

OT MARKETS PTY LTD

AML MANUAL

The manual is property of OT MARKETS PTY LTD The reproduction in whole or in part in any way including the reproduction in summary form, the reissue in a different manner and any changes in the original manual or any translated version is strictly forbidden and is only allowed with the prior written consent of OT MARKETS PTY LTD .

Table of Contents

I. INTRODUCTION	5
1. Simplified Outline	5
2. Duty to cooperate for prevention of Money Laundering and other criminal activities	6
3. The role of the Board	6
4. The role of the Senior Management	7
5. Appointment of a compliance officer and establishment of procedures	8
II. IDENTIFICATION PROCEDURES	9
1. Identification procedures for certain pre commencement customers	9
2. Verification of identity of pre commencement customer	9
3. Identification procedures for certain low risk services	9
4. Verification of identity of low risk service customer	10
5. Identification procedures	10
a. Simplified customer due diligence	18
b. Enhanced customer due diligence	18
6. Verification of identity	19
7. Ongoing customer due diligence	22
8. General provisions	22
III. REPORTING OBLIGATIONS	23
1. Simplified Outline	23
2. Suspicious Matters	24
3. Threshold transactions	26
4. International funds transfer instructions	27
5. AML/ CTF compliance reports	28
6. General provisions	28

7. AML/ CTF Rules may make provision in relation to reports by registered remittance affiliates.	29
8. Request to obtain information about the identity of holders of foreign credit cards and.	30
9. Reporting Entities Roll	31
IV. REPORTS ABOUT CROSS-BOARDER MOVEMENTS OF PHYSICAL CURRENCY AND.	32
1. Simplified Outline	32
2. Reports about physical currency.	32
3. Information about reporting obligations.	35
V. ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING PROGRAMS	35
1. Simplified Outline	35
2. Company’s Obligations.	36
3. Applicable customer identification procedures - customers other than individuals.	37
4. Applicable customer identification procedures - disclosure certificates.	38
VI. CORRESPONDENT BANKING	38
1. Simplified Outline	38
2. Prohibition of entry into correspondent banking relationships with shell banks.	39
3. Termination of correspondent banking relationship with shell bank.	39
4. Due diligence assessments before entering into correspondent banking relationships.	40
5. Regular due diligence assessments of correspondent banking relationships.	40
VII. COUNTERMEASURES	40
VIII. RECORD KEEPING REQUIREMENTS	42
1. Simplified Outline	42
2. Records of transactions	42
3. Transaction records to be retained	42
4. Records of identification procedures	43

5. Records about anti money laundering and counter terrorism financing programs	45
IX. SECURITY AND ACCESS.....	45
1. Simplified Outline.....	45
2. Disclosure of information.....	45
X. ADMINISTRATION	46
1. Establishment of AUSTRAC	46
2. AML/ CTF Rules.....	47

I. INTRODUCTION

OT Markets Pty Ltd (ACN 621 714 181) (OTCapital, us, we or the “**Company**”) a Corporate Authorized Representative (CAR) license number 001258906 of AGM Markets Pty Ltd AFSL 422662.. The Company is committed to the highest standards of the Anti-Money Laundering (AML) compliance and Anti-Terrorist Financing and requires the management, and employees to fully observe and follow the named standards. The Company therefore takes all necessary measures to detect and counter money laundering and terrorism financing. The internal rules are observed in accordance with the relevant legal framework and AML requirements.

It should be stated that the present AML Manual adopts and is in a state of compliance with the provisions of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (the “**Act**”) and the Anti Money Laundering/ Counter Terrorism Financing Rules (the “**AML/ CTF Rules**”) and any other Regulations, Guidelines, Directives and Reports which are issued by the Relevant Authorities. Regarding the terms and terminology which are used in this Manual, the definitions are as indicated in the Act and the AML/ CTF Rules.

1. Simplified Outline

The following is a simplified outline of this Act:

- The Company must carry out a procedure to verify the customer’s identity before providing a designated service to the customer. However, in special cases, the procedure may be carried out after the provision of the designated service. The Company shall establish and implement policies and protocols to identify and avoid money laundering transactions and to ensure compliance with the relevant international requirements.
- Certain pre commencement customers are subject to modified identification procedures.
- Certain low risk services are subject to modified identification procedures.
- The Company must carry out ongoing customer due diligence.
- The Company must report the following to the Chief Executive Officer of AUSTRAC (the Australian Transaction Reports and Analysis Centre):
 - a. suspicious matters;
 - b. certain transactions above a threshold;
 - c. cross boarder movements of physical currency must be reported to the AUSTRAC CEO, a customs officer or a police officer if the total amount moved is above a threshold

- The Company must have and comply with anti money laundering and counter terrorism financing programs.

2. Duty to cooperate for prevention of Money Laundering and other criminal activities

- i. The Company shall determine the identity of the beneficial ownership of all their clients' accounts and shall not open or maintain such accounts, unless they are satisfied of this requirement.
- ii. The Company shall take all reasonable measures to ensure that accounts are not used for the purpose of holding assets obtained as the result of, or for facilitating the commission of any criminal activity.
- iii. The Company shall develop and implement policies and procedures to identify and avoid money laundering transactions and to ensure compliance with the relevant international requirements.
- iv. The Company shall, on a regular basis, evaluate the effectiveness of their policies and control procedures in complying with the international requirements and any relevant guidelines, and such evaluation shall be an integral component of any internal audit.
- v. The Company shall be vigilant in ensuring the prevention of their involvement or misuse in money laundering activities, and shall not knowingly accept assets or enter into business relationships where there is reasonable cause to believe that such assets may have been acquired illegally or that they represent the proceeds of criminal activity.
- vi. The Company shall establish procedures to obtain appropriate evidence of client identity, and shall maintain adequate records of client identity and transactions involved in such a manner as to assist, if necessary, in the investigation of criminal offences.

3. The role of the Board ;

- i. The Board has the ultimately responsibility for the effectiveness of the Company's AML framework. The Board's oversight role is intended to ensure, inter alia, that there is compliance with all the relevant international laws and regulations. Such compliance should assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.
- ii. The Board should therefore demonstrate its commitment to an effective AML programme by:
 - a. Understanding the AML and Anti-Terrorist Financing standards placed upon it, their staff and the entity it represents;
 - b. Approving AML policies and procedures that are appropriate for the risks faced by the Company. Evidence of consideration and approval of these policies should be reflected in the board minutes and noted in the policy;
 - c. Appointing an individual within the organization to ensure that the Company's AML procedures are being

managed effectively.

4. The role of the Senior Management

- i. The Senior Management is responsible for the development of sound risk management programmes and for keeping the Board adequately informed about these programmes and their effectiveness. These programmes, which should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments, should be formally documented and, at a minimum, irrespective of whether the Company receives funds from third parties or not, should provide for:
 - a. The development of internal policies, procedures and controls for, inter alia:
 - i. The opening of customer accounts and verification of customer identity;
 - ii. Establishing business relations with third parties (including custodians, fund managers, correspondent banks, business introducers);
 - iii. Determining business relationships that the financial institution will not accept by requiring graduated customer acceptance policies and procedures with more extensive due diligence for higher risk customers;
 - iv. Determining an exit strategy to terminate undesired relationships with existing customers;
 - v. The timely detection of unusual activities and reporting of suspicious transactions;
 - vi. Internal reporting; and
 - vii. Records retention.
 - b. The recruitment of a level of staff, appropriate to the nature and size of the business, to carry out identification, research of unusual transactions and reporting of suspicious activities;
 - c. Designation of a compliance officer at an appropriate level of authority, seniority and independence to coordinate and monitor the compliance program;
 - d. An ongoing training programme designed to ensure employees adhere to the internal procedures and become familiar with the dangers they and the business entity face and on how their job responsibilities can encounter specified money laundering and terrorist financing risks;
 - e. Establishment of management information/reporting systems to scrutinize customer account activity and facilitate aggregate and group-wide monitoring of significant balances regardless of whether the accounts are held on balance sheet, as assets under management or on a fiduciary basis.
 - f. An effective independent risk-based oversight function to test and evaluate the compliance program; and
 - g. Screening procedures for hiring, and ongoing systems to promote high ethical and professional standards to prevent the financial institution from being used for criminal activity. This should include but is not limited to enquiries about the personal history of the potential employee and verifying appropriate refer

ences on the individual.

- ii. Policies should be periodically reviewed for consistency with the business model, and product and service offering. Special attention should be paid to new and developing technologies.

5. Appointment of a compliance officer and establishment of procedures

i. The Company shall:

- a. appoint a compliance officer who shall be responsible for ensuring the Company's compliance with the international requirements;
- b. establish and maintain internal policies, procedures, controls and systems to:
 - implement the customer identification requirements;
 - implement record keeping and retention requirements;
 - implement the monitoring requirements;
 - implement the reporting requirements;
 - make its officers and employees aware of the laws relating to combating money laundering and financing of terrorism. In particular, the law on customer due diligence and suspicious transaction reporting;
 - make its officers and employees aware of the procedures and policies adopted by it to deter money laundering and the financing of terrorism;
 - screen persons before hiring them as employees;
 - disseminate warning notices and other information received from the competent authority relating to a weakness in the anti-money laundering and combating of financing of terrorism systems of other countries; and
- c. conduct ongoing training of its officers, employees and agents to ensure that employees are kept informed of new developments, including information on current money laundering and terrorist financing techniques, methods and trends.

ii. The Company shall:

- a. enable any person identified in accordance with subsection (i) (a) as well as other appropriate staff to have timely and unimpeded access to information that may be relevant to determining whether sufficient basis exists to report the matter; and

- b. require the identified person to report the matter in the event that he determines that sufficient basis exists.
- iii. The person identified in subsection (i) (a) shall:
 - a. be of an officer of a rank at management level or above with relevant qualifications and experience to enable him to respond sufficiently well to inquiries relating to the Company and the conduct of its business and possess core competencies and knowledge in administering anti-money laundering measures;
 - b. be responsible for establishing and maintaining such manual of compliance procedures in relation to its business;
 - c. be responsible for ensuring compliance by staff of the Company with:
 - any law relating to money laundering or terrorist financing; and
 - any manual of compliance procedures established.

II. IDENTIFICATION PROCEDURES

1. Identification procedures for certain pre commencement customers

This section applies to the provision by the Company of a service (the post commencement service) to a customer if, at a time before the commencement of this section, the Company commenced to provide a service to the customer.

2. Verification of identity of pre commencement customer

This section applies to the Company if:

- a. at a time before the commencement of this section, the Company commenced to provide a service to a customer; and
- b. after the commencement of this section, a suspicious matter reporting obligation arises for the Company in relation to the customer.

Requirements:

The Company must:

- a. take such action as is specified in the AML/ CTF Rules; and
- b. do so within the time limit allowed under the AML/ CTF Rules.

3. Identification procedures for certain low risk services

This section applies to the provision by the Company of a service to a customer if, under the AML/ CTF Rules, the

service is taken to be a low risk service

4. Verification of identity of low risk service customer

This section applies to the Company if:

- a. at a particular time (the relevant time), the Company commences to provide a service to a customer; and
- b. under the AML/ CTF Rules, the service is taken to be a low risk designated service; and
- c. at the relevant time or a later time, a suspicious matter reporting obligation arises for the Company in relation to the customer

Requirements:

The Company must:

- a. take such action as is specified in the AML/ CTF Rules; and
- b. do so within the time limit allowed under the AML/ CTF Rules.

5. Identification procedures

5.1 Carrying out the applicable customer identification procedure before the commencement of the provision of a service

For the purposes of this Manual, if the Company commences to provide a service to a customer, there are taken to be special circumstances that justify the carrying out of the applicable customer identification procedure in respect of the customer after the commencement of the provision of the service if, and only if:

- a. there are no special circumstances that justify carrying out the applicable customer identification procedure in respect of the customer after the commencement of the provision of the service; and
- b. such other conditions (if any) as are set out in the AML/ CTF Rules are satisfied.

5.2 Special circumstances that justify carrying out the applicable customer identification procedure after the commencement of the provision of a service

For the purposes of this Manual, if the Company commences to provide a service to a customer, there are taken to be special circumstances that justify the carrying out of the applicable customer identification procedure in respect of the customer after the commencement of the provision of the service if, and only if:

- a. the service is specified in the AML/ CTF Rules; and

- b. such other conditions (if any) as are set out in the AML/ CTF Rules are satisfied.

5.3 Carrying out the applicable customer identification procedure after the commencement of the provision of a service

If:

- a. the Company has commenced to provide a service to a customer; and
- b. when the Company commenced to provide the service to the customer, there were special circumstances that justified the carrying out of the applicable customer identification procedure in respect of the customer after the commencement of the provision of the service; and
- c. the Company has not previously carried out the applicable customer identification procedure in respect of the customer; and
- d. the Company has not carried out the applicable customer identification procedure in respect of the customer within whichever of the following periods is applicable:
 - iii. if the service is specified in the AML/ CTF Rules - the period ascertained in accordance with the AML/ CTF Rules; or
 - iv. in any other case - the period of five (5) business days after the day on which the Company commenced to provide the service.

A period ascertained in accordance with AML/ CTF Rules made for the purposes of subparagraph (d)(i):

- must commence at the time when the Company commences to provide the service concerned; and
- may be expressed to end on the occurrence of a specified event.

5.4 Customer Due Diligence

- i. The Company shall establish the identity and verify the identity of any customer of the Company by requiring the customer to produce an identification record or such other reliable, independent source document.
- ii. The obligation to identify customers exists if the customers proceed with the following:
 - a. Opens an account with the Company
 - b. Engages the services of the Company
 - c. Enters into a business relationship with the Company
- iii. The Company must carry out a prescribed identification process on:
 - a. a person conducting a transaction

- b. a person whose behalf a transaction is being conducted
- c. a beneficial owner
- iv. The requirements of subsection (i) shall apply when:
 - a. The Company carries out an electronic currency transfer for the Customer,
 - b. Suspects that the Customer is involved in proceeds of crime, a financing of terrorism or a serious offence,
 - c. Suspects that the transaction involves proceeds of crime, or may be used for financing terrorism or for committing a serious offence or.
 - d. There are doubts on the veracity or adequacy of the customer identification or information that had previously obtained.
- i. In order to confirm the identity of the corporate customer, the Company must acquire:
- v. Generally, the Company should not accept funds from prospective customers unless the necessary verification has been completed.
- vi. Without limiting the generality of the aforementioned, the Company shall:
 - a. when establishing a business relationship, obtain information on the purpose and nature of the business relationship and the source of funds;
 - b. if the transaction is conducted by a natural person, adequately identify and verify his identity including information relating to:
 - the person's name and address;
 - the national identity card, social security document, passport or other applicable official identifying document;
 - the source of funds;
 - c. if the transaction is conducted by a legal person or legal arrangement, obtain information on that legal person or legal arrangement, adequately identify the company, the beneficial owner and ultimate natural persons providing the funds of such legal person or legal arrangement and take reasonable measures to identify and verify the legal status, ownership and control structure, including information relating to:
 - proof of incorporation or similar evidence of establishment or existence; and;
 - the customer's name, name of trustee and ultimate settler (for trusts) and of persons providing funds and council members (for foundations), legal form, head office address and identities of

- directors (for legal persons) and source of funds;
- d. have appropriate risk management systems to determine if a potential customer, customer or beneficial owner is, is likely to be, is found to be or becomes a politically exposed person, and if so, shall:
 - adequately identify and verify his/ her identity as set out in this section;
 - obtain the approval of Senior Management before establishing or continuing a business relationship with the politically exposed person;
 - take reasonable measures to establish the source of funds and source of property; and
 - conduct regular enhanced ongoing monitoring of the business relationship.;
 - e. perform due diligence measures on a risk sensitive basis; and
 - f. upon the establishment of a business relationship, and when completing the verification of the identity of the customer and beneficial owner, ensure that money laundering risks are effectively managed.
 - vii. The Company shall, in relation to its higher risk category of customers or business relationship, conduct annual reviews of its record to ensure that the documents, data or information obtained pursuant to subsection (vi) is kept up-to-date and relevant.
 - viii. If it appears to the Company that an applicant requesting it to enter into any business relationship or transaction, whether or not in the course of a continuing business relationship, is acting on behalf of another person, the Company shall establish the true identity of any person on whose behalf or for whose ultimate benefit the applicant may be acting in the proposed transaction, whether as a trustee, nominee, agent or otherwise.
 - ix. Nothing in this section shall require the production of any evidence of identity where:
 - a. the customer is itself a financial institution to which the legislative applies and which has been licensed or registered, and is supervised for anti-money laundering and countering the financing of terrorism measures by a regulatory authority and the Company has satisfied itself as to the adequacy of the measures to prevent money laundering and the financing of terrorism; or
 - b. there is a transaction or a series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity.
 - x. The Company does not rely on an intermediary or third party to undertake its obligations under the above subsections or to introduce business to it.
 - xi. The Company does not accept anonymous accounts or accounts in fictitious names.

- xii. As part of the due diligence process, the Company should:
 - a. Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset of a business relationship. This process should include, where appropriate:
 - i. Taking reasonable measures to understand the ownership and control structure of the customer;
 - ii. Obtaining information on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and
 - iii. Discontinuing the transaction, if customer documentation information is not forthcoming.
 - b. Employ enhanced due diligence procedures for high risk customers or transactions or business relationships such as private banking operations, non-resident customers, trust arrangements, companies having nominee shareholders or customers who the financial institution has reasons to believe are being refused banking facilities by another financial institution; The Company does not accept this type of customer.
- xiii. When an existing customer closes one account and opens another, or enters into a new agreement to purchase products or services, there is no need to re-verify identity or address. However, the opportunity should be taken to confirm the relevant customer information. This is particularly important when a previously dormant account has been reactivated or if there has been no recent contact or correspondence with the customer within the last twelve (12) months.

5.5 KYC Documentation for natural persons

- i. The Company must obtain and document the following basic information when seeking to verify identity:
 - a. True name/ names used and correct permanent residential address including postcode (if applicable);
 - b. Valid photo-bearing identification, with unique identifier, (e.g. passport, social security card or driver's license along with a passport or social security card);
 - c. Date and place of birth and nationality (indication should be made if dual citizenship is maintained);
 - d. Contact details, e.g. telephone number, fax number and e-mail address;
 - e. Signature;
 - f. Purpose of the account and the nature of the business relationship.
- ii. The following information may also be required when the Company seeks to verify identity:
 - a. Occupation and name of employer (if self-employed, the nature of the self-employment);
 - b. Estimated level of account activity including:
 - 1. Size in the case of investment and custody accounts;

2. Balance ranges, in the case of current and deposit accounts;
 3. An indication of the expected transaction volume of the account;
 - c. Source of funds; and
 - d. Any other information deemed appropriate and relevant.
- iii. Identification documents, should be pre-signed and bear discernible photograph of the applicant, for example: current valid passport.
 - iv. One or more of the following steps used in order to confirm customer's addresses:
 - a. Checking the Register of Electors;
 - b. Provision of a recent utility bill, tax assessment or bank or credit union statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
 - c. Checking the telephone directory; and
 - d. Record of home visit..
 - v. Where prospective customers provide documents with which a financial institution is unfamiliar, either because of origin, format or language, the financial institution must take reasonable steps to verify that the document is indeed authentic, which may include contacting the relevant authorities or obtaining a notarized translation.
 - vi. In circumstances where the Company's customer is considered a high risk client, the Company should also take reasonable measures to establish the customer's source of wealth and document findings.

5.6 KYC Documentation for corporate customers

- i. To satisfy itself as to the identity of the corporate customer, the Company obtain
 - a. Name of corporate entity;
 - b. Principal place of business and registered office;
 - c. Mailing address;
 - d. Contact telephone and fax numbers;
 - e. Board resolution authorizing the opening of the account and conferring authority on signatories to the account;
 - f. An extract from the Commercial Register, or equivalent document, evidencing the registration of corporate acts and amendments;
 - g. Satisfactory evidence of the identity of all account signatories, details of their relationship with

the company and if they are not employees, an explanation of the relationship. All signatories must be verified in accordance with the identification and verification of identity requirements of natural persons:

- h. Identity information on the natural persons with a controlling interest in the corporate entity. This information should extend, as far as practicable, to identifying those with a minimum of 10% shareholding, those who ultimately own and have principal control over the company's assets, including anyone who is giving instructions to the financial institution to act on behalf of the company. However, if the company is publicly listed on a recognized stock exchange and not subject to effective control by a small group of individuals, identification and verification of the identity of shareholders is not required;
- i. Confirmation before a business relationship is established, by way of company search and/ or other commercial enquiries that the applicant company has not been, or is not in the process of being dissolved, struck off the companies register, wound-up or terminated. Such confirmation may be verified by obtaining a current Certificate of Good Standing or equivalent document or alternatively, obtaining a set of consolidated financial statements that have been audited by a reliable firm of auditors and that show the group structure and ultimate controlling party;

5.7 TKYC Documentation for trust clients

In the case of a nominee relationship, obtain identification evidence for the beneficial owner(s).

5.8 Customers' Profile Policy

- i. A customer profile policy is determined and implemented under particular criteria related with clients' risk profile. In particular, the factors that specify the risk category at which a client is attributed are mainly dealing with client:
 - a. The nature of the customer's business (whether cash intensive e.g. casinos and restaurants);
 - b. The nature and frequency of the activity;
 - c. The complexity, volume and pattern of transactions;
 - d. Type, status and value of account;
 - e. Type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place);
 - f. Type of product/ service (e.g. whether private banking, one-off transaction, mortgage);
 - g. Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash withdrawals);

- h. Geographical origin of the customer;
- i. Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of money laundering/ financing of terrorism, whether the customer is subject to regulatory or public disclosure requirements);
- j. Whether the origin of wealth and/or source of funds can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;
- k. Unwillingness of the customer to cooperate with the financial institution's customer due diligence process for no apparent reason;
- l. Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

5.9 Risk based approach

- i. The Company's risk-based approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme. This should be evidenced by categorization of the customer base, products and services by risk rating and identification of assigned actions by risk types.
- ii. Prior to establishing a business relationship, the Company should assess the potential risk inherent in each new client relationship. This assessment should take into account the products or facilities to be used by the customer and whether and to what extent a customer may expose the Company to risk. The financial institution should then decide whether or not to establish or continue with a relationship.
- iii. The Company categorises customers in terms of risk in three (3) groups, namely:
 - a. Low Risk
 - b. Medium Risk
 - c. High Risk
- iv. The Company's risk based approach take into account customer acceptance and on-going monitoring policies and procedures that assist the Company in identifying the types of customers that are likely to pose higher than average money laundering and terrorist financing risk.
- v. The Company is required to risk rate all client relationships including those in existence prior to the implementation of these Guidelines. All risk ratings should be documented and should be in place for all customers.
- vi. The Company adopted reasonable criteria for assessing the risks (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place).

- vii. The Company conducts periodic reviews (however, not more than two years apart) to determine whether any adjustment should be made to its risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

a. **Simplified customer due diligence**

Reduced due diligence is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national systems

b. **Enhanced customer due diligence**

- i. A more extensive customer due diligence process should be adopted for higher risk customers. In particular, the Company applies enhanced due diligence to customers where the risk of being used for money laundering or terrorist financing is high. It follows, then, that simplified customer due diligence measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

- ii. The Company may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A financial institution may be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries.

- iii. Applying a risk-based approach, enhanced due diligence for high risk accounts may include, where deemed relevant, and with more frequency than applied for low risk customers:

- a. An evaluation of the principals;
- b. A review of current financial statements;
- c. Verification of the source of funds;
- d. Verification of source of wealth;
- e. The conduct of reference checks;
- f. Checks of electronic databases; and
- g. Periodic reporting to the Board about high risk accounts.

- iv. The Company should give particular attention to the following business relations and transactions:

- a. An evaluation of the principals;

- b. A review of current financial statements;
- c. Verification of the source of funds;
- d. Verification of source of wealth;
- e. The conduct of reference checks;
- v. In particular, the Company defines the following types of customers as high-risk clients and therefore enhanced due diligence are applied:
 - a. Non-Face to Face Customers
 - b. Politically Exposed Persons
 - c. High-Risk Countries;

6.0 Verification of identity

6.1 Verification of identity of customer

This section applies to the Company if:

- a. at a particular time, the Company has carried out, or has purported to carry out, the applicable customer identification procedure in respect of a particular customer to whom the reporting entity provided, or proposed to provide, a designated service; and
- b. at a later time, any of the following subparagraphs applies:
 - i. an event prescribed by the AML/ CTF Rules happens;
 - ii. a circumstance specified in the AML/ CTF Rules comes into existence;
 - iii. a period ascertained in accordance with the AML/ CTF Rules ends.

Requirements:

The Company must:

- i. take such action as is specified in the AML/ CTF Rules; and
- ii. do so within the time limit allowed under the AML/ CTF Rules.

6.2 Use and disclosure of personal information for the purposes of verifying an individual's identity

- A. **The Company may disclose certain personal information to credit reporting bodies for identity verification purposes**

- The Company may, to assist in verifying the identity of an individual, the regulations or the AML/CTF Rules:
 - a. disclose any or all of the following personal information to a credit reporting body for the purposes of making a request referred to in paragraph (b):
 - i. the individual's name;
 - ii. the individual's residential address;
 - iii. the individual's date of birth; and.
 - b. request the credit reporting body to provide an assessment of whether the personal information so disclosed matches (in whole or part) personal information held by the credit reporting body.
- The Company must not make a verification request in relation to an individual unless, before making the request:
 - a. the individual was given information about:
 - i. the reasons for making the request; and
 - ii. the personal information about the individual that may be disclosed to the credit reporting body; and
 - iii. the fact that the Company may request the credit reporting body to provide an assessment of whether the personal information matches (in whole or part) personal information held by the credit reporting body; and
 - iv. the fact that the credit reporting body may prepare and provide to the reporting entity such an assessment; and
 - v. the fact that the credit reporting body may use the personal information about the individual, and personal information held by the body that is the names, residential addresses and dates of birth of other individuals, for the purpose of preparing such an assessment; and
 - b. the individual expressly agreed to the making of the request and the disclosure of the personal information; and
 - c. an alternative means of verifying the identity of the individual was made available to the individual.

B. Credit reporting bodies may use and disclose certain personal information for identity verification purposes

1. A credit reporting body that receives a verification request from the Company in relation to an individual may:

- a. prepare and provide to the Company an assessment in accordance with this section of whether any or all of the following personal information matches (in whole or part) personal information held by the credit reporting body:
 - i. the individual's name;
 - ii. the individual's residential address;
 - iii. the individual's date of birth; and
 - b. use the personal information about the individual, and personal information held by the credit reporting body that is the names, residential addresses and dates of birth of other individuals, for the purpose of preparing the assessment.
2. An assessment provided under subsection (1) to the Company;
 - a. be responsible for ensuring compliance by staff of the Company with:
 - b. any law relating to money laundering or terrorist financing; and

C. The Company to notify inability to verify identity

1. This section applies if:
 - a. the Company makes a verification request in relation to an individual; and
 - b. an assessment is provided in relation to the individual; and
 - c. the Company is unable to verify the identity of the individual, having regard to the assessment.
2. The Company must give a written notice to the individual:
 - a. stating that the Company is unable to verify the identity of the individual having regard to the assessment; and
 - b. specifying the name of the credit reporting body that provided the assessment; and
 - c. offering the individual an alternative means of verifying the identity of the individual..

D. Retention of verification information

1. The Company that makes a verification request in relation to an individual must make a record of the following:
 - a. the name of the credit reporting body to which the request was made;
 - b. the personal information about the individual that was provided by the Company to the credit reporting body;
 - c. the assessment (if any) provided by the credit reporting body in relation to the individual;

- d. such other information about the verification request as is specified in the AML/ CTF Rules.
2. The Company must retain the record, or a copy of the record, until the end of the first seven (7) year period:
 - a. that began at a time after the verification request was made; and
 - b. throughout the whole of which the Company did not provide any designated services to the individual
3. The Company that retains a record, or a copy of a record, under subsection (2) must delete the record at the end of the seven (7) year period referred to in that subsection.

E. Access to verification information

The Company in possession or control of personal information, or other information of a kind referred to in the above subsections, that relates to a verification request or an assessment in relation to an individual must take reasonable steps to ensure that the individual can obtain access to the information.

7.0 Ongoing customer due diligence

The Company must:

- a. monitor its customers in relation to the provision by the Company of services at or through a permanent establishment of the Company in Australia, with a view to (i) identifying, (ii) mitigating, (iii) managing the risk the Company may reasonably face that the provision by the Company of a service at or through a permanent establishment of the Company in Australia might (whether inadvertently or otherwise) involve or facilitate (i) money laundering; or (ii) financing of terrorism; and
- b. do so in accordance with the AML/ CTF Rules.

8.0 General provisions

8.1 Applicable customer identification procedures may be carried out by an agent of a reporting entity

1. The principles of agency apply in relation to the carrying out by the Company of an applicable customer identification procedure or an identity verification procedure.
2. For example, the Company may authorise another person to be its agent for the purposes of carrying out applicable customer identification procedures or identity verification procedures on the Company's behalf.
3. To avoid doubt, if the Company provides a service to a customer through an agent of the Company, the latter may authorise (a) that agent; or (b) any other person to be its agent for the purposes of carrying out the applicable customer identification procedure or an identity verification procedure in respect of

the customer on the Company's behalf.

8.2 Applicable customer identification procedures deemed to be carried out by the Company

If:

- a. the Company carried out the applicable customer identification procedure in respect of a particular customer to whom the Company provided, or proposed to provide, a designated service; and
- b. the applicable customer identification procedure was carried out in such circumstances as are specified in the AML/ CTF Rules; and
- c. the customer is or becomes a customer to whom another Company provides, or proposes to provide, a service; and
- d. such other conditions set out in the AML/ CTF Rules are satisfied

8.3 General exemptions

1. This Part does not apply to a service that is of a kind specified in the AML/ CTF Rules.
2. The AML/ CTF Rules may provide that a specified provision of this Part does not apply to a designated service that is of a kind specified in the AML/ CTF Rules.
3. This Part does not apply to a service that is provided in circumstances specified in the AML/ CTF Rules.
4. The AML/ CTF Rules may provide that a specified provision of this Part does not apply to a service that is provided in circumstances specified in the AML/ CTF Rules.
5. This Part does not apply to a service that is provided by the Company at or through a permanent establishment

III. REPORTING OBLIGATIONS

1. Simplified Outline

The following is a simplified outline of this Part:

- The Company must give the AUSTRAC CEO reports about suspicious matters.
- If the Company provides a service that involves a threshold transaction, the Company must give the AUSTRAC CEO a report about the transaction.
- If a person sends or receives an international funds transfer instruction, the person must give the AUSTRAC CEO a report about the instruction.

- The Company may be required to give AML/ CTF compliance reports to the AUSTRAC CEO. Outline

2. Suspicious Matters

2.1 Suspicious matter reporting obligation

1. A suspicious matter reporting obligation arises in relation to a person (the first person) if, at a particular time (the relevant time):
 - a. the Company commences to provide, or proposes to provide, a service to the first person; or
 - b. both:
 - i. the first person requests the Company to provide a service to the first person; and
 - ii. the service is of a kind ordinarily provided by the Company; or
 - c. both:
 - i. the first person inquires of the Company whether it would be willing or prepared to provide a service to the first person; and
 - ii. the service is of a kind ordinarily provided by the Company;and any of the following conditions is satisfied:
 - d. at the relevant time or a later time, the Company suspects on reasonable grounds that the first person is not the person the first person claims to be;
 - e. at the relevant time or a later time, the Company suspects on reasonable grounds that an agent of the first person who deals with the Company in relation to the provision or prospective provision of the service is not the person the agent claims to be;
 - f. at the relevant time or a later time, the Company suspects on reasonable grounds that information that the Company has concerning the provision, or prospective provision, of the service:
 - i. may be relevant to investigation of, or prosecution of a person for, an evasion, or an attempted evasion, of a taxation law; or
 - ii. may be relevant to investigation of, or prosecution of a person for, an evasion, or an attempted evasion, of a law of a State or Territory that deals with taxation; or
 - iii. may be relevant to investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a State or Territory; or
 - iv. may be of assistance in the enforcement of the Proceeds of Crime Act 2002 or regulations under that Act; or

- v. may be of assistance in the enforcement of a law of a State or Territory that corresponds to the Proceeds of Crime Act 2002 or regulations under that Act;
- g. at the relevant time or a later time, the Company suspects on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence covered by paragraph (a), (b) or (c) of the definition of financing of terrorism;
- h. at the relevant time or a later time, the Company suspects on reasonable grounds that information that The Company has concerning the provision, or prospective provision, of the service may be relevant to the investigation of, or prosecution of a person for, an offence covered by paragraph (a), (b) or (c) of the definition of financing of terrorism;
- i. at the relevant time or a later time, the Company suspects on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence covered by paragraph (a) or (b) of the definition of money laundering;
- j. at the relevant time or a later time, the Company suspects on reasonable grounds that information that the Company has concerning the provision, or prospective provision, of the service may be relevant to the investigation of, or prosecution of a person for, an offence covered by paragraph (a) or (b) of the definition of money laundering.

2.2 Report

1. If a suspicious matter reporting obligation arises for the Company in relation to a person, the Company must give the AUSTRAC CEO a report about the matter.
2. A report under subsection (1) must:
 - a. be in the approved form; and
 - b. contain such information relating to the matter as is specified in the AML/ CTF Rules; and
 - c. contain a statement of the grounds on which the Company holds the relevant suspicion.
3. Reasonable grounds for suspicion: The AML/ CTF Rules may specify matters that are to be taken into account in determining whether there are reasonable grounds for the Company to form a suspicion.

2.3 Reporting of suspicious transactions by the Company

1. The Company shall pay special attention to:
 - a. all complex, unusual or large business transactions, or unusual patterns of transactions, whether completed or not, and to insignificant but periodic transactions, that have no apparent economic or lawful purpose;
 - b. business relations and transactions with persons including legal persons and arrangements, from or in jurisdictions that do not have adequate systems in place to prevent or deter money laundering or terrorist financing;

- c. electronic funds transfer that do not contain complete originator information and shall adopt effective risk-based procedures to identify and handle any such transfer.
2. In relation to subsection (i), the Company shall set forth in writing the specific information regarding the transaction(s) or business relations specified in subsection (i) (a) to (c) of this section, its background and purpose to the extent known, and the identity of the persons involved
3. The Company shall conduct ongoing due diligence on its business relationships and scrutinize transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with information that the Company has of its customer and the profile of the customer's business and where necessary the source of funds.
4. Whenever the Company suspects or has reasonable grounds to suspect that any transaction, proposed transaction or attempted transaction is related to the commission of a money laundering offence or terrorist financing offence or is related or linked to, or is to be used in connection with a terrorist act or for the financing of terrorism, or that the funds or property are the proceeds of crime, it shall as soon as possible but not later than 1 days after forming that suspicion and wherever possible before the transaction is carried out:
 - a. take reasonable measures to ascertain the purpose of the transaction, the origin and ultimate destination of the funds involved and the identity and address, of any ultimate beneficiary;
 - b. prepare a report of the transaction.;
5. Overall the Company shall report any suspicious transaction or activity, and/ or any large cash transactions that may be out of the scene.
6. A report required shall:
 - a. set forth all particulars known regarding the transaction;
 - b. contain a statement of the grounds on which the Company holds the suspicion; and
 - c. be signed or otherwise authenticated by the Company.

3. Threshold transactions

3.1 Reports of threshold transactions

- a. This section applies to the Company if (a) the Company commences to provide, or provides, a service to a customer; and (b) the provision of the service involves a threshold transaction.
- b. The Company must, within ten (10) business days after the day on which the transaction takes place, give the AUSTRAC CEO a report of the transaction.
- c. A report under subsection (B) must:

- i. be in the approved form; and
- ii. contain such information relating to the transaction as is specified in the AML/ CTF Rules.

3.2 Exemptions

- a. This Division does not apply to a that is of a kind specified in the AML/ CTF Rules.
- b. The AML/ CTF Rules may provide that a specified provision of this Division does not apply to a service that is of a kind specified in the AML/ CTF Rules.
- c. This Division does not apply to a service that is provided in circumstances specified in the AML/ CTF Rules.
- d. The AML/ CTF Rules may provide that a specified provision of this Division does not apply to a service that is provided in circumstances specified in the AML/ CTF Rules.

4. International funds transfer instructions

4.1 Reports of international funds transfer instructions

1. This section applies to a person if:
 - a. the person is:
 - i. the sender of an international funds transfer instruction transmitted out of Australia; or
 - ii. the recipient of an international funds transfer instruction transmitted into Australia; and
 - b. if the regulations provide that this paragraph is applicable - the total amount or value that is to be, or is, transferred is not less than the amount specified in the regulations; and
 - c. such other conditions (if any) as are set out in the AML/ CTF Rules are satisfied.
2. The person must, within ten (10) business days after the day on which the instruction was sent or received by the person, give the AUSTRAC CEO a report about the instruction.
3. A report under subsection (2) must:
 - a. be in the approved form; and
 - b. contain such information relating to the matter as is specified in the AML/ CTF Rules.
4. For the purposes of this section, it is immaterial whether the person sent or received the international funds transfer instruction in the capacity of interposed institution in a funds transfer chain.
5. This section does not apply to an international funds transfer instruction that is of a kind specified in the AML/

CTF Rules.

6. This section does not apply to an international funds transfer instruction that is sent or received in circumstances specified in the AML/ CTF Rules.

5. AML/ CTF compliance reports

1. This section applies if the AML/ CTF Rules provide that, for the purposes of this section (a) a specified period is a reporting period; and (b) a specified period beginning at the end of a reporting period is the lodgement period for that reporting period.
2. The Company must, within the lodgement period, give the AUSTRAC CEO a report relating to the Company's compliance with this Act, the regulations and the AML/ CTF Rules during the reporting period.
3. A report under subsection (2) must:
 - a. be in the approved form; and
 - b. contain such information as is required by the approved form.
4. If the Company is a member of a designated business group, the obligation imposed on the Company by subsection (2) may be discharged by any other member of the group.
5. If two (2) or more Companies are members of a designated business group, reports under subsection (2) relating to those reporting entities may be set out in the same document.
6. AML/ CTF Rules made for the purposes of this section may make different provision with respect to different reporting entities.
7. A person is not excused from giving a report under the subsections (1) - (6) on the ground that the report might tend to incriminate the person or expose the person to a penalty.

6. General provisions

1. If the Company communicates information to the AUSTRAC CEO under the provisions of the above sections, then:
 - a. the AUSTRAC CEO; or
 - b. the Commissioner of the Australian Federal Police; or
 - c. the Chief Executive Officer of the Australian Crime Commission; or
 - d. the Commissioner of Taxation; or
 - e. the Comptroller General of Customs; or

- f. the Integrity Commissioner; or
- g. an investigating officer who is carrying out an investigation arising from, or relating to the matters mentioned in, the information;

may, by written notice given to the Company or any other person, require the Company or other person (1) to give such further information as is specified in the notice, within the period and in the manner specified in the notice, to the extent to which the Company or other person has that information; or (2) to produce, within the period and in the manner specified in the notice, such documents as are:

- i. specified in the notice; and
 - ii. relevant to the matter to which the communication under the aforementioned sections relates; and
 - iii. in the possession or control of the Company or other person.
2. A person (the issuer) must not give a notice under subsection (1) to another person (the recipient) unless the issuer reasonably believes that the recipient has knowledge of the information, or possession or control of the document, that is specified in the notice.
 3. The period specified in the notice for giving the information or document must be at least fourteen (14) days after the notice is given unless:
 - a. the recipient is the Company who communicated information to the AUSTRAC CEO under the aforementioned sections; or
 - b. both of the following apply:
 - i. the issuer considers that specifying a shorter period is necessary;
 - ii. the shorter period specified is reasonable in the circumstances.

7. AML/ CTF Rules may make provision in relation to reports by registered remittance affiliates

1. The AML/ CTF Rules may make provision for and in relation to reports required by this Part to be given by the Company that is a registered remittance affiliate of a registered remittance network provider.
2. Without limiting subsection (1), the AML/ CTF Rules may provide:
 - a. that an obligation imposed by this Part upon a registered remittance affiliate of a registered remittance network provider to provide a report is taken instead, or in addition, to be an obligation imposed upon the registered remittance network provider; and
 - b. that an obligation imposed by this Part on a registered remittance affiliate of a registered remittance

network provider may be discharged by the registered remittance network provider; and

- c. that a report required to be provided as mentioned in paragraph (a) must, or may, be given by the registered remittance network provider in the manner specified in the AML/CTF Rules.

8. Request to obtain information about the identity of holders of foreign credit cards and foreign debit cards

1. This section applies to the Company if:
 - a. the AUSTRAC CEO or the Commissioner of Taxation has required the Company to give information about the identity of:
 - i. the holder of, or a signatory to, a particular credit card account; or
 - ii. the holder of, or a signatory to, a particular debit card account; and
 - b. the account relates to a credit card, or a debit card, that was issued by a person (the card issuer) outside Australia; and
 - c. the Company does not have that information.
2. The AUSTRAC CEO or the Commissioner of Taxation may, by written notice given to the Company, direct the Company to give the card issuer a request, in a form specified in the notice, to give the information to the Company.
3. The Company must comply with the direction within ten (10) business days after the day on which the direction is given.
4. If the Company gives the card issuer a request under subsection (2) that was directed by the AUSTRAC CEO, the Company must, within:
 - a. twenty (20) business days after the day on which the subsection (2) direction was given; or
 - b. if the AUSTRAC CEO, by written notice given to the Company, allows a longer period - that longer period; give the AUSTRAC CEO a report about the card issuer's response, or lack of response, to the request.
5. If the Company gives the card issuer a request under subsection (2) that was directed by the Commissioner of Taxation, the Company must, within:
 - a. twenty (20) business days after the day on which the subsection (2) direction was given; or
 - b. if the Commissioner of Taxation, by written notice given to the Company, allows a longer period - that

longer period;

give the Commissioner of Taxation a report about the card issuer's response, or lack of response, to the request.

6. A report under subsection (4) or (5) must:
 - a. be in the approved form; and
 - b. in a case where the card issuer has given the information to the Company - contain the information; and
 - c. contain such other information (if any) relating to the matter as is required by the approved form.

9. Reporting Entities Roll

9.1 Reporting entities must enrol

1. If a person's name is not entered on the Reporting Entities Roll, the person must:
 - a. if the Company commences to provide a service should apply in writing to the AUSTRAC CEO within twenty eight (28) days after commencing to provide the designated service.
2. The AUSTRAC CEO must maintain a roll for the purposes of this Part, to be known as the Reporting Entities Roll.
3. The AUSTRAC CEO may maintain the Reporting Entities Roll by electronic means.
4. The Reporting Entities Roll is not a legislative instrument.
5. The AML/ CTF Rules may make provision for and in relation to either or both of the following:
 - a. the correction of entries in the Reporting Entities Roll;
 - b. any other matter relating to the administration or operation of the Reporting Entities Roll, including the removal of names and enrolment details from the Reporting Entities Roll.
6. A person may apply in writing to the AUSTRAC CEO for enrolment as a reporting entity. The application must:
 - a. be in accordance with the approved form, or in a manner specified in the AML/ CTF Rules; and
 - b. contain the information required by the AML/ CTF Rules.
7. A person who is enrolled under this Part must advise the AUSTRAC CEO, in accordance with the aforementioned subsections, of any change in the person's enrolment details that is of a kind specified in the AML/ CTF Rules.
8. A person who is required by subsection (7) to advise the AUSTRAC CEO of a change in enrolment details must

do so:

- a. within fourteen (14) days of the change arising; and
- b. in accordance with the approved form, or in a manner specified in the AML/ CTF Rules.

9.2 Removal of entries from the Reporting Entities Roll

1. A person may, in writing, request the AUSTRAC CEO to remove the person's name and enrolment details from the Reporting Entities Roll.
2. The request must:
 - a. be in the approved form; and
 - b. contain the information required by the AML/ CTF Rules.
3. The AUSTRAC CEO must consider the request and remove the person's name and enrolment details from the Reporting Entities Roll if the AUSTRAC CEO is satisfied that it is appropriate to do so, having regard to:
 - a. whether the person has ceased to provide designated services; and
 - b. the likelihood of the person providing a service in the financial year beginning after the request is given; and
 - c. any outstanding obligations the person has (if any) to provide a report regarding:
 - i. threshold transaction reports;
 - ii. international funds transfer instruction reports;
 - iii. AML/ CTF compliance reports.

IV. REPORTS ABOUT CROSS-BORDER MOVEMENTS OF PHYSICAL CURRENCY AND BEARER NEGOTIABLE INSTRUMENTS

1. Simplified Outline

The following is a simplified outline of this Part:

- Cross border movements of physical currency must be reported to the AUSTRAC CEO, a customs officer or a police officer if the total value moved is above a threshold.
- If a bearer negotiable instrument is produced to a police officer or a customs officer by a person leaving or arriving in Australia, the officer may require the person to give a report about the instrument to the AUSTRAC CEO, a customs officer or a police officer.

2. Reports about physical currency

2.1 Reports about movements of physical currency into or out of Australia

1. A person commits an offence if:
 - a. either:
 - i. the person moves physical currency into Australia; or
 - ii. the person moves physical currency out of Australia; and
 - b. the total amount of the physical currency is not less than \$10,000; and
 - c. a report in respect of the movement has not been given in accordance with this section.

Penalty: Imprisonment for two (2) years or 500 penalty units, or both.

2. A person must not (a) move physical currency into Australia; or (b) move physical currency out of Australia if:
 - a. the total amount of the physical currency is not less than \$10,000; and
 - b. a report in respect of the movement has not been given in accordance with this section.
3. Subsections (1) and (2) do not apply to a person if:
 - a. the person is a commercial passenger carrier;
 - b. the physical currency is in the possession of any of the carrier's passengers;
 - c. the person is a commercial goods carrier;
 - d. the physical currency is carried on behalf of another person;
 - e. the other person has not disclosed to the carrier that the goods carried on behalf of the other person include physical currency.
4. A report under this section must:
 - a. be in the approved form; and
 - b. contain such information relating to the matter being reported as is specified in the AML/ CTF Rules; and
 - c. be given to the AUSTRAC CEO, a customs officer or a police officer.

2.2 Timing of reports about physical currency movements

1. A report under section 2.1. above must be given:

- a. if the movement of the physical currency is to be effected by a person bringing the physical currency into Australia with the person - at the time worked out under subsection (2); or
- b. if the movement of the physical currency is to be effected by a person taking the physical currency out of Australia with the person; or
- c. if the physical currency is to be taken out of Australia by a person by consignment of the physical currency:
 - i. through the post to a place outside Australia; or
 - ii. to another person for carriage to a place outside Australia by that other person or by a third person; at any time before the time when the physical currency is irrevocably committed by the first mentioned person to the Australian Postal Corporation or to the other person, as the case may be; or
- d. in any other case - at any time before the movement of the physical currency takes place.

2.3 Reports about receipts of physical currency from outside Australia

1. A person commits an offence if:
 - a. the person receives physical currency moved to the person from outside Australia; and
 - b. at the time of the receipt, the total amount of the physical currency is not less than \$10,000; and
 - c. a report in respect of the movement has not been made in accordance with the aforementioned sections before the movement; and
 - d. a report in respect of the receipt is not given in accordance with this section before the end of the period of five (5) business days beginning on the day of the receipt.

Penalty: Imprisonment for two (2) years or 500 penalty units, or both.

2. Strict liability applies to paragraphs (1)(c) and (d).
3. A person must not receive physical currency moved to the person from outside Australia if:
 - a. at the time of the receipt, the total amount of the physical currency is not less than \$10,000; and
 - b. a report in respect of the movement has not been made in accordance with the aforementioned sections before the movement; and
 - c. a report in respect of the receipt is not given in accordance with this section before the end of the period of five (5) business days beginning on the day of the receipt.
4. A report under this section must:

- a. be in the approved form; and
- b. contain such information relating to the matter being reported as is specified in the AML/ CTF Rules; and
- c. be given to the AUSTRAC CEO, a customs officer or a police officer.

3. Information about reporting obligations

1. This section applies to a written notice:
 - a. that relates to reporting obligations under this Part; and
 - b. the form and contents of which are specified in the AML/ CTF Rules.
2. A customs officer may affix, or arrange for another person to affix, one or more notices:
 - a. on any part of an aircraft or ship; or
 - b. in any other place specified in the AML/ CTF Rules.
3. A person commits an offence if:
 - a. a notice has been affixed under this section; and
 - b. the person engages in conduct; and
 - c. the person's conduct results in:
 - i. interference with the notice; or
 - ii. the removal of the notice; or
 - iii. defacement of the notice.

Penalty: 50 penalty units.

4. Subsection (3) does not apply if the person's conduct is authorised by the AUSTRAC CEO or the Comptroller General of Customs.
5. An offence against subsection (3) is an offence of strict liability.
 - a.

V. ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING PROGRAMS

1. Simplified Outline

The following is a simplified outline of this Part:

- The Company must have and comply with an anti money laundering and counter terrorism financing program.
- An anti money laundering and counter terrorism financing program is divided into Part A (general) and Part B (customer identification).
- Part A of an anti money laundering and counter terrorism financing program is designed to identify, mitigate and manage the risk the Company may reasonably face that the provision by the Company of designated services at or through a permanent establishment of the entity in Australia might involve or facilitate:
 - a. money laundering; or
 - b. financing of terrorism.
- Part B of an anti money laundering and counter terrorism financing program sets out the applicable customer identification procedures for customers of the Company.

2. Company's Obligations

1. The Company must have in place an updated anti money laundering and counter terrorism financing program that applies to the Company. The Company should strictly follow the provisions of this AML Manual and the programs contained herein so that it complies with its anti-money laundering and counter terrorism financing obligations.
2. A standard anti money laundering and counter terrorism financing program is a written program that:
 - a. applies to the Company; and
 - b. is divided into the following parts:
 - i. Part A (general);
 - ii. Part B (customer identification).
3. Part A of the standard anti money laundering and counter terrorism financing program is a part:
 - a. the primary purpose of which is to:
 - i. identify; and
 - ii. mitigate; and
 - iii. manage;

the risk the Company may reasonably face that the provision by the Company of services at or through a permanent establishment of the Company in Australia might involve or facilitate money laundering or financing of terrorism; and

- b. if the Company provides designated services at or through a permanent establishment of the Company in a foreign country - another purpose of which is to ensure that the Company takes such action (if any) as is specified in the AML/ CTF Rules in relation to the provision by the Company of designated services at, or through a permanent establishment of the Company in a foreign country; and
 - c. that complies with such requirements (if any) as are specified in the AML/ CTF Rules.
4. Part B of the standard anti money laundering and counter terrorism financing program is a part:
- a. the sole or primary purpose of which is to set out the applicable customer identification procedures for the purposes of the application of the Anti Money Laundering Regulations to customers of the Company; and
 - b. that complies with such requirements (if any) as are specified in the AML/ CTF Rules.

3. Applicable customer identification procedures - customers other than individuals

1. AML/ CTF Rules require that Part B of a standard anti money laundering and counter terrorism financing program must provide that, if a customer of the Company is:
- a. a company; or
 - b. a trust; or
 - c. a partnership; or
 - d. a corporation sole; or
 - e. a body politic;
- one or more elements of the applicable customer identification procedure for the customer must involve the taking of steps specified in the AML/ CTF Rules in relation to a person who is:
- i. associated with the customer; and
 - ii. specified in the AML/ CTF Rules.
2. AML/ CTF Rules require that a special anti money laundering and counter terrorism financing program must provide that, if a customer of the Company is:
- a. a company; or
 - b. a trust; or
 - c. a partnership; or
 - d. a corporation sole; or

e. a body politic;

one or more elements of the applicable customer identification procedure for the customer must involve the taking of steps specified in the AML/ CTF Rules in relation to a person who is:

- a. associated with the customer; and
- b. specified in the AML/ CTF Rules.

4. Applicable customer identification procedures - disclosure certificates

1. AML/ CTF Rules require that, if:

- a. a service is provided to a customer specified in the AML/ CTF Rules; or
- b. a service is provided to a customer in circumstances specified in the AML/ CTF Rules;

Part B of the standard anti money laundering and counter terrorism financing program must provide that one (1) or more elements of the applicable customer identification procedure for the customer must involve the Company obtaining a certificate, to be known as a disclosure certificate, from:

- a. the customer; or
- b. person who is:
 - i. associated with the customer; and
 - ii. specified in the AML/ CTF Rules.

2. If the customer does not comply with the request, the Company may do any or all of following:

- a. refuse to continue to provide the service to the customer;
- b. refuse to commence to provide the service to the customer;
- c. restrict or limit the provision of the service to the customer;

until the customer provides the information covered by the request.

VI. CORRESPONDENT BANKING

1. Simplified Outline

The following is a simplified outline of this Part:

- The Company must not enter into a correspondent banking relationship with:
- a shell bank; or
- another financial institution that has a correspondent banking relationship with a shell bank.
- Before the Company enters into a correspondent banking relationship with another financial institution, the Company must carry out a due diligence assessment.
- If the Company has entered into a correspondent banking relationship with another financial institution, the Company must carry out regular due diligence assessments.

2. Prohibition of entry into correspondent banking relationships with shell banks

1. The Company must not enter into a correspondent banking relationship with another person if the person does so reckless as to whether:
 - a. the other person is a shell bank; or
 - b. the other person is a financial institution that has a correspondent banking relationship with a shell bank.

3. Termination of correspondent banking relationship with shell bank

1. If (a) the Company is in a correspondent banking relationship with another person and (b) the Company becomes aware that the other person is a shell bank, it must, within:
 - a. twenty (20) business days after becoming aware as mentioned in paragraph (1); or
 - b. such longer period (if any) as the AUSTRAC CEO allows;terminate the correspondent banking relationship.
2. If (a) the Company is in a correspondent banking relationship with another financial institution and (b) the Company becomes aware that the other financial institution has a correspondent banking relationship with a shell bank, the Company must, within:
 - a. twenty (20) business days after becoming aware as mentioned in paragraph (2); or
 - b. such longer period (if any) as the AUSTRAC CEO allows;either:
 - a. terminate the correspondent banking relationship mentioned above; or
 - b. request the other financial institution to terminate the correspondent banking relationship mentioned above.

3. If (a) the Company makes a request under sub-paragraph (2) of another financial institution and (b) at the end of the period of twenty (20) business days after the request was made, the other financial institution has not complied with the request, the Company must, within:
 - a. twenty (20) business days after the end of the period mentioned above; or
 - b. such longer period (if any) as the AUSTRAC CEO allows;terminate its correspondent banking relationship with the other financial institution.

4. Due diligence assessments before entering into correspondent banking relationships

1. Before the Company enters into a correspondent banking relationship with another financial institution, it must carry out an assessment of the risk it may reasonably face that the correspondent banking relationship might involve or facilitate money laundering or financing of terrorism.
2. Before the Company enters into a correspondent banking relationship with another financial institution, the Company must:
 - a. carry out an assessment of such matters as are specified in the AML/ CTF Rules; and
 - b. prepare a written record of the assessment as soon as practicable after the completion of the assessment;if carrying out the assessment is warranted by the risk identified in the assessment carried out by the Company under the above subsections.

5. Regular due diligence assessments of correspondent banking relationships

1. If the Company has, whether before or after the commencement of this section, entered into a correspondent banking relationship with another financial institution, the Company must carry out regular assessments of the risk it may reasonably face that the correspondent banking relationship might involve or facilitate money laundering or financing of terrorism.
2. If the Company has entered into a correspondent banking relationship with another financial institution, it must:
 - a. carry out regular assessments of such matters as are specified in the AML/ CTF Rules; and
 - b. prepare a written record of each assessment as soon as practicable after the completion of the assessment;if carrying out those assessments are warranted by the risk identified in an assessment carried out by the Company under the aforementioned subsections.
3. The intervals between subsequent assessments must not be longer than the period ascertained in accordance with the AML/ CTF Rules.

VII. COUNTERMEASURES

The regulations may make provision for or in relation to prohibiting or regulating the entering into of transactions, where:

- a. both:
 - i. one of the parties to the transaction is a resident of Australia; and
 - ii. the other party, or any of the other parties, is a resident of a prescribed foreign country; or
- b. both:
 - i. one of the parties to the transaction enters into the transaction in the course of carrying on an activity or business at or through a permanent establishment of the party in Australia; and
 - ii. the other party, or any of the other parties, is a resident of a prescribed foreign country; or
- c. both:
 - i. one of the parties to the transaction is a resident of Australia; and
 - ii. the other party, or any of the other parties, is a corporation incorporated in a prescribed foreign country; or
- d. both:
 - i. one of the parties to the transaction enters into the transaction in the course of carrying on an activity or business at or through a permanent establishment of the party in Australia; and
 - ii. the other party, or any of the other parties, is a corporation incorporated in a prescribed foreign country; or
- e. both:
 - i. one of the parties to the transaction is a resident of Australia; and
 - ii. the other party, or any of the other parties, is an individual who is physically present in a prescribed foreign country; or
- f. both:
 - i. one of the parties to the transaction enters into the transaction in the course of carrying on an activity or business at or through a permanent establishment of the party in Australia; and

- ii. the other party, or any of the other parties, is an individual who is physically present in a prescribed foreign country.

The provisions of the AML/ CTF Rules will apply in regards to this section.

VIII. RECORD KEEPING REQUIREMENTS

1. Simplified Outline

The following is a simplified outline of this Part:

- The AML/ CTF Rules provide that the Company must make a record of the service. The Company must retain the record for seven (7) years.
- If a Company's customer gives the Company a document relating to the provision of the service, the Company must retain the document for seven (7) years.
- The Company must retain a record of an applicable customer identification procedure for seven (7) years after the end of the Company's relationship with the relevant customer.
- The Company must retain a copy of its anti money laundering and counter terrorism financing program at all times.

2. Records of transactions

1. (1) The AML/ CTF Rules provide that, if the Company commences to provide, or provides, services to customers, it must make a record of information relating to the provision of the said services.
2. (2) The AML/ CTF Rules may provide that, if the Company provides services to customers in circumstances specified in the AML/ CTF Rules, it must make a record of information relating to the provision of the services.
3. (3) A record under subsection (1) or (2) must comply with such requirements as are specified in the AML/ CTF Rules.
4. (4) The Company must comply with AML/ CTF Rules made for the purposes of this section.

3. Transaction records to be retained

1. The Company must retain:
 - a. the record; or

- b. a copy of the record; or
- c. an extract from the record showing the prescribed information;

for seven (7) years after the making of the record.

4. Records of identification procedures

4.1 Copying documents obtained in the course of carrying out an applicable customer identification procedure

- a. If a document is produced to the Company in the course of an applicable customer identification procedure; and
- b. If the Company makes a copy of the document;

Then it is taken to have made a record of the information contained in the document.

4.2 Making of records of identification procedures

1. This section applies to the Company if it carries out an applicable customer identification procedure in respect of a particular customer to whom the Company provided, or proposed to provide the services.
2. The Company must make a record of:
 - a. the procedure; and
 - b. information obtained in the course of carrying out the procedure; and
 - c. such other information (if any) about the procedure as is specified in the AML/ CTF Rules.
3. A record under subsection (2) must comply with such requirements (if any) as are specified in the AML/ CTF Rules.

4.3 Retention of records of identification procedures

1. The Company must retain the record, or a copy of the record, until the end of the first seven (7) year period:
 - a. that began at a time after the procedure was carried out; and
 - b. throughout the whole of which the Company did not provide any services to the customers.

4.4 Records of identification procedures deemed to have been carried out by the Company

1. This section applies if:

- a. on a particular day (the customer identification day), the Company carried out the applicable customer identification procedure in respect of a particular customer to whom the Company provided, or proposed to provide, a designated service; and
- b. if the applicable customer identification procedure had also been carried out in respect of the customer by another reporting entity (the second reporting entity); and
- c. the Company made a record of:
 - i. the procedure; or
 - ii. information obtained in the course of carrying out the procedure; or
 - iii. such other information (if any) about the procedure as is specified in the AML/ CTF Rules; and
- d. the record is not declared by the AML/ CTF Rules to be exempt from this section.

Copy of record to be given to second reporting entity

2. If:

- a. on the customer identification day, the customer is a customer to whom the second reporting entity provides, or proposes to provide, a designated service; and
- b. the second reporting entity does not already have a copy of the record;

the second reporting entity must, by written notice given to the Company within five (5) business days after that day, request the Company to give the second reporting entity a copy of the record within five (5) business days after the request is given.

3. If:

- a. on a day later than the customer identification day, the customer becomes a customer to whom the second reporting entity provides, or proposes to provide, a designated service; and
- b. the second reporting entity does not already have a copy of the record;

the second reporting entity must, by written notice given to the Company within five (5) business days after that later day, request the Company to give the second reporting entity a copy of the of the record within five (5) business days after the request is given.

4. The Company must comply with a request under whichever of subsections (2) and (3) is applicable.

Retention of copy by second reporting entity

5. If the Company gives a copy of the record to the second reporting entity, the second reporting entity must retain the copy until the end of the first seven (7) year period:
 - a. that began at a time after the applicable customer identification procedure was carried out; and
 - b. throughout the whole of which the second reporting entity did not provide any designated services to the customer.

5. Records about anti money laundering and counter terrorism financing programs

1. The Company must:
 - a. make a record of the adoption; and
 - b. retain the record, or a copy of the record, throughout the period:
 - i. beginning at the completion of the preparation of the record; and
 - ii. ending seven (7) years after the day on which the adoption ceases to be in force.
2. The Company must retain the program, or a copy of the program, throughout the period:
 - a. beginning at the time of the adoption; and
 - b. ending seven (7) years after the day on which the adoption ceases to be in force.
3. If the program is varied while the adoption is in force, the Company must retain the variation, or a copy of the variation, throughout the period:
 - a. beginning at the time of the variation; and
 - b. ending seven (7) years after the day on which the adoption ceases to be in force.

IX. SECRECY AND ACCESS

1. Simplified Outline

The following is a simplified outline of this Part:

- Except as permitted by the Act, an AUSTRAC official must not disclose information or documents obtained under the Act.
- The Company must not disclose that it has:
 - reported, or is required to report, information to the AUSTRAC CEO; or
 - formed a suspicion, about a transaction or matter.

- The Australian Taxation Office and certain other Australian government bodies may access AUSTRAC information.

2. Disclosure of information

1. If:

- a suspicious matter reporting obligation arises or has arisen for the Company in relation to a person; and
- the Company has communicated information to the AUSTRAC CEO;

the Company 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.

X. ADMINISTRATION

1. Establishment of AUSTRAC

1. The Australian Transaction Reports and Analysis Centre established under the Financial Transaction Reports Act 1988. The Australian Transaction Reports and Analysis Centre may also be known as AUSTRAC.
2. AUSTRAC consists of:
 - a. the AUSTRAC CEO; and
 - b. the staff of AUSTRAC.
3. The function of AUSTRAC is to assist the AUSTRAC CEO in the performance of the AUSTRAC CEO's functions.
4. The functions of the AUSTRAC CEO are:
 - a. to retain, compile, analyse and disseminate eligible collected information; and
 - b. to provide advice and assistance, in relation to AUSTRAC information, to the persons and agencies who are entitled or authorised to access AUSTRAC information; and
 - c. to advise and assist reporting entities in relation to their obligations under the Act, the regulations and the AML/ CTF Rules; and
 - d. to advise and assist the representatives of the Company in relation to compliance by the Company with the Act, the regulations and the AML/ CTF Rules; and
 - e. to promote compliance with the Act, the regulations and the AML/CTF Rules; and
5. In performing the AUSTRAC CEO's functions, the AUSTRAC CEO must:
 - a. consult with the following:
 - i. reporting entities or the representatives of reporting entities;

- ii. the Commissioner of the Australian Federal Police;
 - iii. the Chief Executive Officer of the Australian Crime Commission;
 - iv. the Commissioner of Taxation;
 - v. the Comptroller General of Customs;
- b. take into account any comments made in the course of those consultations.
6. In performing the AUSTRAC CEO's functions under this Act, the AUSTRAC CEO must have regard to:
- a. any relevant FATF Recommendations; and
 - b. any relevant Conventions; and
 - c. any relevant Resolutions.
7. Any failure to comply with the requirements of subsection (2), (3) or (4) in relation to the performance of a function of the AUSTRAC CEO does not affect the validity of the performance of the function.

2. AML/ CTF Rules

1. The AUSTRAC CEO may, by writing, make rules (the AML/ CTF Rules) prescribing matters required or permitted by any other provision of the Act to be prescribed by the AML/ CTF Rules.
2. AML/ CTF Rules are legislative instruments.