedures in Section 26 of this Program.

26. OVERSIGHT BY THE BOARD / UPDATING THE PROGRAM

26.1 The Board of Directors is ultimately responsible for the AML/CTF efforts of OT . Part A of this Program and any subsequent amendment is to be approved the Board of Directors.

26.2 The AML/CTF Compliance Officer will report to the Board of Directors on a regular basis in relation to:

a) significant changes to the ML/TF risks affecting OT ;

b) compliance with this Program, the AML/CTF Act and Rules by OT ;

c) the results of and any report produced for any internal or external review of this Program;

d) any AUSTRAC feedback; and

e) changes to relevant legislation.

26.3 The AML/CTF Compliance Officer will propose amendments to this Program when required by the Program, AML/CTF Act or Rules or as a result of any of the matters in Section 26.2 of this Program. Subject to Section 26.4 of this Program, such amendments, if made to Part A of the Program, should be considered and approved by the Board of Directors before they become effective.

26.4 The AML/CTF Compliance Officer can implement a change to this Program immediately if the change is in relation to Part B of this Program. The Board of Directors should be informed of the change as soon as practically possible. Updated employee training sessions should also be held in a timely manner to ensure that all staff members follow the most up-to-date procedures.

27. REPORTS TO BE LODGED WITH AUSTRAC

27.1 Suspicious Matter Reporting:

OT has implemented Suspicious Matters Reporting (“SMR”) procedures to meet its SMR reporting obligations. Details are set out in section 18.

27.2 Threshold Transactions Reporting (TTRs)

OT does not have TTR obligations. Should the circumstances change and this reporting obligation arises, the AML/CTF Compliance Officer will update the AML/CTF Program and to organise the appropriate staff training to ensure that OT meets TTR obligation.

27.3 International Funds Transfer Instructions (IFTIs)

OT does not have IFTI reporting obligations. Should the circumstances change and this reporting obligation arises, the AML/CTF Compliance Officer will update the AML/CTF Program and to organise the appropriate staff training to ensure that OT meets IFTI reporting obligation.

27.4 AML/CTF Compliance Report

Under section 47(2) of the AML/CTF Act, OT is required to periodically provide an AML/CTF compliance report to AUSTRAC. This report sets out a reporting entity's compliance with the AML/CTF Act and Regulations. The report contributes to AUSTRAC's monitoring of ongoing industry compliance with the AML/CTF Act.

The AML/CTF Compliance Officer is required to diarise the lodgement date for each reporting period. The reporting period relates to January to December each year, and the report must be lodged by the end of March the following year.

In preparing the report, the AML/CTF Compliance Officer must carefully review all questionnaire and accurately complete the report. The statements in the report must accurately reflect the policies and procedures set out in the AML/CTF Program. During the course of completing the report, if weaknesses in OT 's policies and procedures are identified, the AML/CTF Compliance Officer must submit a report to the senior management and Board of Directors, together with a rectification plan.

The rectification plan must be implemented as soon as practicable and follow up review must be undertaken to ensure that the plan has been implemented effectively.

27.5 Change of Enrolment Details

The AML/CTF Compliance Officer is to ensure that the reporting entity's enrolment details remain correct and up to date. Should there be any changes in relation to the enrolment details, the AML/CTF Compliance Officer is to advise the AUSTRAC CEO of the changes within 14 days of the change arising, and in accordance with the approved form, or in a manner specified in the AML/CTF Rules.

PART B – CUSTOMER IDENTIFICATION

28. INTRODUCTION

28.1 **Part B** of this Program sets out the customer identification procedures for OT's customers.

28.2 These procedures include:

(a) prescribed processes for the collection and verification of KYC and beneficial ownership Information; and

(b) risk based systems and controls to determine what (if any) other information will be collected and verified in relation to a customer, having regard to the ML/TF risk relevant to the provision of OT's designated services.

28.3 OT will consider the following factors when identifying its exposure to MLTF risks and developing its customer identification procedures, the:

(a) customer types, including beneficial owners of customers and any PEPs;

(b) customers' source of funds and wealth;

(c) the nature and purpose of the business relationship with its customers;

(d) the control structure of non-individual customers;

(e) types of designated services provided;

(f) methods by which those designated services are delivered; and

(g) any foreign jurisdictions with which OT deals.

The customer identification and verification procedures are reviewed on a regular basis to ensure they remain relevant, appropriate and up-to-date. The verification of customer information collected can be carried out via:

(1) reliable and independent documentation; (2)

reliable and independent electronic data; or

(3) a combination of (1) and (2) above.

Where discrepancies are present, one or more enhanced customer due diligence procedures may be carried out.

29. APPLICATION OF PART B

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTIONS**
AUSTRAC Guidance Note: Risk management and AML/CTF programs.	Parts 9.1, 9.2 and 9.3

29.1 Part B of this Program applies to OT , including any functions carried out by a responsible third party.

29.2 The procedures set out in Part B apply on and from 12 December 2007, except in relation to customers to whom OT has provided designated services prior to 12 December 2007 (**"existing customers"**).

30. KYC – CUSTOMER IDENTIFICATION AND VERIFICATION PROCEDURES

30.1 The customer identification and verification procedures must be carried out by OT or a responsible third party in accordance with the ML/TF risk category of the customer:

(a) prior to commencing to provide a designated service to a customer (other than an existing customer), unless OT has already carried out the applicable customer identification procedure in respect of the customer; and

(b) when OT 's employee is responsible for the customer (or another OT employee on their behalf), unless the AML/CTF Compliance Officer authorises that these procedures can be conducted by an external party.

31. KNOW YOUR CUSTOMER – CONSIDERATIONS

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
AUSTRAC Guidance Note: Risk management and AML/CTF programs.	Part 6.5

A number of factors that may be relevant and may warrant further information to be collected and/or verified include:

31.1 In re-assessing the AML/CTF Customer Type Risk for OT , it may consider, where appropriate and among other factors, whether:

(a) the customer is involved in a complex business ownership structure with no legitimate commercial rationale;

(b) the non-individual customer (for example, a trust, company or partnership) has a complex business structure with little commercial justification, which obscures the identity of the ultimate beneficiaries of the customer;

(c) the customer is in a position which may expose OT to the possibility of corruption;

(d) the customer is based in, or conducting business through or in, a highrisk jurisdiction;

(e) the customer is engaged in business which involves significant amounts of cash;

(f) there is no clear commercial rationale for the customer seeking a designated service;

(g) the customer is a PEP;

(h) an undue level of secrecy is requested regarding a designated service;

(i) the source of funds is difficult to verify;

(j) the beneficial owners of a non-individual customer are difficult to identify and/or verify;

(k) the beneficial owners of the non-individual customer are a resident in a high-risk jurisdiction;

(l) there is a one-off transaction in comparison with an ongoing business relationship or series of transactions;

(m) a designated service can be used for ML or TF (and the extent to which it can be used);

(n) the customer makes or accepts payments (for example, electronic transfers) to or from accounts which have not been identified by the RE;

(o) the customer makes or accepts payments (for example, electronic transfers) to or from offshore accounts;

(p) the customer has access to offshore funds (for example, cash withdrawal or electronic funds transfer);

(q) the customer when migrating from one designated service to another carries a different type and level of ML/TF risk;

(r) the customer has income which is not employment-based or from a regular known source;

(s) the customer is new, rather than having a long-term and active business relationship with the RE;

(t) the customer's business is registered in a foreign jurisdiction with no local operations or domicile;

(u) the customer's business is an unregistered charity, foundation or cultural association;

(v) the customer is represented by another person, such as under a power of attorney.

32. INDIVIDUALS: IDENTIFICATION PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.2

Identification and verification procedures regarding individual customers set out in Part B apply to individual customers, directors of companies or corporate trustees (unless exceptions are applicable), individual trustees, and *beneficial owners* of nonindividual entities.

32.1 Where a new customer is an individual (other than an individual who notifies the RE that he or she is a customer of OT in his or her capacity as a sole trader), OT must collect, at a minimum, the customer's:

a. full name;

b. date of birth; and

c. residential address.

32.2 Where a new customer notifies OT that he or she is a customer in his or her capacity as a sole trader, OT must collect, at a minimum, the:

a. customer's full name;

b. customer's date of birth;

c. full business name (if any) under which the customer carries on his or her business;

d. full address of the customer's principal place of business (if any) or the customer's residential address; and

e. ABN issued to the customer.

32.3 Where the ML/TF risk posed by the provision of a designated service to a particular individual is assessed as medium or high under Section 31.1 of this Program, the AML/CTF Compliance Officer may require OT 's employee to be responsible for the customer. One or more of the following pieces of information may be collected:

a. any alias names used by the customer;

b. the customer's occupation or business activities;

c. the source of the customer's funds including the origin of funds;

d. income and assets of the customer;

e. the nature and level of the customer's intended transaction behaviour;

f. the beneficial ownership of the funds used by the customer/the customer's account with the RE; and

g. details of the customer's employment (e.g. name of employer, length of employment, type of institution).

32.4 The information collection requirements in this section are not intended to conflict with any other obligation OT has under other legislation including the *Privacy Act* 1998. Any conflicts, which arise, should be immediately notified to the AML/CTF Compliance Officer.

33. INDIVIDUALS: VERIFICATION – PRINCIPLES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.2

33.1 These procedures do not apply to OT 's customers prior to 12 December 2007.

33.2 At a minimum, the following KYC Information about a customer in section 32 of this Program, must be verified:

a. the customer's full name; and

b. either the customer's:

i. date of birth; or

ii. residential address.

33.3 Where it has been determined that the ML/TF risk posed by the provision of a designated service to an individual is medium or high under the assessment carried out under Section 31.1 of this Program and additional KYC Information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC Information which has been collected. The AML/CTF Compliance Officer will determine what additional KYC Information will be verified in respect of that customer.

33.4 Information which is required to be verified as indicated in section 33.2, of this Program, must be based on:

a. reliable and independent documentation;

b. reliable and independent electronic data; or

c. a combination of a. and b. above.

34. INDIVIDUALS: VERIFICATION – PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
IFSA/FPA Industry Guideline: Managing mutual obligations under Chapter 7 of the AML/CTF Rules – July 2007.	Schedule 1
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.2

34.1 The risk-based verification procedures are set out as follows:

Low Risk Individuals

- Full name against the date of birth against at least one permitted documentation or data source; and

- Full name against residential address against at least one permitted documentation or data source

The permitted documentation can be from one of the following

- At least 1 primary photographic identification document; or
- 1 primary non-photographic primary identification document AND 1 secondary identification document

Medium Risk Clients

- Full name against the date of birth against at least one permitted documentation or data source; and
- Full name against residential address against at least two permitted documentation or data sources

The permitted documentation can be from one of the following

- 2 primary photographic identification documents; or
- 1 primary photographic identification document AND 1 primary non-photographic identification document

High Risk Clients

- Full name against the date of birth against at least two permitted documentation or data sources; and
- Full name against residential address against at least two permitted documentation or data sources

The permitted documentation can be from one of the following options:

- 2 primary photographic identification documents;
- 1 primary photographic identification document AND 1 primary non-photographic identification document;
- 2 non-photographic identification documents and 1 secondary identification document

Accepted Verification Documents

Primary Photographic IDs

- Current domestic/international driver licence;
- Australian passport (current or has been expired for no longer than 2 years);
- Current passport or a similar document issued by a foreign government, the United Nations or one of its agencies for the purpose of international travel;
- Current Australian Age Card; or
- Current national identification card, issued by a foreign government, the United Nations or one of its agencies for the purpose of identification

Primary Non-photographic IDs

- Australian birth certificate or birth extract;
- Current Australian pension card;
- Citizenship certificate issued by the Australian or a foreign government;
- Birth certificate issued by a foreign government

Secondary IDs

- A notice issued by the Commonwealth of Australia, a State or Territory within 12 months, that contains the name and the residential address of the individual, which also records the provision of financial benefits to the individual under a law of the Commonwealth, State or Territory;
- A notice issued by the ATO within 12 months, that contains the name and the residential address of the individual, which records a debt payable to or by the individual by or to (respectively) the Commonwealth under a Commonwealth law relating to taxation; or
- A notice issued by a local government body or utilities provider within 6 months, that contains the name and the residential address of the individual, which records the provision of services by that local government body or utilities provider to that address or to that person.

34.2 Where an individual claim to be an agent of a customer, both the customer and the agent are to be identified in accordance with Part B of this Program. A Power of Attorney is to be completed and signed by both the customer and the agent.

34.3 Politically exposed persons, regardless of domestic or international, are deemed to be high risk customers and must be identified and verified in accordance with the procedures applicable to high risk customers.

35. COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.3

35.1 Where a new customer is a company, either domestic or foreign, OT has implemented risk-based systems and controls that allow OT to be reasonably satisfied that:

(a) the company exists; and

(b) the beneficial owners have been appropriately identified and verified.

35.2 **Information Collection:** The following KYC Information must be collected by OT's employee who is responsible for a customer that is a company, at a minimum, in order to determine its existence:

(a) in the case of a domestic company:

i. the full name of the company as registered by the Australian Securities and Investments Commission (**"ASIC"**);

ii. the full address of the company's registered office;

iii. the full address of the company's principal place of business (if any);

iv. the ACN/ABN issued to the company;

v. the AFSL number issued to the company (if relevant);

vi. whether the company is registered by ASIC as a proprietary or public company; and

vii. if the company is registered as a proprietary company, the name of each Director of the company.

(b) in the case of a registered foreign company:

i. the full name of the company as registered by ASIC;

ii. the full address of the company's registered office in Australia;

iii. the full address of the company's principal place of business in Australia (if any) or the full name and address of the company's local agent in Australia (if any);

iv. the ARBN issued to the company;

v. the AFSL number issued to the company (if relevant);

vi. the country in which the company was formed, incorporated or registered;

vii. whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; and

viii. if the company is registered as a private company by the relevant foreign registration body - the name of each Director of the company.

(c) in the case of an unregistered foreign company:

i. the full name of the company;

ii. the country in which the company was formed, incorporated or registered;

iii. whether the company is registered by the relevant foreign registration body and if so:

A. any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;

B. the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and

C. whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;

iv. if the company is registered as a private company by the relevant foreign registration body – the name of each Director of the company; and

v. if the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation.

35.3 Where the ML/TF risk posed by the provision of a designated service to a particular company is assessed as medium or high under Section 31.1 of this Program, the AML/CTF Compliance Officer may require OT 's employee responsible for the customer to collect one or more pieces of the following information:

a) all business names used by the company;

b) the full name, date of birth and residential address of each director and beneficial owner of the company;

c) the nature of the business activities conducted by the company;

d) the source of the customer's funds including the origin of funds;

e) the nature and level of the customer's intended transaction behaviour;

f) the name of the company secretary;

g) the name of the CEO or managing director (if any);

h) in the case of a foreign company:

i. the name of the relevant foreign registration body;

ii. any identification number issued to the company by the relevant foreign registration body;

iii. for an unlisted public company other than an Australian regulated company, the full name and address of each beneficial owner;

iv. in the case of listed companies other than domestic listed companies and companies listed on a recognised foreign stock exchange and their majority owned subsidiaries (**approved listed companies**) and Australian regulated companies, the full name and address of the beneficial owners of the top twenty (20) shareholdings;

details of any current or recent prosecutions and inquiries related to ML, terrorist links, tax offences and corruption in respect of the company.

35.4 The AML/CTF Compliance Officer may also determine, where the ML/TF risk posed by the company is medium or high, that the individuals referred to in Sections 35.3(b),(f) and (g), of this Program, must be screened against the lists mentioned in Section 53.1 of this Program.

35.5 The verification procedures in Section 37, of this Program, must also be followed, having regard to the ML/TF risk relevant to the provision of the designated service.

36. COMPANIES: VERIFICATION PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.3

36.1 The following verification procedures need to be followed for companies:

(a) Government database verification (refer to Section 53 of this Program); and

(b) PEP verification (refer to Section 54 of this Program); and

(c) Foreign high-risk jurisdiction verification (refer to Section 52 of this Program); and

(d) A verification procedure (refer to Section 36.2 of this Program) that may be electronic or document based.

36.2 At a minimum, the following KYC Information about a customer in Section 35 of this Program must be verified:

a. in the case of a domestic company:

i. the full name of the company as registered by ASIC;

ii. the ACN or ABN issued to the company;

iii. whether the company is registered by ASIC as a proprietary or public company; and

b. in the case of a registered foreign company:

i. the full name of the company as registered by ASIC;

ii. the ARBN issued to the company;

iii. the country in which the company was formed, incorporated or registered;

iv. whether the company is registered by the relevant foreign registration body and if so, whether it is registered as a private or public company or some other type of company;

c. in the case of an unregistered foreign company:

i. the full name of the company;

ii. the country in which the company was formed, incorporated or registered;

iii. whether the company is registered by the relevant foreign registration body and if so:

A. any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;

B. the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and

C. whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;

iv. if the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation.

36.3 If the company is an unregistered foreign company, the AML/CTF Compliance Officer may determine that it is necessary to seek an explanation as to why the company is not registered.

36.4 Where it has been determined under an assessment conducted under Section 31.1, of this Program, that the ML/TF risk posed by the provision of a designated service to a company is medium or high and additional KYC Information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC Information that has been collected. The AML/CTF Compliance Officer will determine what additional KYC Information will be verified in respect of that customer.

36.5 Unless the simplified verification procedures apply to a particular company customer, all directors and beneficial owners of the company are to be identified and verified as if they were individual customers under section 34 of

this Program.

36.6 For information that is required to be verified as indicated in Section 36.2 of this Program and, the following can be used:

a. reliable and independent documentation (refer to Section 38 of this Program);

b. reliable and independent electronic data (refer to Section 40 of this Program); or

c. a combination of a. and b. above.

37. COMPANIES: SIMPLIFIED VERIFICATION PROCEDURES

37.1 The criteria in Section 36, of this Program, does not have to be satisfied where OT confirms that the company is:

a. a domestic listed public company;

b. a majority owned subsidiary of a domestic listed public company; or

c. licenced and subject to regulatory oversight of a Commonwealth, State or Territory regulator in relation to its activities as a company,

by obtaining one (1) or a combination of the following:

d. a search of the relevant domestic stock exchange;

e. a public document issued by the relevant company;

f. a search of the relevant ASIC database; or

g. a search of the licence or other records of the relevant regulator.

38. COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.3

38.1 The following types of reliable and independent documentation are acceptable for verification of company information:

a. an original and currently valid Australian financial services licence issued by ASIC;
b. an original or certified copy of the currently valid company registration certificate issued by ASIC; or
c. in relation to the beneficial ownership of a company, a recent company statement or company extract that was issued by ASIC within the past 12 months. A disclosure certificate that verifies information about the beneficial ownership of a company may also be accepted (subject to this Program).

38.2 Disclosure Certificates:

a. For a company other than a foreign company, i.e. an Australian company, a disclosure certificate may be considered as a 'reliable and independent documentation' to verify additional information collected in respect of a company.

b. For a foreign company where other reliable verification information is not otherwise reasonably available, a disclosure certificate verifying information about a foreign company may be relied upon by OT for new customer KYC verification if given approval by the AML/CTF Compliance Officer.

c. The AML/CTF Compliance Officer, in determining whether to rely on a disclosure certificate for verification purposes, will take into consideration the ML/TF risk relevant to the provision of the designated service, including the jurisdiction of incorporation of the company as well as the jurisdiction of the primary operations of the company and the location of the foreign stock or equivalent exchange (if any), and the activities undertaken by the company and the availability of evidence about the activities and existence of the company. The AML/CTF Compliance Officer may require further information to be collected and/or verified regarding the company. Where the ML/TF risk is deemed high, it may be appropriate for the AML/CTF Compliance Officer to seek the opinion of the Board of Directors as to whether to accept the customer or refuse to provide the customer with the requested designated service(s).

39. COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT ELECTRONIC DATA

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**

39.1 KYC Information collected from a customer may also be verified using reliable and independent electronic data.

39.2 For the purposes of verification of a company other than a foreign company, the following sources, either used directly or indirectly, are considered to provide reliable and independent electronic data, having regard to the matters outlined in Section 41.1 of this Program:

a. ASIC (www.asic.gov.au);

b. ASX (www.asx.com.au); and

c. APRA (www.apra.gov.au).

39.3 For the purposes of verification of a foreign company, the following sources are considered to provide reliable and independent electronic data, having regard to the matters outlined in Section 40.1 of this Program:

a. a search of the relevant foreign stock or equivalent exchange (if any) – refer to section 39.4 of this Program; and

b. a search of the records of the relevant regulator.

39.4 A relevant foreign stock or equivalent exchange is one that is approved by ASIC for recognition, including, but not limited to the following financial markets:

a. American Stock Exchange;
b. Borsa Italiana;
c. Bourse de Paris;
d. Bursa Malaysia Main Board and Bursa Malaysia Second Board;
e. Eurex Amsterdam;
f. Frankfurt Stock Exchange;
g. Hong Kong Stock Exchange;
h. JSE Securities Exchange;
i. London Stock Exchange;
j. NASDAQ National Market;
k. New York Stock Exchange;
l. New Zealand Stock Exchange;
m. Stock Exchange of Singapore;
n. SWX Swiss Exchange;
o. Tokyo Stock Exchange; and
p. Toronto Stock Exchange.

39.5 For the purposes of verification of a foreign listed public company, OT must have regard to the ML/TF risk relevant to the provision of the designated services being

provided (or potentially provided), including the location of the foreign stock or equivalent exchange (if any). Where the ML/TF risk is medium or high, the AML/CTF Compliance Officer is to review all information that has been collected and/or verified regarding the customer. Senior management approval may also be appropriate.

40. COMPANIES: VERIFICATION – ALTERNATIVE DATA

40.1 Where the data in Sections 37 and 39, of this Program, cannot be obtained or is not sufficient to verify the required data listed in Sections 35.2 and 36 of this Program, in consultation with the AML/CTF Compliance Officer, OT's employee responsible for the customer will determine whether alternative sources of data can be obtained. This alternative data must be reliable and independent such that it can be accepted into the verification process. In making this determination, the following factors need to be taken into account:

a. the accuracy of the data;
b. how secure the data is;
c. how the data is kept up-to-date;
d. how comprehensive the data is (for example, by reference to the range of persons included in the data and the period over which the data has been collected);
e. whether the data has been verified from a reliable and independent source;
f. whether the data is maintained by a government body or pursuant to legislation; and
g. whether the electronic data can be additionally authenticated.

41. COMPANIES: VERIFICATION – INDEPENDENT CONTACT

41.1 To verify KYC Information collected from a customer, OT's employee responsible for the customer may independently initiate contact with the company. This contact will be made using information contained in public resources such as the:

a. White Pages Directory;
b. Yellow Pages Directory;
c. ASIC Database;
d. internet searches;
e. APRA database;
f. Overseas equivalent of the above;
g. The company's website.

41.2 Any of the electronic data in Sections 39.2 or 390..3, of this Program, can also be used for the purposes of this Section.

42. TRUSTEES: CUSTOMER IDENTIFICATION PRINCIPLES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.4

42.1 Where a new customer acts in the capacity of a trustee of a trust, OT has implemented risk-based systems and controls to identify and verify the customer in order to be reasonably satisfied that:

(a) the trust exists; and
(b) the name of each trustee and beneficiary, or a description of each class of beneficiary, of the trust has been provided.

43. TRUSTEES: PART 1 – CUSTOMER IDENTIFICATION PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.4

43.1 In accordance with section 42.1(a) of this Program, the following KYC Information must be collected from a customer:

a. the full name of the trust;
b. the full business name (if any) of the trustee in respect of the trust;
c. the type of the trust;
d. the country in which the trust was established;
e. the full name of the settlor of the trust unless:
    i. the material asset contribution to the trust by the settlor at the time the trust is established is less than $10,000;
    ii. the settlor is deceased; or
    iii. the trust is verified using the simpliefied trustee verification procedure as prescribed in section 4.4.8 of the AML/CTF Rules;
f. if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual under Sections 32 to 34 of this Program;

g. if any of the trustees is a company, then in respect of one of those companies – the information required to be collected from a company under Sections 35 to 40 of this Program;

h. if the trustees comprise individuals and companies then in respect of either an individual or a company – the information required to be collected from the individual or company (as the case may be) under the applicable customer identification procedures in Sections 32 to 40 of this Program.

43.2 Where it is determined under an assessment carried out under Section 31.1, of this Program, that the ML/TF risk posed by the provision of a designated service to a trustee of a trust is medium or high, the AML/CTF Compliance Officer may require the OT employee responsible for the customer to collect one or more pieces of the following information:

a. all business names used by the trusts and any other name under which the trust operates;
b. the nature of the business activities conducted by the trust;
c. the source of the customer's funds including the origin of funds;
d. the jurisdiction in which the trust was established;
e. details of any current or recent prosecutions and inquiries related to ML, terrorist links, tax offences and corruption in respect of the trust;
f. the nature and level of the customer's intended transaction behaviour;
g. the income and assets (including location) of the trust;
h. details of any parties with which the trust owns property, is in partnership or undertakes a joint venture.

44. TRUSTEES: PART 1 – VERIFICATION – PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.4

44.1 The following verification procedures need to be followed for trusts:

a. Government database verification (refer to Section 52 of this Program);
b. PEP verification (refer to Section 53 of this Program);
c. Foreign high-risk jurisdiction verification (refer to Section 51 of this Program); and
d. a document or electronic data based verification procedure (refer to Section 44.2 of this Program).

44.2 At a minimum, the following KYC Information about a customer in Section 43 of this Program must be verified:

a. the full name of the trust from a trust deed, certified copy or certified extract of the trust deed, reliable and independent documents relating to the trust or reliable and independent electronic data;

b. if any of the trustees is an individual, then in respect of one of those individuals – information about the individual in accordance with the customer identification procedures applicable to individuals in Sections 32 to 34 of this Program;

c. if any of the trustees is a company, then in respect of one of those companies – information about the company in accordance with the procedures in Sections 35 to 40 of this Program; and

d. if the trustees comprise individuals and companies then in respect of either an individual or a company – the information about the individual or company (as the case may be) in accordance with the applicable procedures in Sections 32 to 40 of this Program.

e. The full name of the settlor of the trust unless
   i. the material asset contribution to the trust by the settlor at the time the trust is established is less than $10,000;
   ii. the settlor is deceased; or
   iii. the trust is verified using the simpliefied trustee verification procedure as prescribed in section 4.4.8 of the AML/CTF Rules;

44.3 Where it has been determined under an assessment carried out under Section 31.1, of this Program, that the ML/TF risk posed by the provision of a designated service to a trustee of a trust is medium or high and additional KYC Information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC Information that has been collected. The AML/CTF Compliance Officer will determine what additional KYC Information will be verified in respect of that customer.

45. TRUSTEES: PART 2 – CUSTOMER IDENTIFICATION PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.4

45.1 In accordance with section 42.1(b) of this Program, the following KYC Information must be collected from a customer as a minimum:

a. the full name and address of each trustee in respect of the trust; and

b. either the:

i. full name of each beneficiary of the trust; or

ii. terms of the trust identify the beneficiaries by reference to membership of a class – details of the class.

45.2 Where the ML/TF risk is deemed to be medium or high in relation to a prospective trust customer, the AML/CTF Compliance Officer may require further information to be collected and/or verified regarding the trust, trustees, and beneficiaries.

46. TRUSTEES: PART 2 – VERIFICATION PROCEDURES

SOURCE OF SECTION	
DOC	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules	Part 4.4

46.1 The information collected under Section 45 of this Program must be verified by:

a. a trust deed, certified copy or certified extract of a trust deed;
b. reliable and independent documents relating to the trust;
c. reliable and independent electronic data; or
d. a combination of a. to c. above.

46.2 For the purposes of sections 46.1(b) and 46.1(c) of this Program, 'reliable and independent documents relating to the trust' includes a disclosure certificate that verifies information about a trust where:

a. the verification is being conducted as a result of a risk-based assessment in section 28.2(b) of this Program determining that additional information is required about the trustee; and

b. the information to be verified is not otherwise reasonably available from the sources in Section 46.1 of this Program.

46.3 For the purposes of verification of a trustee, OT must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided). The AML/CTF Compliance Officer is to review all information collected and/or verified regarding a trust account where the ML/TF risk is deemed to be high. Senior management approval may be appropriate to

determine whether OT is to accept the new trust customer or to refuse to provide the requested designated service(s).

47. TRUSTEES: SIMPLIFIED VERIFICATION PROCEDURES

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).	Part 4.4

47.1 The criteria in Sections 44 and 45 of this Program will not need to be satisfied where it can be verified that a trustee falls into one of the following categories:

a. a managed investment scheme registered by ASIC;

b. a managed investment scheme that is not registered by ASIC and that:

i. only has wholesale clients; and
ii. does not make small scale offerings to which section 1012E of the *Corporations Act* 2001 (Cth) applies;

c. registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust; or

d. a government superannuation fund established by legislation.

49. AGENTS: IDENTIFICATION PROCEDURES

49.1 Where an agent requests the provision of a designated service on behalf of a customer, OT must collect, at a minimum the following:

a. the full name of the person who purports to act on behalf of the customer; and

b. evidence of the customer's authorisation of the person to act on its behalf.

49.2 Where an agent requests the provision of a designated service on behalf of a customer, OT will carry out the relevant customer identification procedure on both the agent and the customer, outlined in Part B of this Program.

50. AGENTS: VERIFICATION PRINCIPLES

50.1 OT will verify the agent in accordance the procedures set out in Part B of this Program as if the agent were a customer. For example, where the agent of a customer is a natural person, then the procedures for individual customers apply.

51. VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

51.1 It is assumed that any document used to verify KYC Information will be sufficiently contemporaneous unless otherwise specified in the AML/CTF Rules or in this Program. For the purposes of this Program, a document will be sufficiently contemporaneous if it has not expired or in the case of an Australian Passport, it has expired within the preceding two years.

51.2 If a customer is unable to provide an original or certified copy of a document for the purposes of verifying KYC Information, the AML/CTF Compliance Officer will need to determine, having regard to the ML/TF risk associated with the provision of a designated service to that customer, whether it is appropriate to rely on a certified copy of the document.

51.3 The AML/CTF Compliance Officer will take steps to determine whether any document produced by a customer has been forged, tampered with, cancelled or stolen.

52. VERIFICATION – FOREIGN JURISDICTIONS

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTION**
AUSTRAC Guidance Note: Risk management and AML/CTF programs.	Part 6.11

52.1 Where OT has the prospect to acquire a new customer from a foreign jurisdiction, an assessment must be made as to whether it is a high-risk jurisdiction. The factors that should be considered in this assessment include, but are not limited to:

a. whether the customer is based in a country that is a Financial Action Task Force (**"FATF"**) member and any FATF reports about that country;

b. the legal framework and standard AML/CTF controls of the foreign jurisdiction; and

c. the economic climate of the foreign jurisdiction.

52.2 The assessment should take into account information from legitimate, respected domestic and/or international bodies.

52.3 Where an assessment is made that the customer is from a high-risk jurisdiction, the matter must be referred to the AML/CTF Compliance Officer who will make a decision as to whether OT should continue dealing with the customer. Senior management approval may be appropriate before OT agrees to provide the customer with the requested designated service(s).

53. VERIFICATION – GOVERNMENT DATABASES

53.1 Where OT is likely to provide designated services to a new customer, the following procedures may be carried out in addition to the KYC procedures discussed elsewhere in this Program by OT 's employee responsible for the customer, as an additional anti-money laundering measure:

Check against:

A. Department of Foreign Affairs and Trade's (**"DFAT"**) Consolidated Sanctions List:

(i) the name of a prospective customer must be checked against the DFAT Consolidated List available at http://www.dfat.gov.au/sanctions/consolidatedlist.html;

(ii) the DFAT Consolidated List must be accessed directly from the DFAT website every time a prospective customer is checked – a copy of this spreadsheet should not be saved on an employee's computer in order to ensure that the most recent version of the Consolidated List is used;

(iii) alternatively, the DFAT 'LinkMatch Lite' software may be used to check the names of a prospective customer – prior to a prospective customer being checked, the most recent version of the 'LinkMatch Lite' software must be downloaded from www.dfat.gov.au/divs/ild/download_lms.html;

(iv) where there is a match it must be **immediately** referred to the AML/CTF Compliance Manager who will carry out the necessary procedures according to http://www.dfat.gov.au/sanctions/consolidated-list.html and

(v) where a match is found on the DFAT Consolidated List, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Officer; or

B. Office of Foreign Affairs Assets Control's Specially Designated Nationals List:

(i) the name of a prospective customer must be checked against the list available at http://sdnsearch.ofac.treas.gov/;

(ii) the list must be accessed directly from the Office of Foreign Affairs Assets Control's website every time a prospective customer is checked – a copy of this spreadsheet should not be saved on an employee's computer in order to ensure that the most recent version of the list is used;

(iii) where there is a match it must be **immediately** referred to the AML/CTF Compliance Officer who will carry out the necessary procedures and

(iv) where a match is found on the list, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Officer;

C. Australian National Security (**"ANS"**):

(i) the name of the new customer must be checked against the ANS Listing of Terrorist Organisations available at http://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/default.asp x;

(ii) the ANS Listing of Terrorist Organisations must be accessed directly from the ANS website listed in Section 52.1(b)(i) of this Program every time a prospective customer is being checked – a copy of this list should not be saved on an employee's computer in order to ensure that the most recent version is used;

(iii) where there is a match it must be **immediately** referred to the AML/CTF Compliance Officer; and

(iv) where there is a match with the ANS Listing of Terrorist Organisations, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Officer.

D. Criminal Code List:

(i) the name of a new customer must be checked against the list contained in the *Criminal Code Regulations* 2002 available at: http://www.comlaw.gov.au/Details/F2013C00934;

(ii) where there is a match it must be **immediately** referred to the AML/CTF Compliance Officer; and

(iii) where there is a match with the Criminal Code List, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Officer.

54. VERIFICATION – PEP

SOURCE OF SECTION CONTENT	
DOCUMENT	**SECTIONS**

54.1 Where OT has the prospect to acquire a new customer, the following procedures must be carried out in addition to the KYC procedures discussed elsewhere in this Policy.

54.2 The individual must be assessed as to whether they may satisfy the definition of a PEP. All prospective customers are require to inform OT their PEP status in the account application process.

54.3 If it is determined that a customer is a PEP, OT will:

a) obtain approval from the AML/CTF Compliance Officer before providing a designated service to the customer;

b) collect information regarding the source of wealth and source of funds used by the customer; and

c) apply the enhanced customer due diligence program outlined in Section 23 of the this Program.

54.4 All customers of OT must undergo the PEP verification process.

54.5 It is the responsibility of all of OT 's employees to be aware of the risks associated with PEP and to report any information or suspicions immediately to the AML/CTF Compliance Officer.

55. NOTIFICATION OF ALL NEW CUSTOMERS TO THE AML/CTF COMPLIANCE OFFICER

55.1 The AML/CTF Compliance Officer must be notified of all new customers.

55.2 Sign-off for each new customer should be obtained from the AML/CTF Compliance Officer where a customer carry high ML/TF risks. Senior management approval may also be sought.

56. TOLERANCE OF DISCREPANCIES AND ERRORS

56.1 **Tolerance of discrepancies:** Where, during the KYC Information collection and verification process, a director, officer or employee of OT discovers any discrepancies in the KYC Information provided by the new customer, the matter should be immediately notified to the AML/CTF Compliance Officer. The discrepancy must not be raised with the new customer without first consulting the AML/CTF Compliance Officer. The AML/CTF Compliance Officer is to investigate into the discrepancies. Enhanced due diligence

procedures may be carried out where appropriate provided the AML/CTF Compliance Officer reasonably believes that doing so should not trigger section 123 of the Act.

56.2 **Pre-defined tolerance levels for matches and errors:** OT will allow for obvious typographical errors in customer information other than name, company registration or identification n u m b e r , or date of birth. Where the error relates to name, company registration or identification number, or date of birth, the AML/CTF Compliance Officer should be notified and no contact should be made to the customer without the approval of the AML/CTF Compliance Officer.